Check the TMG 2010 virtual private network server - Part 3: Configure TMG Firewall as L2TP / IPsec Remote Access VPN Server

In Part 3 of this series, I will show you how to configure TMG Firewall as the L2TP / IPsec Remote Access VPN Server.

Network Administration **- In Part 3 of this series, I will show you how to configure TMG Firewall as an L2TP / IPsec Remote Access VPN Server.**

>> Check the TMG 2010 virtual private network server - Part 1
>> Check the TMG 2010 virtual private network server - Part 2

In the previous article in this series, I showed you how to configure TMG firewall to make PPTP remote access VPN server. As you can see, configuring the TMG firewall to make the PPTP remote access VPN server is quite simple. That's why PPTP VPN servers are so popular.

In this section we will show you how to configure the TMG firewall as an L2TP / IPsec VPN server. Need to say that this is a simple configuration like the PPTP VPN server configuration. That's because, if you want to configure the L2TP / IPsec remote access VPN server correctly, you need to handle the certificates. Obviously you can avoid all certificate issues by using pre-shared keys, but pre-shared keys are usually unsafe keys and they are almost impossible to expand. We will show you how to use a pre-shared key at the end of this section but first let us take a look at how to do it differently.

In order for all components to work in the safest environment for L2TP / IPsec, make sure you have the following:

- The TMG firewall must have a server certificate with the common name that the VPN client will use to connect to the VPN server. This means that the VPN server on the Internet must be able to identify this generic name into an IP address on the external interface of the TMG firewall.
- The TMG firewall must trust the CA that issued the server certificate used by the VPN server. In the example used in this article, the TMG firewall is a domain member and an enterprise CA and is installed on the domain controller, so the CA certificate is automatically installed on the TMG firewall because it is a member. domain.
- The VPN client must trust that the CA has issued the TMG firewall server certificate used by the VPN configuration. Because the VPN client in the example we used in the lab is a domain member, it will have the CA certificate installed in its Trusted Root Certification Authorities repository.

Server configuration

Let's start by looking at the **Certificates** MMC on the TMG firewall. The focus here is the machine certificate store, as shown in Figure 1 below. Note that the computer seems to have installed a certificate. However, this is a computer certificate that is automatically installed for autoenrollment. We cannot use this certificate for L2TP / IPsec because the generic name on the certificate is not a name that can be resolved on the Internet. In addition, we really don't want to disclose the TMG firewall's name to potential intruders, so that's one reason not to use this certificate, even if we can.

Figure 1

Once here, let's create a certificate. Right-click in the middle pane of the interface and point to **All Tasks** then click **Request New Certificate** , as shown in Figure 2 below.

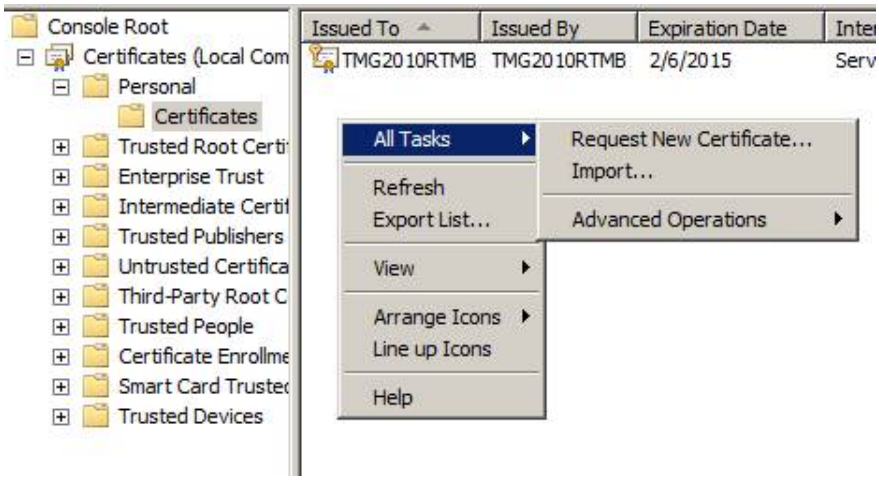

Figure 2

Click **Next** on the **Certificate Enrollment** page, as shown in Figure 3.

Figure 3

On the **Select Certificate Enrollment Policy page** , see Figure 4, click **Next** .

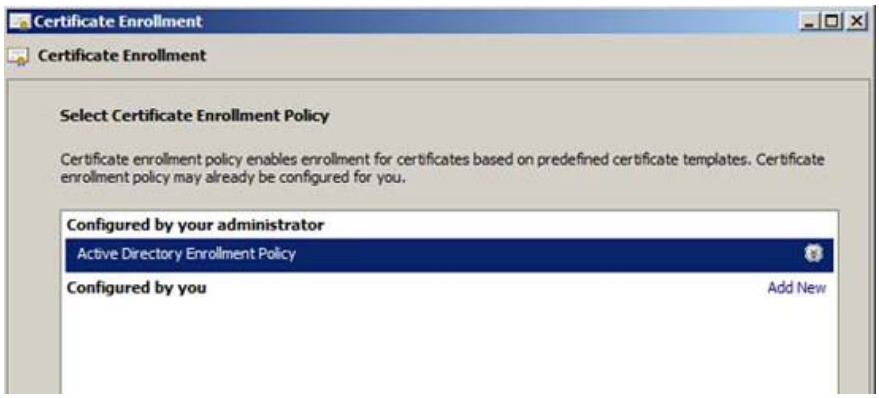

Figure 4

In Figure 5 below, you can see the **Web Server** certificate, which is the sample certificate we want to use. However, this template is not available to us. Here, you may start to suspect that maybe things won't be as easy as you think.

Figure 5

What should be done now? You may recall that we used the enrollment site during the Windows Server 2003 period. Let's try it. In Figure 6 below, you can see that we have entered the URL **http:/// dc1 / certsrv** . It seems that we do not install the enrollment site on the certificate server.

