Configuration examples for the D-Link NetDefend Firewall series

Scenario: How to create CA (Certification Authority) and import into firewall

Platform Compatibility: All NetDefend Firewall Series

Last update: 2008-03-12

Overview

In this document, the notation *Objects->Address book* means that in the tree on the left side of the screen **Objects** first should be clicked (expanded) and then **Address Book**.

Most of the examples in this document are adapted for the DFL-800. The same settings can easily be used for all other models in the series. The only difference is the names of the interfaces. Since the DFL-1600 and DFL-2500 has more than one lan interface, the lan interfaces are named lan1, lan2 and lan3 not just lan.

The screenshots in this document is from firmware version 2.11.02. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see on your browser.

To prevent existing settings to interfere with the settings in these guides, reset the firewall to factory defaults before starting.

How to create CA (Certification Authority) and import into firewall

In this guide we have used Microsoft CA (Certification Authority) to generate client and gateway certificates. Certification Services is a standard component in Windows 2000/2003 server.

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.

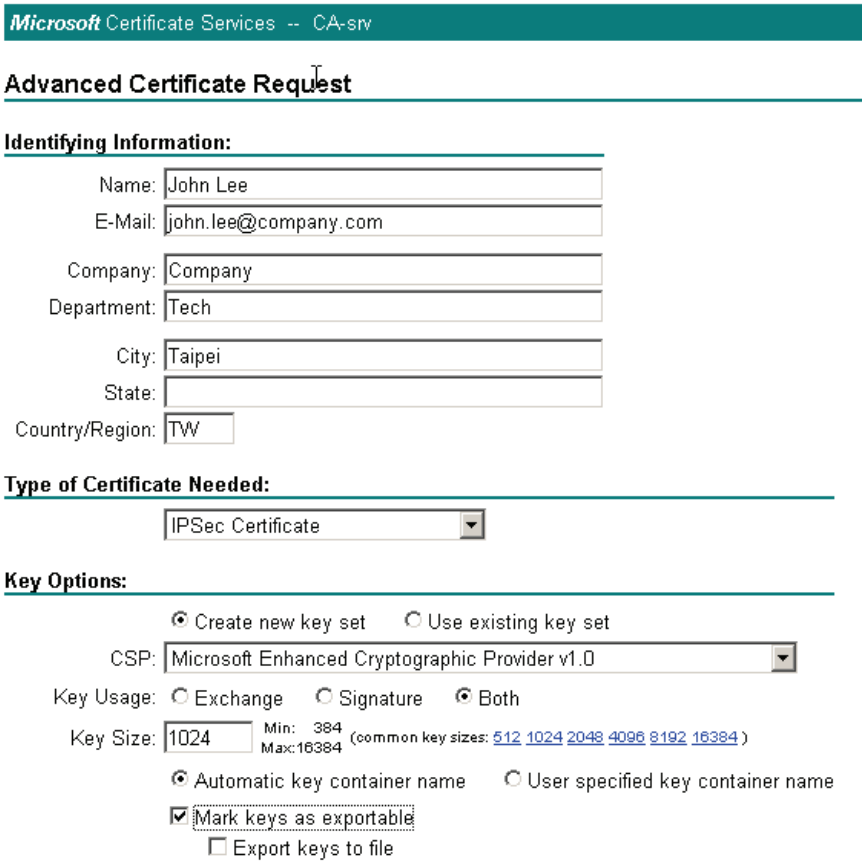
1.2 Save the CA server root certificate

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

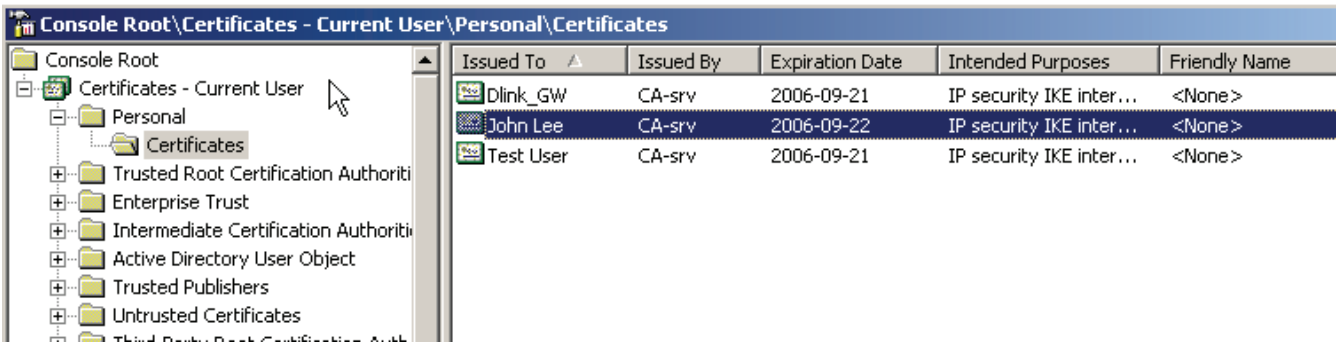
- Open up the page **http://localhost/certsrv** with Internet Explorer.
- Select **Request a certificate**, **advanced certificate request** and **Create and submit a request to this CA**.
- Enter the certificate information and select **IPsec Certificate**. (see picture below)



