

# **Bài 6: Cấu hình VPN Host to Lan (Client to Site)**

## **I. Mục tiêu bài lab**

- Trang bị cho sinh viên kỹ năng cấu hình VPN Host to lan (Client to site)
- Ôn tập lại cách cấu hình Load balance cho router

## **II. Nội dung bài lab**

- a. Chuẩn bị**
- b. Sơ đồ**
- c. Yêu cầu bài lab**
- d. Cấu hình**
- e. Cách test**
- f. Bài tập**

## **III. Hướng dẫn chi tiết**

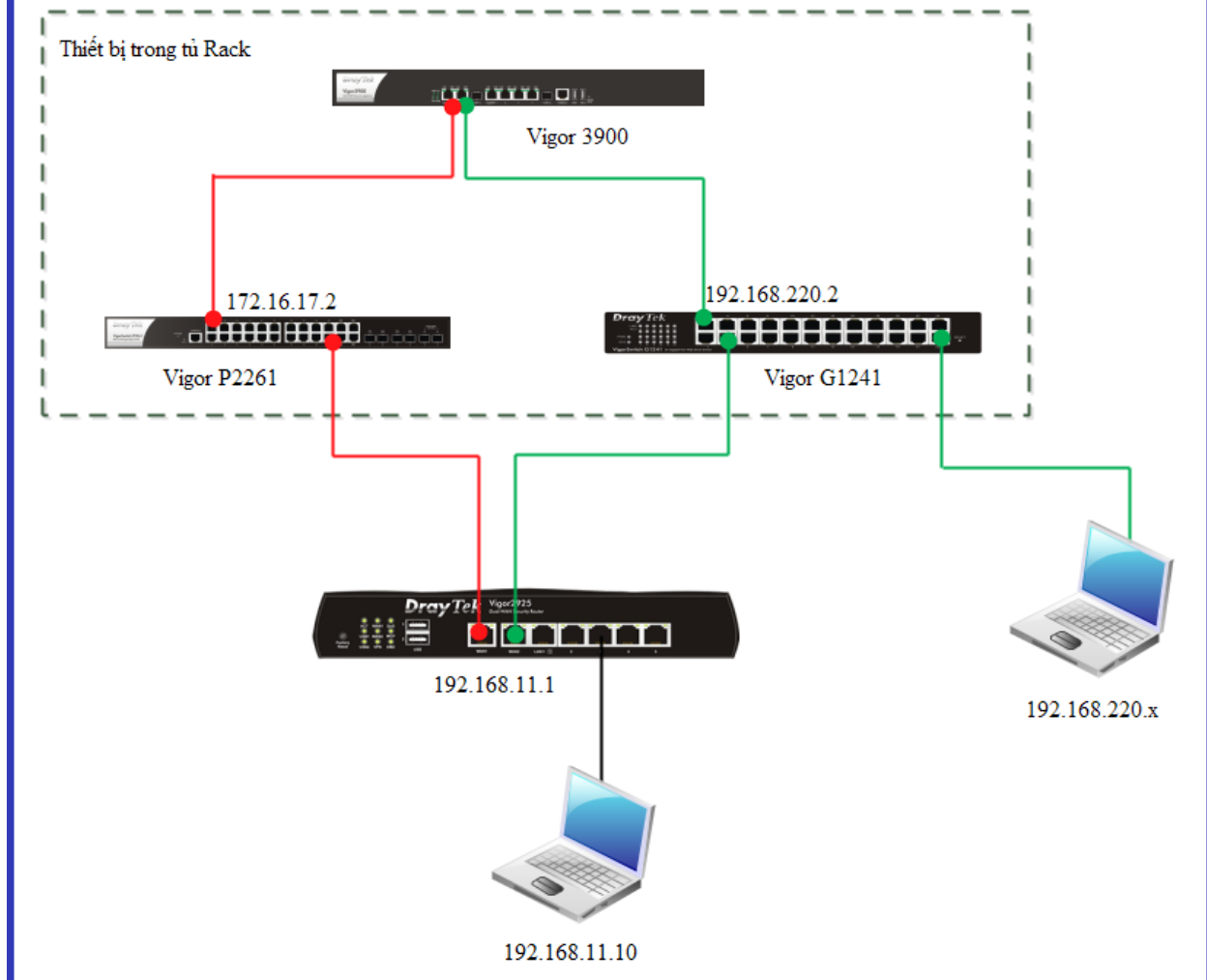
### **a. Chuẩn bị**

- Sử dụng 1 router Vigor 2925/2912,
- 2 laptop trong đó 1 laptop nối vào switch G1241 và sẽ nhận được IP bất kì thuộc lớp 192.168.220.x/24
- Thực hiện thao tác reset default (reset cứng) router 2925/2912
- 4 sợi cáp mạng RJ45
- Nối Wan 1 của router vào cổng bất kì trên switch P2261, nối Wan 2 của router vào cổng bất kì trên switch G1241
- Cấu hình lên Load balance cho router với Wan 1 mode PPPoE, Wan 2 mode Static or Dynamic IP
- Đổi lớp mạng router thành 192.168.11.x/24

