

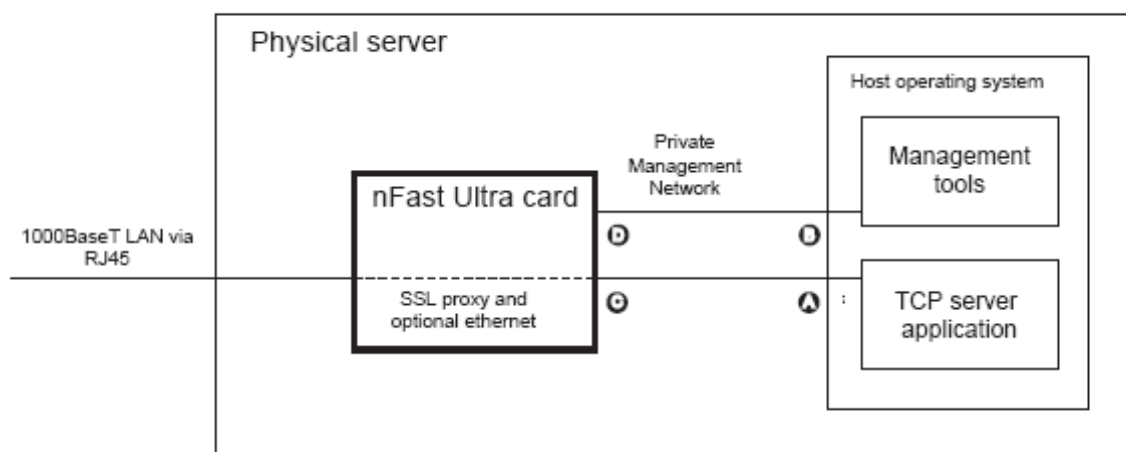
## nFast Ultra PCI 簡易安裝及設定

將 nCipher 光碟放入光碟機中開始安裝 nFast Ultra 的驅動程式及 management console，並重新開機

nFast Ultra 上有二個 MAC address，其 MAC 前三位數是 00-07-AE，將具有較高數值的 MAC 設定其 IP 為 10.100.0.1，subnet 為 255.255.255.0。將另一組 MAC 設定為 Server 的 IP

nFast Ultra 就如同 SSL Proxy，所有從 client 端來的 SSL 加密封包都在 nFast Ultra 上解密，再以明碼的形式，送到 Web Server 上。

其概念如下：



A: Host Server Interface (Server IP)

B: Host Management Interface (10.100.0.1)

C: TCP output of an SSL proxy

D: nFast Ultra management Interface (10.100.0.8)

其中，D 的 IP:10.100.0.8 是出廠預設值，是 B 用來與 nFast Ultra 作管理設定的連線之用。

請在 nfast\bin\的目錄下下 nfultra 的指令，以進入管理介面。

一開始請設定密碼，本密碼是用來保密金鑰、憑證及 proxy 的設定。

有關金鑰和憑證的產生、匯入，請詳閱 Administrator Guide，Working with Keys and

Certificates。若已有密碼，請輸入 123456，您可以在 Global Settings 裡變更此密碼。

**【範例】**

假設有一網站網址為 w.x.y.z，欲使用 nFast Ultra 來處理有關 SSL 的加解密，並仍保持一般的非 SSL 連線，則設定如下：

在Global Settings裡將Pass-through mode啓動，若將Pass-through mode disable，則除了SSL外，其他的TCP protocol將無法通過nFast Ultra。

Proxy Setting:

