Internet Security Protocols and Standards

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

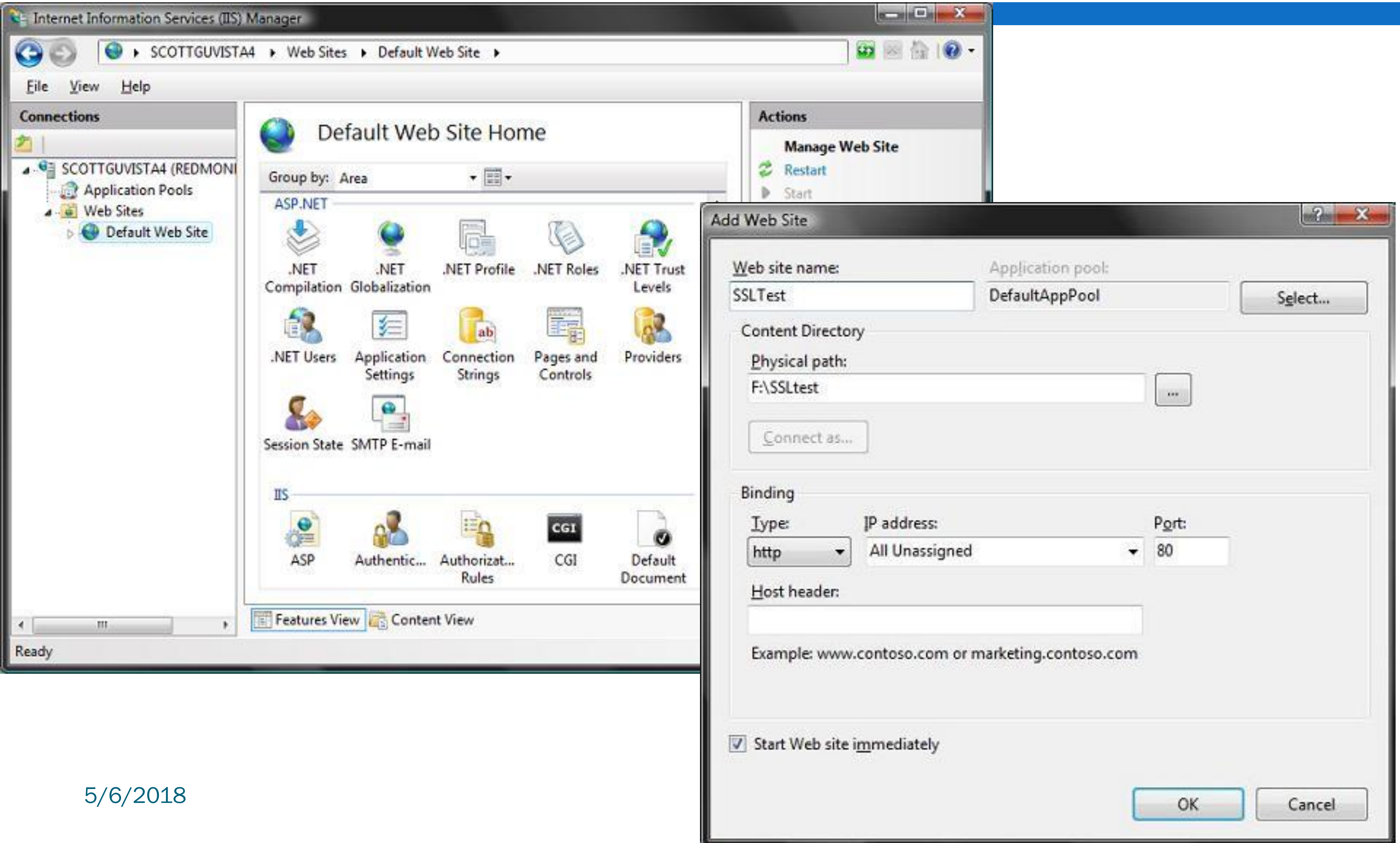
Practice

- HTTPS: (HTTP over SSL)
  - Check if a web browser can establish a secure connection (TLS/SSL) with the site.
  - **configure** the HTTPS service **in** Internet Information Services (IIS)
- VPN with IPSec

Configure the HTTPS service in IIS

- Step 1: Create a New Web Site
- Step 2: Create a new Self Signed Certificate
- Step 3: Enable HTTPS Bindings for our New Site
- Step 4: Test out the Site

