Department of Information Systems
Arkansas. A State of Technology.

VPN - Routing and Remote Access

Obtaining a Certificate for K12.AR.US

1. You will need to get an A record created for the school for something.k12.ar.us through the UNIX Group.
2. You will need a 1-1 NAT to the VPN Server and open port 443. If you are going to setup L2TP for Mac OS and Chromebooks then you will need ports 50, 51, 500, 1701, 4500 on TCP and UDP open also.
3. Create a child incident for Arkansas .GOV Approvals Group
4. Request a SSL Certificate for the school A record.
5. Send an e-mail to DIS.Security.Architecture@arkansas.gov with the CSR info. (Direction to create CSR further down)
6. You will get an e-mail from Certificate Services Manager support@cert-manager.com with the links to download the Certificate. (Forward to the tech in case they need it later on.)
7. If the school is getting the certificate from another Signing Authority (Go-Daddy, Digicert, etc…) the directions should work for those too.

Example of ASA Rule:

Put the Public and Private IP for your school:

```
object network VPN_SVR_Public
 host 170.211.xxx.xxx
object network VPN_SVR_Private
host 10.xxx.xxx.xxx
```

This creates a service group of the allowed ports:

```
object-group service VPN_access_svcs
 service-object tcp destination eq 1701
 service-object tcp destination eq pptp
 service-object tcp destination eq https
 service-object tcp destination eq 47
 service-object tcp destination eq 51
service-object tcp destination eq 50
service-object tcp destination eq 500
service-object tcp destination eq 4500
service-object udp destination eq 51
service-object udp destination eq 50
service-object udp destination eq isakmp
service-object udp destination eq 4500
service-object udp destination eq 1701
service-object tcp destination eq www
service-object udp destination eq 443
service-object udp destination eq www
```

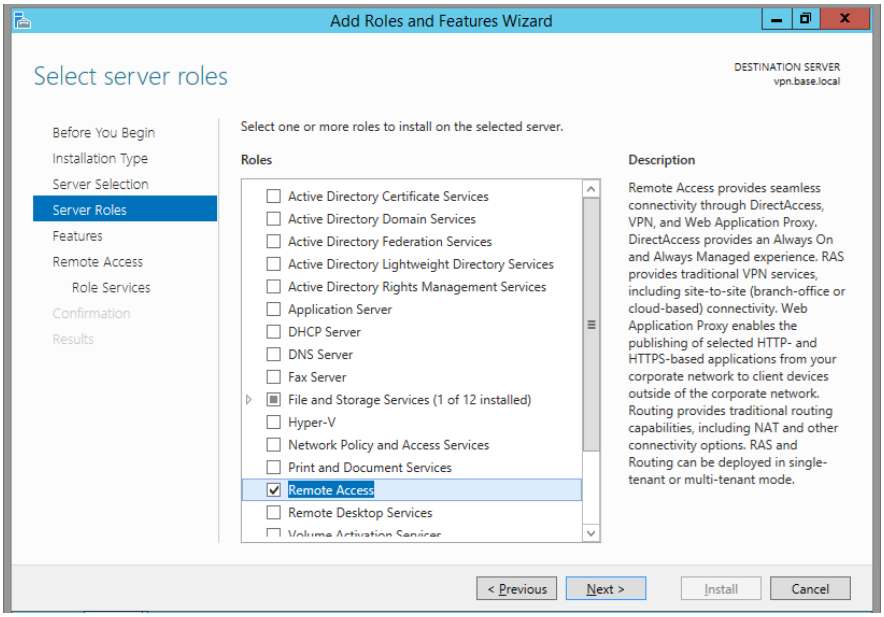
This uses the service group to allow access:

```
access-list acl-out extended permit object-group VPN_access_svcs any object VPN_SVR_Private
```

Install the RRAS Role

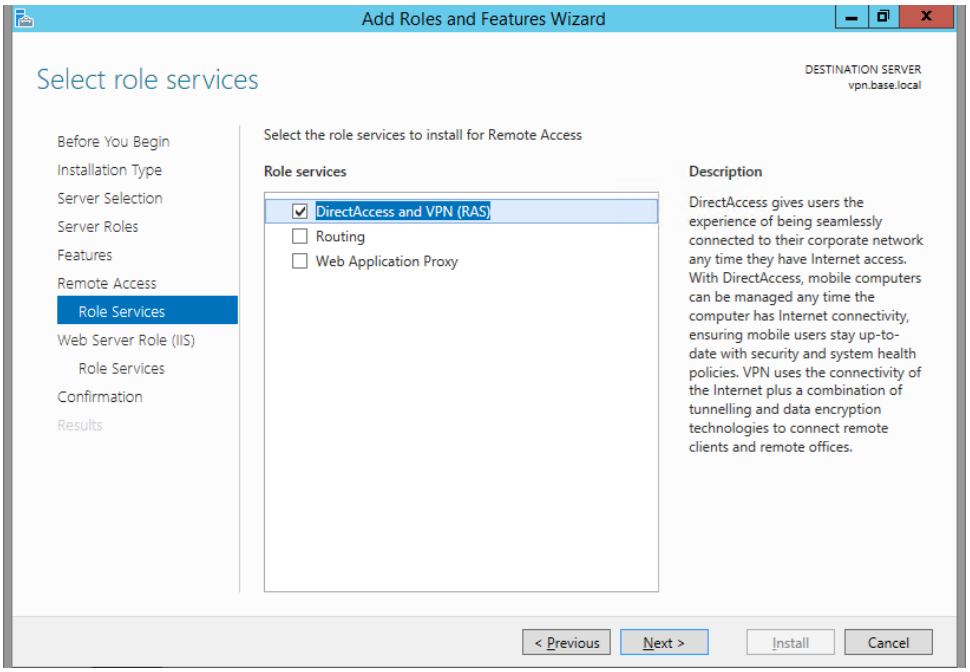
Step 1

Add the Remote Access role. Server Manager -> Manage -> Add Roles and Features -> **Remote Access**.



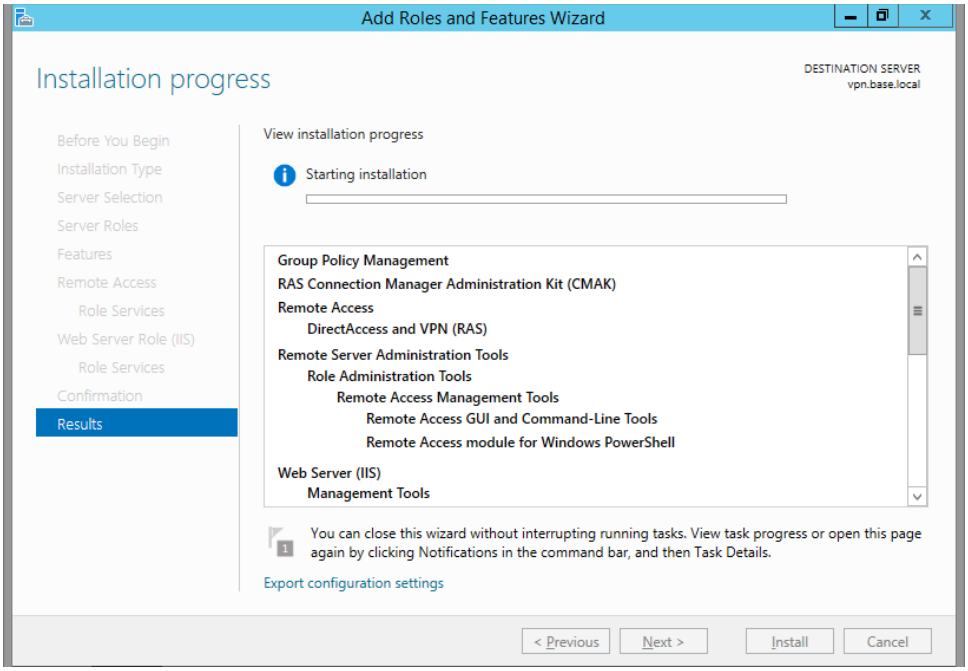
Step 2

Click Next a couple times, then just click **DirectAccess and VPN**. Click Add Features. We are not setting up DirectAccess at this time. There is a separate document for that.



Step 3

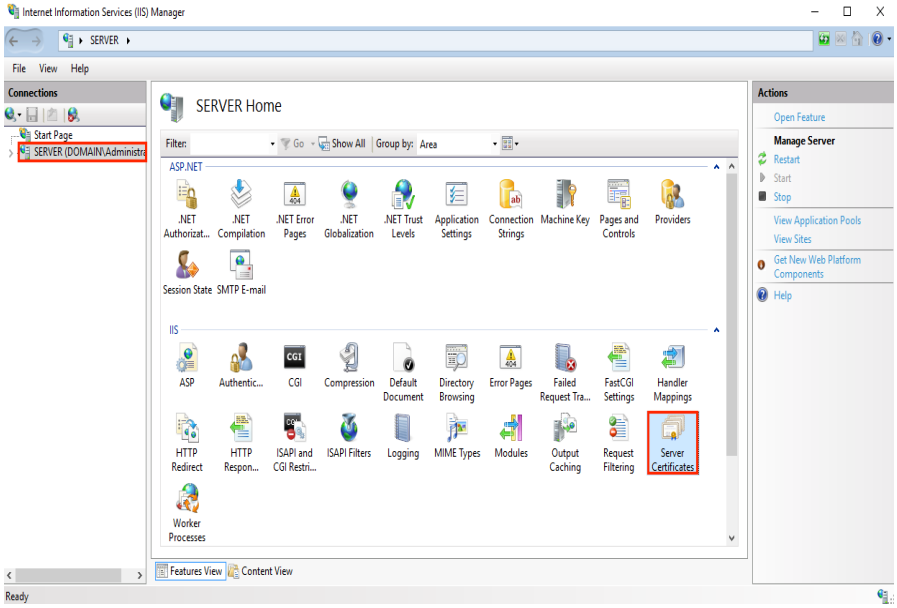
Next a couple times. It will install IIS, Click **Next** on **IIS** and **IIS Role Services**. Go ahead and click **Install**.



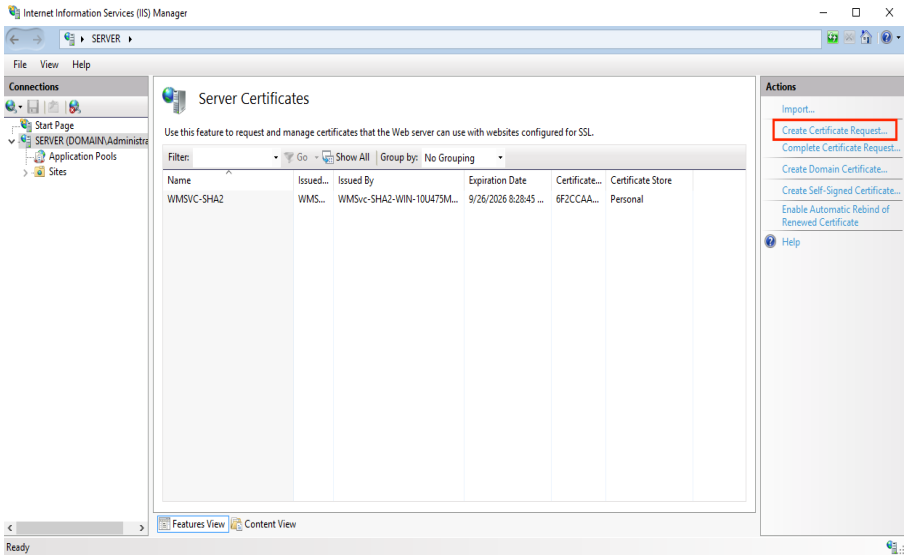
Before we can continue with the RRAS setup we need to create the CSR and complete the certificate request. We are going to use IIS to complete the certificate, so we are going to wait on the configuration and finish the RRAS setup later.

Using IIS 10 to Create Your CSR

1. In the **Windows** start menu, type ***Internet Information Services (IIS) Manager*** and open it.
2. In **Internet Information Services (IIS) Manager**, in the **Connections** menu tree (left pane), locate and click the server name.

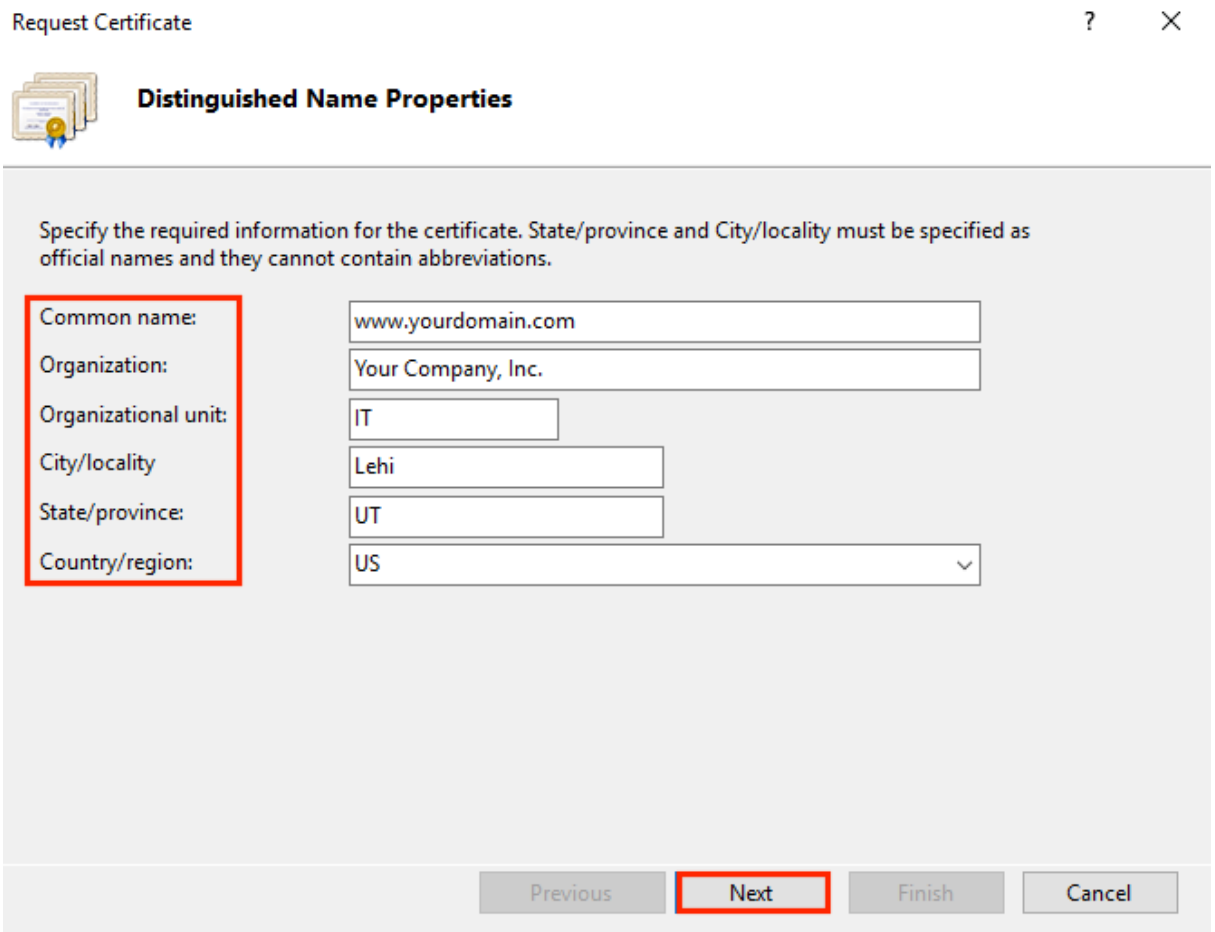


3. On the server name **Home** page (center pane), in the **IIS** section, double-click **Server Certificates**.
4. On the **Server Certificates** page (center pane), in the **Actions** menu (right pane), click the **Create Certificate Request…** link.