Lưu ý: Các bạn liên hệ với giảng viên hướng dẫn để lấy thông tin Account PPPoE và IP để cấu hình Wan

### **b. Sơ đồ**

### Sơ đồ VPN Host to Lan (Client to site)



#### c. Yêu cầu bài lab

- Cấu hình VPN host to lan cho thiết bị thiết bị laptop đang gắn vào switch G1241 có thể truy cập dữ liệu máy 192.168.1.10

#### d. Cấu hình

- Tạo user để VPN: Vào VPN and Remote Access >>> Remote Dial-in User >>> Chọn Index 1



## Remote Access User Accounts:

[Set to Factory Default](#)
View: ☒ All ☐ Online ☐ Offline
 

Index	User	Active	Status	Index	User	Active	Status
<u>1.</u>	???	<input type="checkbox"/>	---	<u>17.</u>	???	<input type="checkbox"/>	---
<u>2.</u>	???	<input type="checkbox"/>	---	<u>18.</u>	???	<input type="checkbox"/>	---
<u>3.</u>	???	<input type="checkbox"/>	---	<u>19.</u>	???	<input type="checkbox"/>	---
<u>4.</u>	???	<input type="checkbox"/>	---	<u>20.</u>	???	<input type="checkbox"/>	---
<u>5.</u>	???	<input type="checkbox"/>	---	<u>21.</u>	???	<input type="checkbox"/>	---
<u>6.</u>	???	<input type="checkbox"/>	---	<u>22.</u>	???	<input type="checkbox"/>	---
<u>7.</u>	???	<input type="checkbox"/>	---	<u>23.</u>	???	<input type="checkbox"/>	---
<u>8.</u>	???	<input type="checkbox"/>	---	<u>24.</u>	???	<input type="checkbox"/>	---
<u>9.</u>	???	<input type="checkbox"/>	---	<u>25.</u>	???	<input type="checkbox"/>	---
<u>10.</u>	???	<input type="checkbox"/>	---	<u>26.</u>	???	<input type="checkbox"/>	---
<u>11.</u>	???	<input type="checkbox"/>	---	<u>27.</u>	???	<input type="checkbox"/>	---
<u>12.</u>	???	<input type="checkbox"/>	---	<u>28.</u>	???	<input type="checkbox"/>	---
<u>13.</u>	???	<input type="checkbox"/>	---	<u>29.</u>	???	<input type="checkbox"/>	---
<u>14.</u>	???	<input type="checkbox"/>	---	<u>30.</u>	???	<input type="checkbox"/>	---
<u>15.</u>	???	<input type="checkbox"/>	---	<u>31.</u>	???	<input type="checkbox"/>	---
<u>16.</u>	???	<input type="checkbox"/>	---	<u>32.</u>	???	<input type="checkbox"/>	---

<< [1-32](#) | [33-64](#) >>[Next](#) >>

Note: User Accounts need to be added into User Group to enable SSL Portal Login.

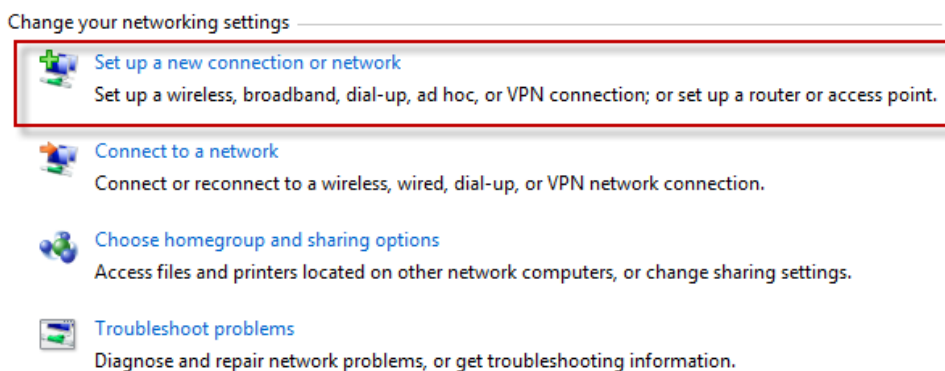
- Chọn Enable this account
- Idle Timeout: chỉnh về 0
- Username: điền tên muốn đặt
- Password: điền password muốn đặt
- Subnet: chọn Lan để cấp IP cho user VPN vào
- Assign Static IP Address: nếu chọn mục này thì bạn sẽ gán IP tĩnh cho user VPN (khi user này VPN vào luôn luôn nhận được IP đã được cấu hình)
- Nhấn OK