Step 1: Create a New Web Site



Web site name: SSLTest

Application pool: DefaultAppPool

Content Directory

Physical path: F:\SSLtest

Binding

Type:	IP address:	Port:
http	All Unassigned	80

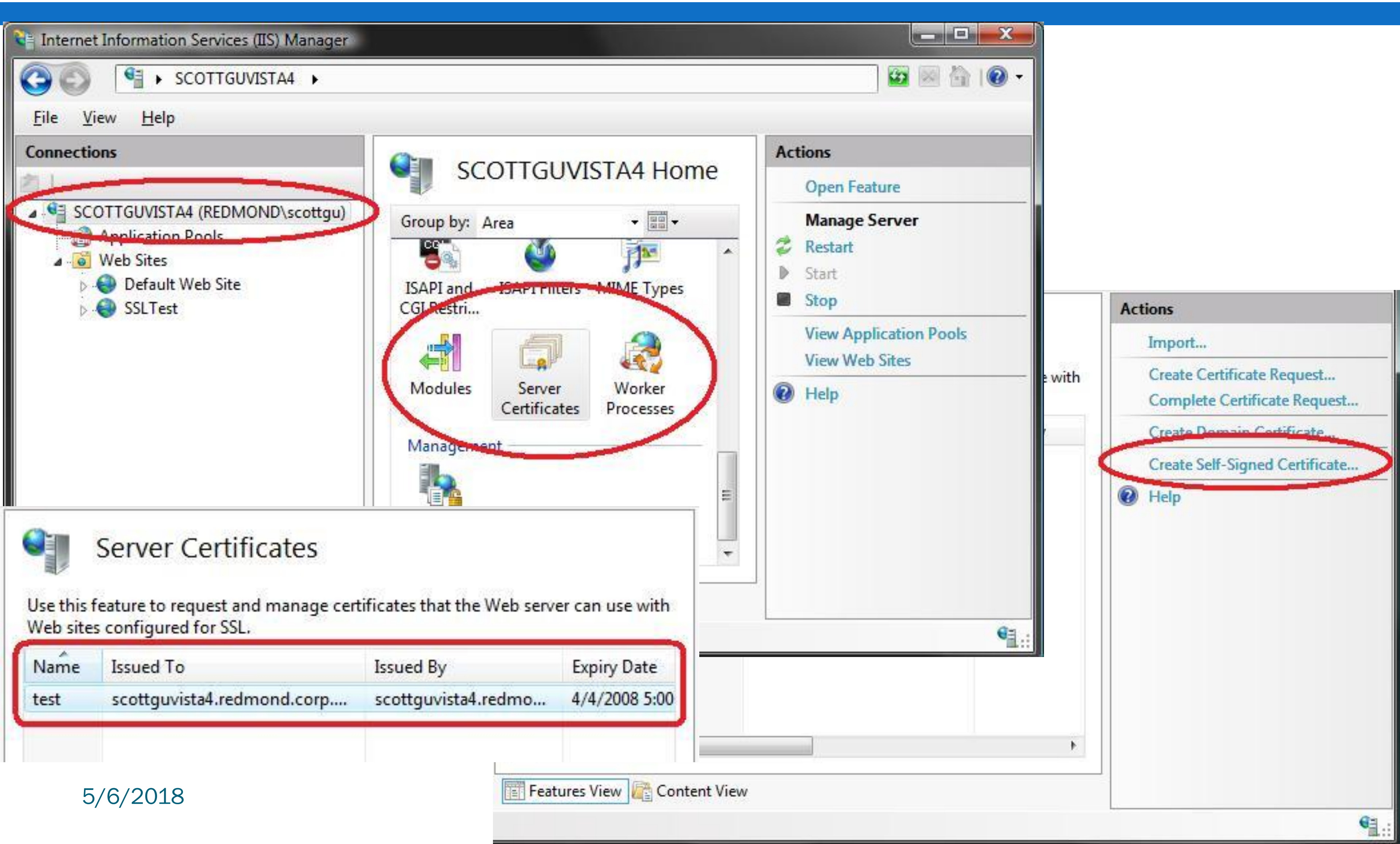
Host header:

Example: www.contoso.com or marketing.contoso.com

☑ Start Web site immediately

5/6/2018

Step 2: Create a new Self Signed Certificate



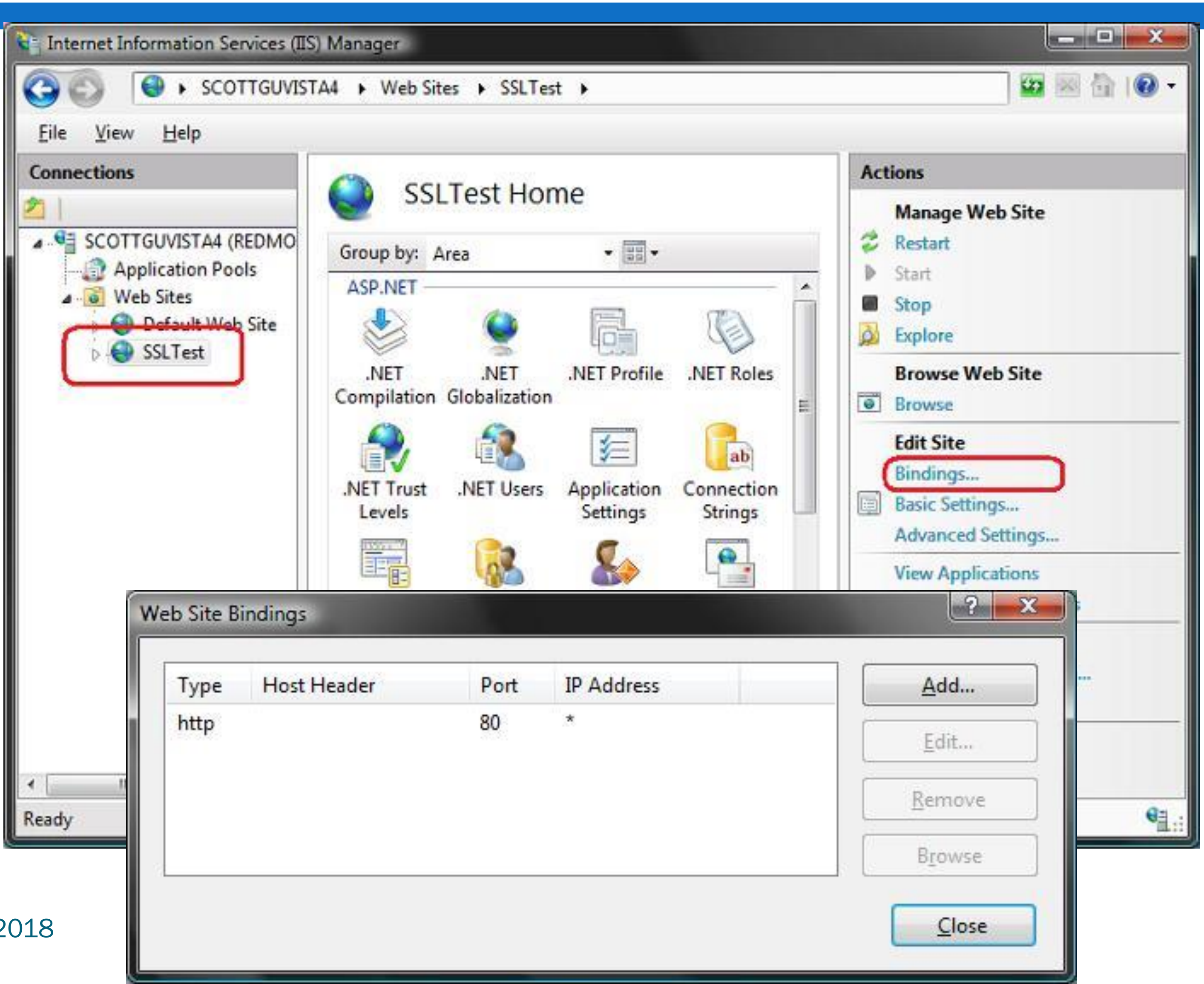
Server Certificates

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

Name	Issued To	Issued By	Expiry Date
test	scottguvista4.redmond.corp....	scottguvista4.redmo...	4/4/2008 5:00