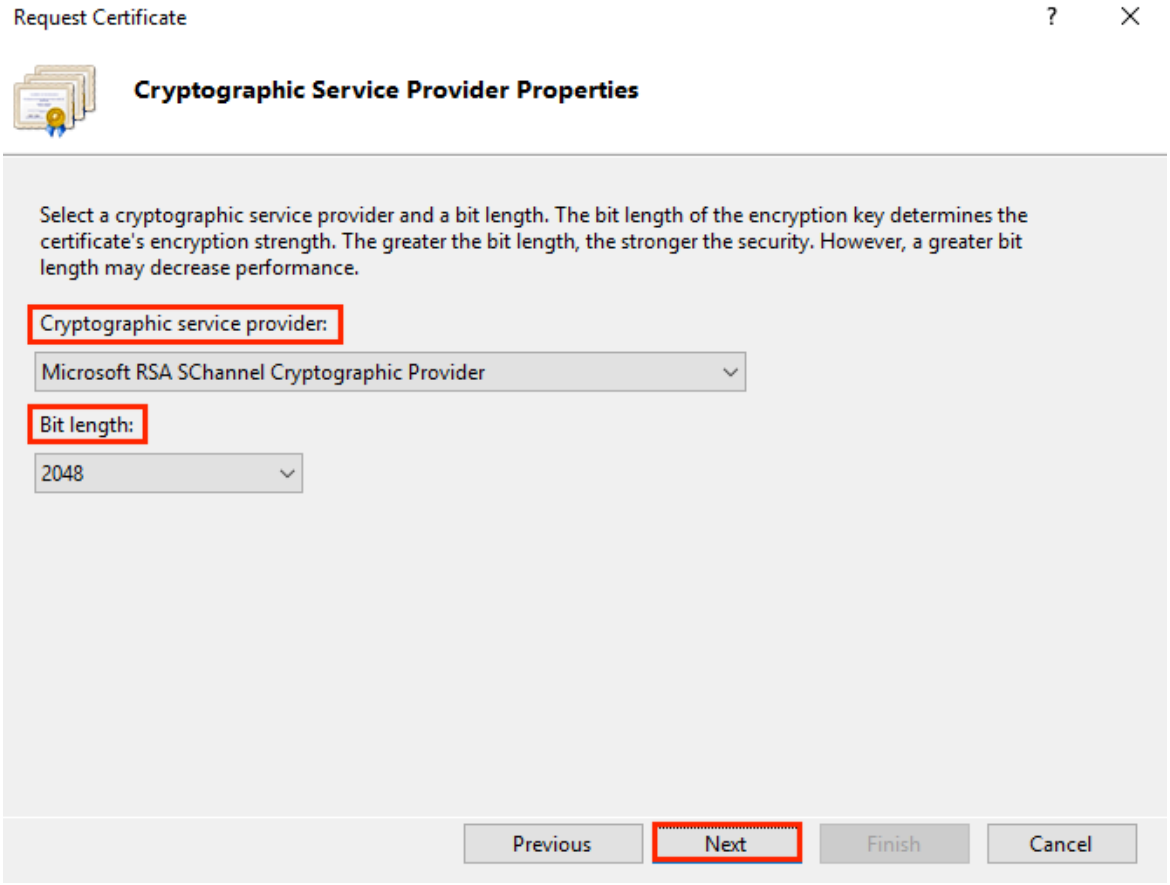
5. In the **Request Certificate** wizard, on the **Distinguished Name Properties** page, provide the information specified below and then click **Next**:

Common name:	Type the fully-qualified domain name (FQDN) (e.g., *www.example.com*).
Organization:	Type your company's legally registered name (e.g., *YourCompany, Inc.*).
Organizational unit:	The name of your department within the organization. Frequently this entry will be listed as "IT", "Web Security," or is simply left blank.
City/locality:	Type the city where your company is legally located.
State/province:	Type the state/province where your company is legally located.
Country:	In the drop-down list, select the country where your company is legally located.



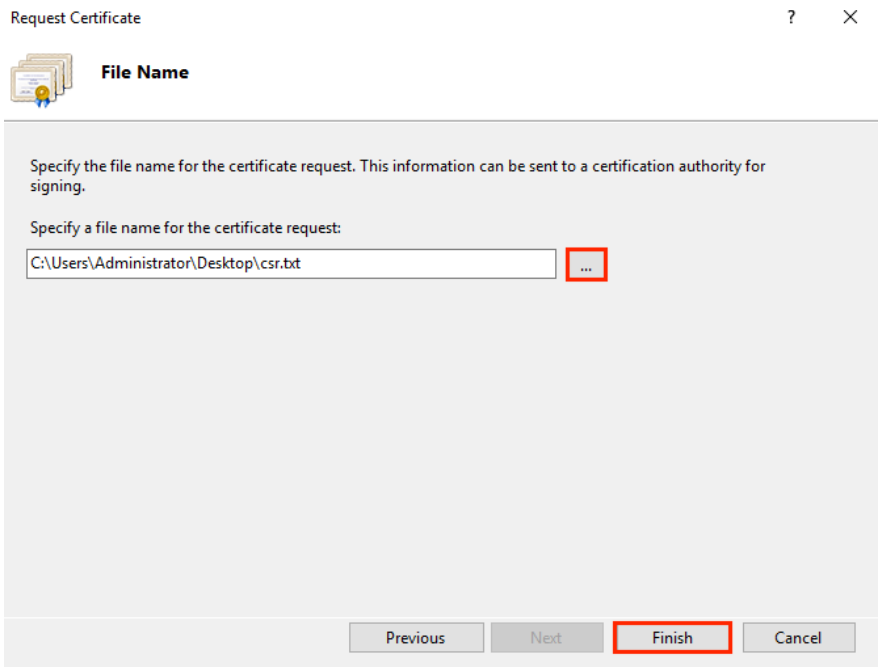
6. On the **Cryptographic Service Provider Properties** page, provide the information below and then click **Next**.

Cryptographic service provider:	In the drop-down list, select **Microsoft RSA SChannel Cryptographic Provider**, unless you have a specific cryptographic provider.
Bit length:	In the drop-down list select **2048**, unless you have a specific reason for opting for larger bit length.



7. On the **File Name** page, under **Specify a file name for the certificate request**, click the **…** box to browse to a location where you want to save your CSR.

   Note: Remember the filename that you choose and the location to which you save your csr.txt file. If you just enter a filename without browsing to a location, your CSR will end up in C:\Windows\System32.



8. When you are done, click **Finish**.

9. Use a text editor (such as Notepad) to open the file. Then, copy the text, including the **-----BEGIN NEW CERTIFICATE REQUEST-----** and **-----END NEW CERTIFICATE REQUEST-----** tags, and this is what you will send to Security Architecture or paste in a third party order form.