Index No. 1

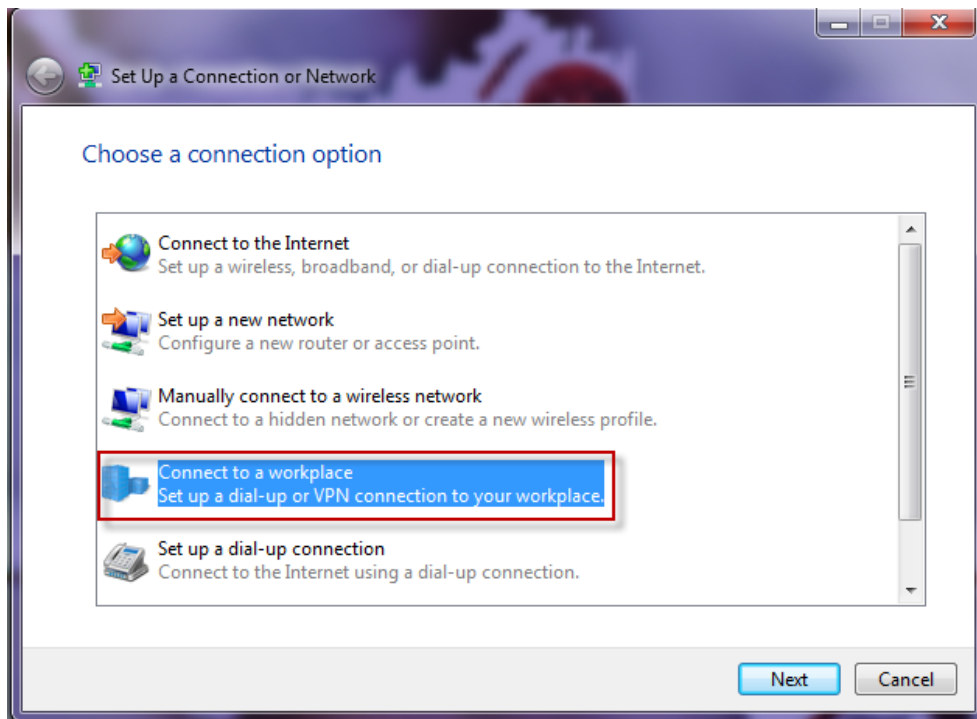
<p><b>User account and Authentication</b></p> <p><input checked="" type="checkbox"/> Enable this account</p> <p>Idle Timeout <input type="text" value="0"/> second(s)</p> <hr/> <p><b>Allowed Dial-In Type</b></p> <p><input checked="" type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> IPsec Tunnel</p> <p><input checked="" type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/></p> <p><input checked="" type="checkbox"/> SSL Tunnel</p> <p><input type="checkbox"/> Specify Remote Node</p> <p>Remote Client IP <input type="text"/></p> <p>or Peer ID <input type="text"/></p> <p>Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block</p> <p>Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block</p> <p>(for some IGMP, IP-Camera, DHCP Relay..etc.)</p> <hr/> <p><b>Subnet</b></p> <p><input type="text" value="LAN 1"/></p> <p><input type="checkbox"/> Assign Static IP Address</p> <p><input type="text" value="0.0.0.0"/></p>	<p>Username <input type="text" value="vpn01"/></p> <p>Password(Max 19 char) <input type="password" value="..."/></p> <p><input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP)</p> <p>PIN <input type="text"/></p> <p>Code <input type="text"/></p> <p>Secret <input type="text"/></p> <hr/> <p><b>IKE Authentication Method</b></p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p>IKE Pre-Shared Key <input type="text"/></p> <p><input type="checkbox"/> Digital Signature(X.509)</p> <p><input type="text" value="None"/></p> <hr/> <p><b>IPsec Security Method</b></p> <p><input checked="" type="checkbox"/> Medium(AH)</p> <p>High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p> <p>Local ID (optional) <input type="text"/></p>
--	--