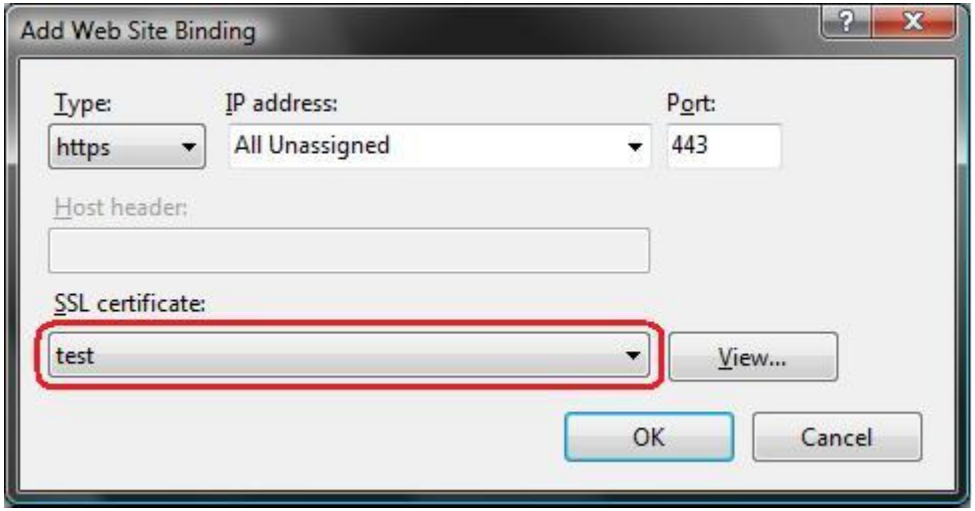
5/6/2018

Step 3: Enable HTTPS Bindings for our New Site



Type	Host Header	Port	IP Address
http		80	*

Step 3: Enable HTTPS Bindings for our New Site



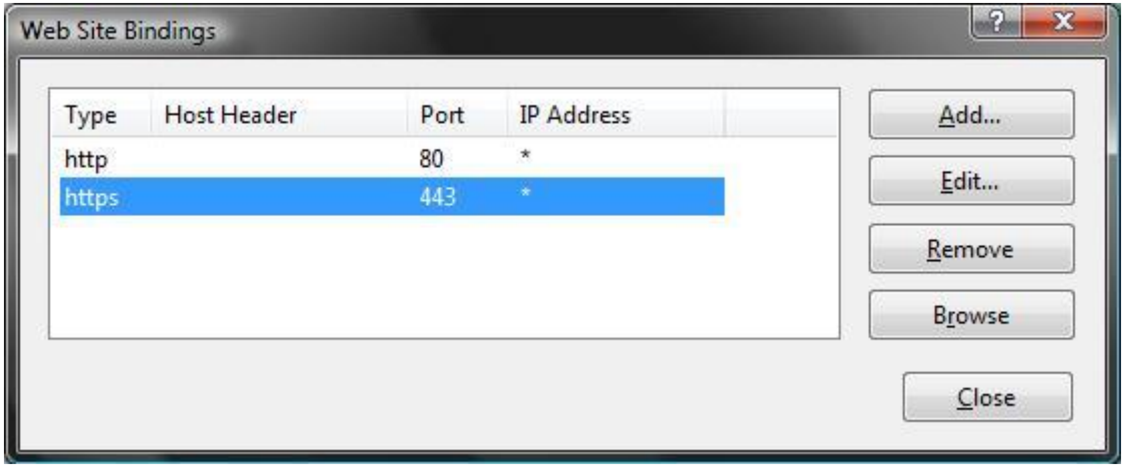
Type: https

IP address: All Unassigned

Port: 443

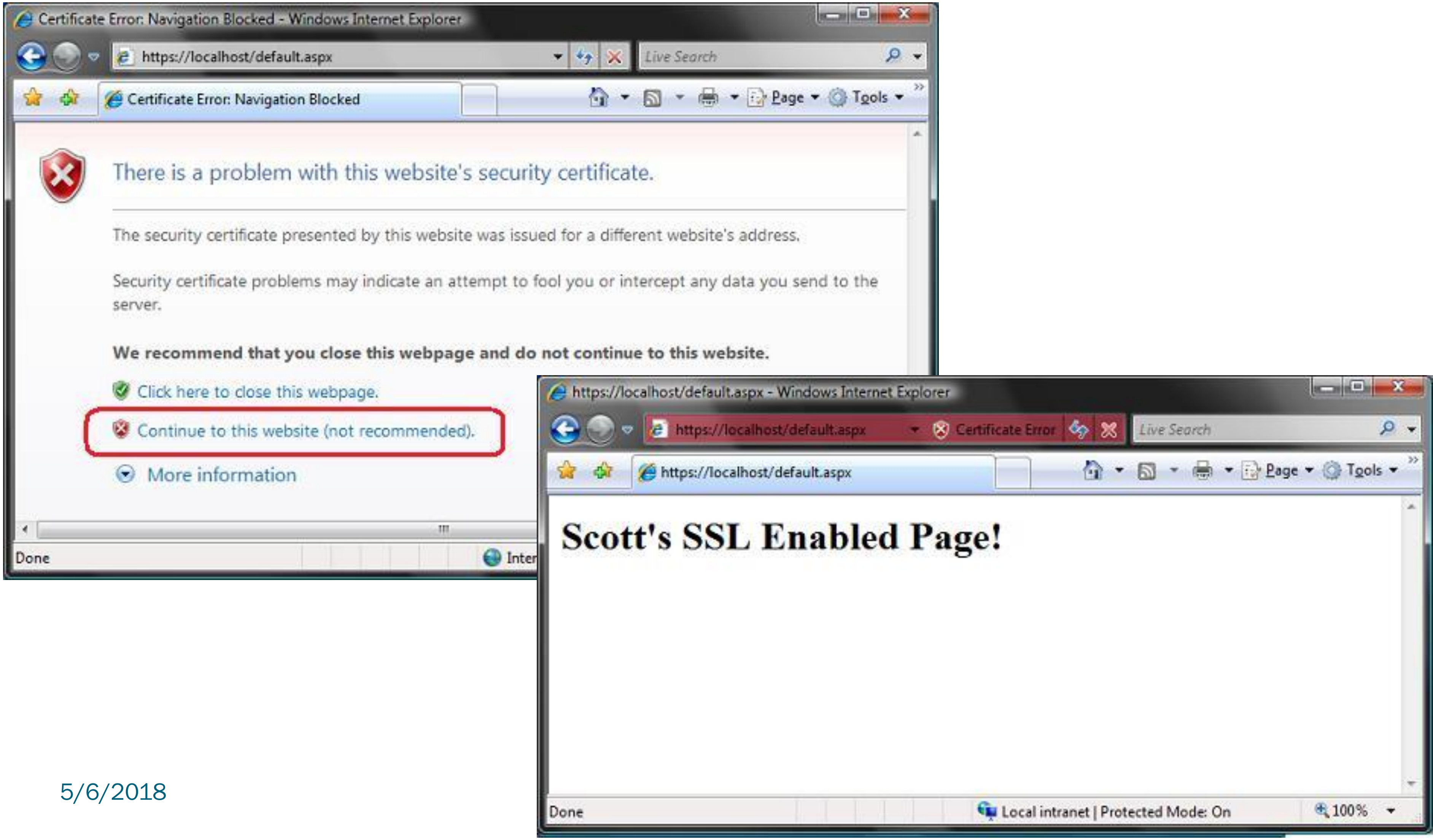
Host header:

SSL certificate: test



Type	Host Header	Port	IP Address
http		80	*
https		443	*

Step 4: Test out the Site


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://localhost/default.aspx
Live Search
Certificate Error: Navigation Blocked
Page
Tools
Done
Inter

There is a problem with this website's security certificate.