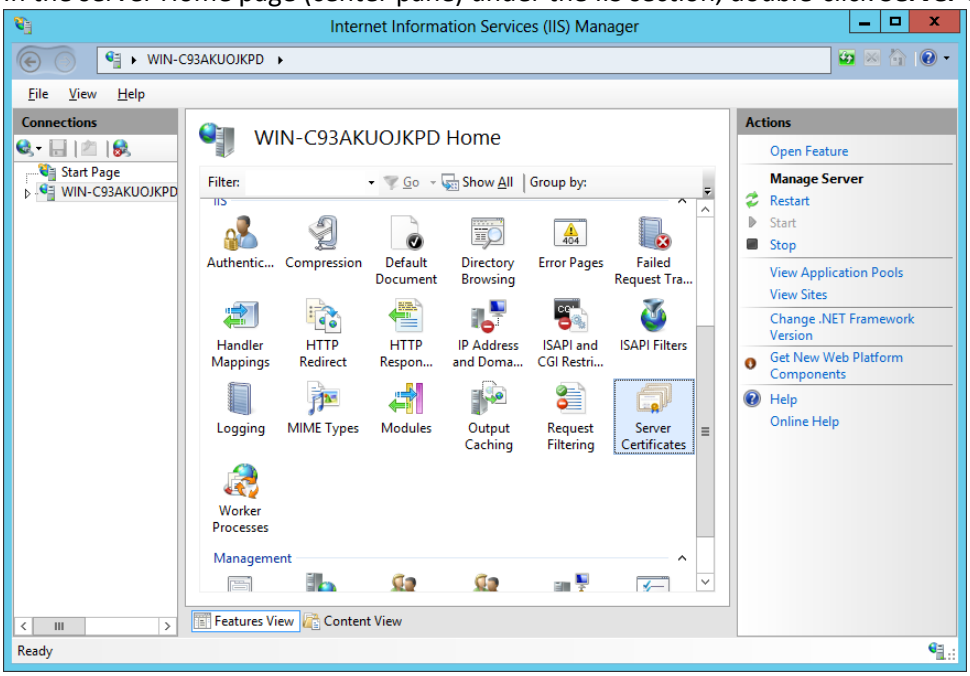
```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCVlvdXJIdGF0ZTER
MA8GA1UEBxMIWW91ckNpdHkxCzAJBgNVBAsTAklUMRowGAYDVQQKExFZb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrB5/vhYfGECLJbc3l
RdEbdXyHDtHklRAoIVQCfjTwBWGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSywqwx
7pVfaDbZPuTgUhw7wksKNFxccG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJUOJtA5MIs/ZjaXfS1LjXurLU0nCOQQIDAQABoAAwDQYJ
KoZIhvcNAQEFBQADggEBAK159goyAYOpcnrQ2EvCGlizrK1kS3D8JjnAiP1NHrjB
/qdTYR+/8Dr/hMcwwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEbO8GA0Fc4rw
ix7vb15vSXe3shGijRGIzzHVGRoR3r7xQtIuMaDAr3xlV8jHbcvZTcpX0Kbq6H1G
NLA4CXsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEWxRWklERgg9/YcWI
obf5ziuNm1Df24NBt5tpCNzfGviKT6/RYfWg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

22. When you get the email from Certificate Service Manager, download the file as **X509 Certificate only, Base64 encoded** and save on the server.

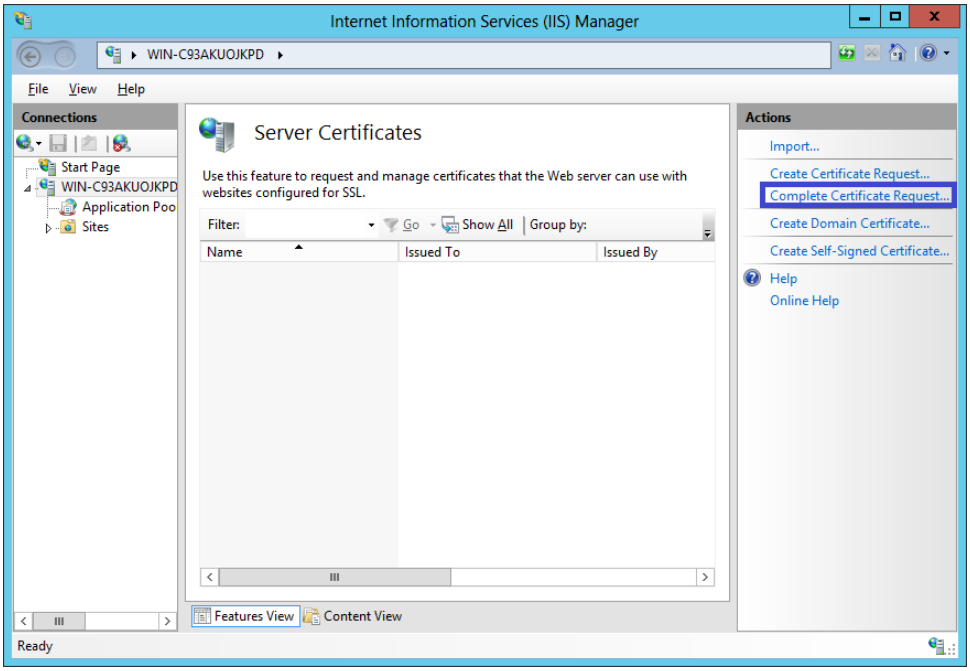
How to install your SSL certificate and configure the server to use it

Install Your SSL Certificate

1. From the **Administrative Tools**, find **Internet Information Services (IIS) Manager** and open it.
2. In the **Connections** pane, locate and click the **server**.
3. In the server Home page (center pane) under the IIS section, double-click **Server Certificates**.

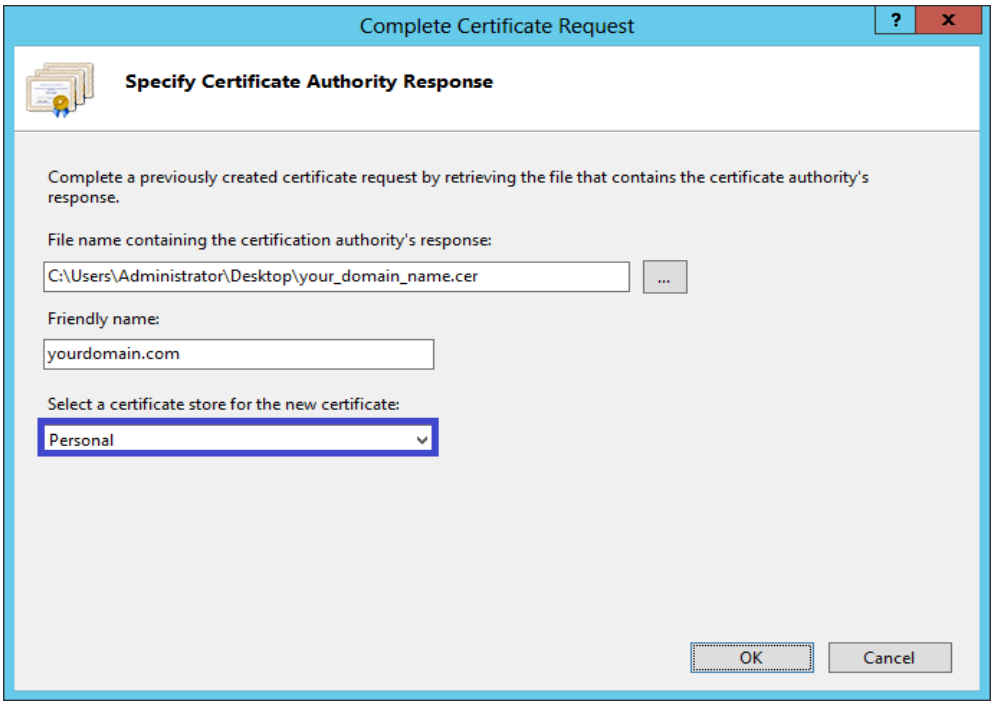


4. In the Actions menu (right pane), click **Complete Certificate Request**.



5. In the Complete Certificate Request wizard, on the Specify Certificate Authority Response page, provide the following information:

File name containing the certificate authority's response:	Click the … button to locate the **.crt** file you received from Certificate Service Manager.
Friendly name:	Type a friendly name for the certificate. This is not part of the certificate; instead, it is used to identify the certificate. I would use the domain name.
Select a certificate store for the new certificate:	In the drop-down list, select Personal.



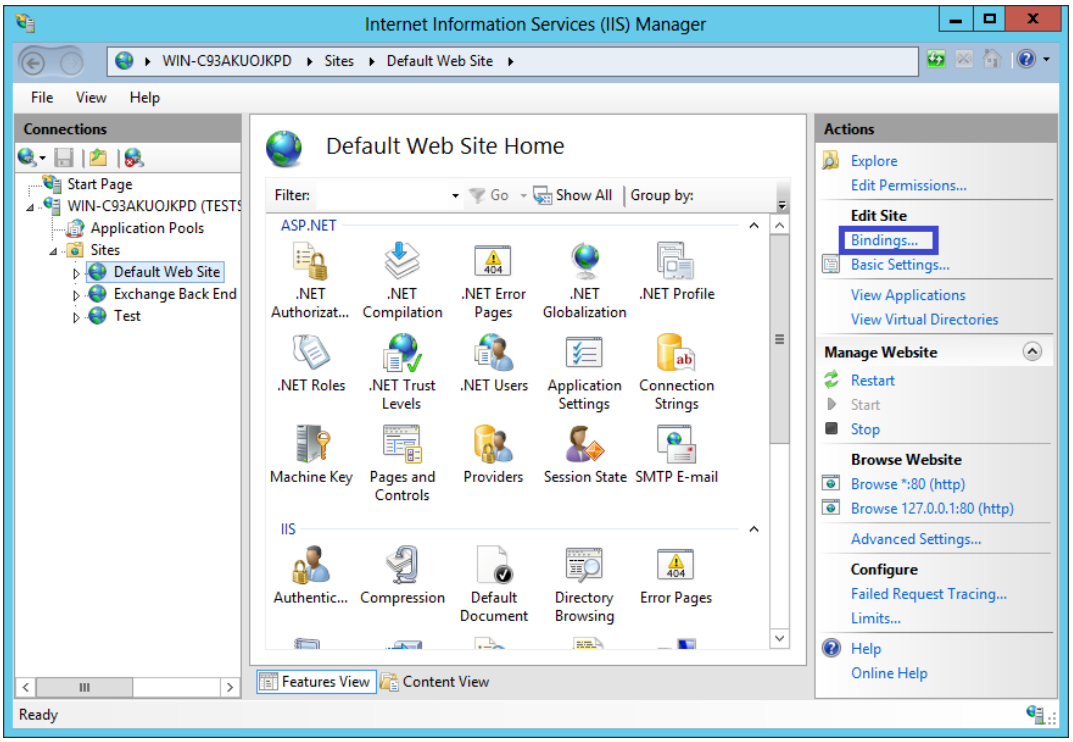
