

## How to Connect to D-Link Firewalls Using VPN Client with Certification (X.509) ?

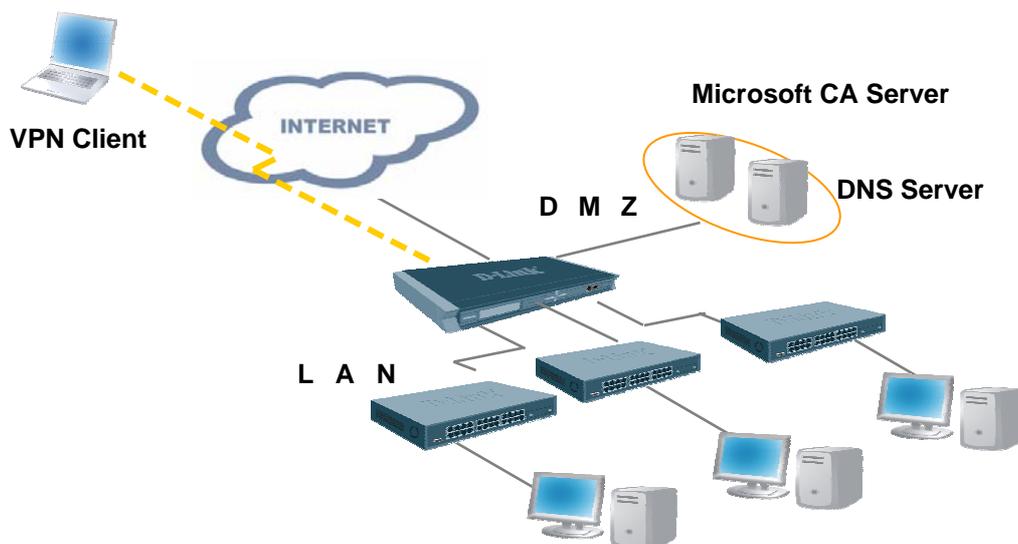
**This HOW TO document applies to :**

Model : DFL-800/1600/2500

Firmware : 2.03 or above

This How To document is intended for providing users a clear guideline to configure DFL series Firewalls with X.509 certification. In this document, we have used Microsoft CA (Certification Authority) to generate client and gateway certificates. Certification Services is a standard component in Windows 2000/2003 server.

Network diagram below provides a concise illustration for the system configuration.



### 1. Microsoft Certification Authority (CA) server

In Windows Server 2003/2000 the CA component is named **Certificates Services** and can be added in section **Add/Remove Programs**. The installation is very straight-forward and won't be explained in this guide.

When you are using a CA server to manage your certificates it is very easy to create and distribute certificates to your clients.

It is also very easy to revoke a client certificate. When a client tries to open up a connection, the firewall will download a revocation list from the CA server and rejects clients with revoked certificates. This is useful if an employee leaves the company as an example.

In this guide we have used Certificate Services in Windows 2003 server.

### ***1.1 Preparing the CA server***

Before you start using the CA server, one setting should be changed on the CA server to simplify creation of certificates:

- Start the program **Administrative Tools\Certification Authority**.
- Right-click on your CA server and select **Properties**.
- Open up the tab **Policy Module** and select **Properties**.
- Select **Follow the settings in the certificate template.....**

This setting will enable the CA server to automatically issue a pending certificate request that is created from the Web page dialogue.

### ***1.2 Save the CA server root certificate***

The CA server root certificate will be imported to the firewall later on:

- Open up the page <http://localhost/certsrv> with Internet Explorer and select **Download a CA certificate.....**
- Select **DER** encoding and **Download CA certificate**. Select a name for your CA root certificate (for example **ca-rootsrv.cer**) and save it on a folder on the server.