OK Clear Cancel

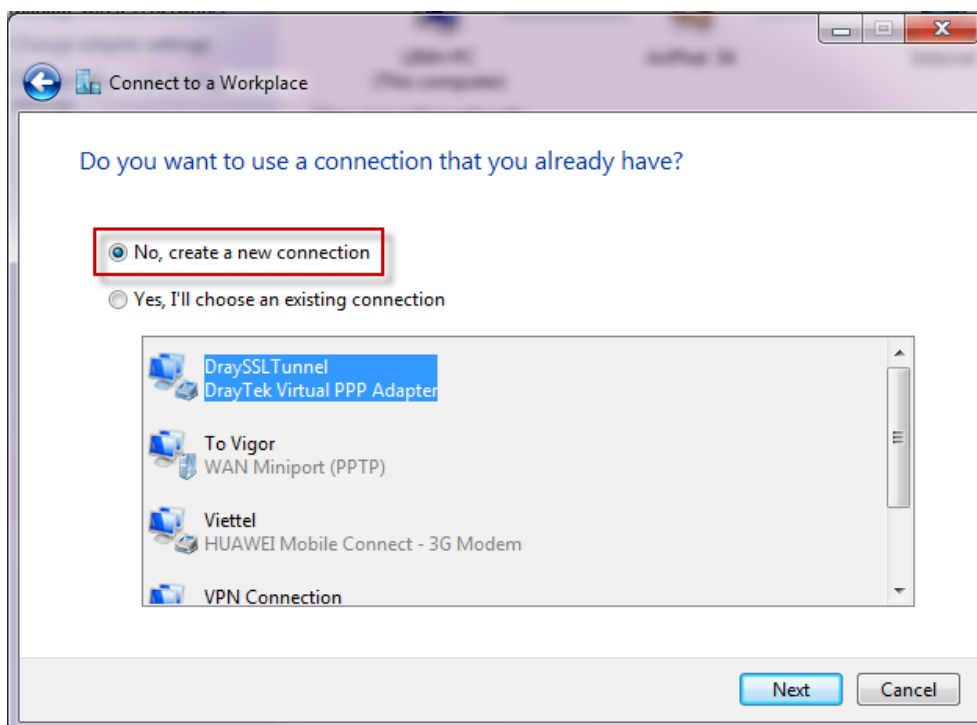
- **Tạo kết nối VPN trên window:** Vào **Start >>> Control Panel >>> Network and Sharing center >>>** chọn **Setup a new connection or network**.



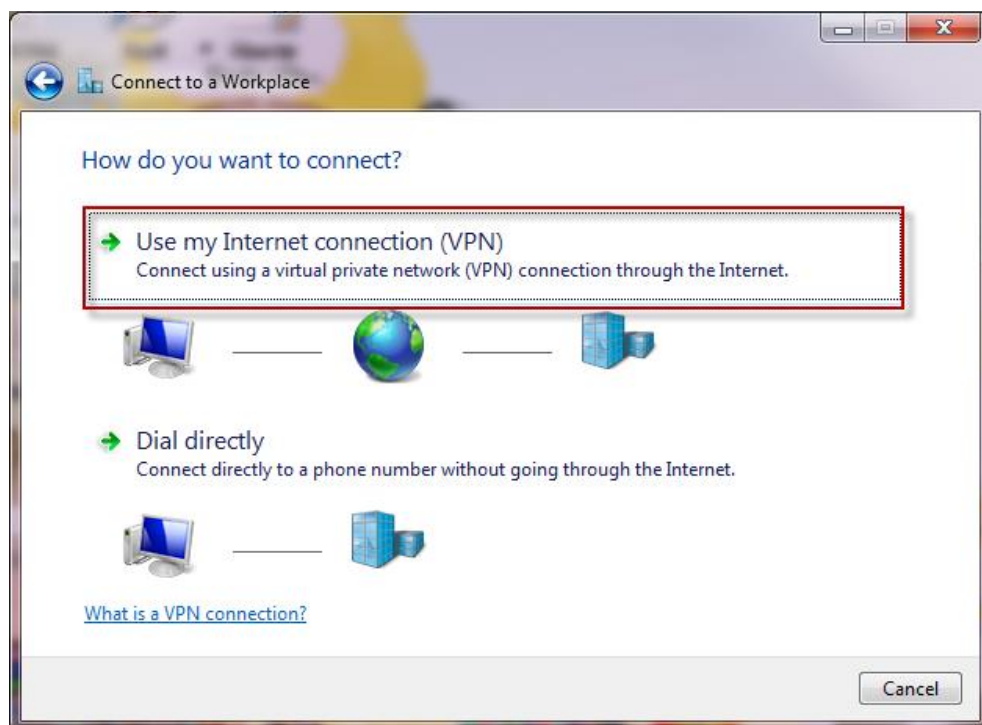
- Chọn **Connect to a workplace >>>** click **Next**.



- Chọn **No**, **creat a new connection** >>> click **Next**.



