Using certificates as authentication method for box to box VPN connection.

This document describes how to use certificates as an authentication method when establishing a VPN box to box connection. The devices used in this example are 2 ProSafe VPN Firewalls, model FVS338.

1. Certificate Authorities
When you do not want to use any external Certificate Authority (CA), for example http://www.rapidssl.com, you need to create your own CA using any of the methods below:

- OpenSSL: http://www.openssl.org
- SimpleCA: http://www.vpnc.org/SimpleCA
- Microsoft IIS

For the purpose of this document, OpenSSL will be used. This can be downloaded via the following link http://www.slproweb.com/products/Win32OpenSSL.html

Additionally, a Perl interpreter needs to be installed, for example ActivePerl which can be downloaded via the following link http://www.activestate.com/Products/activeperl/index.mhtml

2. Creating a CA with OpenSSL
First create your own CA following the instructions available at the following link http://sandbox.rulemaker.net/ngps/m2/howto.ca.html

**Note 1:** NETGEAR does not support ST relative distinguished (state/province) name so please edit the openssl.cnf file (in the original location and in your new CA folder) to avoid using this parameter.

**Note 2:** From the CA guide above, only the steps up to number 4 need to be followed.

3. Generate Self Certificate Request for Router 1
On the first FVS338 (Router1), go to VPN -> Certificates and generate the self certificate request for this router as below.
4. Generate Self Certificate Request for Router 2
On the second FVS338 (router2), go to VPN -> Certificates and generate the self certificate request for this router as below.

- Set Name to **first**
- Set Subject to **CN=router2**
- Set Hash Algorithm to **MD5**
- Set Signature Algorithm to **RSA**
- Set Signature Key Length to **1024**
- Press Generate

- After pressing Generate, the Self Certificate Request will appear.
- Press View.

- After pressing View, the Certificate Request Data will appear.
- Copy all the text appearing in the field marked ⬇ and paste into a text file called `router1.csr`
Using certificates as authentication method for box to box VPN connection

Version 1.0

5. Signing the certificates
The next step is to sign both certificates using the new CA that was created in Step 2 above. This is done for both certificates using the syntax below:

```bash
openssl x509 -req -days 365 -in router1.csr -CA cacert.crt -CAkey cakey.pem -CAcreateserial -out router1.crt

openssl x509 -req -days 365 -in router2.csr -CA cacert.crt -CAkey cakey.pem -CAcreateserial -out router2.crt
```

where:

- `router1.csr`, `router2.csr` – generated self certificate requests (for Router 1 and Router 2 accordingly)
- `cacert.crt` – CA certification
- `cakey.pem` – CA keys
- `router1.crt`, `router2.crt` – signed certificates (for Router 1 and Router accordingly)

6. Loading the certificates into the devices
The CA certificate will need to be loaded on to both devices. This is done by going to VPN -> Certificates on each device.

- Browse to `cacert.crt` and upload it.

- Once uploaded it will appear as shown.

The next step is to upload the signed certificate for Router 1 as follows.

- Browse to `router1.crt` and upload it.
Using certificates as authentication method for box to box VPN connection

Version 1.0

Once uploaded it will appear as shown.

Next, the signed certificate for Router 2 needs to be uploaded as follows.

• Browse to router2.crt and upload it.

• Once uploaded it will appear as shown.

Finally for this step, reboot both devices.

7. Creating the VPN tunnel between the 2 devices
Run the VPN Wizard on both devices entering the relevant details (connection name, pre-shared key, remote WAN IP address, remote LAN IP address and subnet mask). This will create a VPN policy and IKE policy on each device. Edit the IKE policy on each device as follows.

Router 1:

1. Set the Local Identifier Type to DER ASN1 DN
2. Set the Local Identifier to CN=router1
3. Set the Remote Identifier Type to DER ASN1 DN
4. Set the Remote Identifier to CN=router2
5. Set Authentication Method to RSA-Signature

Finally, apply these changes.
Router 2:

1. Set the Local Identifier Type to **DER ASN1 DN**
2. Set the Local Identifier to **CN=router2**
3. Set the Remote Identifier Type to **DER ASN1 DN**
4. Set the Remote Identifier to **CN=router1**
5. Set Authentication Method to **RSA-Signature**

Finally, apply these changes.

Once these changes have been made, the VPN tunnel will establish between both units.