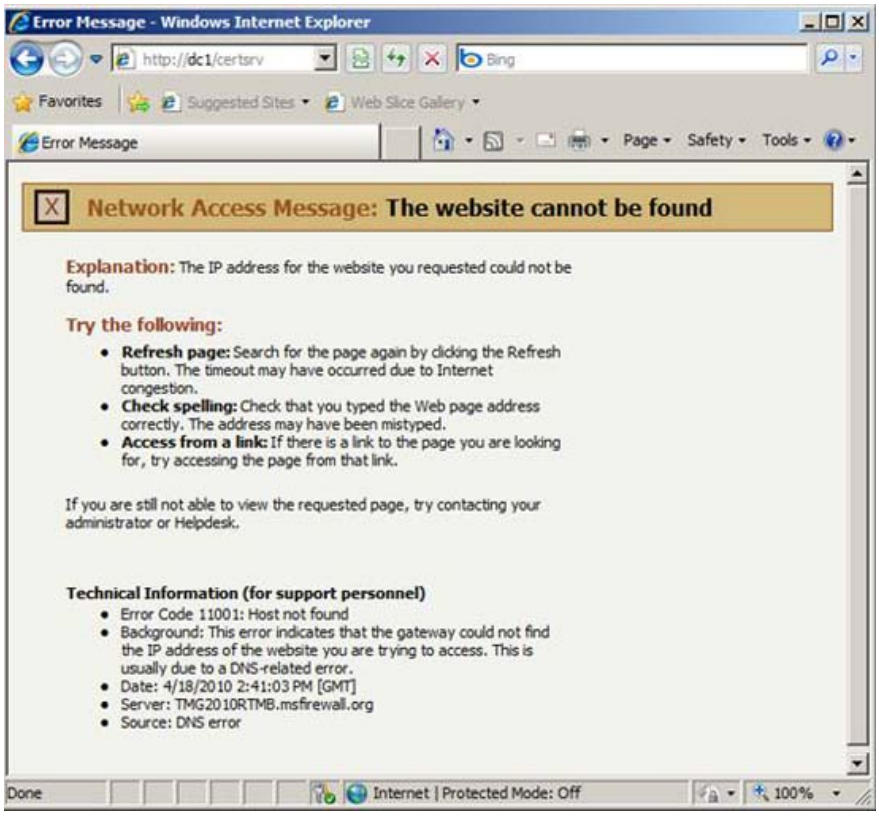

Figure 6

Now we need to point out what to do. We can go back and install the Web enrollment site, but this doesn't really fix the problem because of changes in Windows Server 2008 and the versions on it don't let you get the certificate. The server is from the Web enrollment site, so that option is irrelevant. We can create a new certificate template and configure the permissions on the template so that we can use the **Certificates** MMC to gain certification. However, if you do that, we will see that you cannot request a certificate from the TMG firewall because by default the TMG firewall's policy will lock down DCOM communications required to request certificates through MMC. We can change System Policy to enable these certificates and then request the certificate, eventually changing System Policy back, but that method seems quite complicated and sophisticated. Alternatively, we can create an offline request using the **Certutil** tool, then use it for CA and receive the certificate, but most of us don't remember the command, and it doesn't really mean that Good in use.

What we search for is a simple way to get a certificate by using something we are running. Fortunately, the Web server role is now installed on the domain controller, because we want to use the website to test the connection. Or, that's a solution: You can use the IIS interface to request a certificate for the TMG firewall and then copy it to the firewall after you're done. A very simple way to do it.

In Figure 7, you can see the **Internet Information Services** console. Click the computer name in the left pane of the interface. In the middle pane of the interface, you will see the **Server Certificates** icon. Double-click this **Server Certificates** icon.

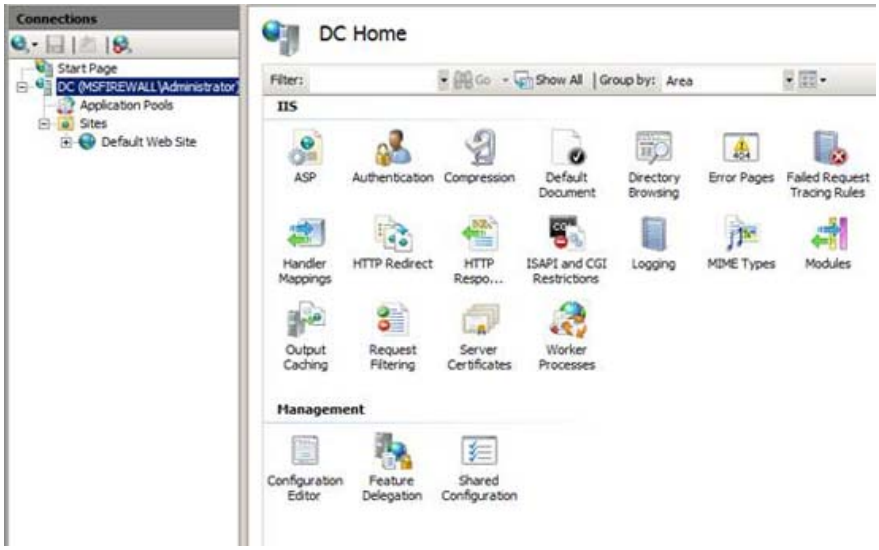

Figure 7

In the right part of the interface, click the **Create Domain Certificate link** , as shown in Figure 8.