Server: w.x.y.z:81

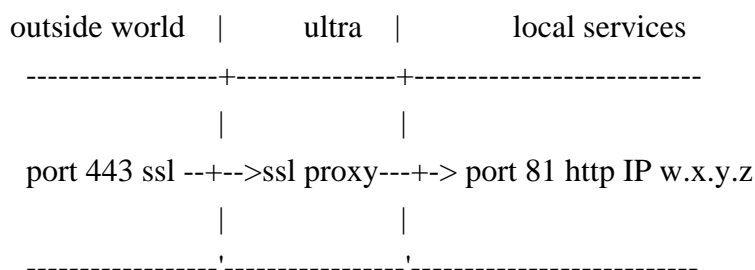
Client: 443

Protocol: SSL only

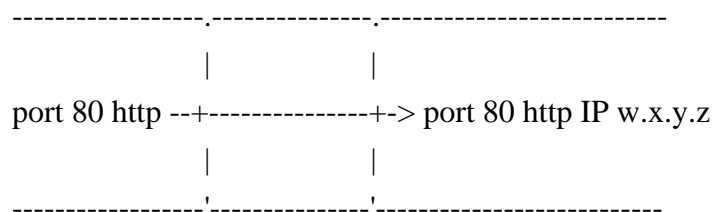
SSL resumption: No

以下是有關這個設定的簡單圖示

https protocol



http protocol



另外，Web Server 需設定為 listen 81 及 80 port。

## 【暨有之 SSL 伺服器憑證之匯入】

注意：必須將憑證檔案轉成 PEM 格式後，方能讓 nFast Ultra 的工具將之匯入，欲將非 PEM 格式之憑證檔案轉成 PEM 格式，須用 openssl 方可。

Openssl可於<http://www.openssl.org/>下載。

當憑證從 Web Server 匯出時，會要求一個 password 來保護匯出的憑證檔，最好是不要輸入任何 password，在轉成 PEM 檔時就不用輸入 password 可以直接按 Enter 鍵。

### Step 1:

憑證檔案為 PFX 格式，執行下列命令：

```
-----  
openssl pkcs12 -nocerts -nodes -in certname.pfx -out privatekey.pem  
-----
```

其中，certname.pfx 是 Windows 匯出的 PKCS#12 格式的憑證檔，privatekey.pem 則是轉成的 PEM 格式之私鑰檔

例如：

有一匯出之 PFX 憑證檔案，檔名為 iis.pfx

```
openssl pkcs12 -nocerts -nodes -in c:\tmp\iis.pfx -out c:\tmp\testpk1.pem
```

```
-----  
openssl pkcs12 -nokeys -clcerts -chain -in certname.pfx -out  
certname.pem  
-----
```

其中，certname.pfx 是 Windows 匯出的 PKCS#12 格式的憑證檔，certname.pem 則是欲轉成的 PEM 格式之憑證檔

例如：

有一匯出之 PFX 憑證檔案，檔名為 iis.pfx

```
openssl pkcs12 -nokeys -clcerts -chain -in c:\tmp\iis.pfx -out c:\tmp\testcert1.pem
```

```
-----  
openssl pkcs12 -nokeys -cacerts -chain -in certname.pfx -out  
ca_certname.pem  
-----
```

其中，certname.pfx 是 Windows 匯出的 PKCS#12 格式的憑證檔，ca\_certname.pem 則是欲轉成的 PEM 格式之簽發憑證 CA 之憑證檔

