



INSTALLATION SSL CERTIFICATE CISCO IOS VPN

Transferring the PKCS#12 packages

In this section, we describe how to transfer the previously generated packages to the Cisco IOS VPN router and the VPN clients.

We used some very basic means to transfer the packages, and an enrollment process using SCEP (Simple Certificate Enrollment Protocol) should be preferred to the process described here.

Free products like OpenCA or IDX-PKI may help you if you want to setup an SCEP capable CA.

To the Cisco IOS VPN router

The transfer is processed through TFTP (any file transfer protocol can be used though, just check the capability of the router).

Configuring a 'trustpoint' on the router

```
router>enable
router#conf t
router(config)#crypto ca trustpoint vpn-tp
router(ca-trustpoint)#usage ike
router(ca-trustpoint)#revocation-check none
router(ca-trustpoint)#^Z
```

Note : we set up a minimal CA, hence no CDP (CRL Distribution Point) is available for our router

Downloading the PKCS#12 package

```
router#copy tftp://10.0.0.1/vpn-server.p12 flash:
```

Note : the vpn-server.p12 file must be copied to the main TFTP directory.

Importing the PKCS#12 package

```
router(config)#crypto ca import vpn-tp pkcs12 flash:vpn-
server.p12 passphrase
```

Note : the passphrase is the one that protects the PKCS#12 vpn-server.p12 file

At this point, the router has its own signed certificate, its private key, and the certificate of the CA.

To the VPN clients

Windows

Just make the client-intranet-access.p12 file accessible through the Windows Explorer, and import it using the Cisco VPN client certificate importation utility (available in the client itself). You will be asked for the passphrase that protects the PKCS#12 file, and you will also be asked to enter a new password to protect the imported private key.



Remember this password, as it will be asked each time you want to connect using the certificate, or even when you want to delete the certificate from the client