### ***1.3 Generate client certificates***

- Open up the page <http://localhost/certsrv> with Internet Explorer.
- Select **Request a certificate, advanced certificate request** and **Create and submit a request to this CA**.
- Enter the certificate information and select **IPsec Certificate**. (see picture below)

Microsoft Certificate Services -- CA-srv

### Advanced Certificate Request

#### Identifying Information:

Name:

E-Mail:

Company:

Department:

City:

State:

Country/Region:

#### Type of Certificate Needed:

#### Key Options:

Create new key set    Use existing key set

CSP:

Key Usage:  Exchange    Signature    Both

Key Size:    Min: 384   Max: 16384   (common key sizes: [512](#) [1024](#) [2048](#) [4096](#) [8192](#) [16384](#))

Automatic key container name    User specified key container name

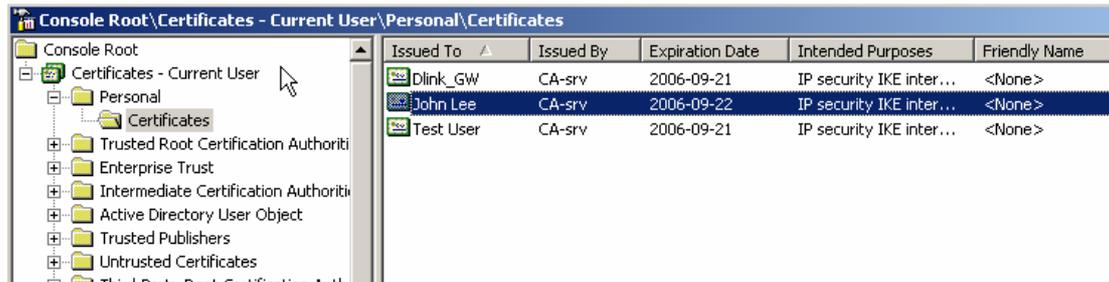
Mark keys as exportable

Export keys to file

- Press **Submit**.
- On the dialogue **This Web site is requesting a new certificate....** select **Yes**.
- Select **Install this certificate** and answer **Yes** on the question if you want to add the certificate.
- Repeat the steps for every client certificate that you want to create.

Now we must export the issued client certificates:

- Select **Start, Run** and type **mmc** and press **Ok**.
- Select **File** and **Add/Remove Snap-in..** followed by **Add**.
- From the list select **Certificates** and **Add**. Select **My User account** and press **Finnish, Close** and **Ok**.
- Expand the section **Certificates\Personal\Certificates**. (See picture below)



- Select the certificate that you want to export, right-click and select **All Task** and **Export**.
- On the **Certificate Export Wizard** select **Next**. Select **Yes, export the private key** followed by **Next**.
- Select **Include all certificates...** and **Delete the private key....** and press **Next**.
- Type in a password. Remember this password because it is needed when importing the certificate on the Windows client.
- Type in a file name (For example **john\_lee.pfx**) and save the certificate in the same folder as we saved the CA root certificate earlier. Press **Next** and **Finish**.

Repeat the steps above for every client certificate.

### 1.4 Generate gateway certificate

- Open up the page <http://localhost/certsrv> with Internet Explorer.
- Select **Request a certificate, advanced certificate request** and **Create and submit a request to this CA.**
- Enter the gateway certificate information and select **IPsec Certificate.** (see picture below)

Microsoft Certificate Services -- CA-srv

#### Advanced Certificate Request

##### Identifying Information:

Name:	Dlink_GW
E-Mail:	gateway@company.com
Company:	Company
Department:	HQ
City:	Taipei
State:	
Country/Region:	TW

##### Type of Certificate Needed:

IPSec Certificate

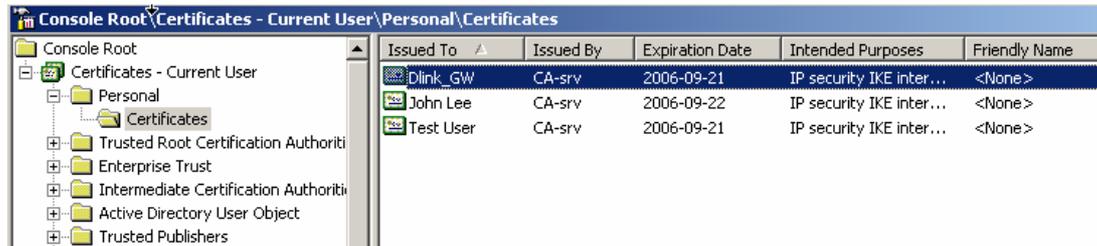
##### Key Options:

Create new key set     Use existing key set  
 CSP: Microsoft Enhanced Cryptographic Provider v1.0  
 Key Usage:  Exchange     Signature     Both  
 Key Size: 1024    Min: 384    Max: 16384    (common key sizes: [512](#) [1024](#) [2048](#) [4096](#) [8192](#) [16384](#))  
 Automatic key container name     User specified key container name  
 Mark keys as exportable  
 Export keys to file

- Press **Submit.**
- On the dialogue **This Web site is requesting a new certificate....** select **Yes.** Select **Install this certificate** and answer **Yes** on the question if you want to add the certificate.
- Repeat the steps for every gateway certificate that you want to create.

Now we must export the issued gateway certificates:

- Select **Start, Run** and type **mmc** and press **Ok**.
- Select **File** and **Add/Remove Snap-in..** followed by **Add**.
- From the list select **Certificates** and **Add**.
- Select **My User account** and press **Finnish, Close** and **Ok**.
- Expand the section **Certificates\Personal\Certificates**. (See picture below)



- Select the gateway certificate that you want to export, right-click and select **All Task** and **Export**.
- On the **Certificate Export Wizard** select **Next**. Select **Yes, export the private key** followed by **Next**.
- Select **Include all certificates...** and **Delete the private key....** and press **Next**.
- Type in a password. Remember this password because it is needed later in section 1.5 when we will extract the certificate and private key from the \*.pfx file.
- Type in a file name (For example **gateway.pfx**) and save the certificate in the same folder as we saved the client certificate earlier. Press **Next** and **Finnish**.

Repeat the steps above for every gateway certificate.

### 1.5 Preparing the gateway certificate for import

The gateway certificate created in previous section (**gateway.pfx**) includes three certificates packed to one file: CA root certificate, personal certificate and private key.

To be able to use the gateway certificate and import it to the firewall we must extract the personal certificate and the private key from the \*.pfx file.

In this example we use **OpenSSL** to extract the files, but this can also be accomplished with other tools.

A very nice tool is **Crypto4** from **Eldos** which will extract these files in fewer steps.

This tool can be downloaded and evaluated from here:

<http://www.eldos.com/c4/>

Download **OpenSSL** and place the file in the same folder as the certificates.

**OpenSSL** can be downloaded from here:

<https://www.zoneedit.com/doc/partner/perl-utils/openssl-win32-binaries/openssl.exe>

First we must convert the pfx certificate to pem format:

- Start a Command Prompt and go to the folder with OpenSSL and your certificates.
- Type **openssl pkcs12 -in gateway.pfx -out gateway.pem -nodes**
- Enter your password from step 1.4 at the prompt and press return.
- You should see the message **MAC verified OK**.
- Exit the command prompt.
- Create two blank documents with the extensions **.cer** and **.key** with **Notepad**. (For example **gateway.cer** and **gateway.key**)
- Start **WordPad** and open the **.pem** file you created earlier.
- Open the blank **.cer** and **.key** files in **Notepad**.
- Locate the section of the file that begins with **-----BEGIN RSA PRIVATE KEY-----** in **WordPad**.
- Copy that line and everything under it up to and including **-----END RSA PRIVATE KEY-----**
- Paste that text into your **.key** file and save it.
- Locate the next section that begins with **-----BEGIN CERTIFICATE-----** in **WordPad**.

- Copy that line and everything under it up to and including -----**END CERTIFICATE**-----.
- Paste that text into your **.cer** file and save it.
- Close **WordPad** and both instances of **Notepad**

Now the personal gateway certificate and the corresponding private key are ready for import to the firewall.