6. Click OK to install the certificate.
7. Check that it completed and kept the certificate in IIS by clicking the refresh button or going out of Server Certificates and back in. If your certificate doesn't show in the list you may need to do a repair on the certificate store (See Below). Now that you've successfully installed your SSL certificate, you need to configure your site to use it.

***Commands for certificate store repair only needed if cert doesn't show in the server cert list in IIS*:**
This command will give you a list of certificates installed and their Thumbprint:
Get-ChildItem -path cert:\LocalMachine\My

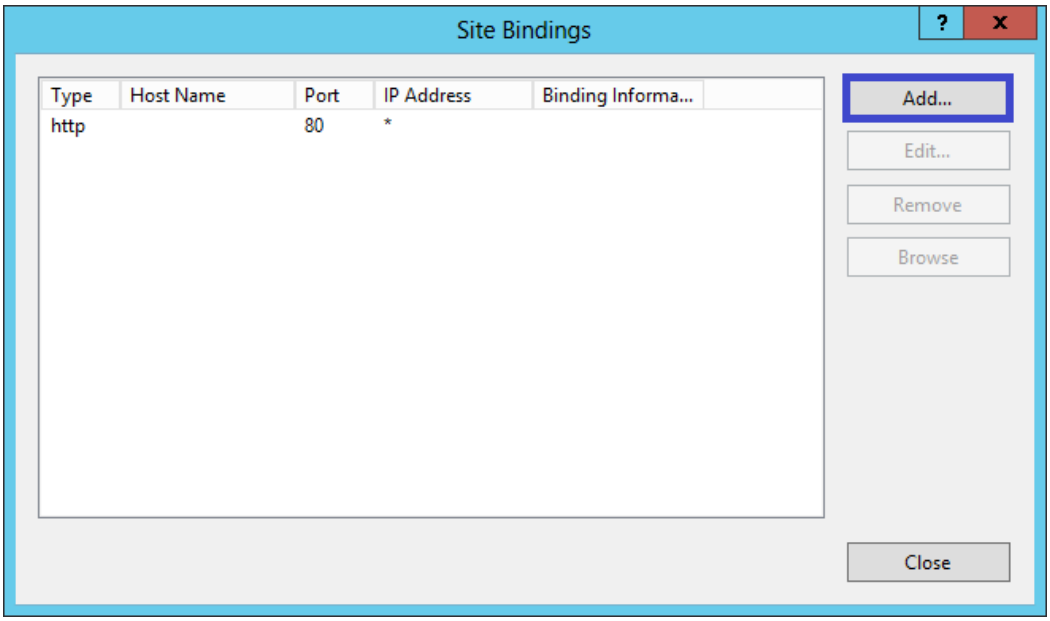
This command uses the ThumbprintNumber for your certificate to repair the store. Your certificate should show in the server certificate list in IIS after the command completes successfully. If it fails then you will have to troubleshoot why:
certutil -repairstore my "ThumbprintNumber"

Assign Your SSL Certificate

8. In **Internet Information Services (IIS) Manager**, in the Connections pane, expand the name of the server on which the certificate was installed. Then expand Sites and click the site you want to secure using the SSL certificate.
9. In the Actions menu (right pane), click **Bindings**.



10. In the Site Bindings window, click **Add**.



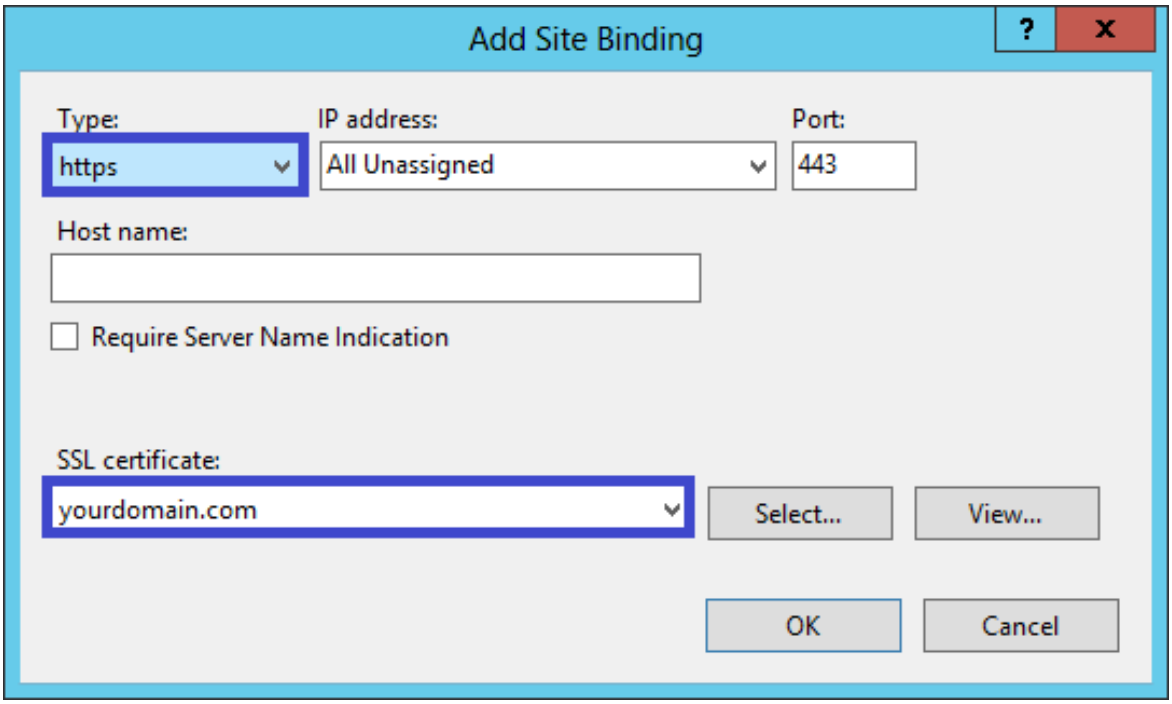
11. In the Add Site Binding window, do the following and then click OK.

    Type: In the drop-down list, select https.

    IP address: In the drop-down list, select the IP address of the site or select All Unassigned.

    Port: Type 443. (SSL uses port 443 to secure traffic.)

    SSL certificate: In the drop-down list, select your new SSL certificate (e.g., *yourdomain.com*).

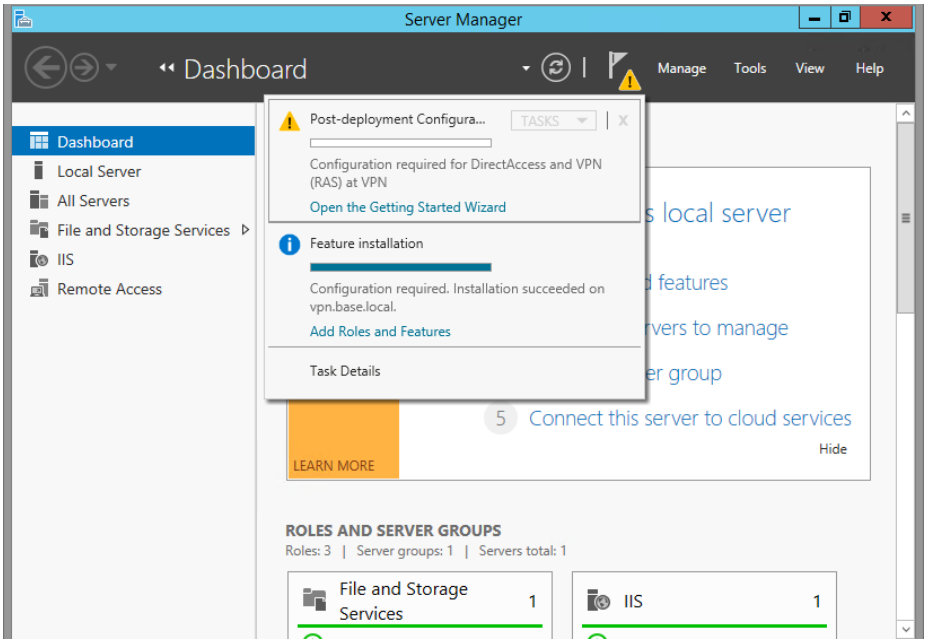


12. Your SSL certificate is now installed, and the website is configured to accept secure connections. The certificate will now show in RRAS server configuration.

Configure RRAS

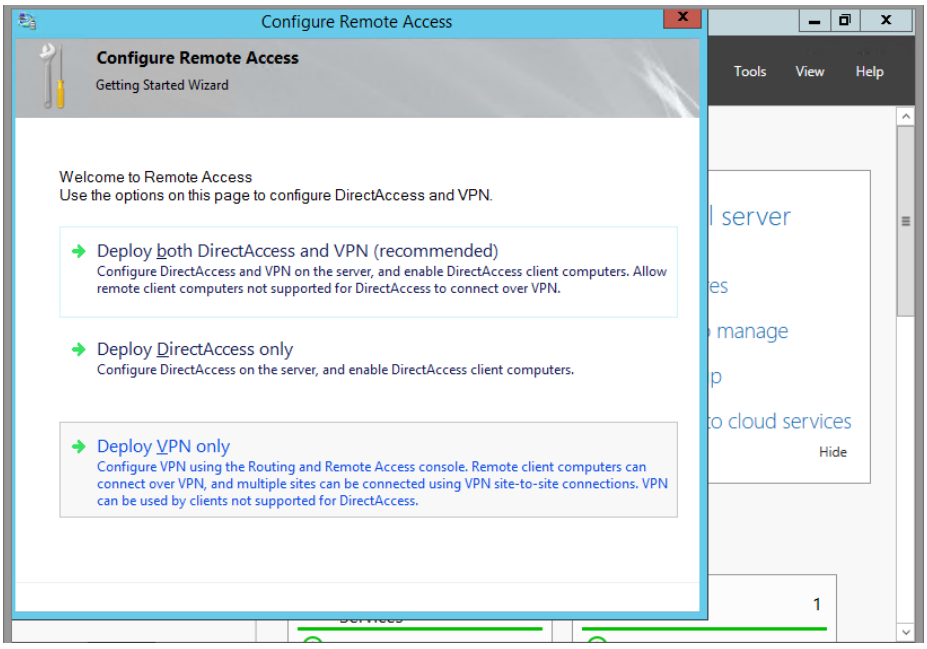
Step 4