- 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

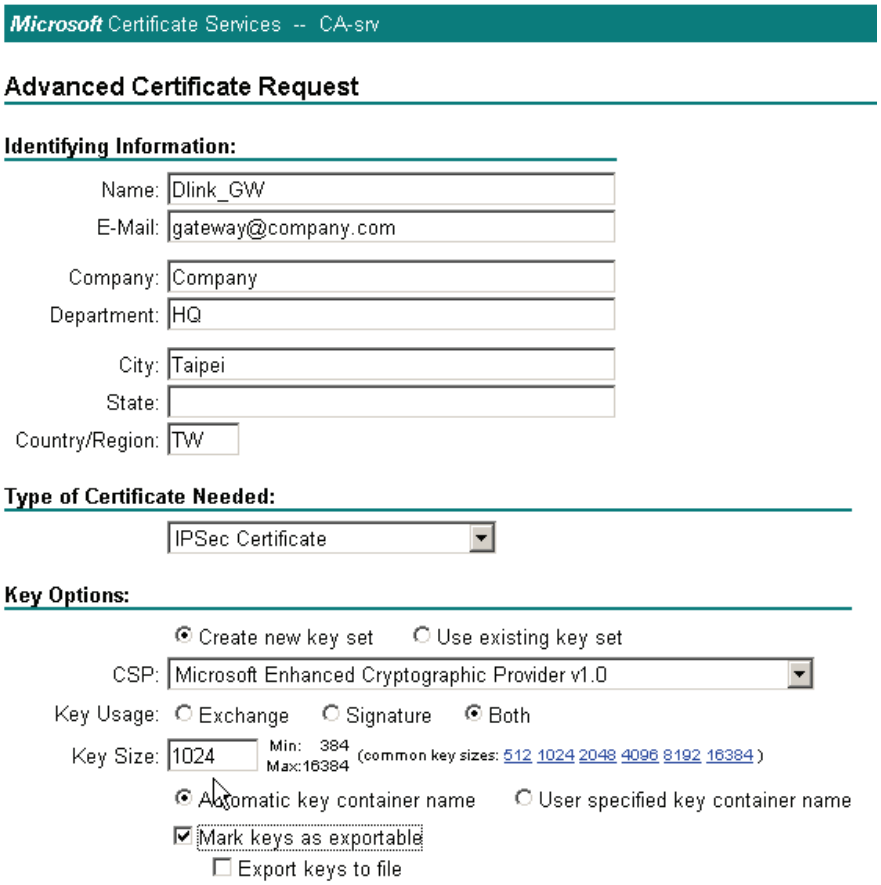
Export.

- 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 **Finnish**.

Repeat the steps above for every client certificate.