## 2. Configuring the Firewall

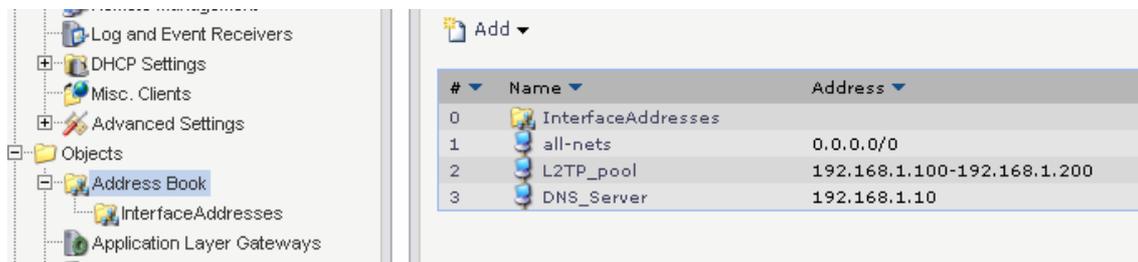
In this guide we assume that you have the firewall up and running and that you have access to the Web configuration interface from the CA Server. Open up the Web configuration interface with Internet Explorer.

### 2.1 Creating needed Objects in Address Book

We must start by creating two objects needed for the configuration: An internal IP pool for the connecting clients and an IP host for our internal DNS server:

- Open **Objects\Address Book** and select **Add** and **IP4 Host/Network**.
- Select a name for the IP pool (for example **L2TP\_pool**) and enter an address range from the internal network that can be issued to the connecting L2TP clients. In our example **192.168.1.100-192.168.1.200**
- Select **Add** and **IP4 Host/Network**.
- Select a name for the internal DNS server (for example **DNS\_Server**) and type in a IP address. In our example **192.168.1.10**

The Object Address book should look like this:



You should also add objects for other DNS and WINS servers that you want to assign to the L2TP clients when they connect and receives an internal DHCP IP address.

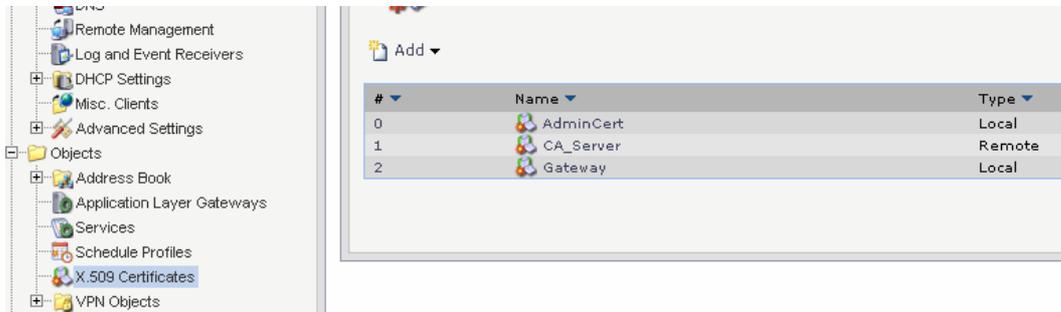
### 2.2 Importing certificates

On the firewall we need to import the CA root certificate and the two gateway certificates created earlier in section 1.2 and 1.5:

- Expand **Objects\X.509 Certificates**. Select **Add** and **X.509 Certificate**
- Type in a name for the CA root certificate (for example **CA\_Server**) and select **Upload a remote Certificate**
- Click on **Browse** and select your CA certificate **ca-rootsrv.cer** and select **Upload X.509 Certificate**.
- Select **Add** and **X.509 Certificate**.

- Type in a name for the gateway certificate (for example **Gateway**) and select **Upload a self-signed X.509 Certificate**
- Click on **Browse** and select your gateway certificate **gateway.cer** and select **Upload self-signed X.509 Certificate**.
- Click on **Browse** and select your gateway private key **gateway.key** and select **Upload X.509 private key**.