Once the SSL Certificate has been installed, click the flag thing at the top of Server Manager, and then **Open the Getting Started Wizard**.



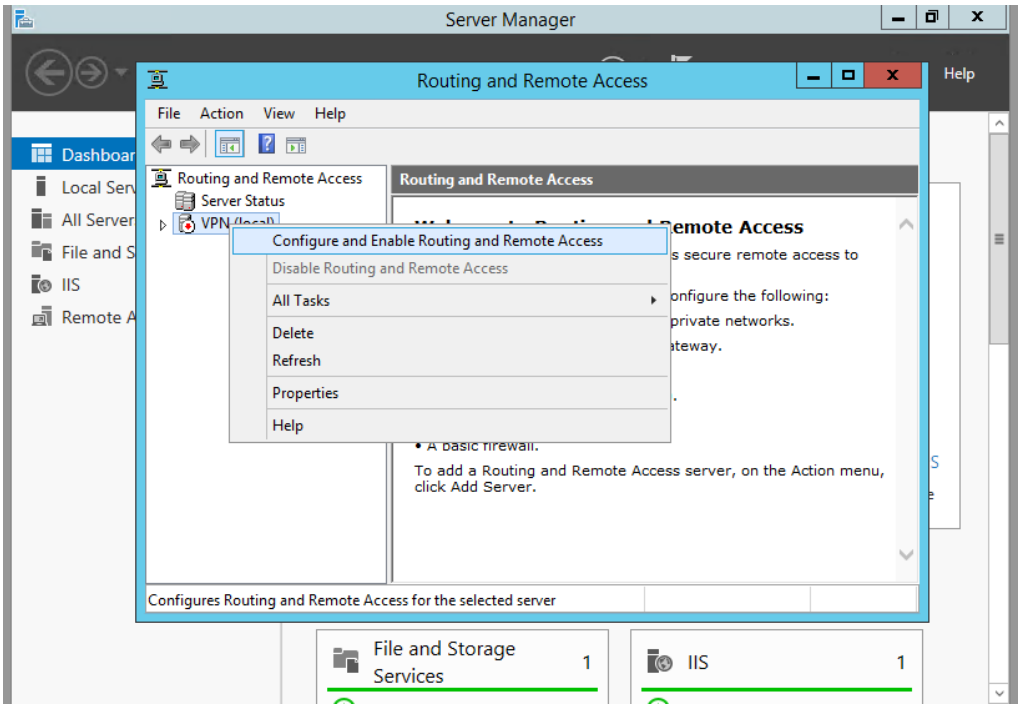
Step 5

Select **Deploy VPN Only**.



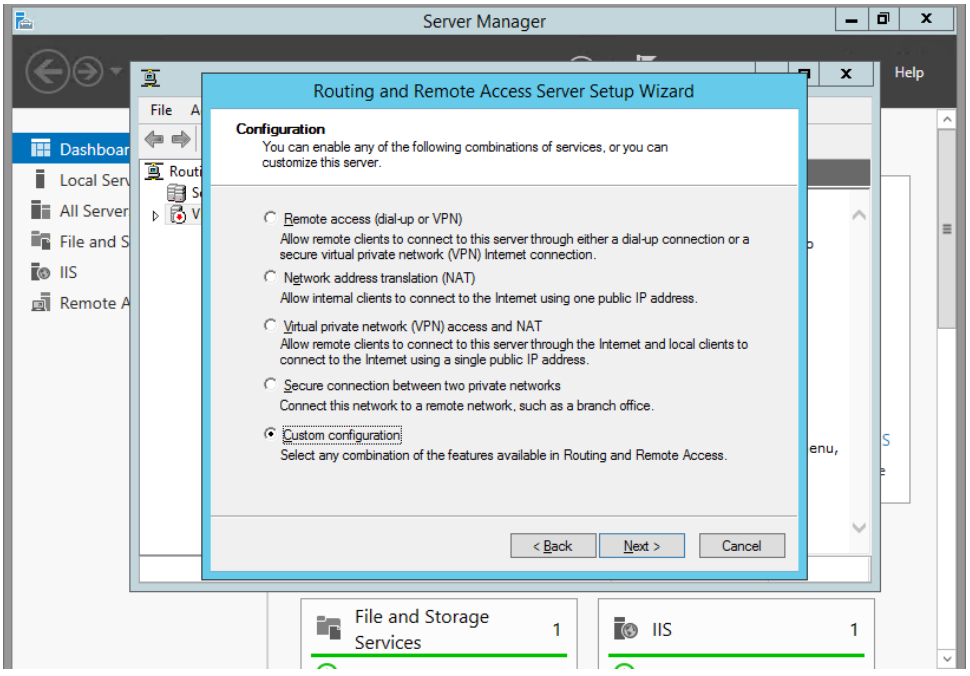
Step 6

If clicking the Open Getting Started Wizard doesn't open, you can go to Administrative Tools and Open Routing and Remote Access. Once the new window pops up, right click your server name (mine is VPN (local)) then **Configure and Enable Routing and Remote Access**.



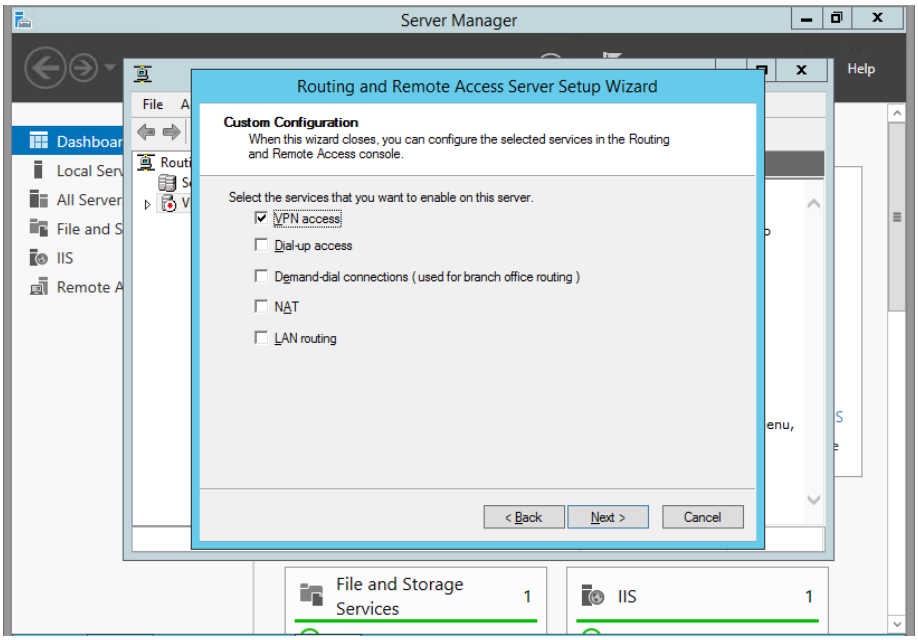
Step 7

We're trying to keep our surface area as small as possible, so click on **Custom Configuration**.



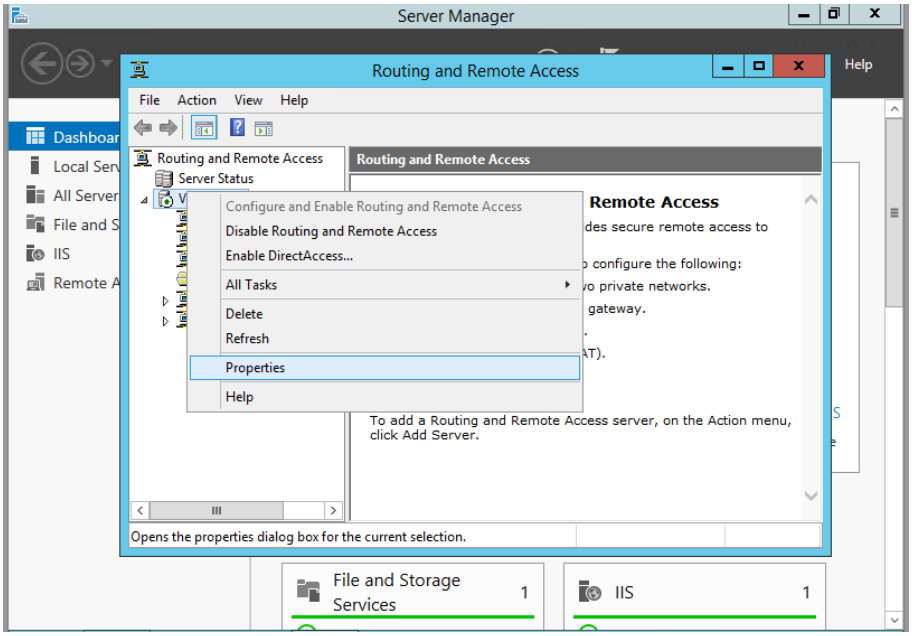
Step 8

Next, only check **VPN Access**. Click **Next** and **Finish.** If the Windows Firewall is on, you may get a popup that you need to enable Routing and Remote Access, but the only exception needed is Secure Socket Tunneling Protocol (SSTP-In).



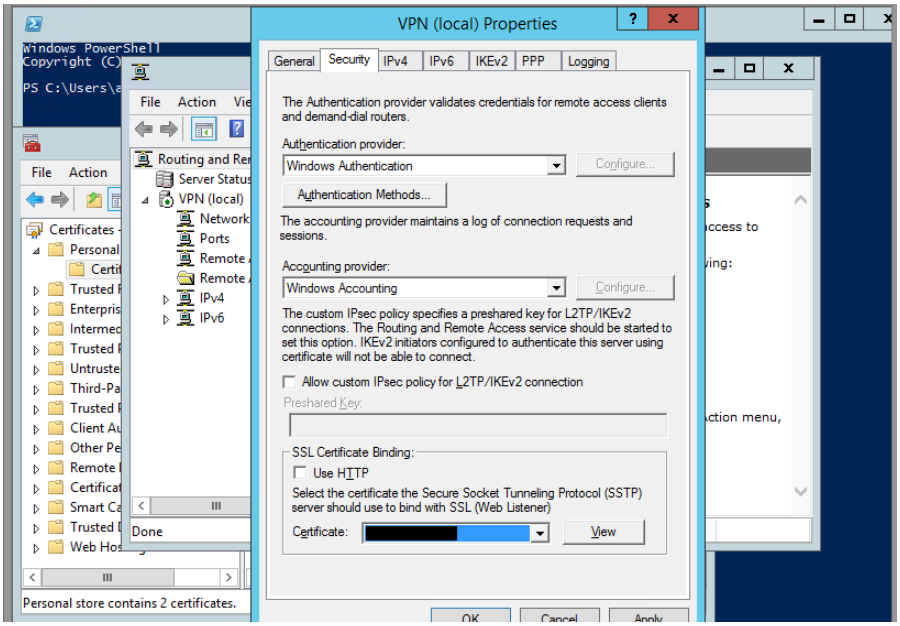
Step 9

The RRAS Service will configure itself, and start the service. It may popup an option to start the service. Click **Start.** ***If the service doesn't start it is likely due to IPV6 being disabled in the registry and you will have to remove the Disabled Component entry that we normally configure.*** You will then be returned to the RRAS config window. Right click your server name, then **Properties**.



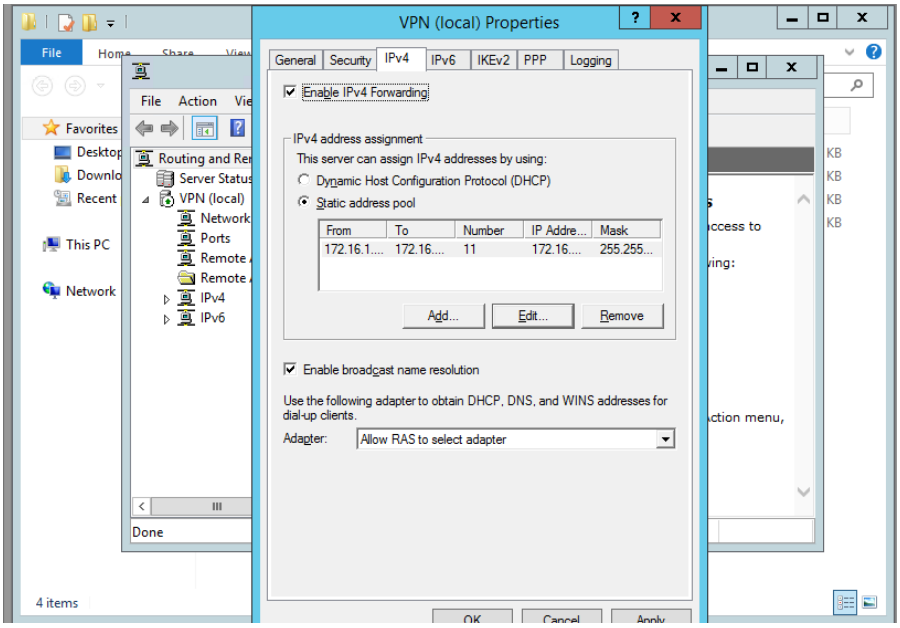
Step 10

Check that your SSL Certificate binding is the newly installed certificate.



Step 11

Next, click on IPv4. Here, you can either do a DHCP forwarding or just give RRAS a few IP addresses to hand out. Click Apply then Okay. You'll be returned again to the RRAS window.



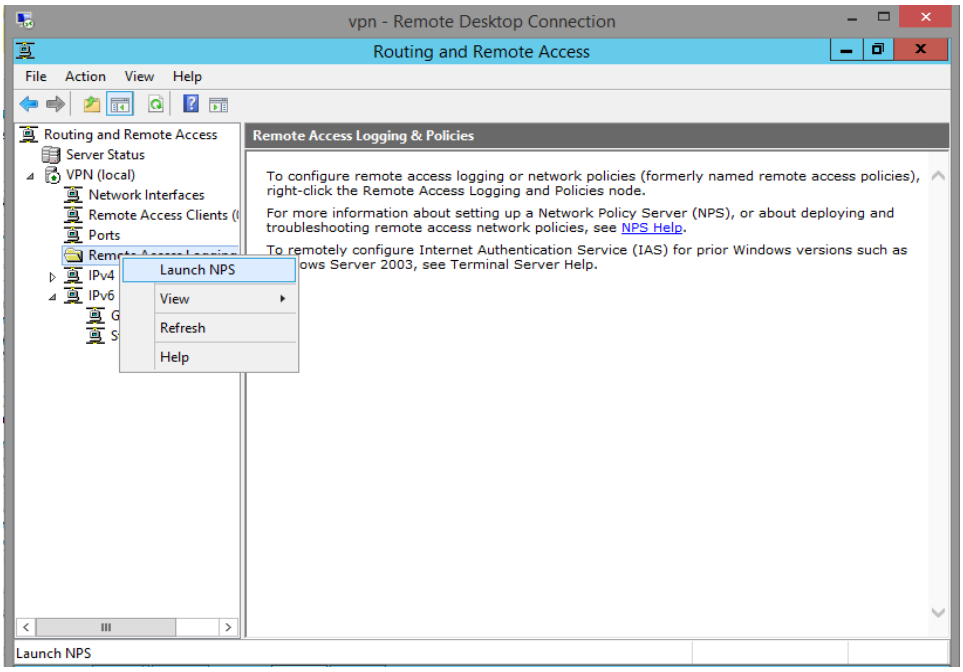
At this point, your RRAS server is setup!

If you don't want to give permission individually to each user that will need VPN access I suggest going through the next section. You will create a VPN group in AD and use it to allow VPN access.

Setup Network Policy Server

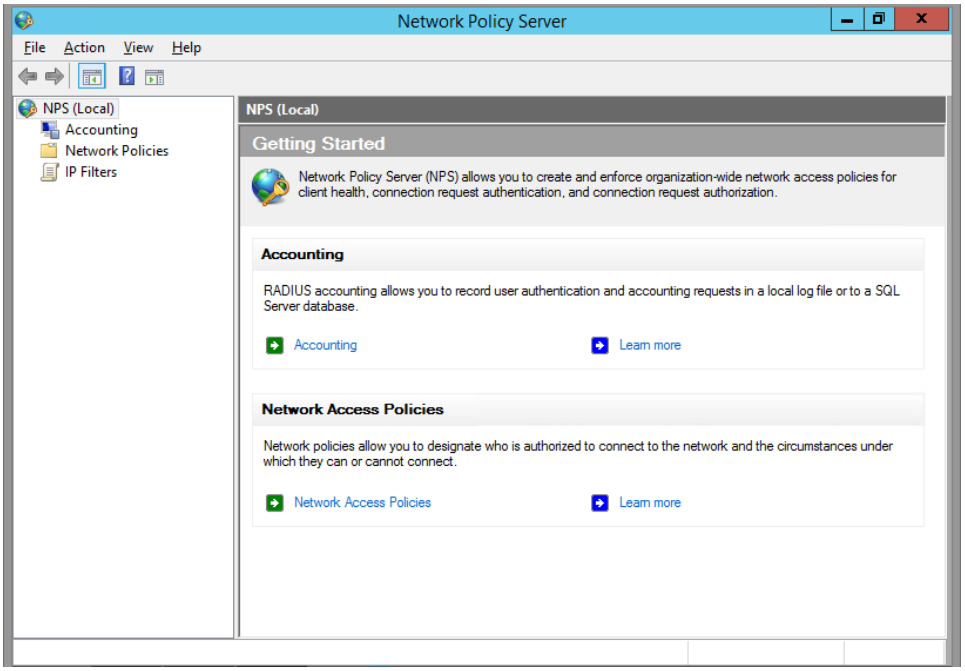
Step 1