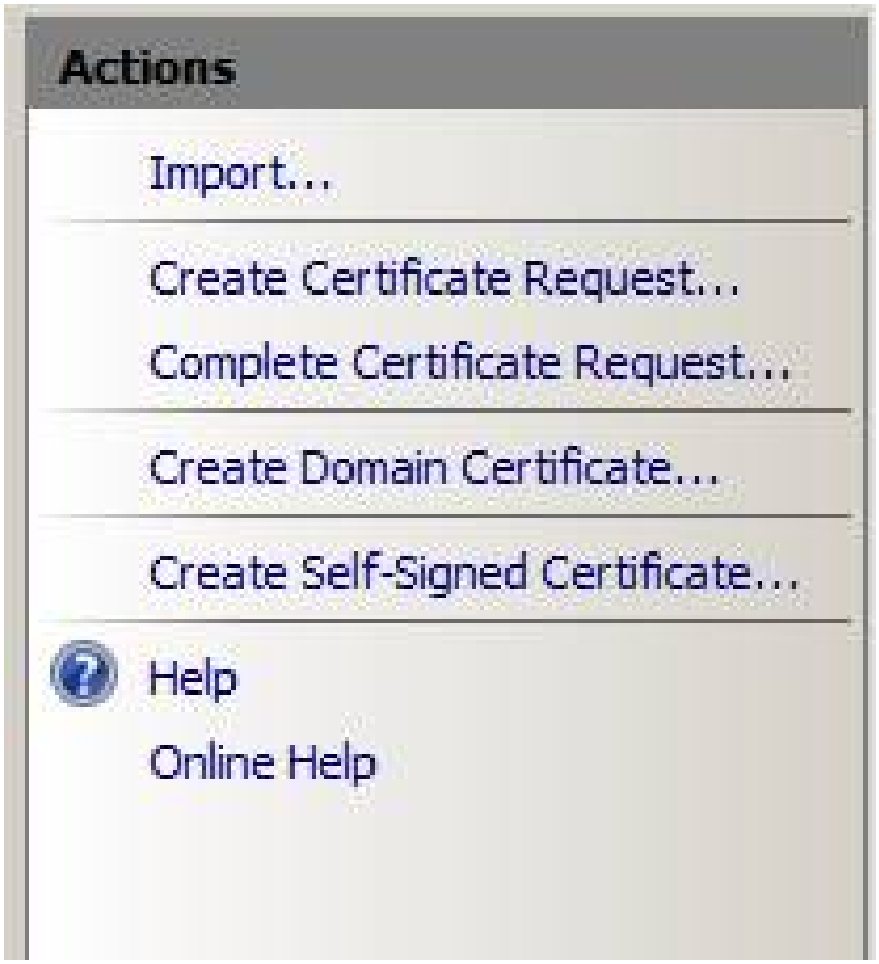

Figure 8

This will open the **Create Certificate** wizard. On the **Distinguished Name Properties** dialog box, the most important item is **Common name** . The name you enter in this text box must match the name you use to connect to the VPN server, this name must resolve to the IP address on the external interface of the TMG firewall (or if the TMG firewall is behind NAT devices, it must resolve to a public address on a NAT device that accepts connections and forward them to the external interface of the TMG firewall). The remaining items on this page are not very important, but you need to fill them out completely, as shown in Figure 9 below. Click **Next** .

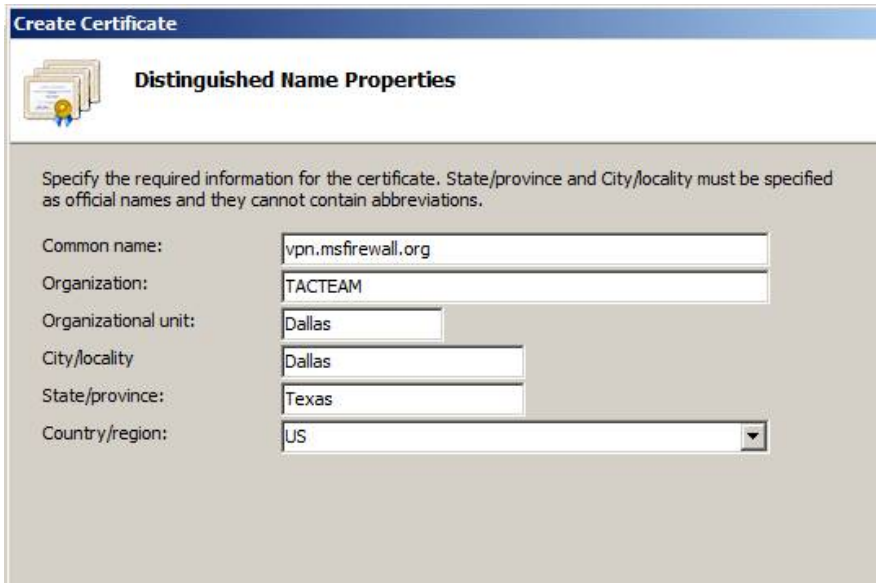

Figure 9

On the **Online Certificate Authority** page, shown in Figure 10, click **Select** .

Figure 10

This will open the **Select Certification Authority** dialog box. In Figure 11 below, you can see that we have an existing CA, **msfirewall-DC-CA name** . Select CA and click **OK** .

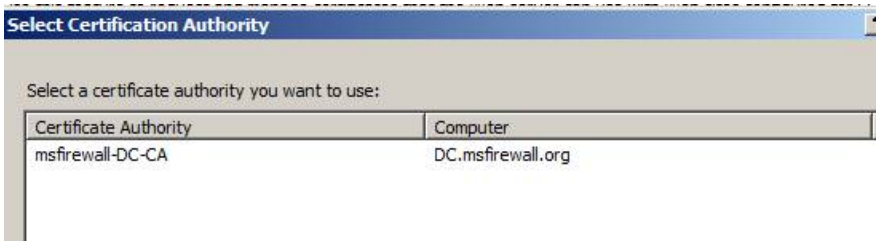

Figure 11

The name of the CA will appear in the **Specify Online Certificate Authority** text box. Enter a name for the certificate in the **Friendly Name** text box. In this example, we assigned the name **L2TP Certificate** , as shown in Figure 12. Click **Finish** .

Figure 12

When you're done, you'll see the new certificate in the list of **Server Certificates** . In Figure 13 below, you can see **L2TP Certificate** in the list.

Figure 13

In order for the certificate to go through the TMG firewall, we must export the certificate. Right-click **L2TP Certificate** and click **Export** , as shown in Figure 14.