例如：

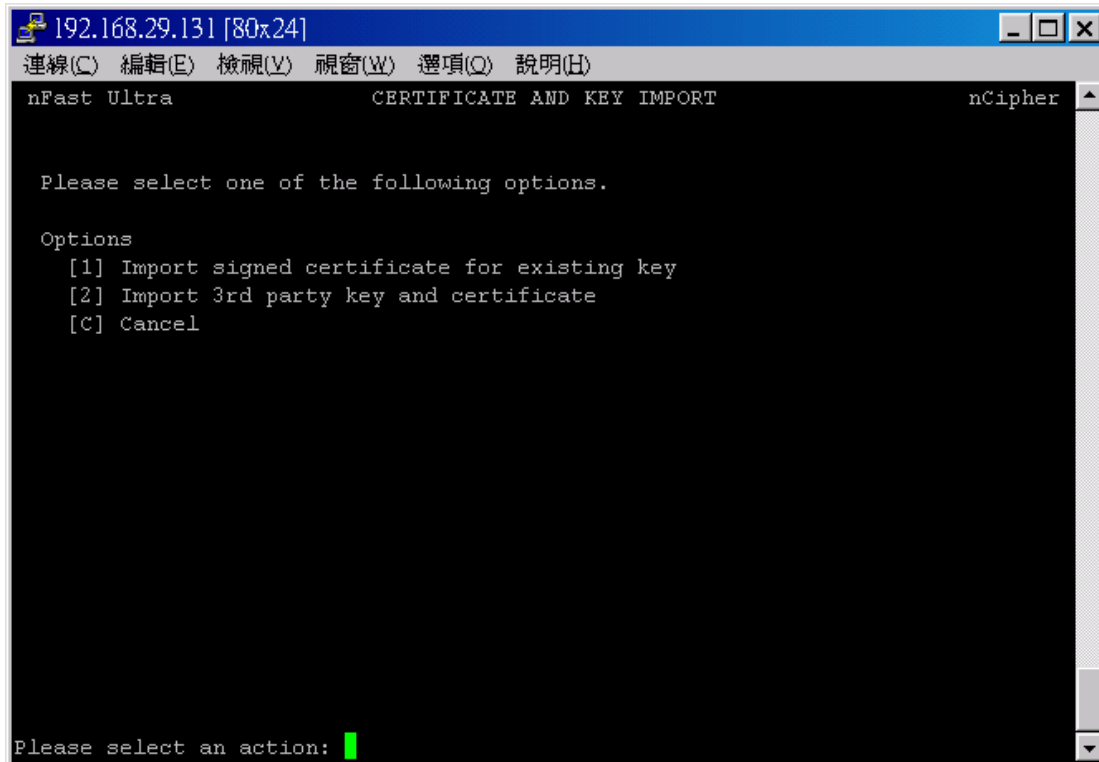
有一匯出之 PFX 憑證檔案，檔名為 iis.pfx

```
openssl pkcs12 -nokeys -cacerts -chain -in c:\tmp\iis.pfx -out c:\tmp\versign_cert.pem
```

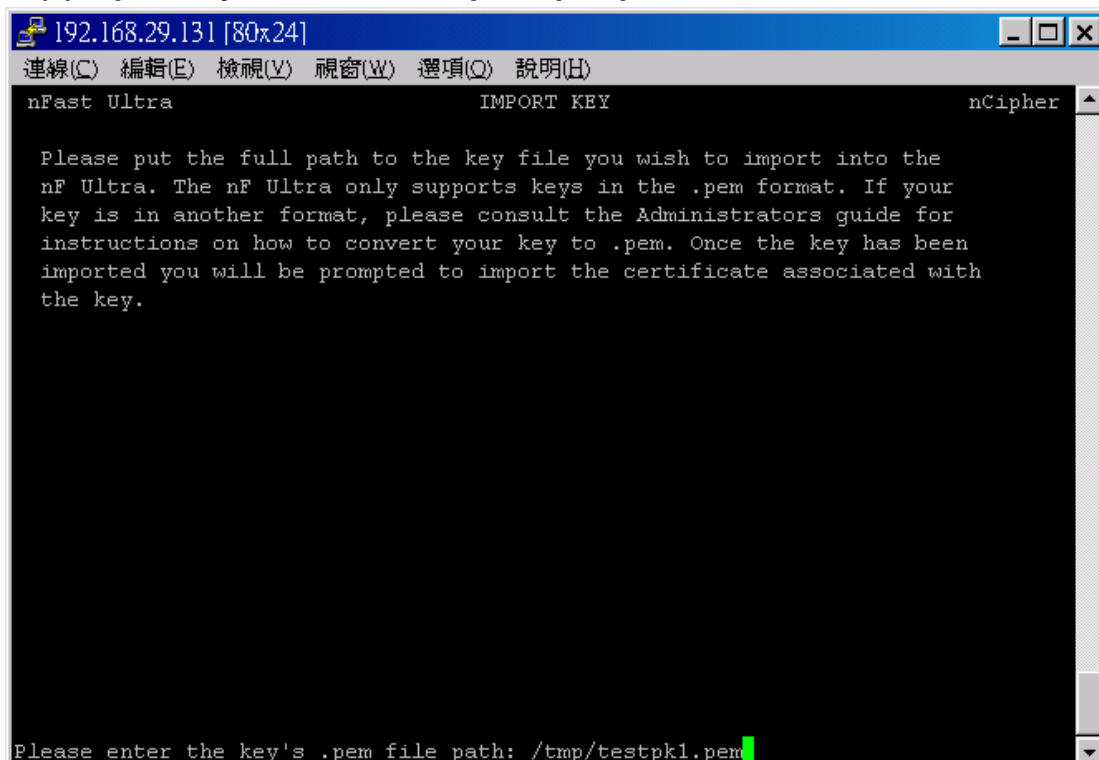
## Step 2:

進入 nFast Ultra Console 來匯入 privatekey.pem 及 certname.pem

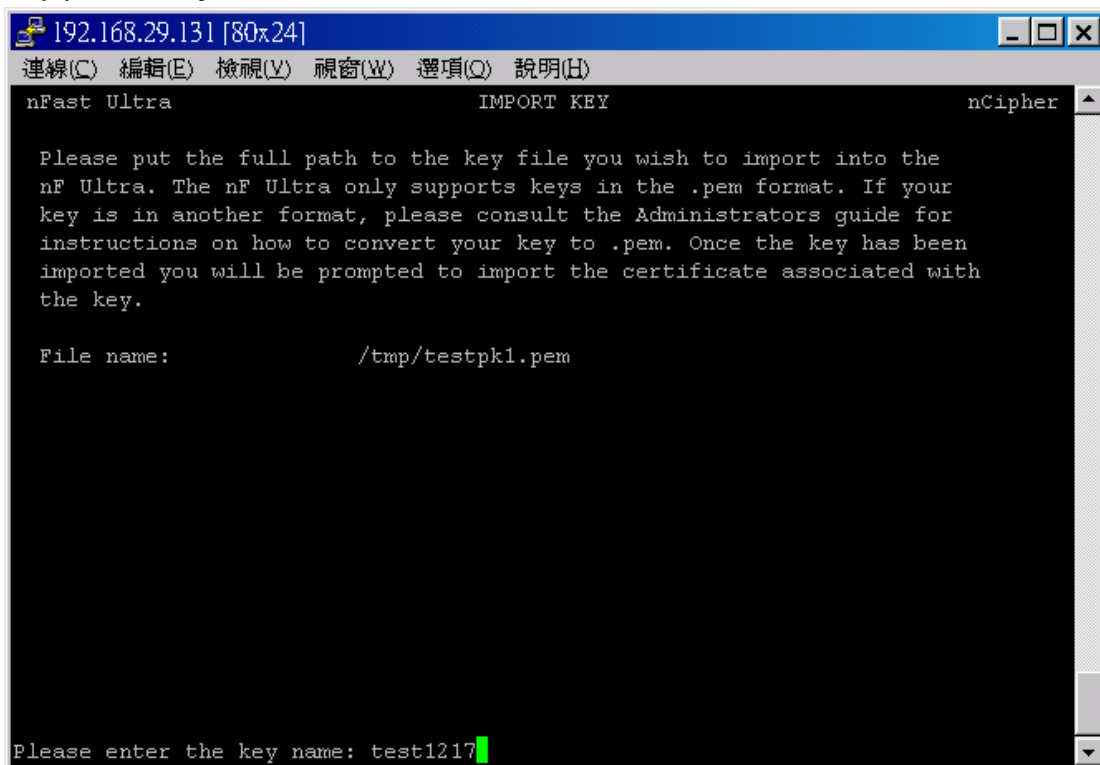
### (1)choice Import 3<sup>rd</sup> party key and certificate