1.4 Generate gateway certificate

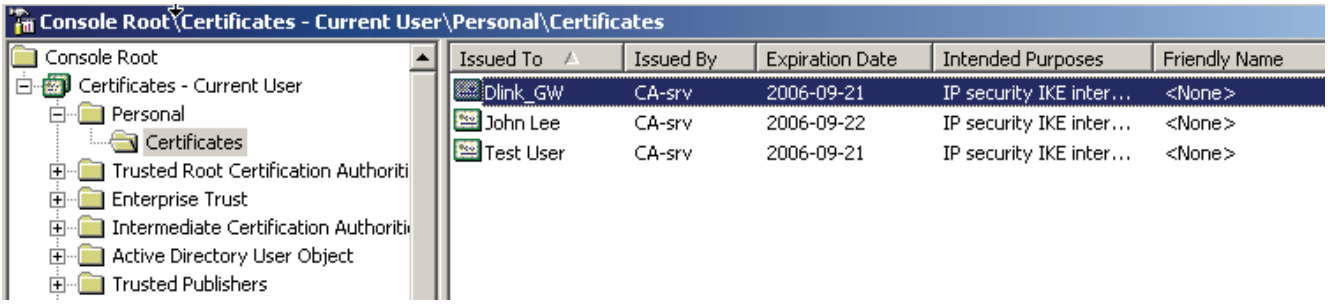
- Open up the page **http://localhost/certsrv** with Internet Explorer.
- Select **Request a certificate**, **advanced certificate request** and **Create and submit a request to this CA**.
- Enter the gateway certificate information and select **IPsec Certificate**. (see picture below)



- 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

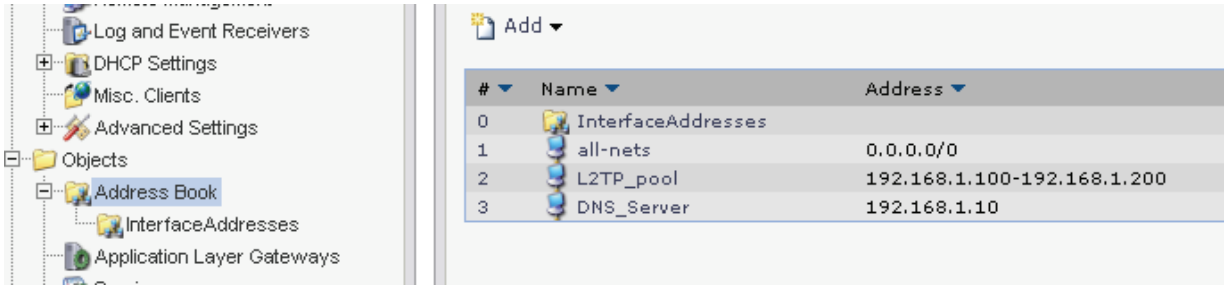
In this guide we assume that you have the firewall up and running and that you have access to the Web configuration interface from the CA Server. Open up the Web configuration interface with Internet Explorer.

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:

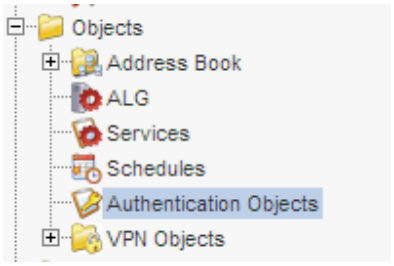


You should also add objects for other DNS and WINS servers that you want to assign to the L2TP clients when they connect and receives an internal DHCP IP address.

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\Authentication Objects**. Select **Add** and **Certificate**

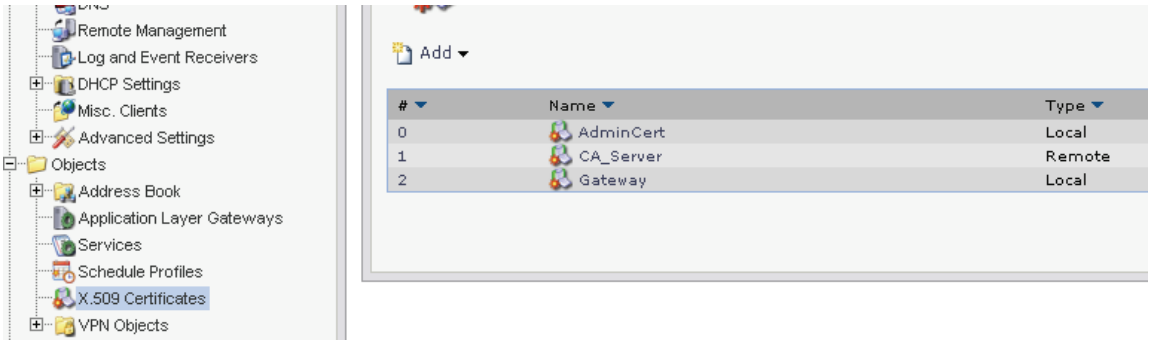


- Type in a name for the CA root certificate (for example **CA_Server**) and select **Upload a remote Certificate**

Click **OK**

- 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 X.509 Certificate**
- Click on **Browse** and select your gateway certificate **gateway.cer** and select **Upload 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)



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.