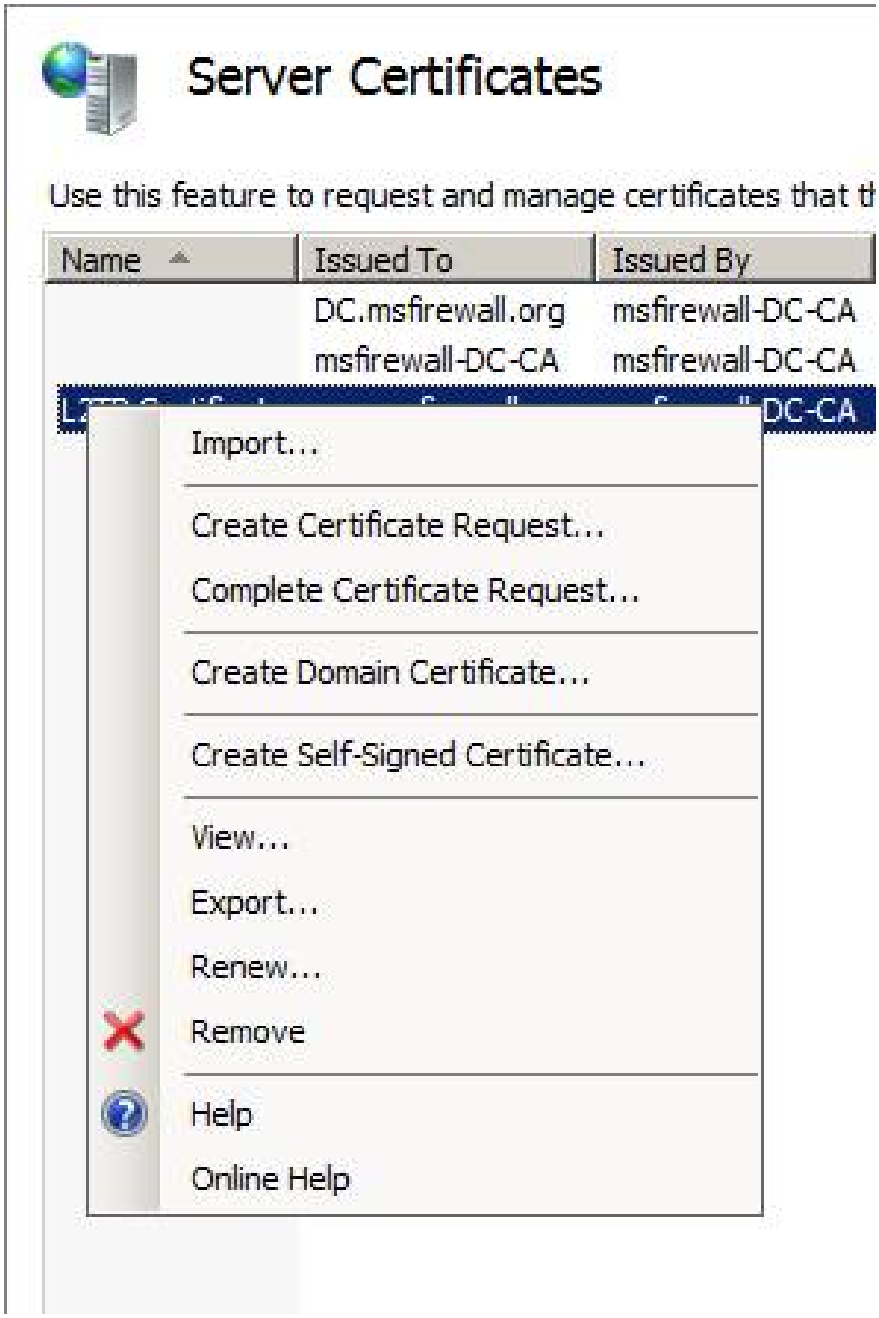

Figure 14

On the **Export Certificate** page, use the '.' button, see Figure 15.

Figure 15

In the **Specify save as file name** text box, as shown in Figure 16, select the location in the left panel, then enter the name of the exported certificate file in the **File name** text box and click **Open** .

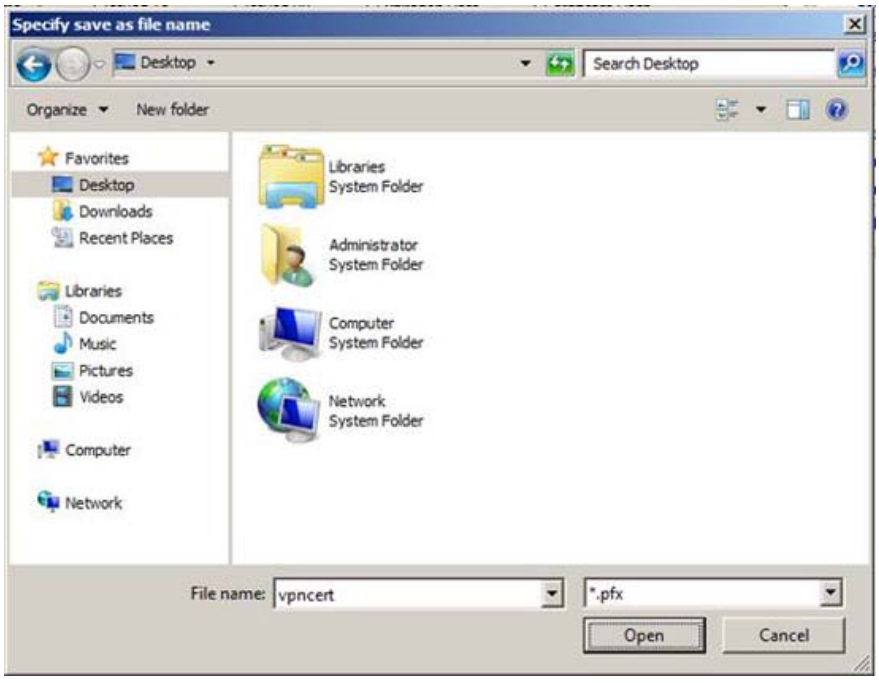

Figure 16

In the **Export Certificate** dialog box, shown in Figure 17, enter the password and confirm the password, and then click **OK** .

Figure 17

Copy the certificate to the TMG firewall. After you copy the certificate to the TMG firewall, open the **Certificates** MMC console and navigate to **Certificates (Local Computer) PersonalCertificates** in the left pane of the interface. In the middle pane, right-click an empty section, point to **All Tasks** , click **Import** , as shown in section 18.

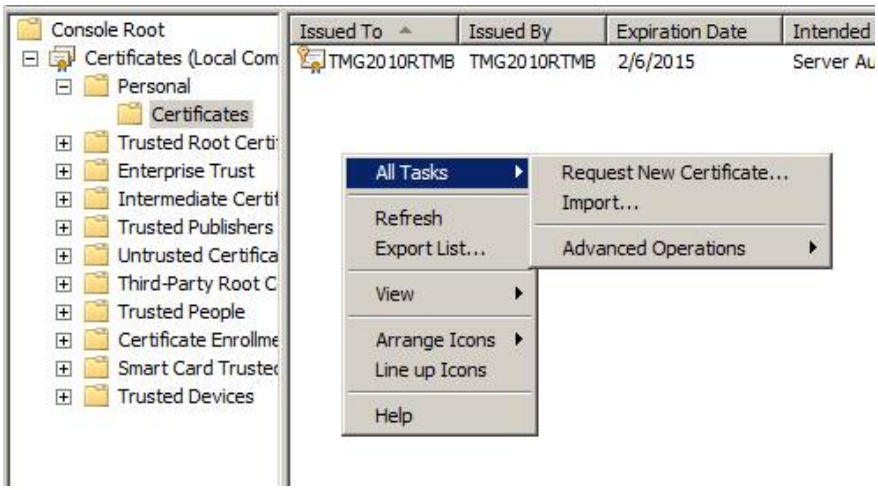

Figure 18

Doing so will open the Certificate Import Wizard. Click **Next** in the **Welcome to the Certificate Import Wizard page** , see Figure 19.