Once you've returned to the RRAS window, *left-click* **Remote Access Logging and Policies**. Then right-click and **Launch NPS**.



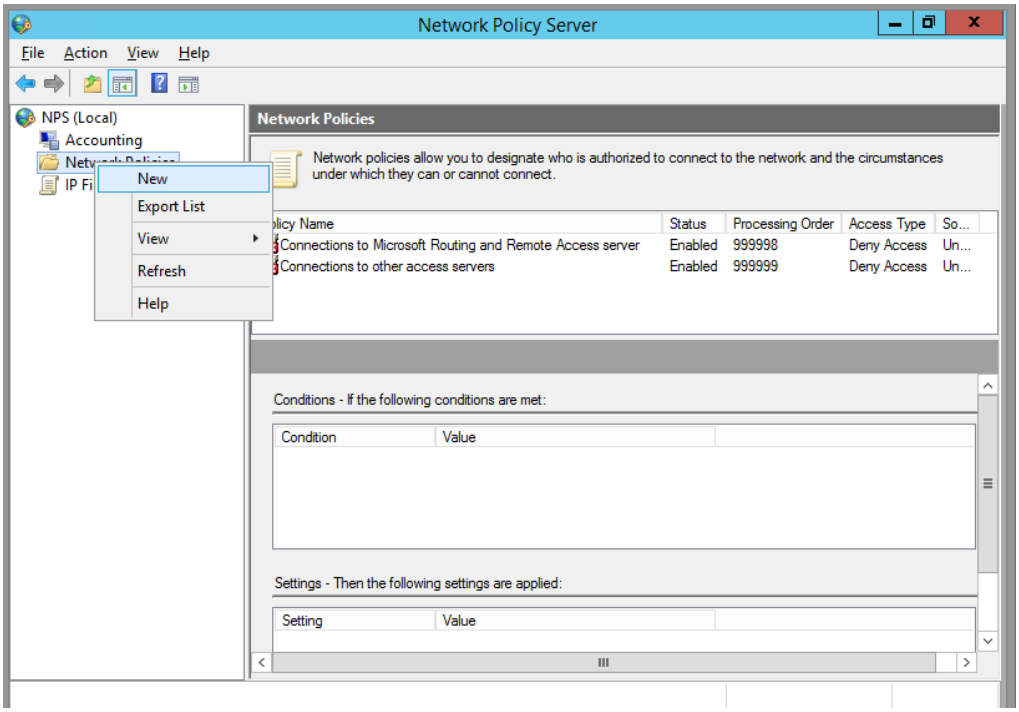
Step 2

A new Network Policy Server window will pop-up. Here, we can set which users can access the VPN, set the type of authentication encryption, and restrict network access.



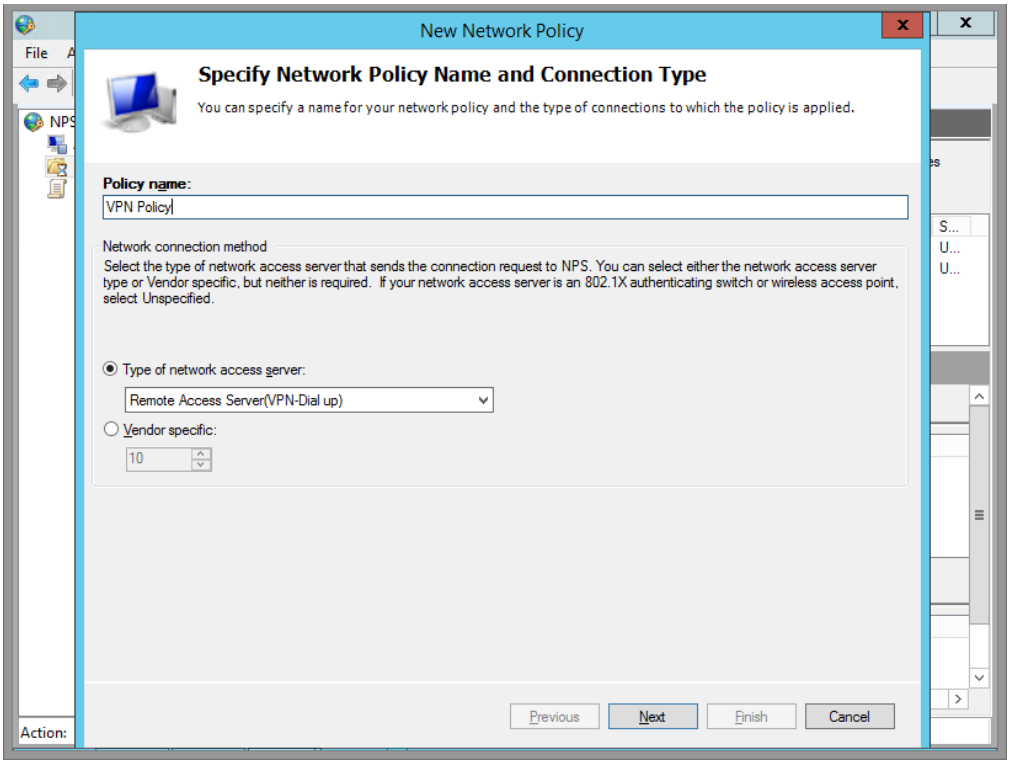
Step 3

We'll start by creating a new Network Policy. Right click **Network Policy** and click **New**.



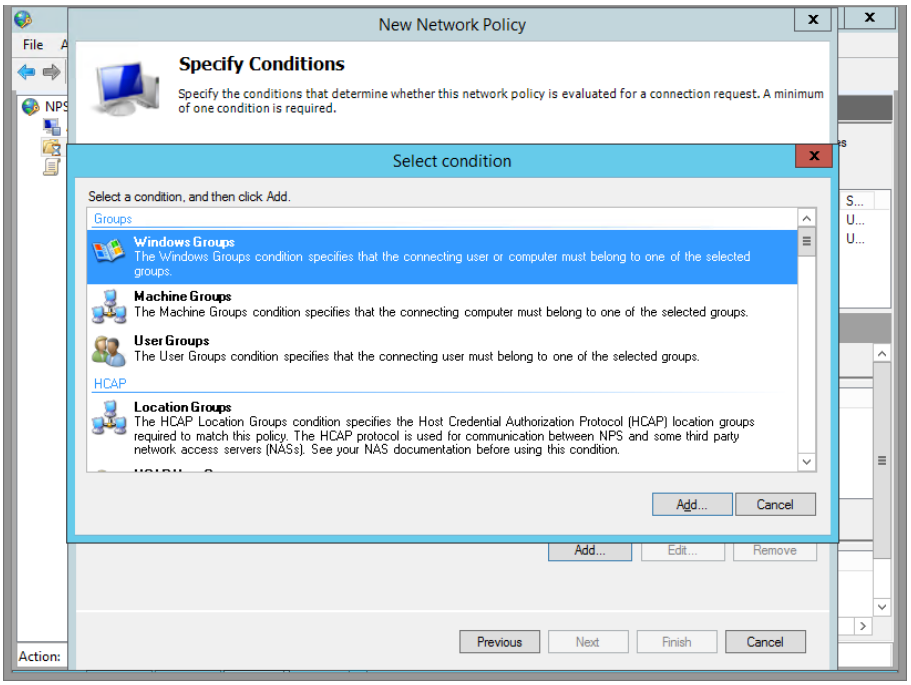
Step 4

Name your Policy, and select **Remote Access Server (VPN/Dial-up)**.



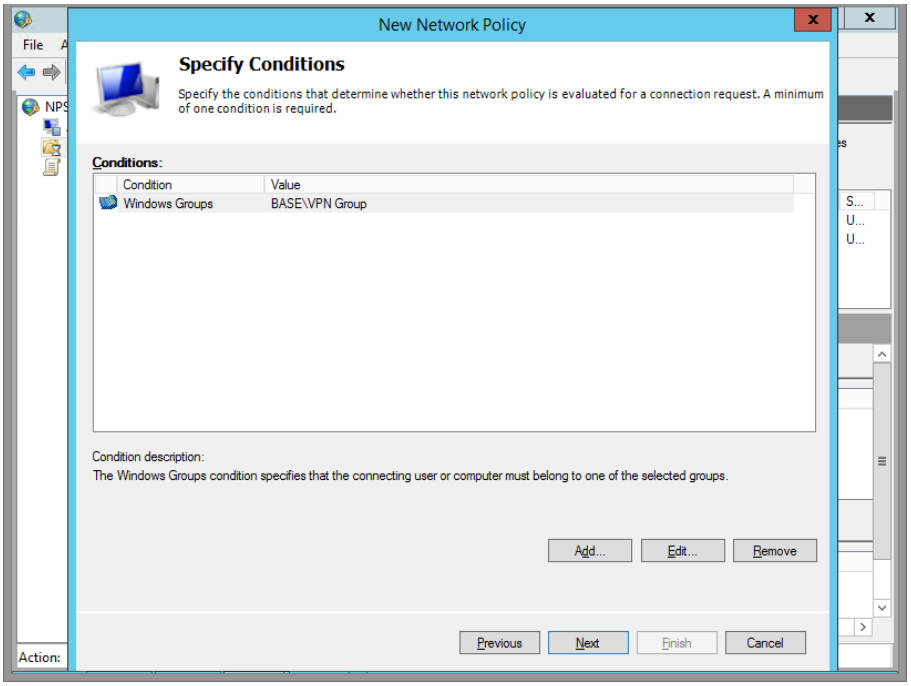
Step 5

Leave this window for a moment, go into AD Users and Computers, create a Group and name it VPN Access or whatever you wish, and add some users. Come back, and add that Windows Group by clicking **Add** -> **Windows Group**.



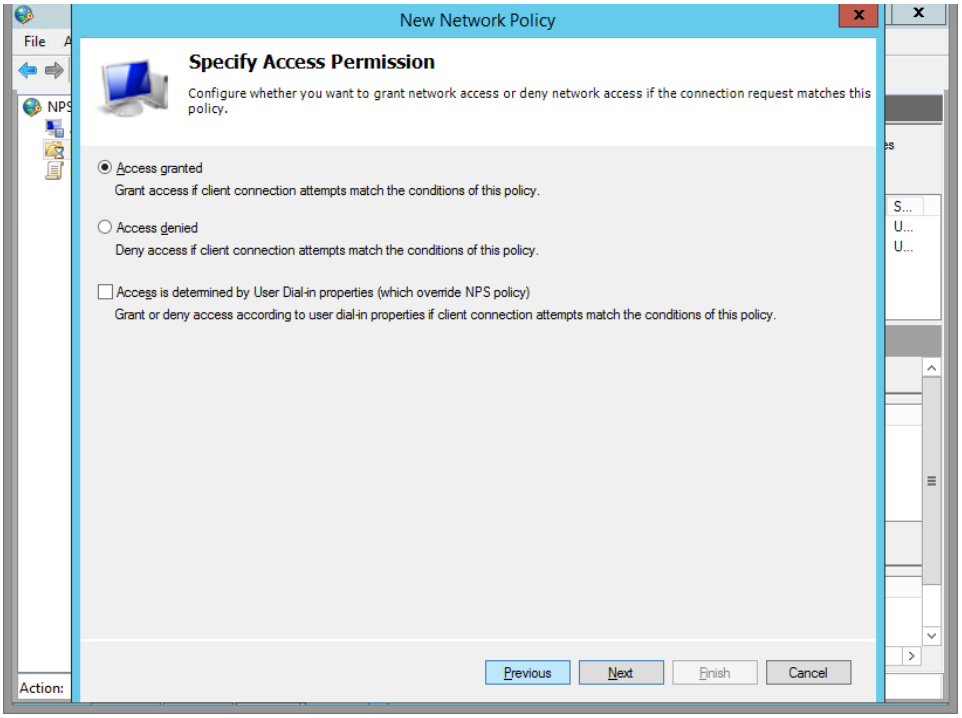
Step 6

Confirm and click Next



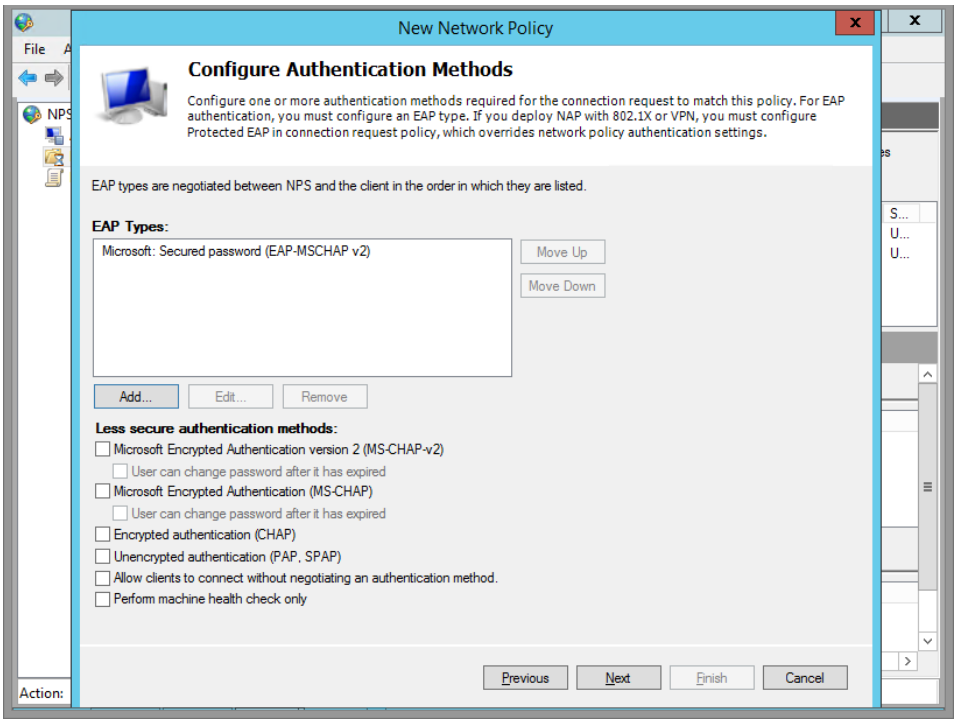
Step 7

Grant this group access.



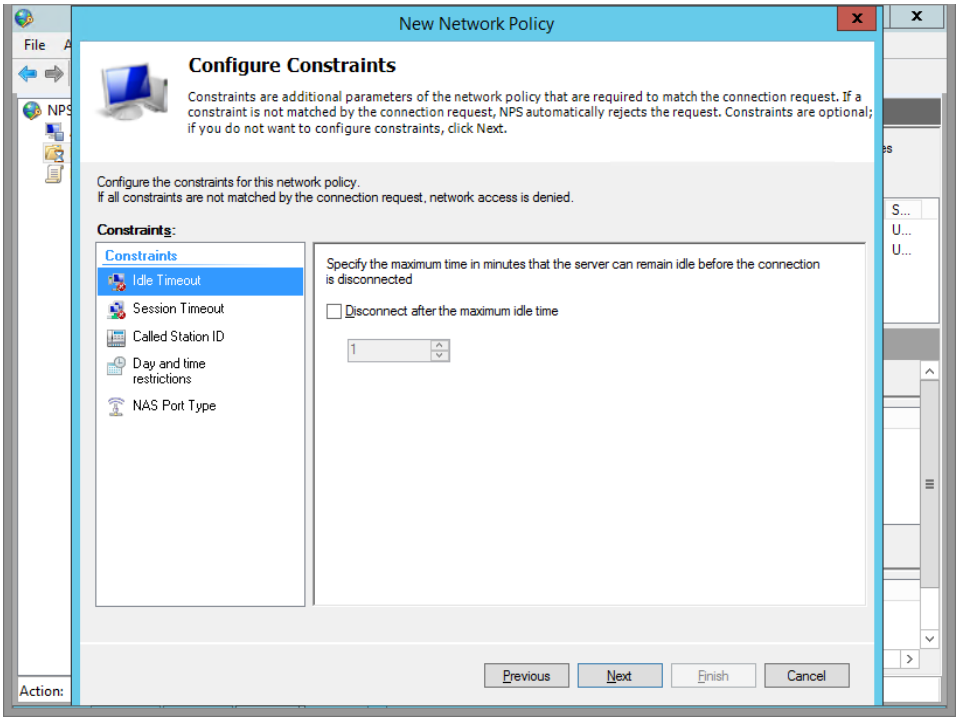
Step 8

Here, you can choose your Authentication Encryption. I disabled all the weaker ones, and only enabled the stronger **Microsoft: Secured Password (EAP-MSCHAP v2)**.



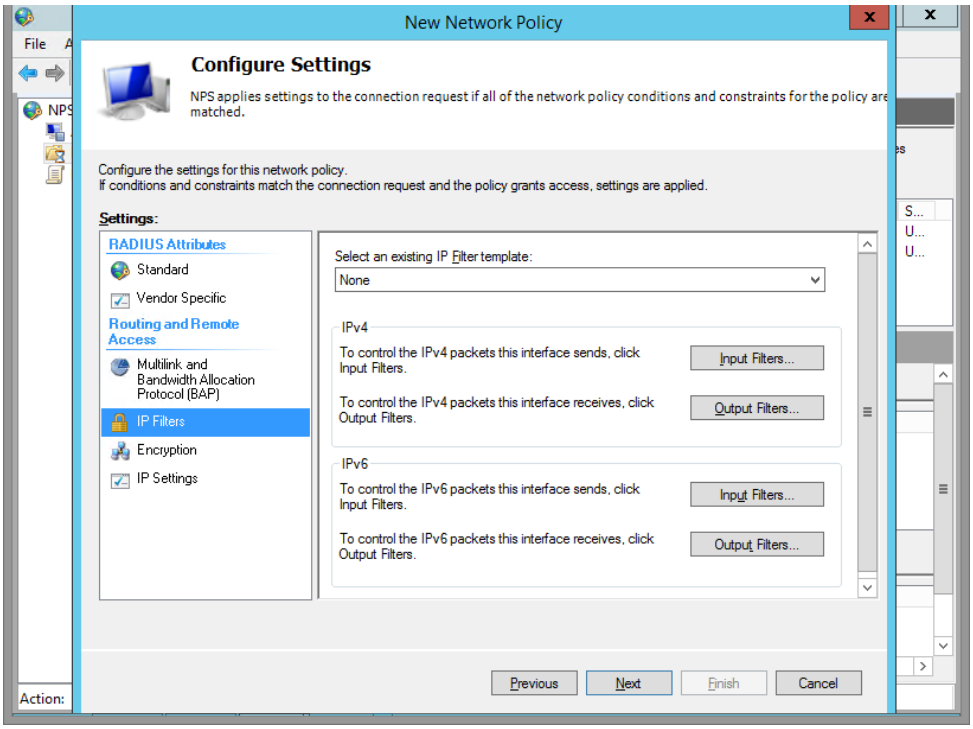
Step 9

Here you can set some restrictions if you like. (Optional) Click Next.



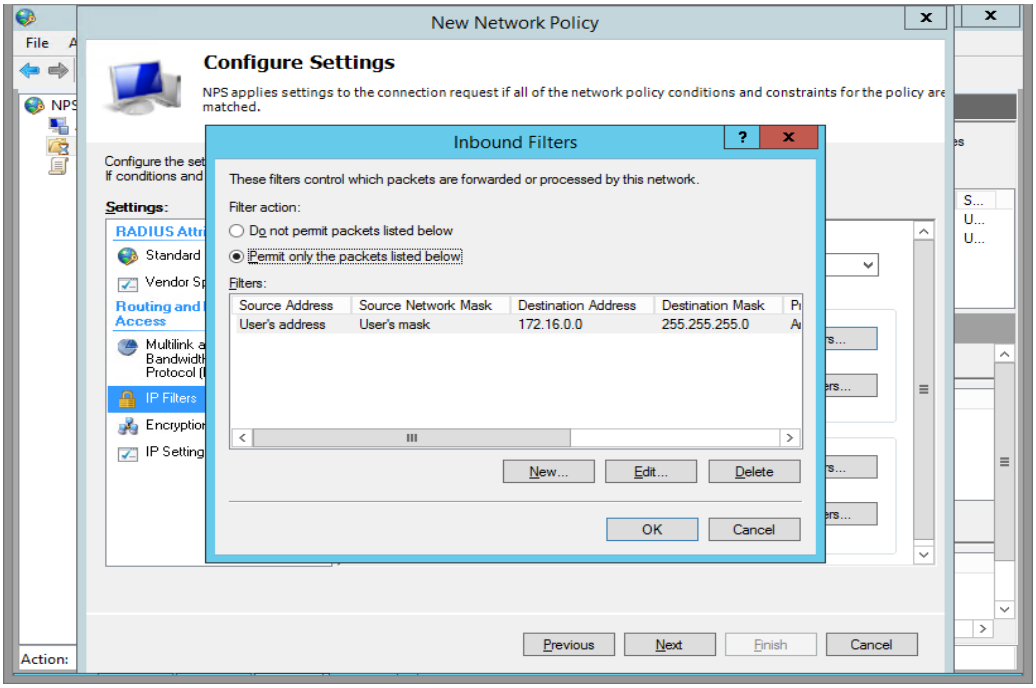
Step 10

Click on **IP Filter**.



Step 11

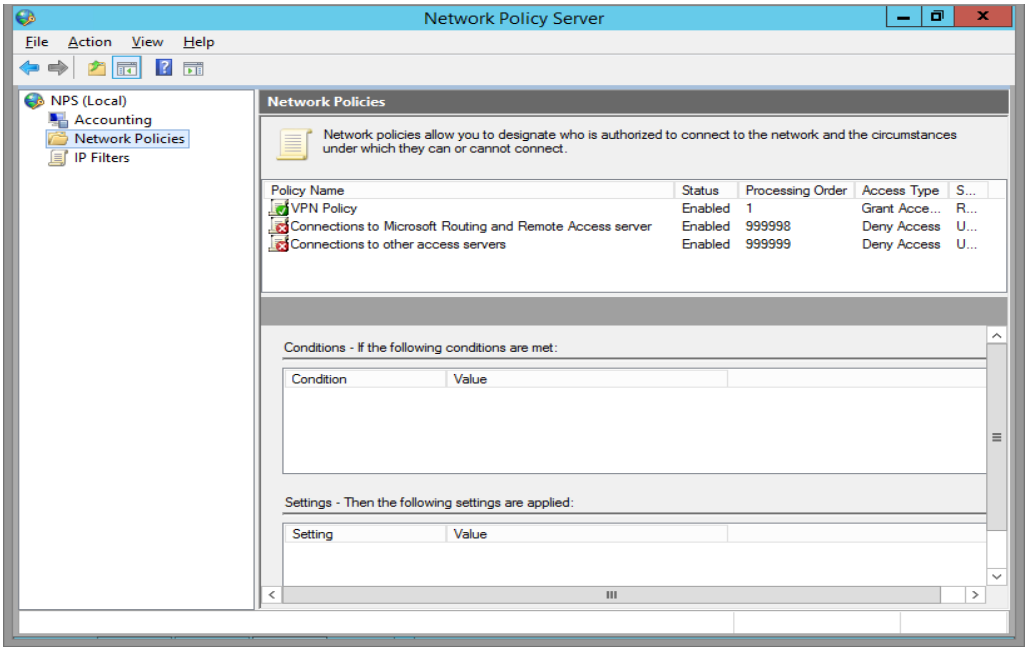
Specify a Filter. I set mine to only allow access to my lab's subnet.



Step 12

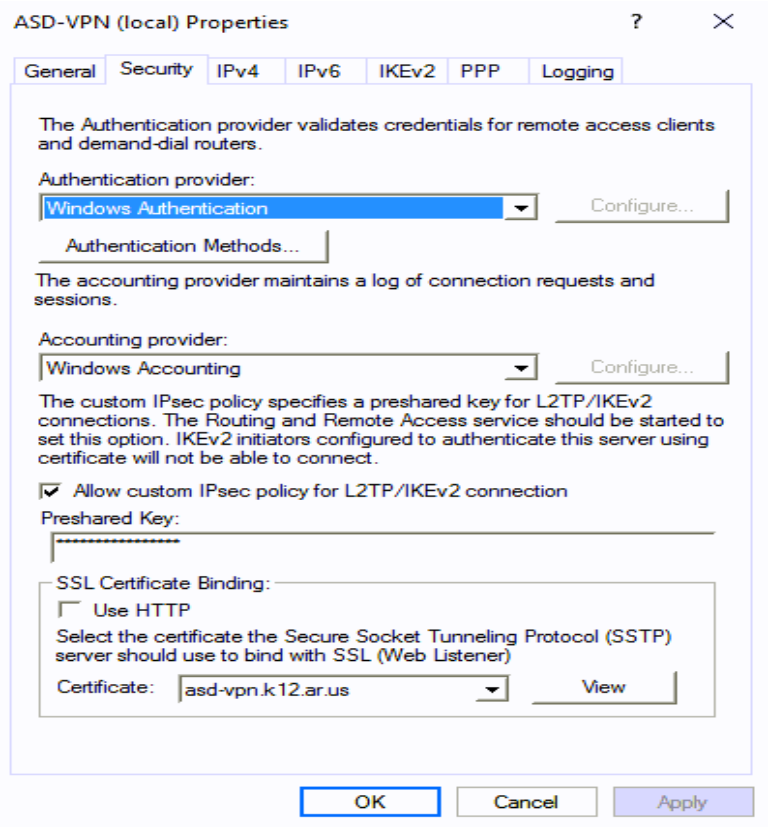
Click OK, next, and you're done setting up NPS!

There's more you can filter by, but this is the basics. You can also configure the Network Policy Server which can lock down your network so that only clients with Firewalls enabled and AVs installed will be allowed to connect.

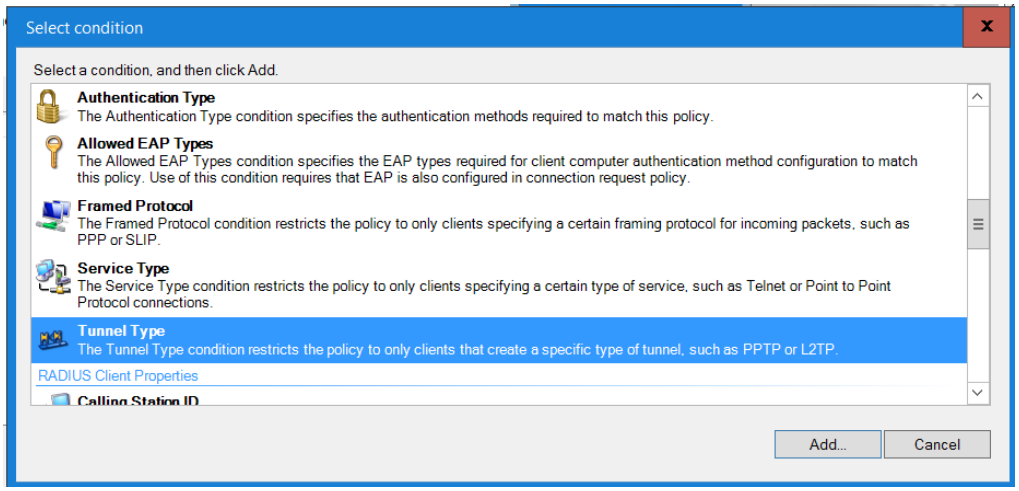


Setup L2TP for Mac OS and Chromebook

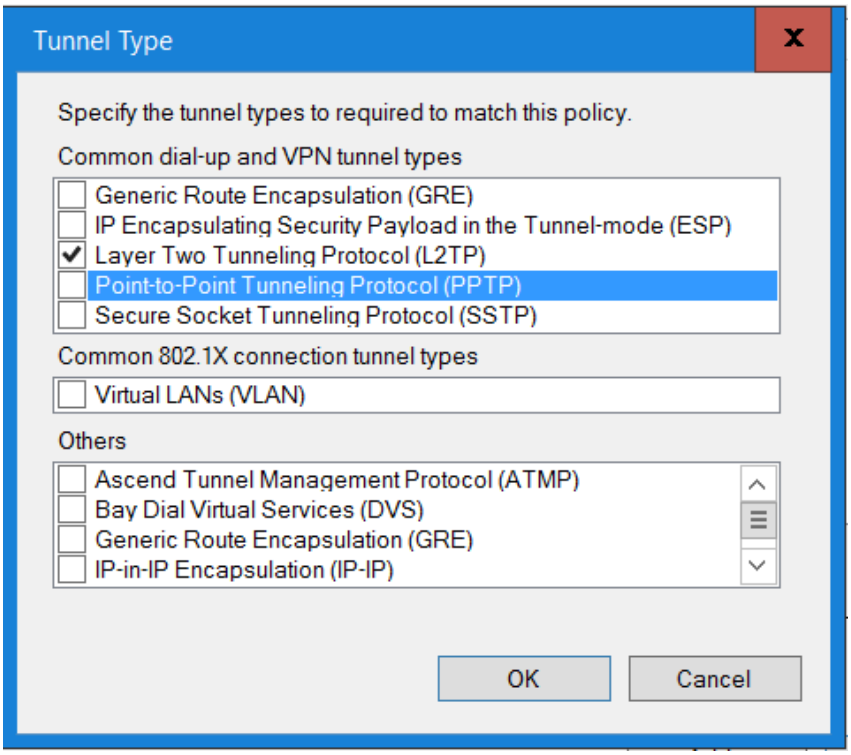