You should now have imported a CA server root certificate and a Gateway certificate.  
(See picture below)

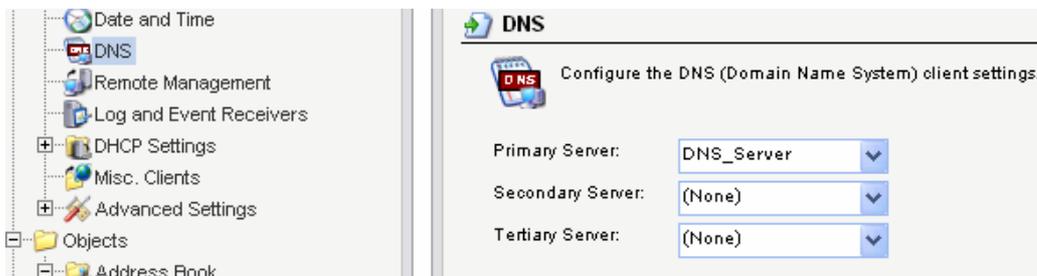


### 2.3 Configure the DNS client

To enable so that the firewall can download the certificate revocation list from the CA server you must specify a DNS server that can resolve the **CRL Distribution point** which contain a URL to the CA server.

This **CRL Distribution point** can be found in the gateway certificate. The DNS server specified must be able to resolve the machine name of the CA server:

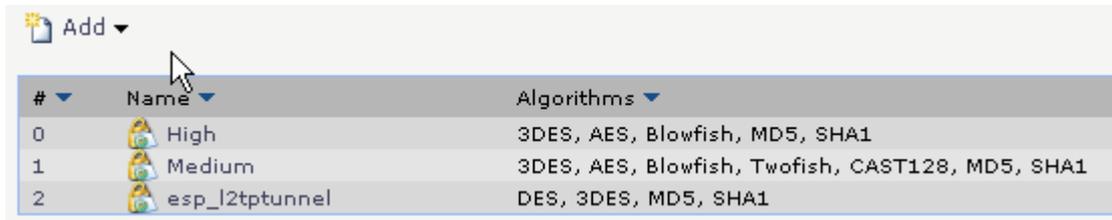
- Open up **System\DNS** and as **Primary Server** select the object created in 2.1 **DNS\_Server**



## 2.4 Create a custom IPsec Algorithm

Microsoft L2TP/IPSec implementation uses slightly different settings for the IPsec proposal so we must create a custom proposal that matches Microsoft clients:

- Expand **Objects\VPN Objects\IPsec Algorithms**.
- Select **Add** and **IPsec Algorithms**.
- Select a name (for example **esp\_l2tptunnel**) and enable **DES** and **3DES**. Keep **128** for **Key Size** and enable **MD5** and **SHA1** as **Integrity Algorithm**
- Press OK. The proposal should look like the picture below



#	Name	Algorithms
0	High	3DES, AES, Blowfish, MD5, SHA1
1	Medium	3DES, AES, Blowfish, Twofish, CAST128, MD5, SHA1
2	esp_l2tptunnel	DES, 3DES, MD5, SHA1

## 2.5 Create an IPsec tunnel

The next step is to create the IPsec interface that the clients will use to encrypt the traffic:

- Go to **Interfaces\IPsec tunnels**. Select **Add** and **IPsec tunnel**.
- In section **General** Select a name for the tunnel, in our example **l2tp\_tunnel**.
- As **Local Network** select the IP address of the external interface that clients connect to from the Internet. In our example **wan1\_ip**
- Both **Remote Network** and **Remote Endpoint** is **All-Nets** since we, in our example, allow L2TP connections from the whole Internet.
- Select **Transport** as **Encapsulation Mode**
- As **IKE Algorithm** select **Medium** and **28800** seconds.
- As **IPsec Algorithm** select the one we just created **esp\_l2tptunnel** and **3600** seconds with **250000** kilobytes in lifetime.