Figure 19

On the **File to Import** page, see Figure 20, click the **Browse** button and locate the certificate. The path and name of the certificate will appear in the **File name** text box. Click **Next.**

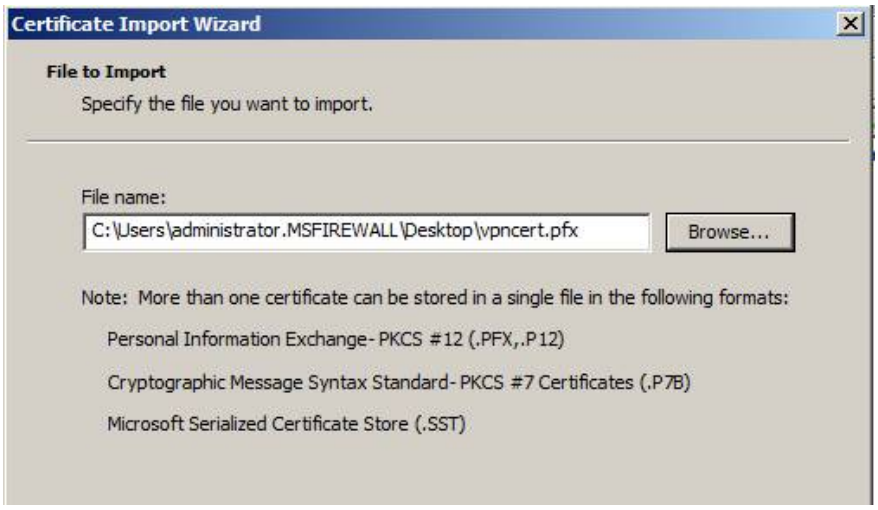

Figure 20

On the **Password** page, see Figure 21, enter the password you created when exporting the certificate. In this example, we selected **Mark this key as exportable. ?ây s? ???c phép b?n ?? ??ng nh?p ho?c t?i thông báo c ?a b?n t?i m?t th?i gian sau** . Click **Next** .

Figure 21

On the **Certificate Store** page, see Figure 22, select the option **all certificates in the following store** . Click **Next** .

Figure 22

On the **Completing the Certificate Import Wizard page** , Figure 23, click **Finish** .

Figure 23

Now, click **OK** in the dialog box informing you that the import process was successful, see Figure 24.

Figure 24

When finished, you will see the certificate in the middle pane of the console, see Figure 25.

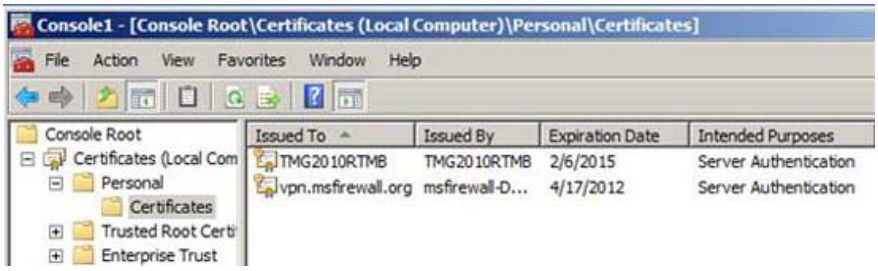

Figure 25

Open the TMG firewall interface and click the **Remote Access Policy (VPN) button** in the left pane. In the right pane of the interface, click **Configure VPN Client Access** , as shown in Figure 26.

Figure 26

On the **VPN Clients Properties** page, see Figure 27, check the box select **Enable L2TP / IPsec** and then click **OK** .

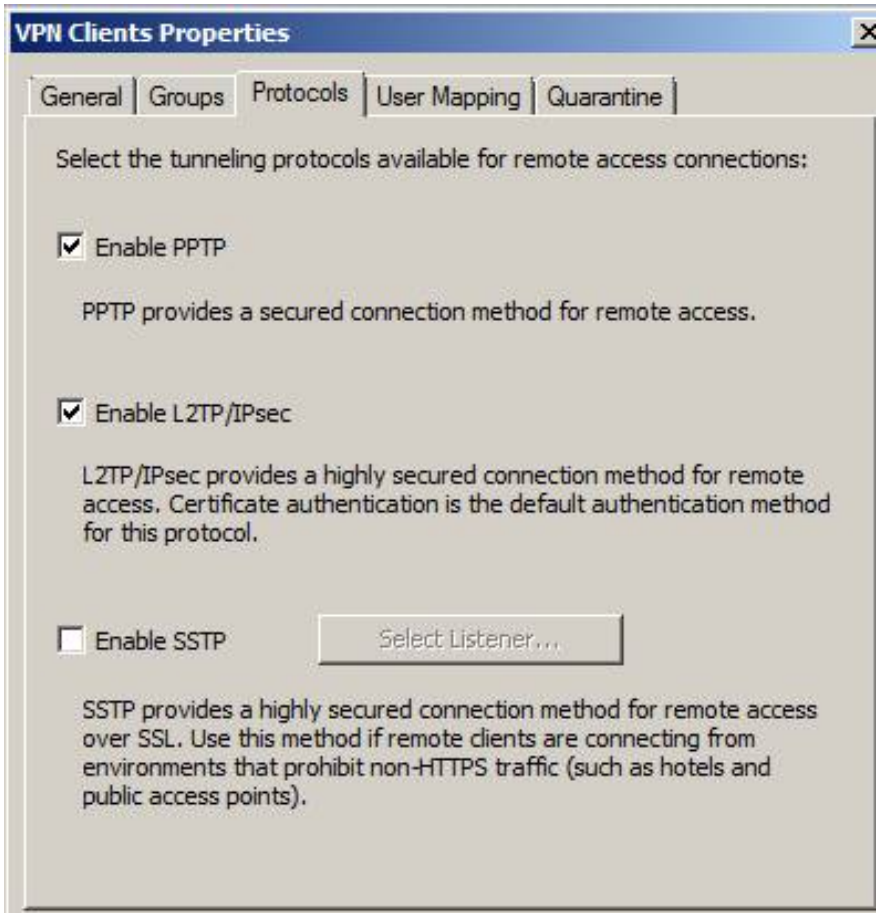

Figure 27

Click **Apply** to save the changes to the firewall policy, see Figure 28. Remember that you always **apply** your changes to them to take effect.

Figure 28

Client configuration

The server is now ready to use, we have traveled half the way. Now we will focus on the client. The first thing we need to do is check to make sure that the CA certificate of the CA issued by the VPN server certificate is in the **Trusted Root Certification Authorities page** . In Figure 29, you can see that **msfirewall-DC-CA is** already in this list, so we'll continue on from here.

Figure 29

In this example, we will use the same VPN connection that we used in the previous section. However, we have to make some changes so that it will use L2TP / IPsec instead of PPTP. Open the **Network Connections** window on Windows 7 client and click **Properties** , as shown in Figure 30.