If you are going to enable L2TP for Mac OS and Chromebook access then you need to create a second Network Policy with these additions. On the Properties of the Routing Remote Access Server, click the box for Allow custom IPsec policy for L2TP/IKEv2 connection and enter a Preshared Key. I would suggest a key that is long and complex. The more simple the key, the more easy it can be hacked.



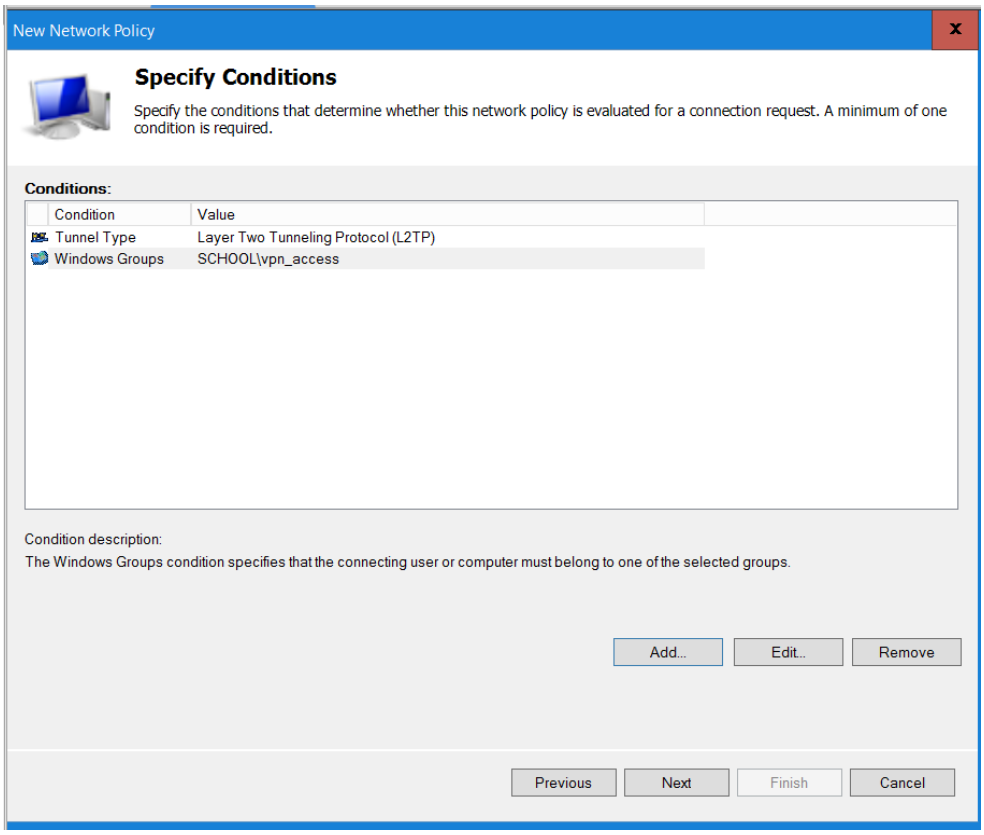
Next follow steps 1-6 of Network Policy Setup, to setup a second Network Policy named L2TP.



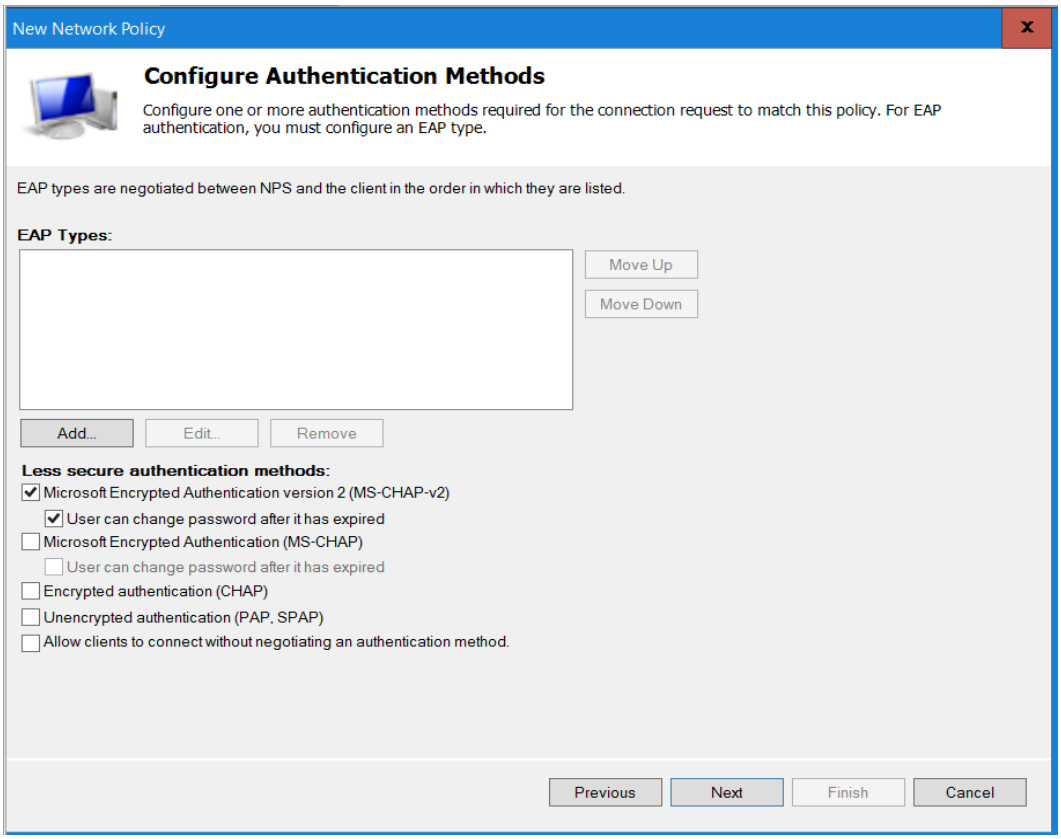
Click Add. Select Tunnel Type and Add.



Click box for Layer Two Tunneling Protocol (L2TP), Click OK.

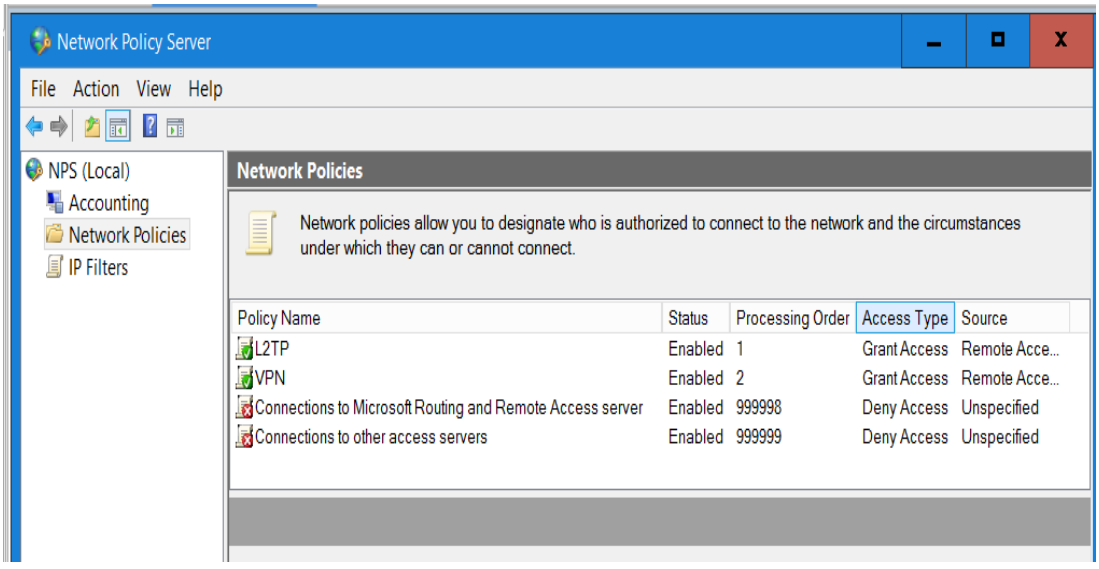


Click Next and Next on Access Granted.



Only Check boxes for MS-CHAP-V2 and User can change password after it has expired. Then Click Next.

Click Next on Configure Constraints and Next on Configure Settings and Finish.



Make sure that the L2TP Rule is first or you will get an error with Authentication.

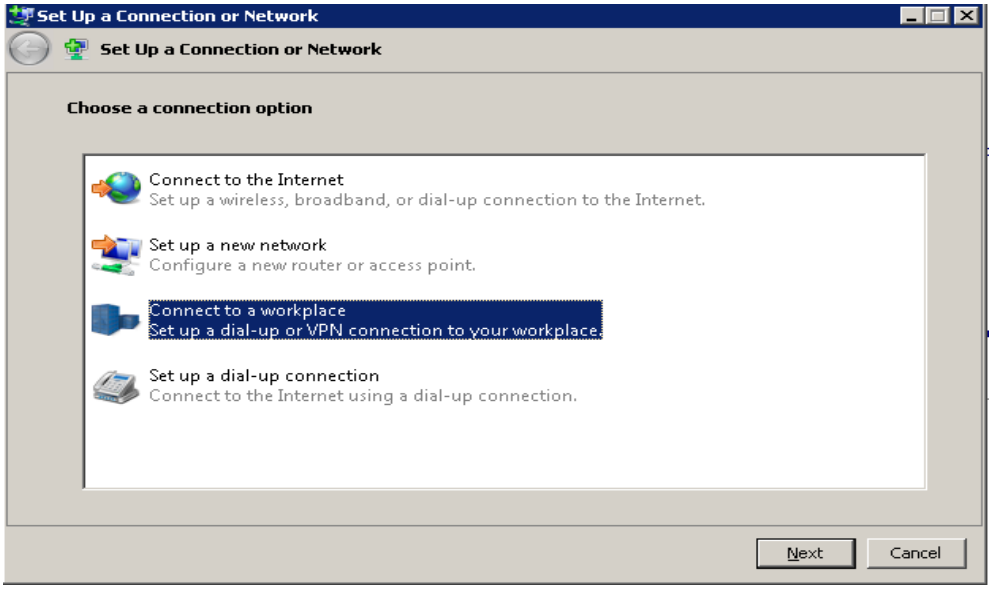
Setup a Windows 7 Client to Connect

Step 1

Log into a Windows machine. SSTP was introduced in Windows Vista, so the OS must be Vista or Greater (or Server 2008 and greater). Go to **Network and Sharing Center**. Click **Setup New Connection or Network**. Steps 2-9 are for Windows 7 and step 10 is for Windows 10.

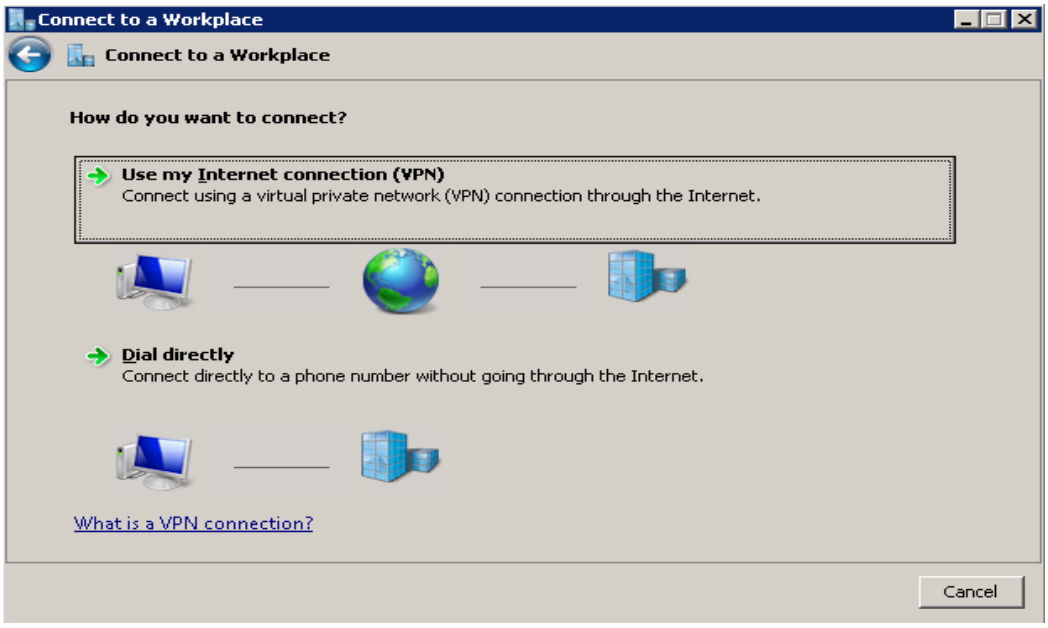
Step 2

Click **Connect to a workplace**.



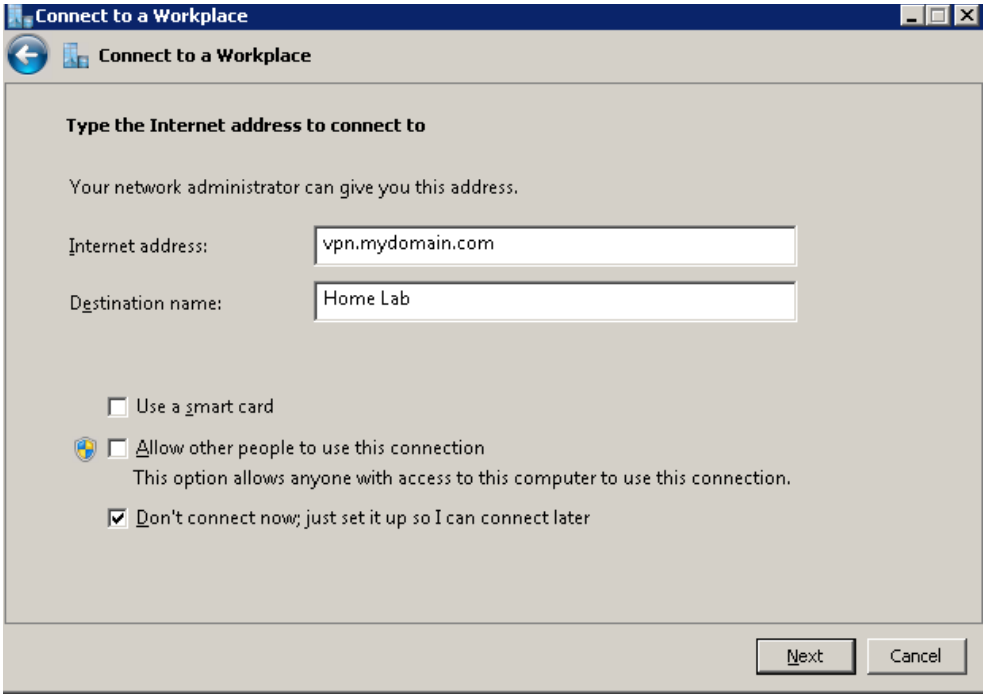
Step 3

Click **Use Internet Connection (VPN)**.



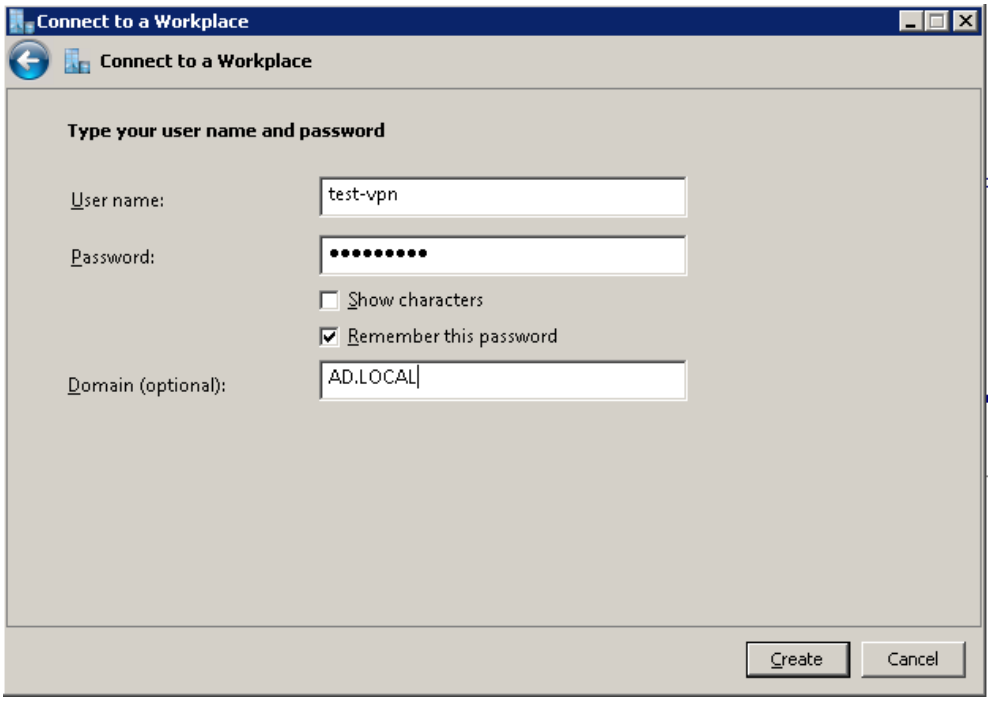
Step 4

Fill in your info, and click **Don’t connect now; just setup so I can connect later**.



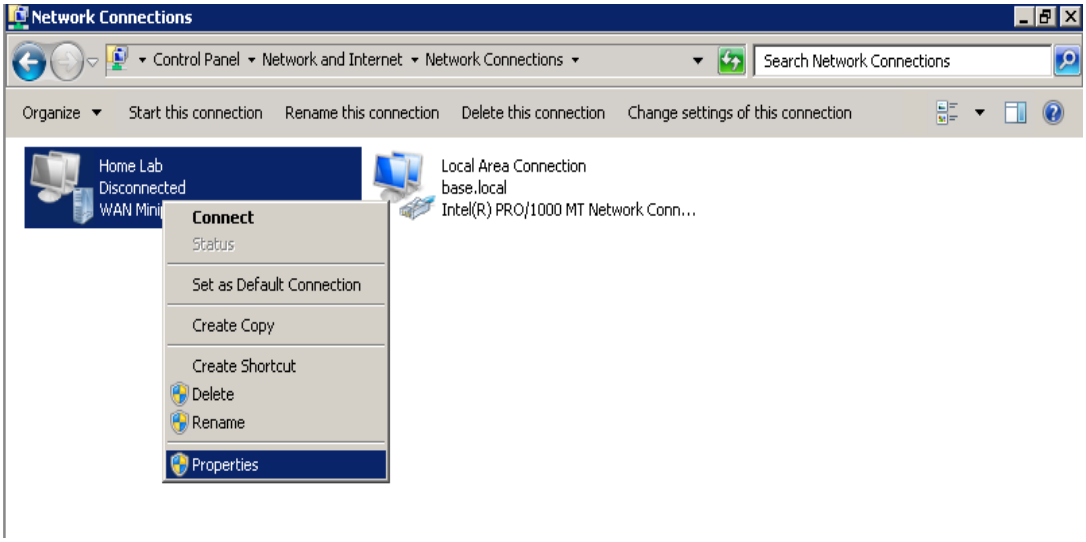
Step 5

Enter your user information. Don’t forget that if you didn’t setup a Group to access the VPN using NAP, you’ll need to enable Dial-In access within Active Directory Users and Computers for that user.



Step 6

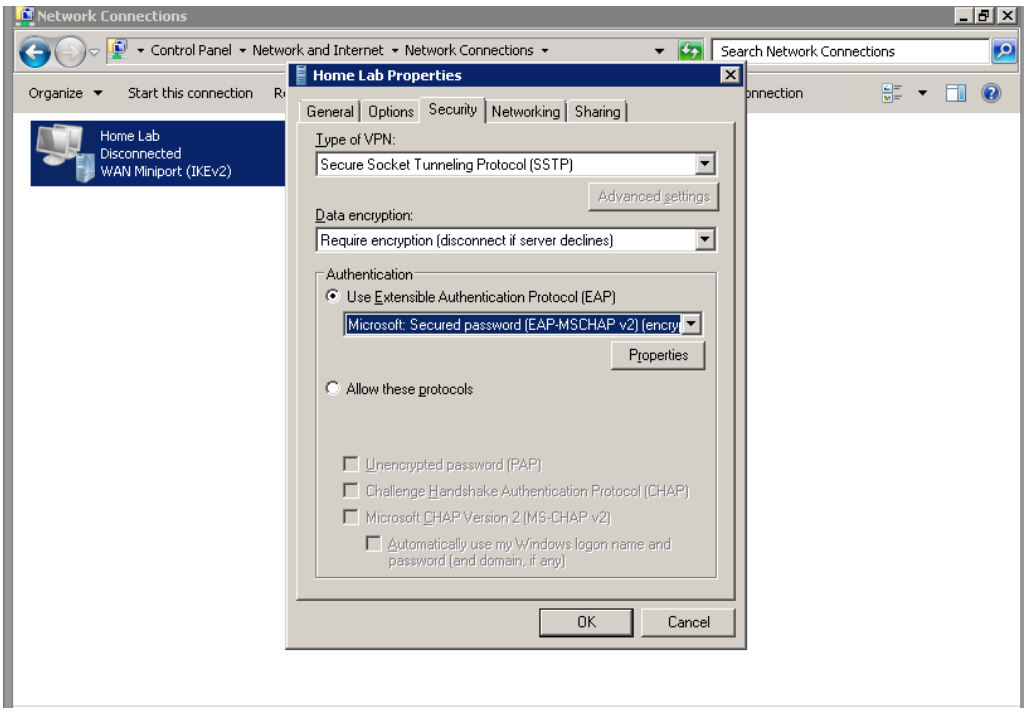
We still need to configure a couple more things. Click on your connection -> Properties.



Step 7

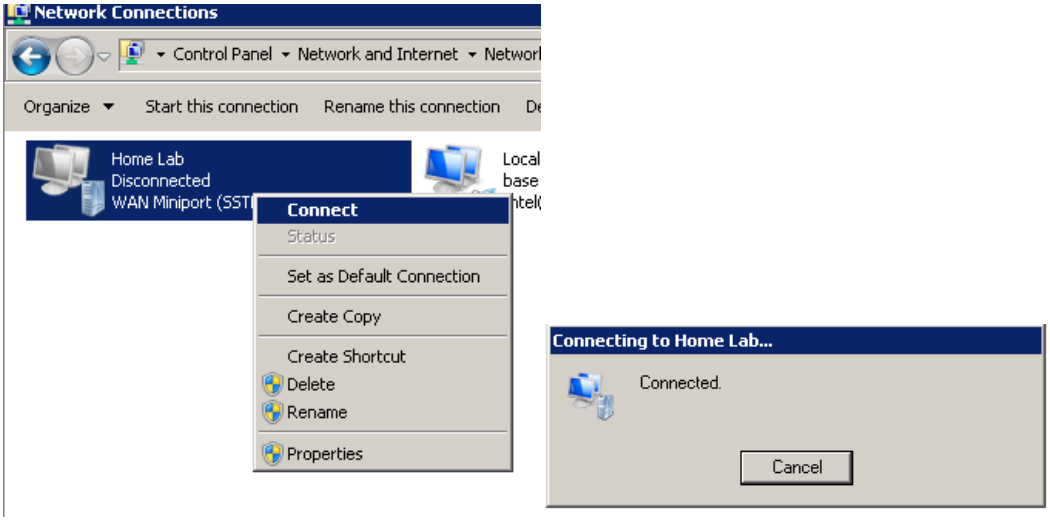