Name:

Local Network:

Remote Network:

Remote Endpoint:

Encapsulation Mode:

**Algorithms**

IKE Algorithms:

IKE Life Time:  seconds

IPsec Algorithms:

IPsec Life Time:  seconds

IPsec Life Time:  kilobytes

- Go to the tab **Authentication** and enable **X.509 Certificate**.
- As **Root Certificate** select our **CA\_Server** certificate. As Gateway **Certificate** select our **Gateway** certificate.

**Authentication**

X.509 Certificate

Root Certificate(s):

Available	Selected
AdminCert Gateway	CA_Server

Gateway Certificate:

Identification List:

- Select the tab **Routing** and enable **Allow DHCP over IPsec....** and **Dynamically add route....**
- Leave all the rest options unchanged and press OK.

#	Name	LocalNetwork	RemoteNetwork	RemoteEndpoint	AuthMethod
0	l2tp_tunnel	wan1_ip	all-nets	all-nets	Certificate

### 2.6 Create a L2TP server

- In section **Interfaces** and **L2TP/PPTP Servers** select **Add** and **L2TP/PPTP Servers**.
- Enter a name for the L2TP server, in our example **l2tp\_server**. As **Inner IP Address** select the IP address of the internal interface. In our example **lan\_ip**.
- **Tunnel Protocol** is **L2TP** and **Outer interface filter** is our IPsec tunnel **l2tp\_tunnel**. Select **wan1\_ip** as **Server IP**

**General**

A PPTP/L2TP server interface terminates PPP (Poi

Name:

Inner IP Address:

Tunnel Protocol:

Outer Interface Filter:

Server IP:

- In section **PPP Parameters** leave all options in **General** and **Microsoft Point-to-point....** Enabled.
- In section **IP Pool** select our created object **L2TP\_Pool** and select any other objects you have created in section **DNS** and **NBNS**. See section 2.1

**IP Pool**

IP Pool:

DNS: Primary  Secondary

NBNS:

- Don't change anything in section **Add Route**. Press **OK**.

Add ▾

#	Name	TunnelProtocol	IP	Interface	IPPool	UseUserAuth
0	l2tp_server	L2TP	lan_ip	l2tp_tunnel	L2TP_pool	Yes

## 2.7 Create a User Database

We must create a local user database that will authenticate the user. This logon information is inserted in the Microsoft L2TP/IPsec client.

You can also authenticate with your local Active Directory username and password. To accomplish this you must set-up a Radius connection from the Firewall to the Microsoft IAS (Internet Authentication Service).

This method is not described in this document.

- Go to **User Authentication\Local User Databases** and select **Add** and **LocalUserDatabase**.
- Select a name for the User database, in our example L2TP\_Users.
- Add all the users that will connect with L2TP with **Add\User**. Enter username and password. Leave the other options unchanged.



### 2.8 Create a user authentication rule

Now we must specify how the users will authenticate against the L2TP server:

- Go to **User Authentication\User Authentication Rules** and select **Add** and **User Authentication Rule**.
- In tab **General** select a name for the authentication rule, in our example **I2tp\_auth**.
- As **Agent** select **PPP** and **Authentication source** is **Local**. **Interface** is our L2TP server **I2tp\_server**.
- **Originator IP** is **All-Nets** and **Terminator IP** is our external IP address **wan1\_ip**.



- In the tab **Authentication Options** select **L2TP\_Users** as **Local User DB**. Leave all the other options unchanged.



## 2.9 Create IP rules for L2TP clients

The final configuration task is to create IP rules that determine what the connected L2TP clients are allowed to do.

- Open **Rules** and **IP Rules**. We will create a dedicated IP Rule Folder for L2TP connections. Select **Add** and **IP Rule Folder**.
- Select a name for the folder, in our example **I2tp**.

We must first create a incoming rule that defines what the clients are allowed to do on our internal network, and then we define a outgoing rule that allows them to access the internet through the L2TP tunnel.