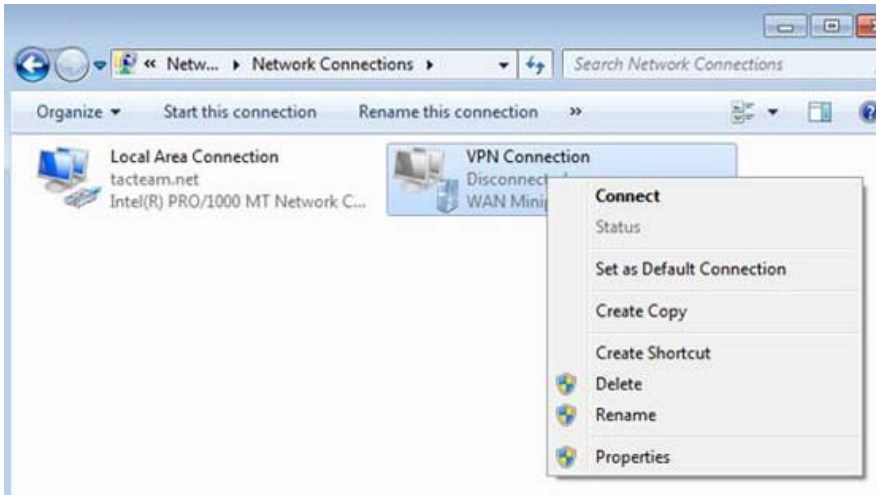

Figure 30

In the **VPN Connection Properties** dialog box, click the **Security** tab. On the **Security** tab, in the **Type of VPN** drop-down list, select the **Layer 2 Tunneling Protocol with IPsec (L2TP / IPsec) option** , then click **OK** , see Figure 31. This will force the client to use L2TP / IPsec without using the VPN protocol. Click **OK** to save the changes.

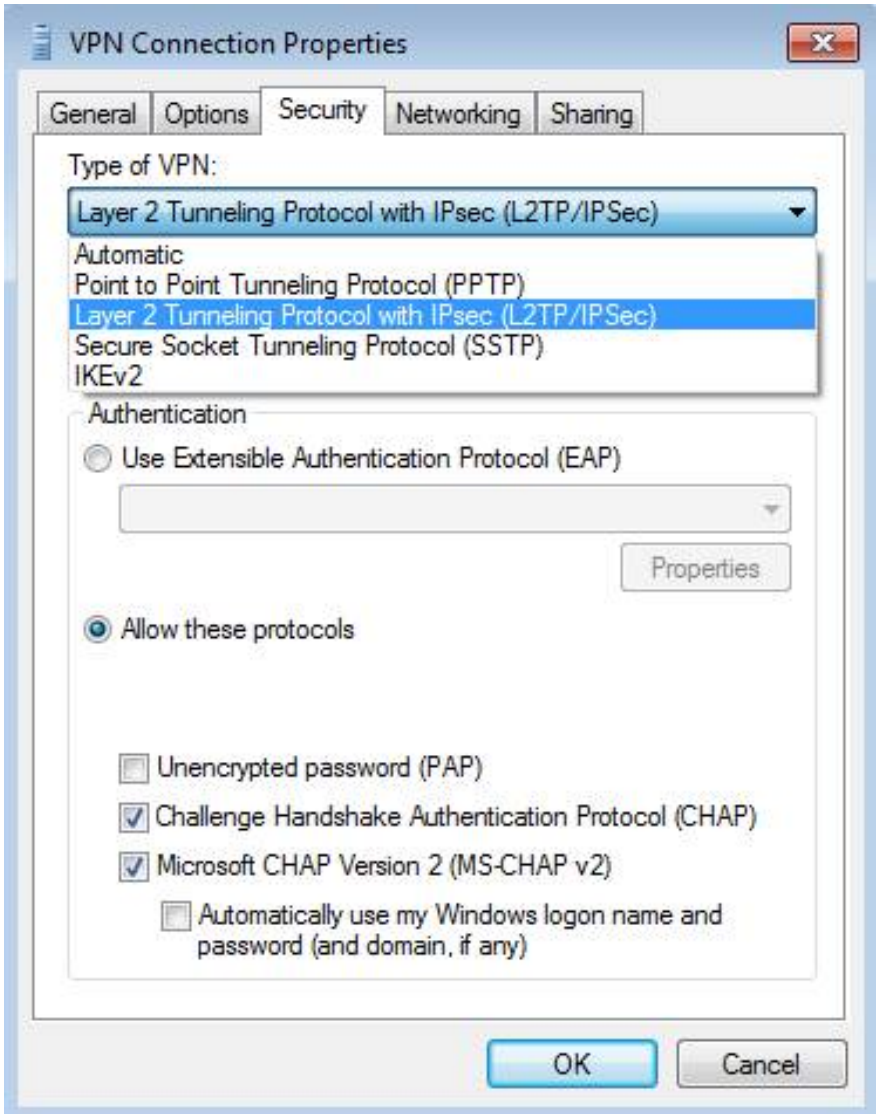

Figure 31

OK! Now is the time to set up the VPN connection. After the connection is established, we can check to see the details of the connection by right-clicking on the VPN connection and clicking **Status** , see Figure 32.

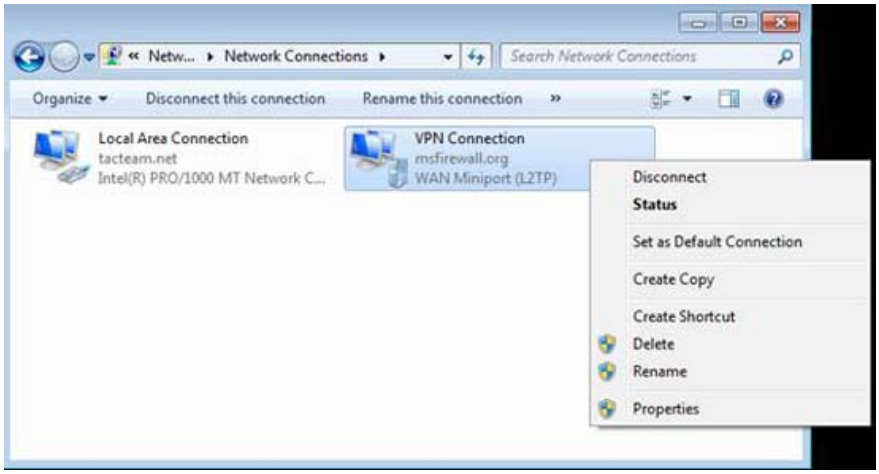

Figure 32

In the **VPN Connection Status** dialog box, click the **Details** tab. In Figure 33, you can see that L2TP / IPsec is used and 128-bit AES encryption is also being used.