### (2)import key ,first ,enter /tmp/testpk1.pem



(3)enter key name : **test1217**



A terminal window titled "192.168.29.131 [80x24]" with a menu bar containing "連線(C)", "編輯(E)", "檢視(V)", "視窗(W)", "選項(O)", and "說明(H)". The window content shows the "nFast Ultra" application in "IMPORT KEY" mode. It displays instructions for importing a key file in .pem format. The "File name:" field is populated with "/tmp/testpk1.pem". At the bottom, a prompt asks for the key name, with "test1217" entered and a green cursor at the end.

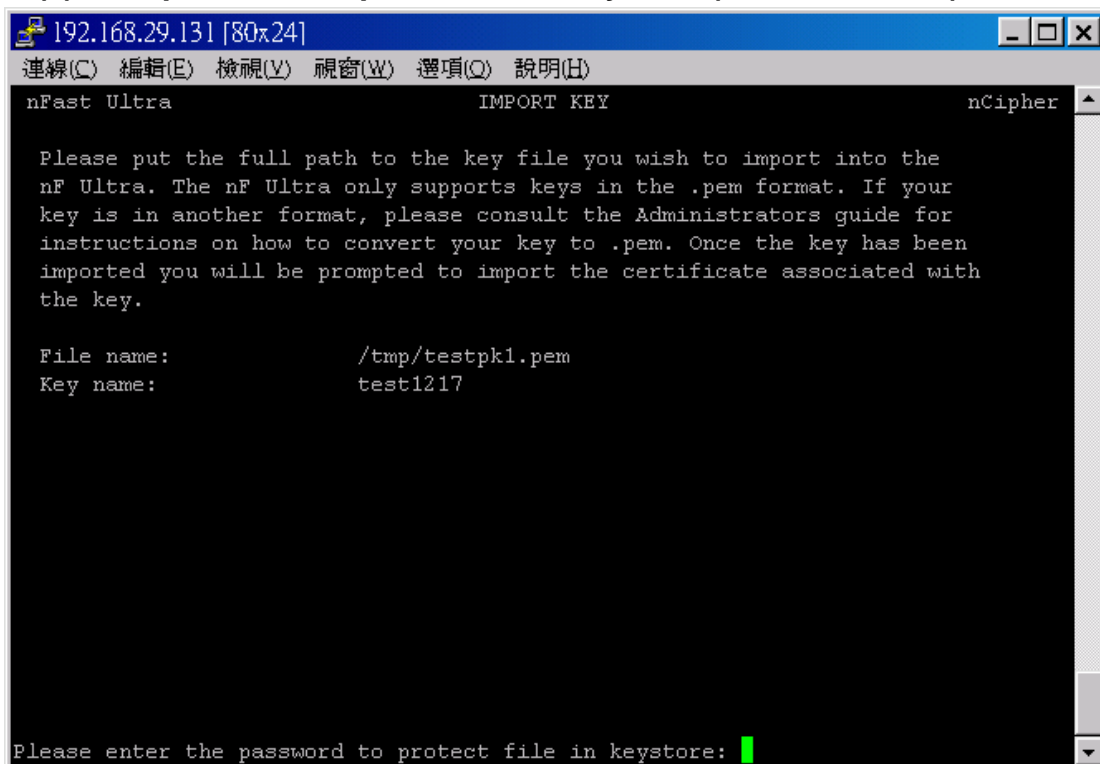
```
192.168.29.131 [80x24]
連線(C) 編輯(E) 檢視(V) 視窗(W) 選項(O) 說明(H)
nFast Ultra                                IMPORT KEY                                nCipher ▲

Please put the full path to the key file you wish to import into the
nF Ultra. The nF Ultra only supports keys in the .pem format. If your
key is in another format, please consult the Administrators guide for
instructions on how to convert your key to .pem. Once the key has been
imported you will be prompted to import the certificate associated with
the key.

File name:                                /tmp/testpk1.pem

Please enter the key name: test1217█
```