- Chọn **Use my internet connection (VPN)**



- Trong **Internet address** : Điền thông tin **IP WAN** hoặc **tên miền động** của Vigor (Bạn vào mục Online Status >>> Physical Connection để lấy IP Wan)

Online Status

Physical Connection

IPv4

IPv6

System Uptime: 0day 0:53:43

LAN Status

Primary DNS: 8.8.4.4

Secondary DNS: 8.8.8.8

IP Address

TX Packets

RX Packets

192.168.11.1

20206

15920

WAN 1 Status

>> Drop PPPoE

Enable

Line

Name

Mode

Up Time

Yes

Ethernet

PPPoE

0:53:35

IP

GW IP

TX Packets

TX Rate(Bps)

RX Packets

RX Rate(Bps)

172.16.17.11

172.16.17.1

8892

260

10834

408

WAN 2 Status

Enable

Line

Name

Mode

Up Time

Yes

Ethernet

Static IP

0:53:34

IP

GW IP

TX Packets

TX Rate(Bps)

RX Packets

RX Rate(Bps)

192.168.220.100

192.168.220.1

6085

195

8417

289

WAN 3 Status

Enable

Line

Name

Mode

Up Time

Signal

Yes

USB

---

00:00:00

-

IP

GW IP

TX Packets

TX Rate(Bps)

RX Packets

RX Rate(Bps)

---

---

0

0

0

0

WAN 4 Status

Enable

Line

Name

Mode

Up Time

Signal

Yes

USB

---

00:00:00

-

IP

GW IP

TX Packets

TX Rate(Bps)

RX Packets

RX Rate(Bps)

---

---

0

0

0

0

- **Internet address:** điền địa chỉ IP wan trên router (có thể dùng IP wan 1 hoặc Wan 2)
- **Destination Name:** có thể mặc định hoặc đổi tên tùy ý
- Chọn **Don't connect now; just set it up so I can connect later >>>** click **Next**

Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 172.16.117.11 ← IP wan của router

Destination name: VPN Connection 2

☐ Use a smart card

☐ Allow other people to use this connection  
This option allows anyone with access to this computer to use this connection.

☒ Don't connect now; just set it up so I can connect later

Next Cancel

- Điền thông tin **username** và **password** của user VPN >>> click **Create**.

Connect to a Workplace

Type your user name and password

User name: vpn01

Password: ...

☐ Show characters

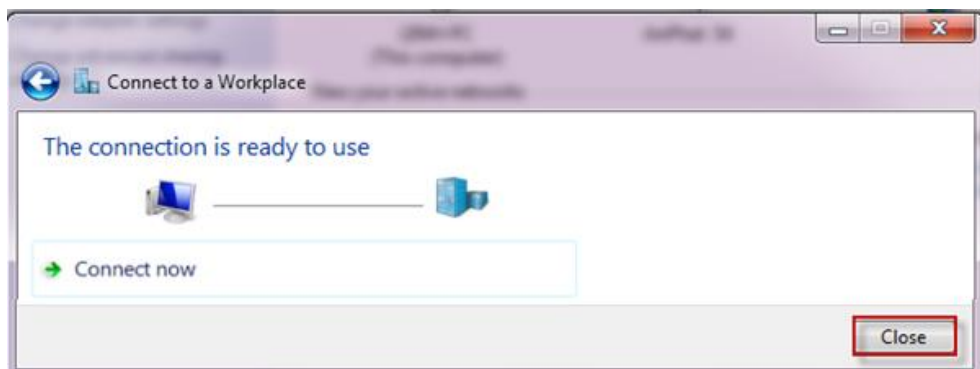
☐ Remember this password

Domain (optional):