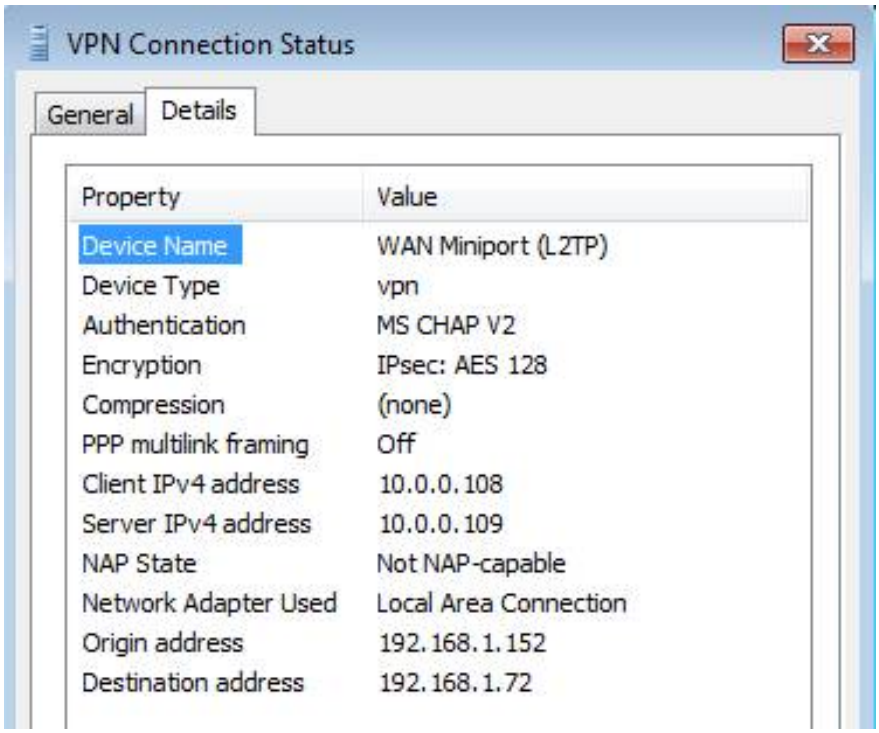

Figure 33

When we return to the TMG firewall console, you can see the **Sessions** section in the **Dashboard** , see Figure 34, that has a **VPN Remote Client** connection.

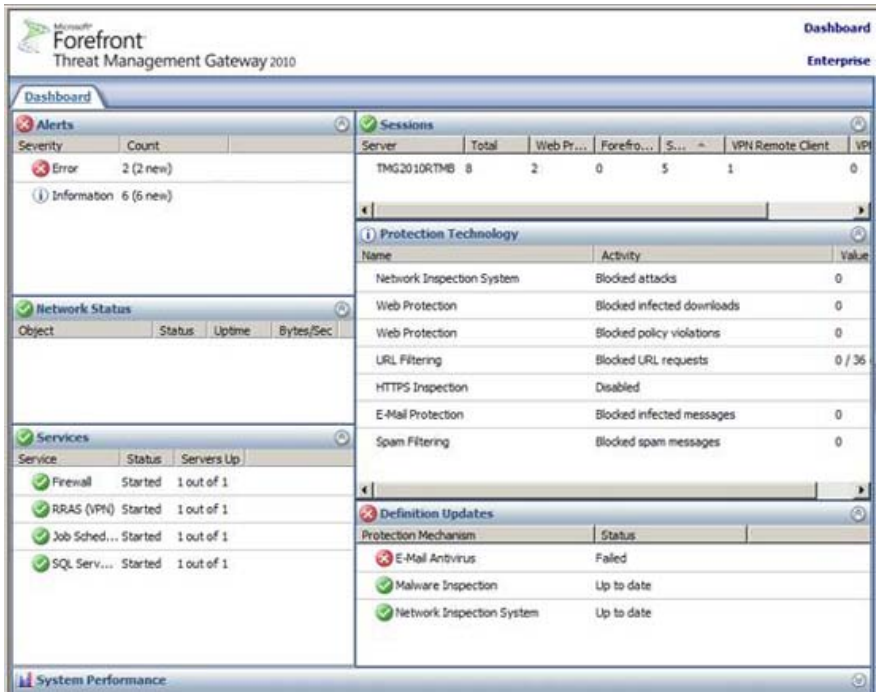

Figure 3 * 4

Click the **Monitoring** button in the left pane of the console. Here in Figure 35, you can see the VPN client connection. Note that the VPN connection type will be listed, as well as the name of the logged-in user. It also includes information about whether NAP is used for connection. In the next section, we will show you how to configure NAP and TMG firewall so that VPN clients must comply with the NAP policy before being allowed to access the network.

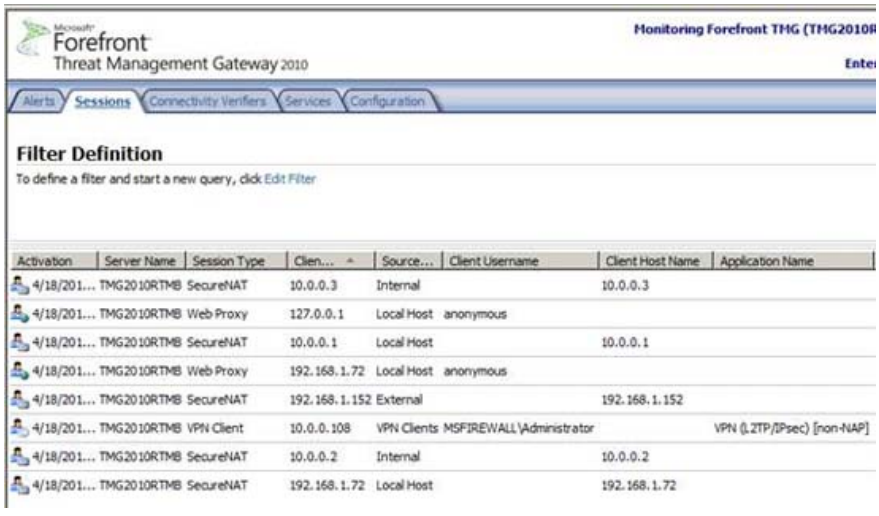

Figure 35

L2TP / IPSec does not need a certificate

We mentioned above, the best way to deploy L2TP / IPsec is to use certificates. However, if it's too fast, or you can't set up a PKI, you can use the pre-shared key instead. In Figure 36 below, you can see the **Authentication** tab in the **Remote Access Policy (VPN) Properties** dialog box **.** At the bottom of this dialog box is a checkbox that says **Allow custom IPsec policy for L2TP connection,** plus a text box named **Pre-shared key** . Note that the pre-shared key is shown in clear text, remind you that this is not a safe option and that you need to use certificates instead !!