(4)enter password to protect file in keystore (enter **12345678**)



A terminal window titled "192.168.29.131 [80x24]" with a menu bar containing "連線(C)", "編輯(E)", "檢視(V)", "視窗(W)", "選項(O)", and "說明(H)". The window content shows the "nFast Ultra" application in "IMPORT KEY" mode. It displays instructions for importing a key file in .pem format. The "File name:" field is populated with "/tmp/testpk1.pem" and the "Key name:" field is populated with "test1217". At the bottom, a prompt asks for the password to protect the file in the keystore, with a green cursor at the end.

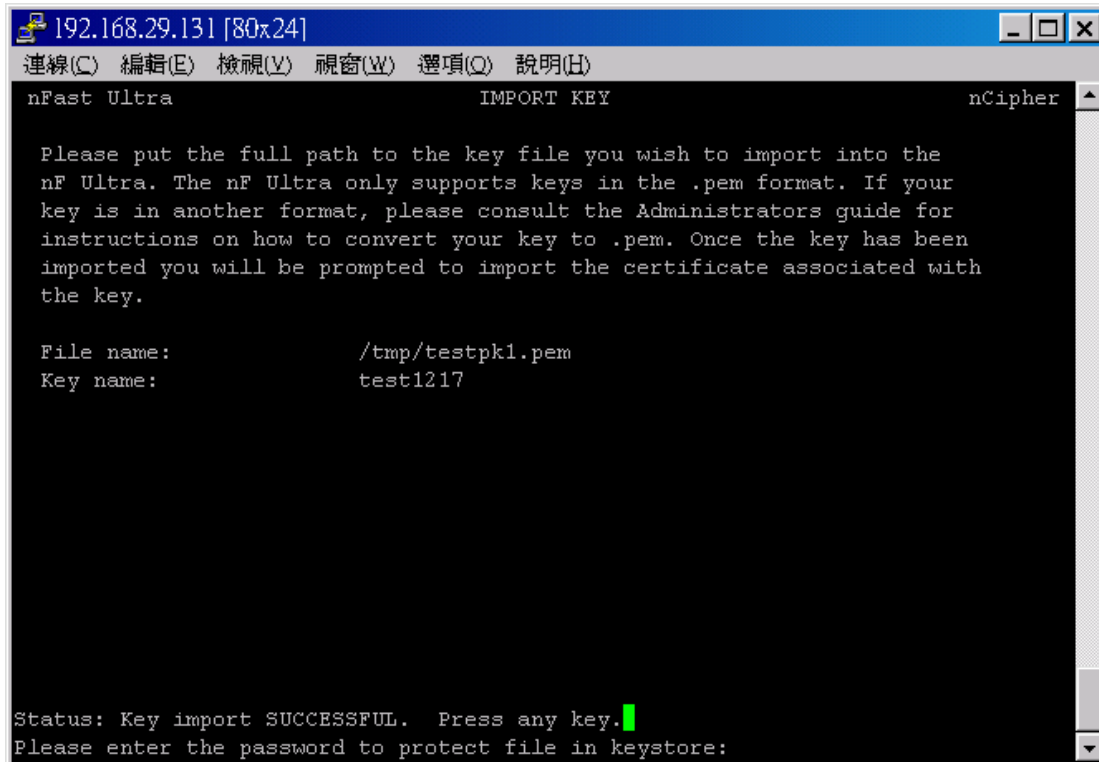
```
192.168.29.131 [80x24]
連線(C) 編輯(E) 檢視(V) 視窗(W) 選項(O) 說明(H)
nFast Ultra                                IMPORT KEY                                nCipher ▲

Please put the full path to the key file you wish to import into the
nF Ultra. The nF Ultra only supports keys in the .pem format. If your
key is in another format, please consult the Administrators guide for
instructions on how to convert your key to .pem. Once the key has been
imported you will be prompted to import the certificate associated with
the key.

File name:                                /tmp/testpk1.pem
Key name:                                  test1217

Please enter the password to protect file in keystore: █
```