The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

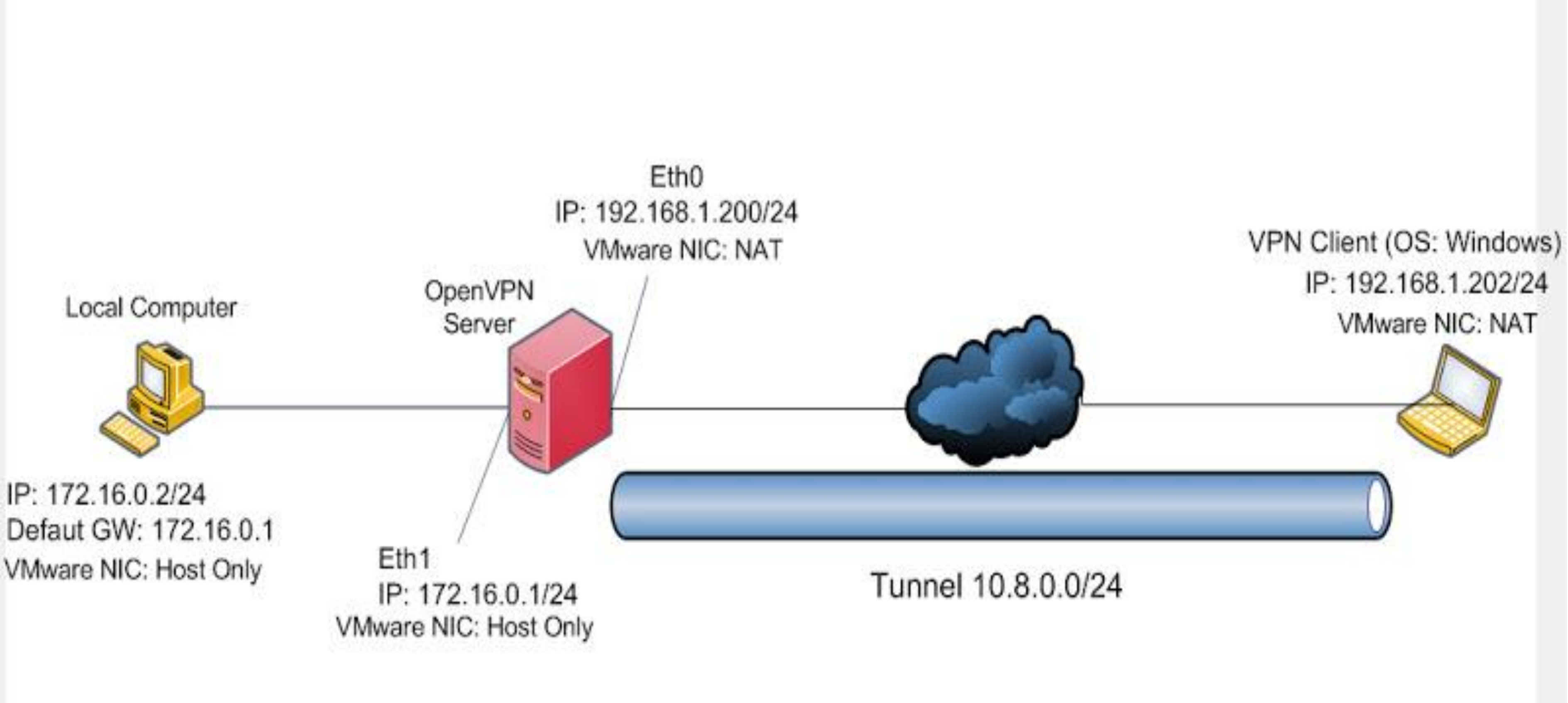
https://localhost/default.aspx - Windows Internet Explorer
https://localhost/default.aspx
Certificate Error
Live Search
https://localhost/default.aspx
Page
Tools

Scott's SSL Enabled Page!

Practice

- Set up VPN with IPSec
  - Client to Site
- Tool
  - Use open source VPN on Linux
  - Windows

Ex: Client-to-Site



At server

Step 1: Install VPN Server:

Copy Lzo-1.08, openvpn-2.0.9 to root.

Install Lzo-1.08, OpenVPN.

Step 2: Create CA Certificate Server

Create opnevpn: mkdir   /etc/openvpn

Copy easy-rsa to /etc/openvpn: cp –r /root/openvpn-2.0.9/easy-rsa/ /etc/openvpn

Move all file in 2.0 to easy-rsa: mv * /etc/openvpn/easy-rsa/2.0/

Change to easy-rsa: cd /etc/openvpn/easy-rsa

Config CA: . ./vars

Create Server CA: ./bulid-ca

Step 3: Create certificate and private key for server

./build-key-server openvpnserver

Create Diffie Hellman (DH) keys: ./build-dh

Create Client Certificate and Private key for Client to authenticate 2 ways

./build-key client1 (common name: client1)

./build-key client2 (common name: client2)

Bước 3: config Forwarding for LanRouting

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Bước 4: Cấu hình VPN Server

Copy file cấu hình server.conf mẫu từ source cài đặt vào

/etc/openvpn/

cp /root/openvpn-2.0.9/sample-config-files/server.conf /etc/openvpn/

Chỉnh sửa file cấu hình:

```
cd /etc/openvpn/
vi server.conf
```

Cấu hình file IP tĩnh tương ứng với từng User:

+ Tạo thư mục ccd (/etc/openvpn/ccd)

```
mkdir /etc/openvpn/ccd
```

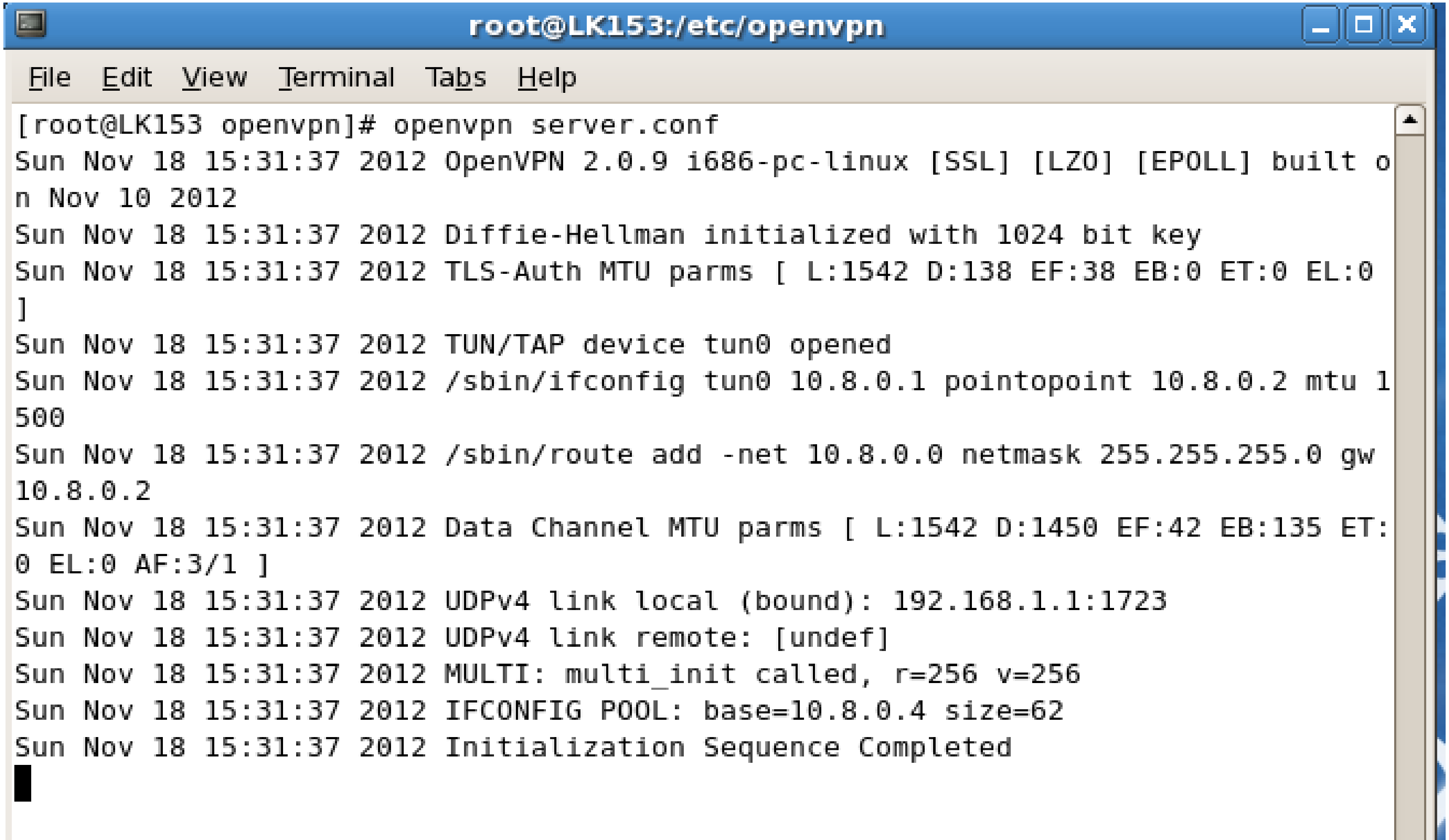
+ Tạo profile cho user client1

```
vi /etc/openvpn/ccd/client1
1: ifconfig-push 10.8.0.2 10.8.0.1
```