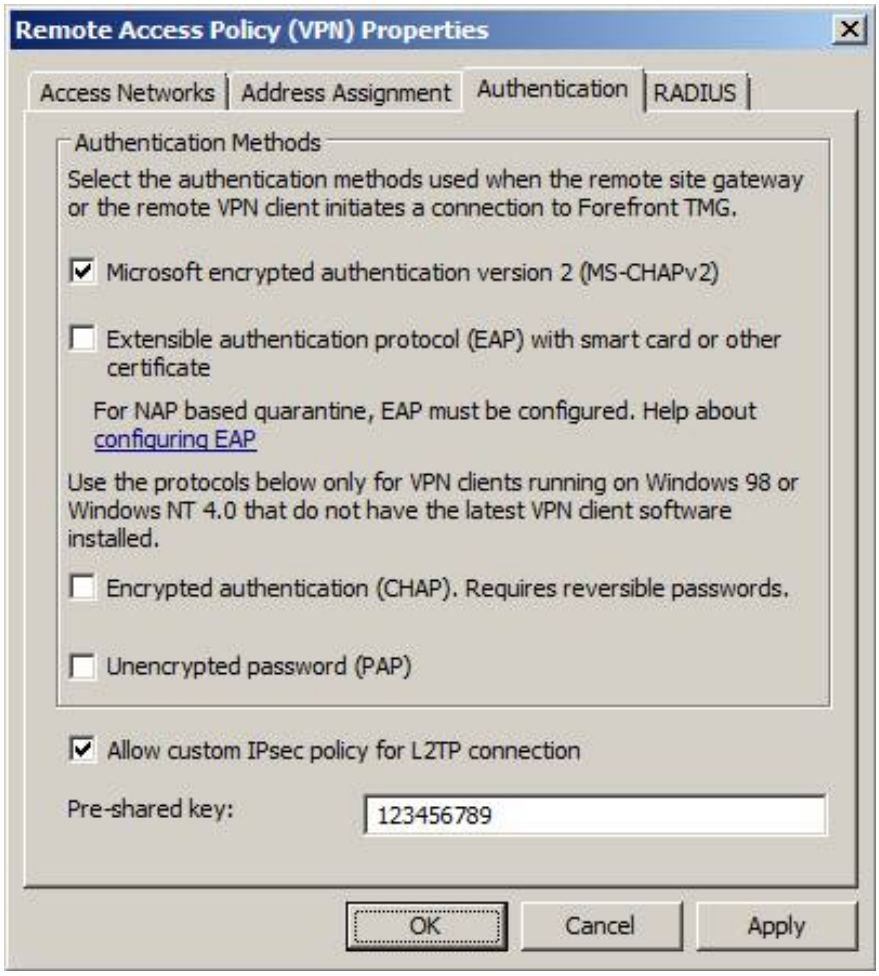

Figure 36

The client also needs to be configured to use pre-shared keys. In the **Properties** dialog box of the VPN connection, click the **Security** tab, as shown in Figure 37. Then click the **Advanced settings** button. Here you can select the option **Use preshared key for authentication** and enter the pre-shared key in the **Key** text box. That's all it takes. Easy as PPTP.

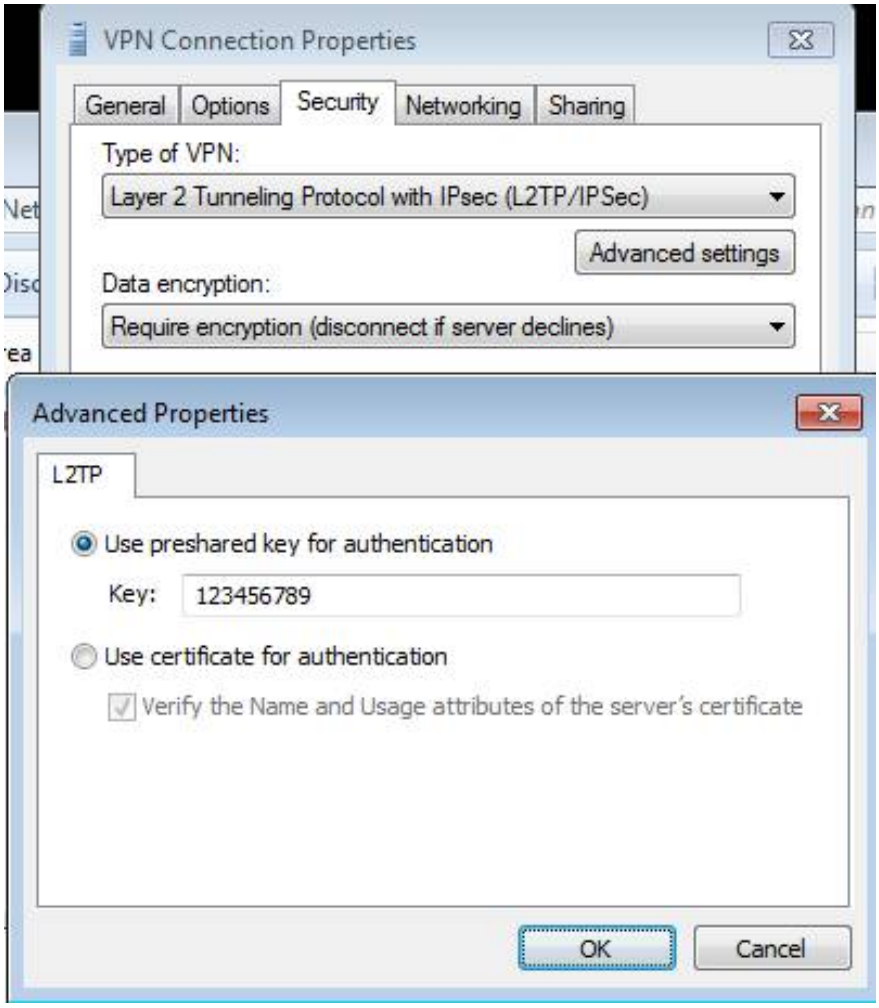

Figure 37

Conclude

In this article, I have shown you how to configure the TMG firewall as an L2TP / IPsec VPN server. We have gone through several different options for how to obtain the server certificate for the TMG firewall and then installed the certificate into the firewall's computer certificate store. We have also made some necessary changes to the firewall configuration to support L2TP / IPsec, making some necessary changes on the VPN client. We then established the connection and confirmed that L2TP / IPsec is in use. The project was successful! In the next article in this series, I will show you how to use NAP to increase the security of the TMG firewall based on a remote access VPN server.

You finished reading the article "**Check the TMG 2010 virtual private network server - Part 3: Configure TMG Firewall as L2TP / IPsec Remote Access VPN Server**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.