- Select **Add** and **IP Rule**. Select a name for your rule, in our example **incoming\_I2tp**. **Action** is **Allow** and in our example **Service** is **all\_services**.
- Source interface is **I2tp\_server** and source network is **I2tp\_pool**.
- Destination interface is **any** and destination network is **lannet**.
- Press **OK**.
- Select **Add** and **IP Rule**. Select a name for your rule, in our example **outgoing\_I2tp**. **Action** is **NAT** and in our example **Service** is **all\_services**.
- Source interface is **I2tp\_server** and source network is **I2tp\_pool**.
- Destination interface is **wan1** and destination network is **all-nets**.
- Press **OK**.



#	Name	Action	SourceInterface	SourceNetwork	DestinationInterface	DestinationNetwork	Service
0	Incoming_I2tp	Allow	I2tp_server	L2TP_pool	any	lannet	all_services
1	Outgoing_I2tp	NAT	I2tp_server	L2TP_pool	wan1	all-nets	all_services

Save and activate the firewall configuration and you are all done configuring the firewall to accept L2TP/IPsec connections.

### 3. Configure the Windows client

In this example we will configure the L2TP connection manually, but in Windows 2003 server Microsoft has released a module called **Connection Manager Administration Kit**.

With this included software you can create a setup file which configures all L2TP/IPsec settings on the client automatically when executed.

More information can be found here:

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/be5c1c37-109e-49bc-943e-6595832d5761.mspx>

Distribution of the client certificates can be done with e-mail, but the import password should be distributed to the end user with either SMS, phone or equivalent.

One problem when importing the client certificate is that if the user only double click on the certificate and use the import wizard the connection won't work.

That is because the certificates gets imported to the **Current User**-store and not to the **Local Computer**-store which is needed for the L2TP/IPsec connection to work.

To use the Microsoft import wizard correctly the end user must open up the **Local Computer**-store with the MMC console and start the import wizard manually.

For some end users this can be difficult.

In this example we have used a free tool that handles this automatically. It can be downloaded from here:

<ftp://ftp.openswan.org/openswan/windows/certimport/>

Here is also a little bat-file that can be used together with the above program **certimport.exe**. The batch file prompts the user for certificate name and password:

Example of **setup.bat**:

-----

```
echo off
```

```
cls
```

```
set /p cert=Please enter the name of your personal certificate with extension:
```

```
set /p pwd=Please enter your certificate import password:
```

```
certimport -p %pwd% %cert%
```

pause

-----

### ***3.1 Import client certificate***

- Distribute the certificate to the end user together with the bat-file and the program **certimport.exe**.
- Tell the user to save all files in the same folder and execute the bat-file.
- The user enters his personal certificate name and the import password.

### 3.2 Create a L2TP/IPSec connection

If you have not prepared a customized setup file with **Connection Manager Administration kit**, the L2TP/IPsec connection must be configured manually:

- Select **Start, Settings and Network Connections**
- Select **Create a new connection and Next**. Select **Connect to the network at my workplace**. Select **Next**
- Select **Virtual Private Network Connection and Next**. Type in a name for the connection. (For example **Company VPN**). Select **Next**.
- Enter the external IP address of the firewall or the registered DNS name (for example **vpn\_gw.company.com**). Press **Next**
- Select **My Use only** and **Next**. Press **Finnish**.
- Select **Properties** for the connection. In the tab **Networking** and in **Type of VPN** select **L2TP IPsec VPN** and press **OK**.
- Enter username and password and select **connect**. This is the information created earlier in the local user database on the firewall.



## 4. Troubleshooting

This is a list of some of the things that should be checked:

- Make sure that the IPsec service running on the client.
- Uninstall any other VPN software on the client
- Make sure that a valid DNS server is specified in the firewall that can resolve the CRL distribution path to the CA server
- Check the IIS log files on the CA server to see if the firewall has downloaded the revocation list.
- Make sure that the client or gateway certificate is valid and not revoked on the CA server.
- Make sure that correct certificate is selected as Gateway and CA root in the IPsec tunnel configuration
- Check the username and password.
- Check that a valid IP pool is used for the client.
- Go through the Firewall configuration section in this document once again.