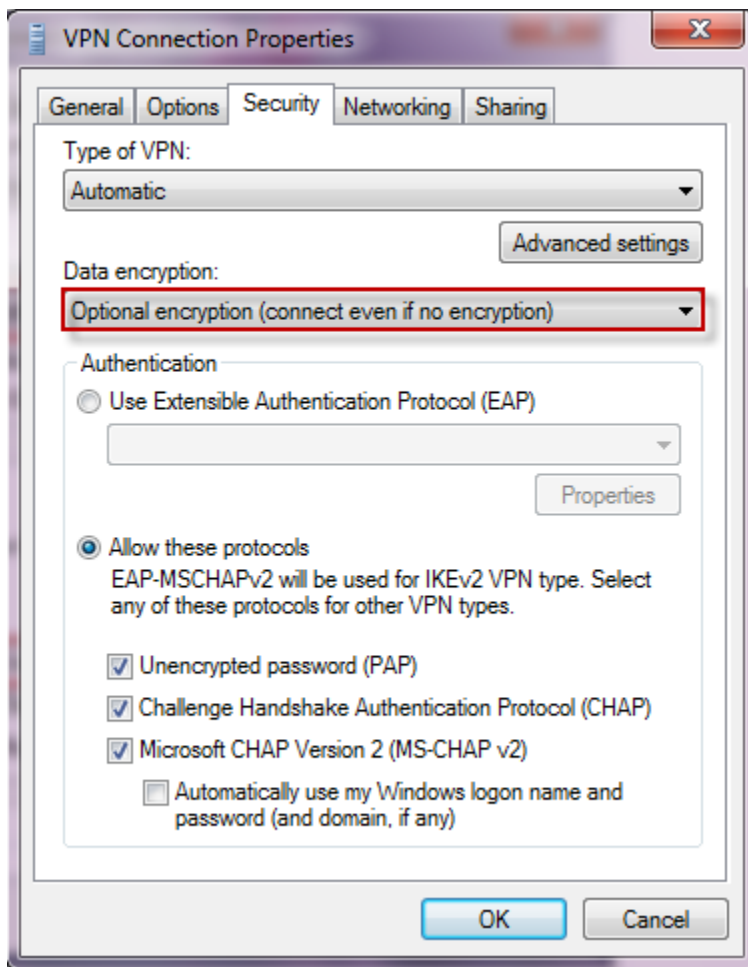
Create Cancel

- Click Close.





- Click **phải** vào kết nối VPN vừa tạo chọn **Properties** >>> qua tab **Security** để chỉnh thông số mã hoá cho kết nối VPN



- Lưu ý: chỉnh Security trên kết nối VPN phải phù hợp với Security trong VPN trên router

- Xem Security VPN trên router Vigor: Vào VPN and remote access >>> PPP General setup