+Theo file cấu hình trên client1 sẽ nhận ip là 10.8.0.2

At server

- *openvpn /etc/openvpn/server.conf*

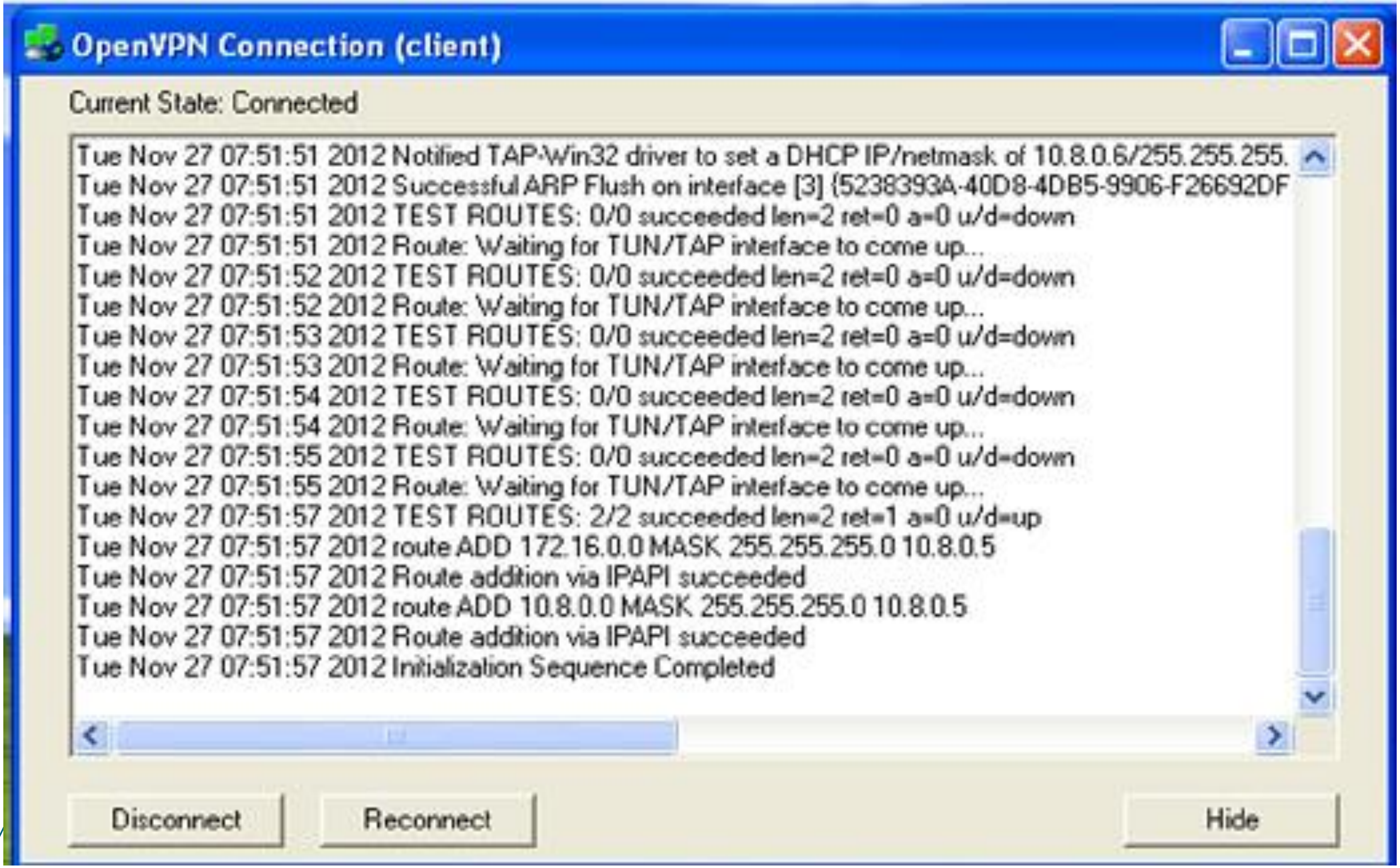


```
[root@LK153 openvpn]# openvpn server.conf
Sun Nov 18 15:31:37 2012 OpenVPN 2.0.9 i686-pc-linux [SSL] [LZO] [EPOLL] built o
n Nov 10 2012
Sun Nov 18 15:31:37 2012 Diffie-Hellman initialized with 1024 bit key
Sun Nov 18 15:31:37 2012 TLS-Auth MTU parms [ L:1542 D:138 EF:38 EB:0 ET:0 EL:0
]
Sun Nov 18 15:31:37 2012 TUN/TAP device tun0 opened
Sun Nov 18 15:31:37 2012 /sbin/ifconfig tun0 10.8.0.1 pointopoint 10.8.0.2 mtu 1
500
Sun Nov 18 15:31:37 2012 /sbin/route add -net 10.8.0.0 netmask 255.255.255.0 gw
10.8.0.2
Sun Nov 18 15:31:37 2012 Data Channel MTU parms [ L:1542 D:1450 EF:42 EB:135 ET:
0 EL:0 AF:3/1 ]
Sun Nov 18 15:31:37 2012 UDPv4 link local (bound): 192.168.1.1:1723
Sun Nov 18 15:31:37 2012 UDPv4 link remote: [undef]
Sun Nov 18 15:31:37 2012 MULTI: multi_init called, r=256 v=256
Sun Nov 18 15:31:37 2012 IFCONFIG POOL: base=10.8.0.4 size=62
Sun Nov 18 15:31:37 2012 Initialization Sequence Completed
```

At Client

- **Install and config OpenVPN GUI at Client**
  - run openvpn-2.0.9-gui-1.0.3-install.exe
  - Copy key files, certificate: ca.crt, client1.crt, client1.key to C:\Program Files\OpenVPN\config
  - Copy client.ovpn from C:\Program Files\OpenVPN\sample-config to C:\Program Files\OpenVPN\config
  - Edit file client.ovpn
- **Dial to VPNServer**

