VPN

Go to **Server Manager** => add **Remote Access**

after installing is finishing, click **"Open the getting started wizard"**

In the wizard choose **"Deploy VPN only"**

R-click on the server and choose **"Configure and enable Routing and Remote Access"**

Choose **"Remote Access (Dialup or VPN)"**

Click **Next**

Select the interface that is connected to the internet, and click **next**

Choose **Automatically** to assign IP configuration from DHCP, and click **next**

Choose to use **Routing and Remote Access** to authenticate connections requests, click **next**

Click Finish

Take a look on **Properties of RRAS** server

Know what do these properties do.

Look at the **"Ports"**, by default you have 128 port available, and you can r-click and choose properties to change the default settings

---

Create **a VPN connection** from a client PC and verify connectivity to the internal network

Edit the **User dial in property** to **allow access**

Open Network Policy Server

Go to **Network Policy** and double click the first policy to view the policy properties

Notice the Policies applies in order, once you hit a condition to allow or deny, you get it. and no further checking is done to the next policy

Edit the policy to **allow access**, and change the user property to **control access through NPS**

Configure VPN using SSTP

First add **"Active Directory Certificate Services"** role, and choose to add **"Certificate Authority"** and **"Certificate Authority Web Enrollment"**

Choose **Stand Alone server**, then choose **Root CA**

choose to create a **new private key**

From **Server Manager**, go to tools then **Internet Information Services (IIS)**

Click on **Server name**, and then **open Server Certificates**

Choose **"Create Self Signed Certificate"** type the server **FQDN** as the name of the certificate

---

Then go **Sites**=> **Default Web Site** ==> and click on **Bindings** to add **HTTPS** in Site Binding

Type **the server name** in **host name**, and select the **certificate** you have created

---

Open **Internet Explorer** and go to **https:// server3.lab.local/certsrv**

Request a certificate, Advanced certificates request, Create and submit a request to this CA

Type the name: **server3.lab.local**

Choose type of certificate method: **Server Authentication Certificate**

In Key Option: check on **Mark keys as exportable** (this allow the machine to import the public and private key from user side)

Go back to: **https:// server3.lab.local/certsrv**

Go to **Certificate Authority** from **Server Manager**

Open **Pending Requests**, r-click and choose **issue**

Go to: **https:// server3.lab.local/certsrv** then click **View the status of a pending certificate request**

Click the **certificate** to request it, then **install the certificate**

Open **MMC**

Add the snapin for **"Certificate for the user", "Certificate for Local Computer"**

Notice: users will not use the certificate that is in Local Computer Certificates, the client can't trust a server just because it says trust me. So you need to export the certificate you as a user just created as exportable

Go to **personal** => **Certificates for current user**, r-click on the **certificate**, => **all tasks** => **export**

Click **Next**, Choose **"Yes, Export private key",** then click **Next**, Choose your **account**, choose the location to save the certificate

From the Computer Side certificates, go to **personal** => **certificates** and **import** the one you just exported

---

Now you need to configure the RRAS server to use the certificate

In order to make it possible for RRAS to use the Server Authentication Certificate you must change the **bindings** for **HTTPS** to use the certificate, Go to **IIS** console to get this done.

Then, Go to **server3**, r-click => **properties**

From **Security** tap, under **SSL Certificate bindings**, Select the **certificate**. (make sure that the right one is selected, not the self signed certificate that the server made for itself)

From Client side you need to adjust the registry to make client accept the fact that you didn't buy the certificate from known certification authority. which will be the case in production environment

Type **Regedit** in **Run**

go to:
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurretControlSet\Services\SstpSvc\Parameters

Add the key: **NoCertRevocationCheck** and change the value to 1

You also need to add the self-signed certificate of the server to the client, so go to https://RRAS.lab.local/certsrv

Download a **CA Certificate**, **Certificate Chain**, or **CRL**

Download **CA Certificate Chain**

Open **MMC**

Add **certificates** for **Local Computer**

Inside **Trusted Root Certificate** add the **certificate** you just downloaded

Now, make a VPN Connection to the Server and make sure the connection name is the name as the certificate name, which is **server3.lab.local**

Check the **connection type** to make sure it is **SSTP**