Click the Security Tab -> Change type of VPN to SSTP. By default, it detects the type of VPN automatically, but slightly slows down the process.

Also change your authentication as seen below. That's all you need. Note that, by default, Windows VPNS will use the remote gateway. If you want to modify that, go to Properties -> Networking -> IPv4 -> Advanced -> Uncheck Use Default Gateway on Remote Network.



Step 8

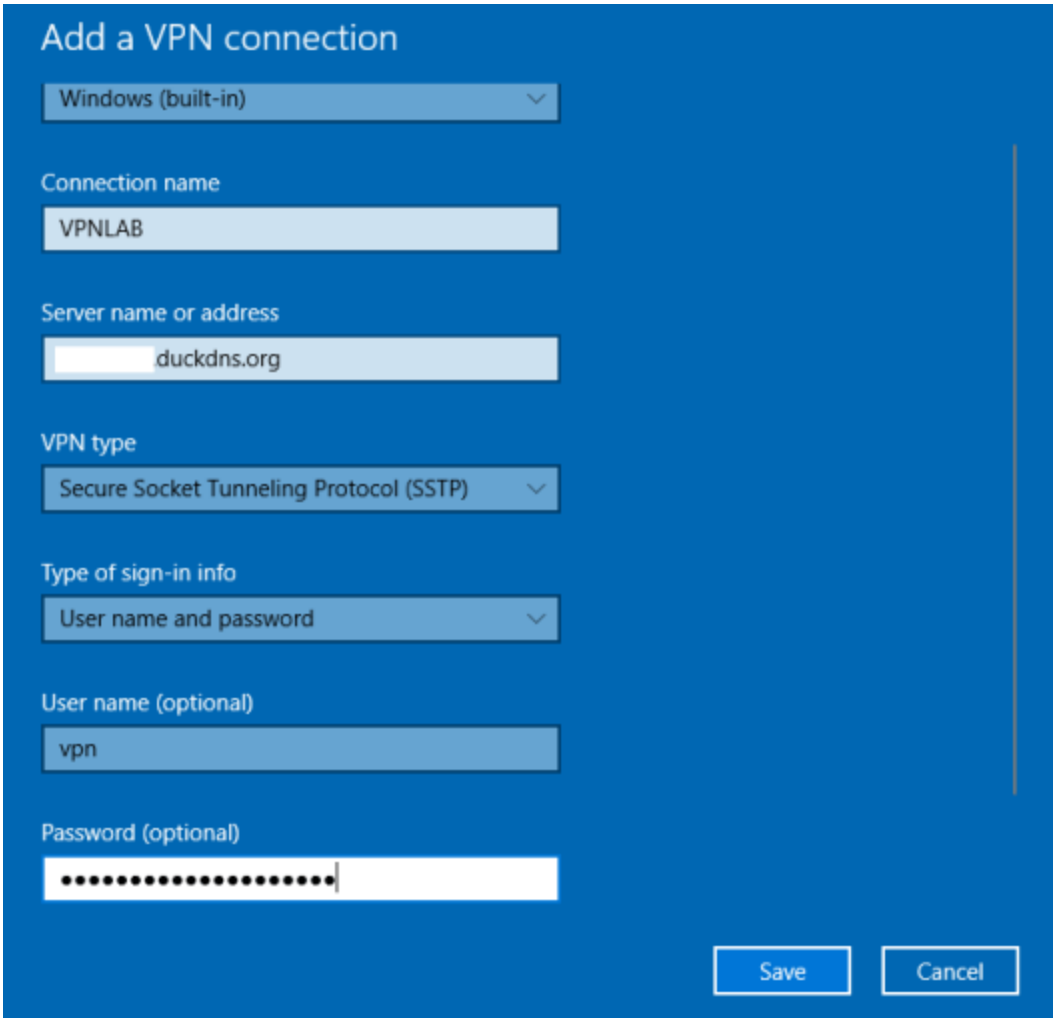
Right-click -> Connect.



Windows 10 VPN Client Setup

In Windows 10 click Settings> Network & Internet> VPN and click add a VPN connection. Select Windows (built-in) as the VPN provider and give the connection a name of your choosing. Enter the external DNS name of your VPN server and choose the VPN type as SSTP.

You can then enter the credentials of the VPN user account, then save the connection.



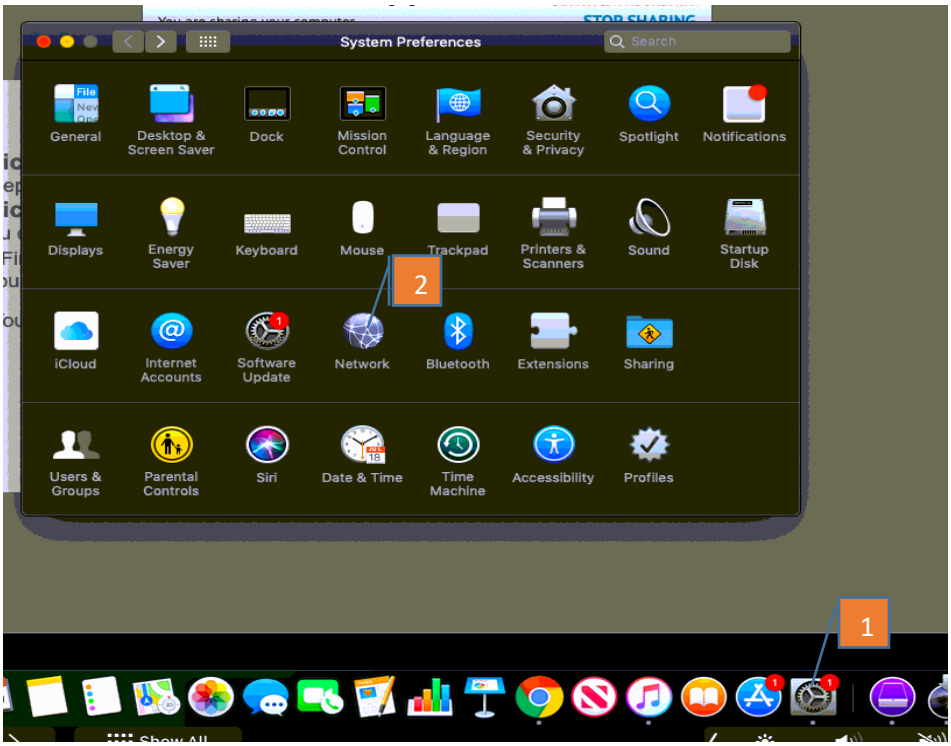
If you are going to use L2TP on Windows you have to add the following Registry DWORD:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent

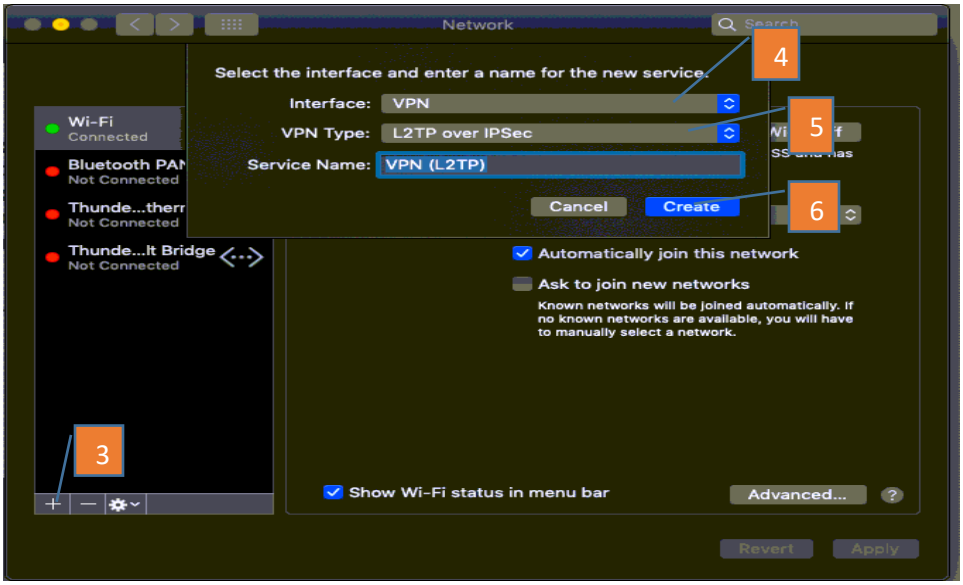
Create a new DWORD parameter with the name AssumeUDPEncapsulationContextOnSendRule and the value 2. Restart the server and the machine in order to apply changes.

This needs to be added on the server and the client machine.

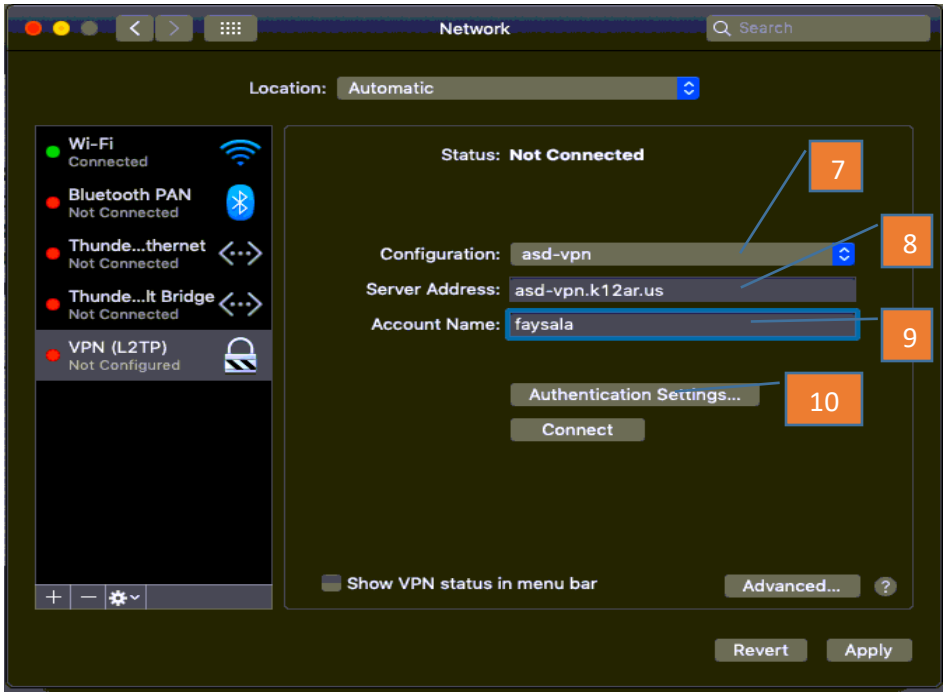
Setup L2TP VPN on Mac OSx



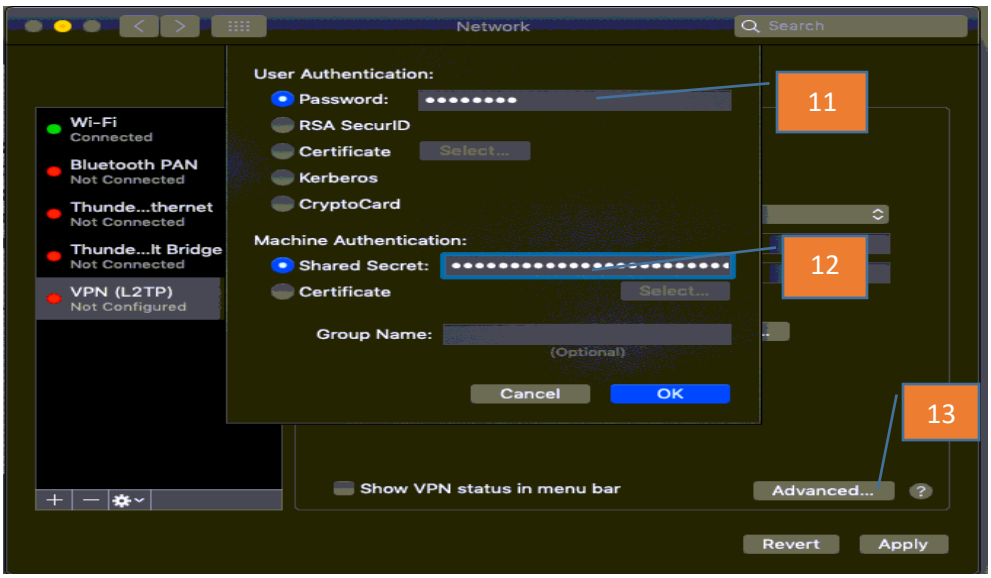
1. **Open System Preferences.**
2. **Open Network.**



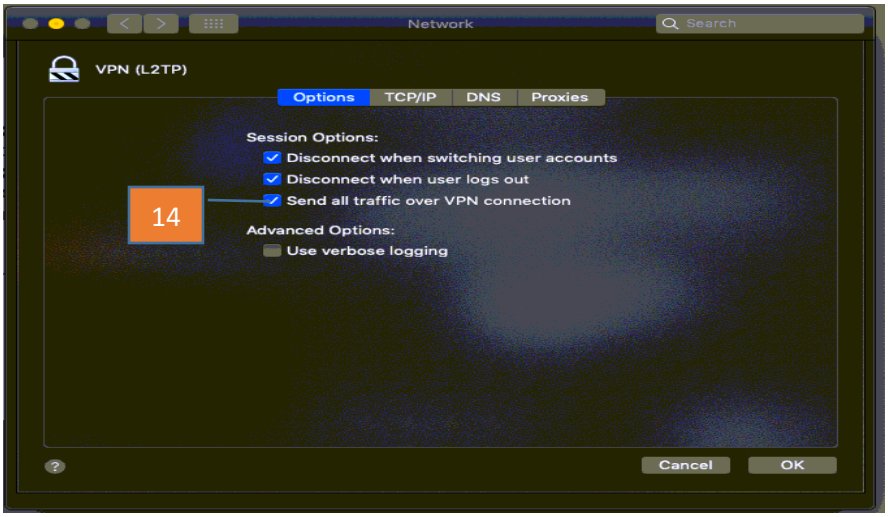
3. **Click the +**
4. **Choose VPN for Interface Type.**
5. **Choose L2TP over IPSec for VPN Type.**
6. **Click Create.**



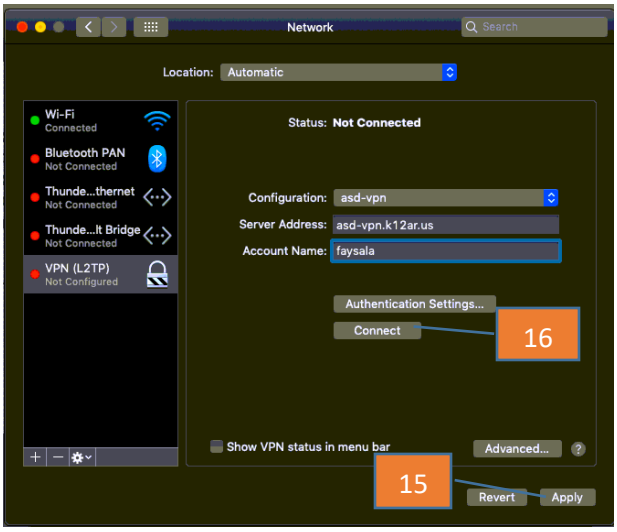
7. **You can leave it Default or choose add a configuration and give it a name.**
8. **Enter the FQDN URL of the VPN Server.**
9. **Enter the AD username. You don't need to enter the domain.**
10. **Click Authentication Settings.**



11. **Enter the AD Password.**
12. **Enter the Preshared Key from the Server Setup. Click OK.**
13. **Click Advanced.**



14. **Click Send all traffic over VPN connection.**



15. **Click Apply.**
16. **Click Connect and it should show Connected.**