Connect to Server

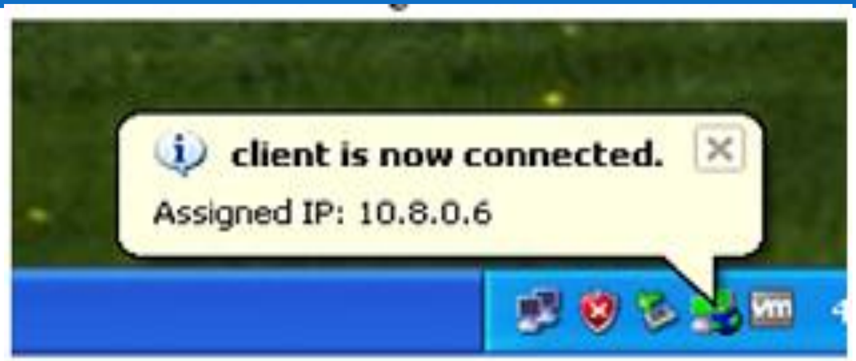


Current State: Connected

```
Tue Nov 27 07:51:51 2012 Notified TAP-Win32 driver to set a DHCP IP/netmask of 10.8.0.6/255.255.255.
Tue Nov 27 07:51:51 2012 Successful ARP Flush on interface [3] {5238393A-40D8-4DB5-9906-F26692DF
Tue Nov 27 07:51:51 2012 TEST ROUTES: 0/0 succeeded len=2 ret=0 a=0 u/d=down
Tue Nov 27 07:51:51 2012 Route: Waiting for TUN/TAP interface to come up...
Tue Nov 27 07:51:52 2012 TEST ROUTES: 0/0 succeeded len=2 ret=0 a=0 u/d=down
Tue Nov 27 07:51:52 2012 Route: Waiting for TUN/TAP interface to come up...
Tue Nov 27 07:51:53 2012 TEST ROUTES: 0/0 succeeded len=2 ret=0 a=0 u/d=down
Tue Nov 27 07:51:53 2012 Route: Waiting for TUN/TAP interface to come up...
Tue Nov 27 07:51:54 2012 TEST ROUTES: 0/0 succeeded len=2 ret=0 a=0 u/d=down
Tue Nov 27 07:51:54 2012 Route: Waiting for TUN/TAP interface to come up...
Tue Nov 27 07:51:55 2012 TEST ROUTES: 0/0 succeeded len=2 ret=0 a=0 u/d=down
Tue Nov 27 07:51:55 2012 Route: Waiting for TUN/TAP interface to come up...
Tue Nov 27 07:51:57 2012 TEST ROUTES: 2/2 succeeded len=2 ret=1 a=0 u/d=up
Tue Nov 27 07:51:57 2012 route ADD 172.16.0.0 MASK 255.255.255.0 10.8.0.5
Tue Nov 27 07:51:57 2012 Route addition via IPAPI succeeded
Tue Nov 27 07:51:57 2012 route ADD 10.8.0.0 MASK 255.255.255.0 10.8.0.5
Tue Nov 27 07:51:57 2012 Route addition via IPAPI succeeded
Tue Nov 27 07:51:57 2012 Initialization Sequence Completed
```

Test at client

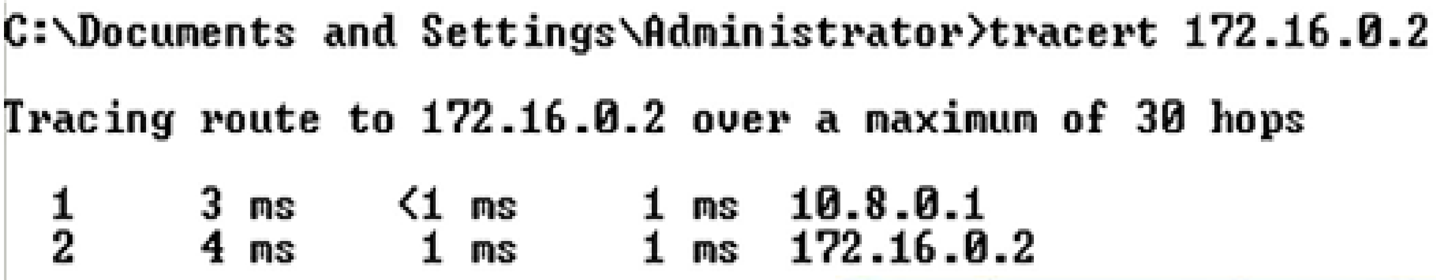
- Assigned IP



client is now connected.

Assigned IP: 10.8.0.6

- Routing:



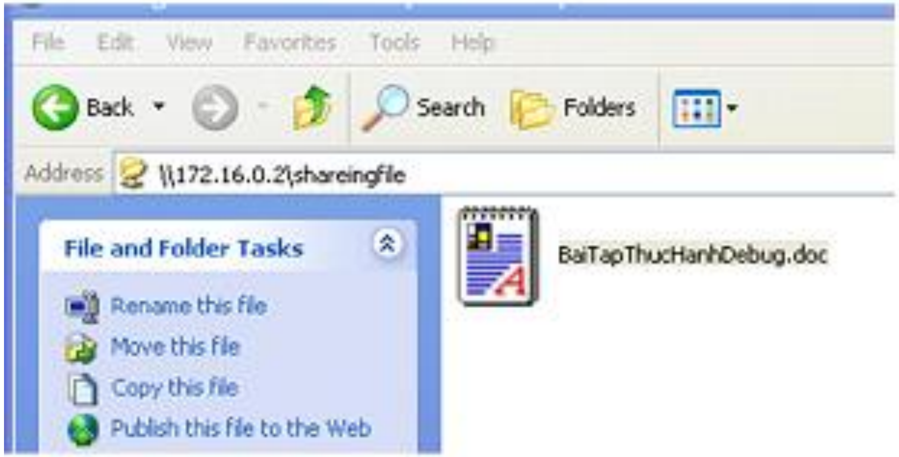
```
C:\Documents and Settings\Administrator>tracert 172.16.0.2

Tracing route to 172.16.0.2 over a maximum of 30 hops

  1     3 ms    <1 ms     1 ms  10.8.0.1
  2     4 ms     1 ms     1 ms  172.16.0.2

Trace complete.
```

- Sharing file:



Address \\172.16.0.2\shareingfile

File and Folder Tasks

- Rename this file
- Move this file
- Copy this file
- Publish this file to the Web

BaiTapThucHanhDebug.doc