## (5)import key successfully



A terminal window titled "192.168.29.131 [80x24]" with a menu bar containing "連線(C)", "編輯(E)", "檢視(V)", "視窗(W)", "選項(O)", and "說明(H)". The window title bar also includes "nFast Ultra" on the left and "nCipher" on the right. The main content area displays the following text:

```
nFast Ultra                                IMPORT KEY                                nCipher

Please put the full path to the key file you wish to import into the
nF Ultra. The nF Ultra only supports keys in the .pem format. If your
key is in another format, please consult the Administrators guide for
instructions on how to convert your key to .pem. Once the key has been
imported you will be prompted to import the certificate associated with
the key.

File name:                                /tmp/testpk1.pem
Key name:                                  test1217

Status: Key import SUCCESSFUL. Press any key.
Please enter the password to protect file in keystore:
```

## (6)import certificate



A terminal window titled "192.168.29.131 [80x24]" with a menu bar containing "連線(C)", "編輯(E)", "檢視(V)", "視窗(W)", "選項(O)", and "說明(H)". The window title bar also includes "nFast Ultra" on the left and "nCipher" on the right. The main content area displays the following text:

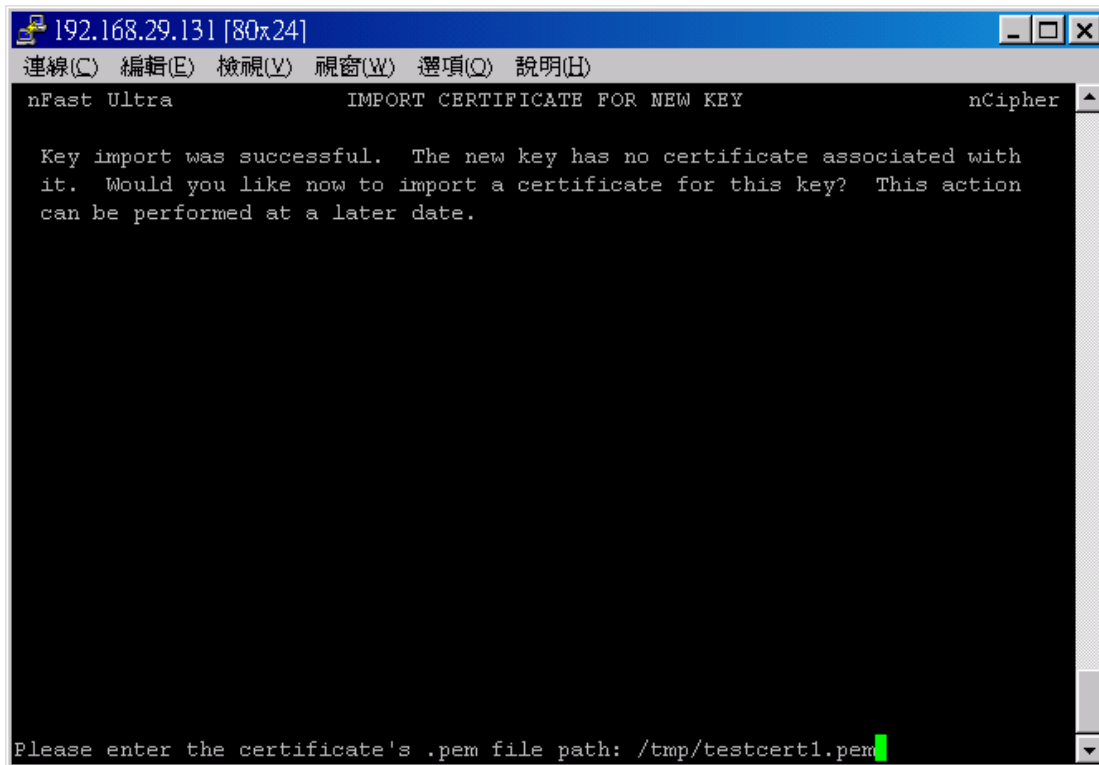
```
nFast Ultra                                IMPORT CERTIFICATE FOR NEW KEY                                nCipher

Key import was successful. The new key has no certificate associated with
it. Would you like now to import a certificate for this key? This action
can be performed at a later date.

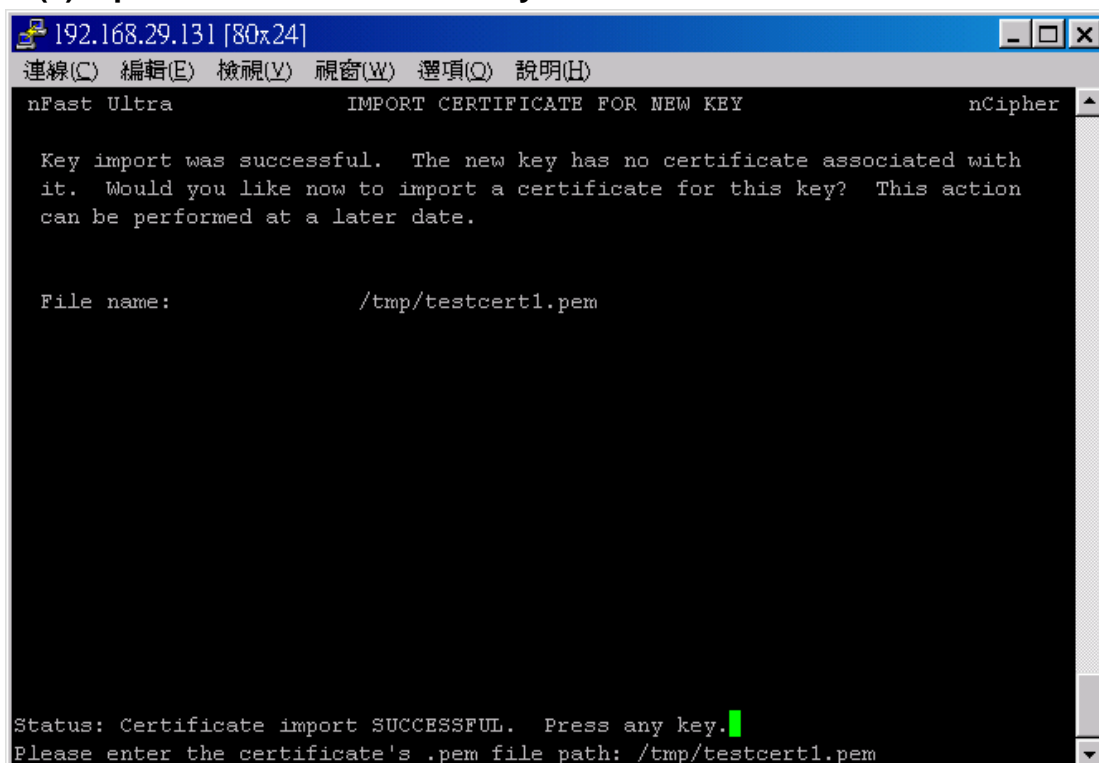
Options
[Y] Yes
[N] No

Do you with to import a certificate?:
```

(7)enter file name : /tmp/testcert1.pem



(8)import certificate successfully



### Step 3:

執行下列命令

---

```
C:\nfast\bin\nfultracli keystore addcert KeyID ca_certname.pem
```

---

其中,KeyID 是之前在 Console 裡匯入的金鑰名稱,而 ca\_certname.pem 則是已轉成 PEM 格式之簽發憑證 CA 之憑證檔。

```
nfultracli keystore addcert test1217 c:\tmp\versign_cert.pem
```

### Step 4:

回到 Console 用匯入之憑證及金鑰所產生之 KeyID 來建立 SSL Proxy