VPN and Remote Access >> PPP General Setup

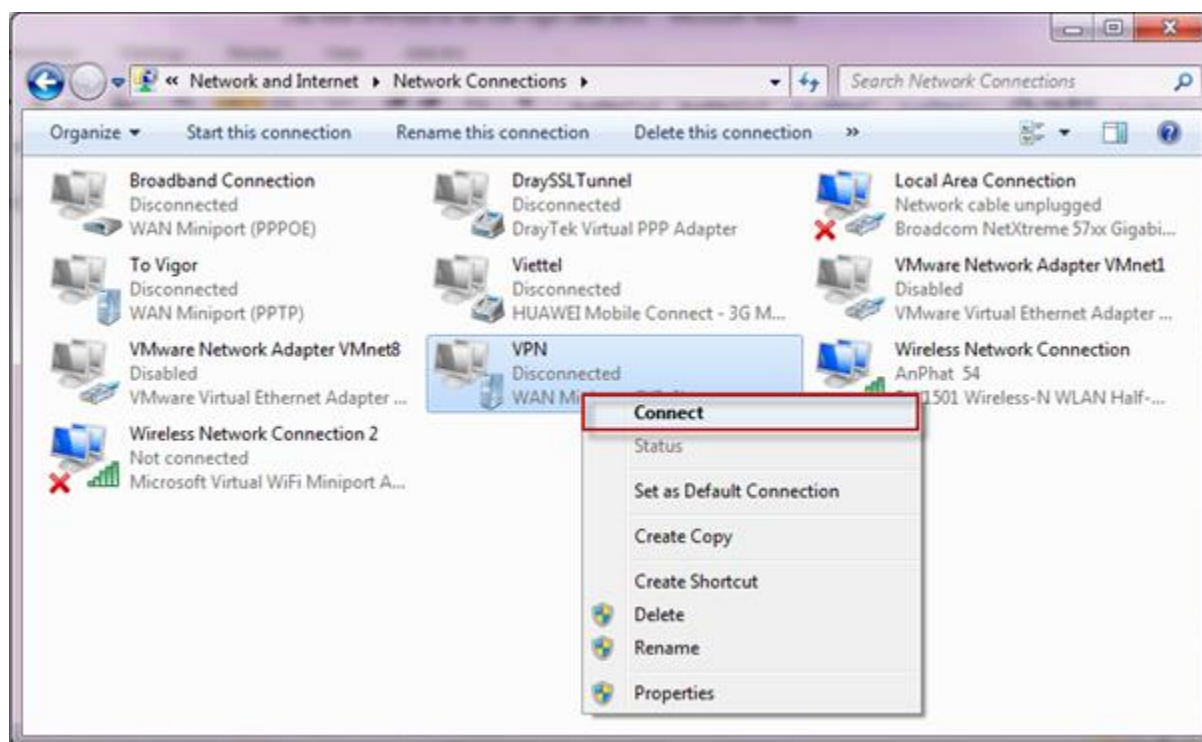
---

**PPP General Setup**

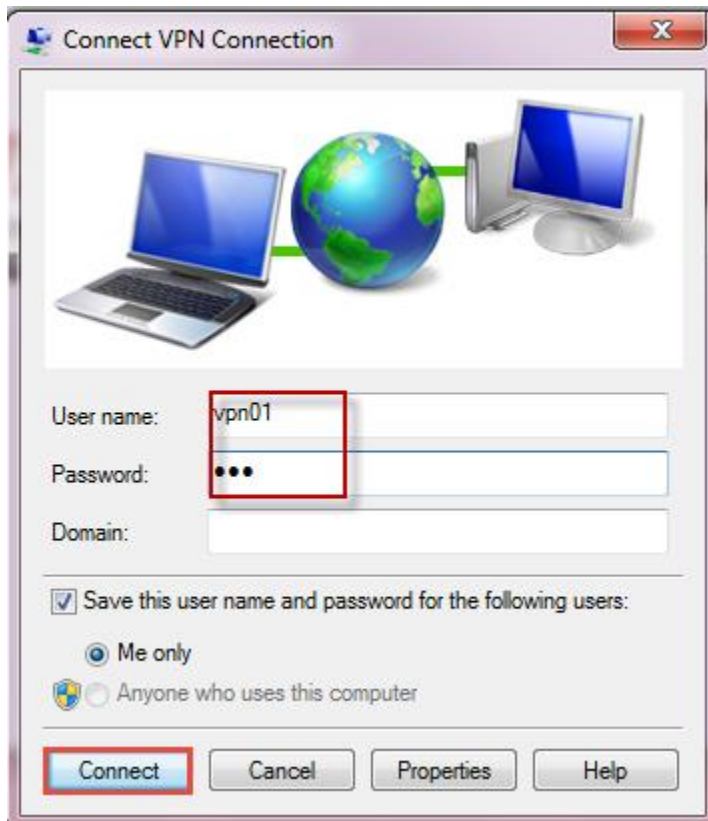
<b>PPP/MP Protocol</b> Dial-In PPP Authentication: <span>PAP/CHAP/MS-CHAP/MS-CHAPv2 ▼</span> Dial-In PPP Encryption(MPPE): <span>Optional MPPE ▼</span> Mutual Authentication (PAP): <input type="radio"/> Yes <input checked="" type="radio"/> No Username: <input type="text"/> Password: <input type="text"/> <b>IP Address Assignment for Dial-In Users (When DHCP Disable set)</b> <table border="1"> <tr><td>Assigned IP start LAN 1</td><td>192.168.11.200</td></tr> <tr><td>LAN 2</td><td>192.168.2.200</td></tr> <tr><td>LAN 3</td><td>192.168.3.200</td></tr> <tr><td>LAN 4</td><td>192.168.4.200</td></tr> <tr><td>LAN 5</td><td>192.168.5.200</td></tr> </table>		Assigned IP start LAN 1	192.168.11.200	LAN 2	192.168.2.200	LAN 3	192.168.3.200	LAN 4	192.168.4.200	LAN 5	192.168.5.200	<b>PPP Authentication Methods</b> <input checked="" type="checkbox"/> Remote Dial-in User <input checked="" type="checkbox"/> RADIUS <input checked="" type="checkbox"/> AD/LDAP <b>PPTP LDAP Profile</b> <input checked="" type="checkbox"/> TACACS+  <b>Note:</b> Please select 'PAP Only 'Dial-In PPP Authentication', if you want to use AD/LDAP or TACACS+ for PPP Authentication.  <b>Note:</b> Default priority is Remote Dial-in User -> RADIUS -> AD/LDAP -> TACACS+.  <b>While using Radius or LDAP Authentication:</b> Assign IP from subnet: <span>LAN1 ▼</span>
Assigned IP start LAN 1	192.168.11.200											
LAN 2	192.168.2.200											
LAN 3	192.168.3.200											
LAN 4	192.168.4.200											
LAN 5	192.168.5.200											

OK

- Click phải vào kết nối VPN vừa mới tạo >>> click Connect



- Điền thông tin **user/pass** của user VPN >>> Nhấn Connect



Connect VPN Connection

User name: vpn01

Password: ●●●

Domain:

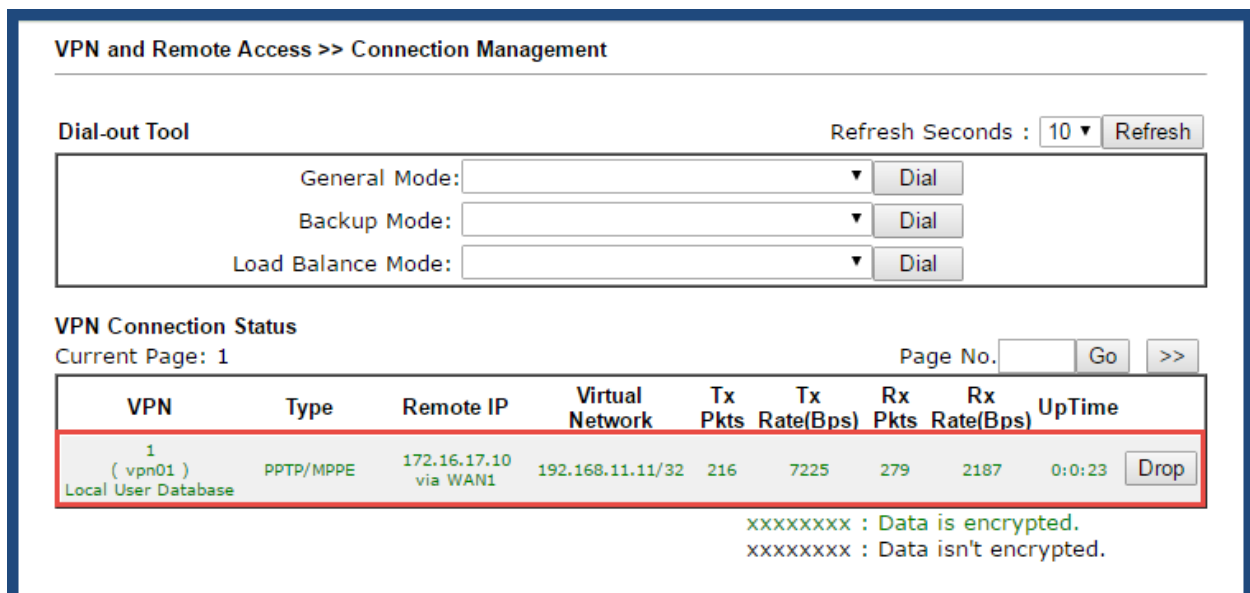
☒ Save this user name and password for the following users:

☒ Me only

☐ Anyone who uses this computer

Connect Cancel Properties Help

- Kiểm tra kết nối VPN: Vào VPN and Remote Access >>> Connection Management



VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Seconds : 10 Refresh

General Mode: Dial

Backup Mode: Dial

Load Balance Mode: Dial

VPN Connection Status

Current Page: 1 Page No. Go >>

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime
1 ( vpn01 ) Local User Database	PPTP/MPPE	172.16.17.10 via WAN1	192.168.11.11/32	216	7225	279	2187	0:0:23 Drop

xxxxxxx : Data is encrypted.

xxxxxxx : Data isn't encrypted.

## e. Cách test

- cmd >>> gõ lệnh ipconfig /all >>> PPP adapter VPN connection

```
C:\Users\Jenny>ipconfig /all
```

- Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

```
C:\Users\Jenny>ping 192.168.11.10 -t
```

```
Pinging 192.168.11.10 with 32 bytes of data:
```

[illegible]

Lưu ý: Khi test ping thì cả 2 máy nên tắt chương trình anti virus và firewall

## **f. Bài tập**

- Cấu hình Internet cho router
- Cấu hình chia Vlan cho router thành 2 Vlan:
  - Lan 1: 192.168.10.x/24 gán vào P1 và P2
  - Lan 2: 192.168.20.x/24 gán vào P3 và P4
- 2 Vlan này có thể thông với nhau
- Tạo 2 user VPN
  - Nv1 nhận IP tĩnh 192.168.10.100
  - Nv2 nhận IP tĩnh 192.168.20.100
  - Sep nhận IP động từ Lan 1
- Tạo firewall
  - Cho phép “nv1” truy cập nội bộ trong lan, không được truy cập Lan khác
  - Cho phép “nv2” chỉ được remote desktop tới 1 máy trong lan 1 có IP 192.168.10.199, không được truy cập những máy khác
  - Cho phép “sep” có thể truy cập được tất cả.



Gợi ý cấu hình Firewall:

- Tạo 3 rule
  - Rule 1: block nv1 truy cập nội bộ trong lan, không được truy cập Lan khác
    - Với source IP: điền địa chỉ IP mà nv1 sẽ nhận được sau khi VPN
    - Destination IP: subnet Lan 2
    - Filter: chọn Block Immediately
  - Rule 2: cho phép nv2 được remote desktop tới 1 máy trong lan 1 có IP 192.168.10.199
    - Với source IP: điền địa chỉ IP mà nv2 sẽ nhận được sau khi VPN
    - Destination IP: IP máy cho phép remote (192.168.10.199)
    - Service type: port 3389
    - Filter: chọn Pass Immediately
  - Rule 3: block nv2 truy cập tới những máy khác trong lan 1
    - Với source IP: điền địa chỉ IP mà nv2 sẽ nhận được sau khi VPN
    - Destination IP: subnet Lan 1
    - Filter: chọn Block Immediately

