

# **Bài 7: Cấu hình VPN Lan to Lan (Site to Site)**

## **I. Mục tiêu bài lab**

- Trang bị cho sinh viên kỹ năng cấu hình VPN Lan to Lan (Site 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**

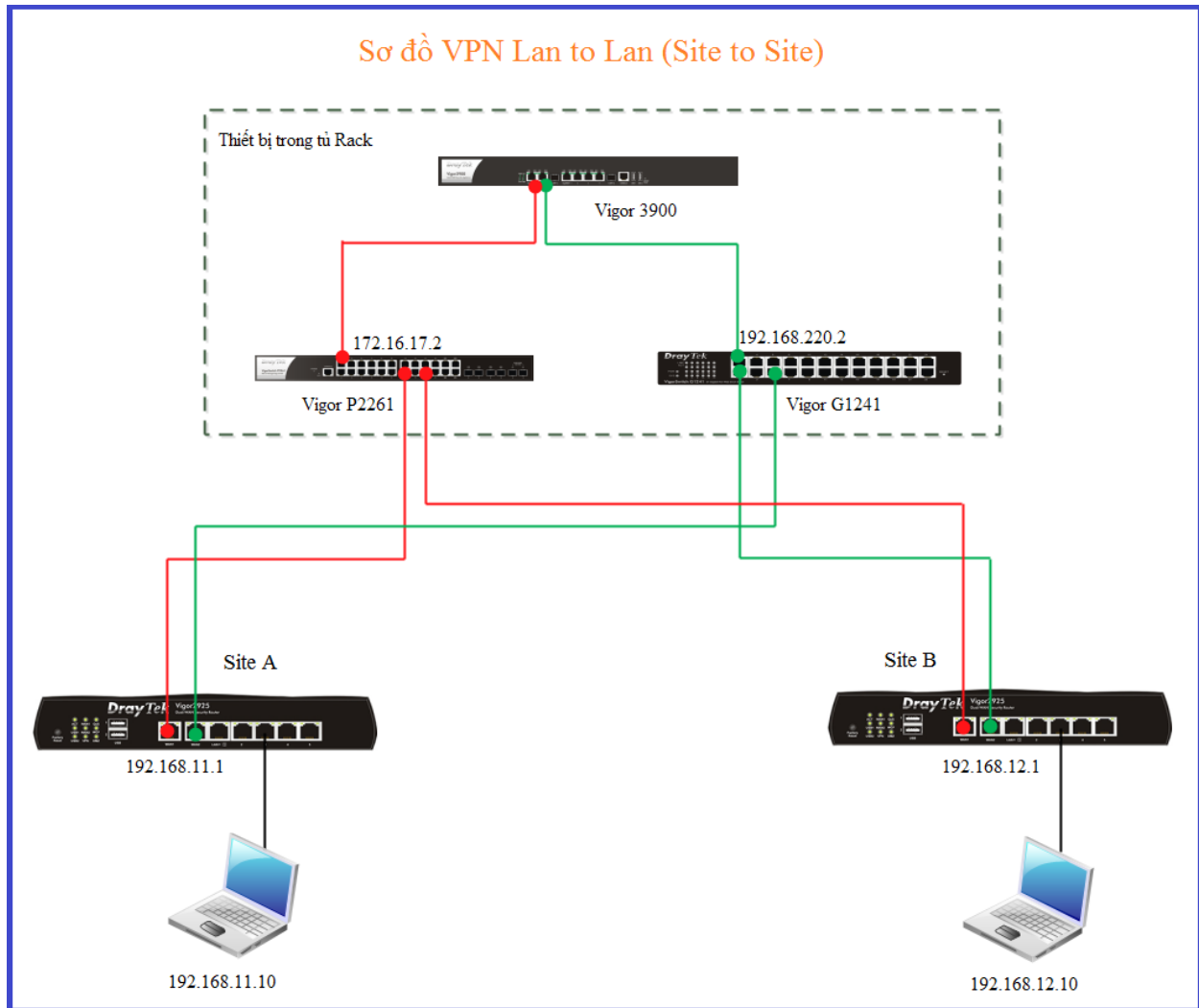
## **III. Hướng dẫn chi tiết**

### **a. Chuẩn bị**

- Sử dụng 2 router Vigor 2925/2912,
- Thực hiện thao tác reset default (reset cứng) router 2925/2912
- 6 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 site A thành 192.168.11.x/24, đổi lớp mạng router site B thành 192.168.12.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**



### c. Yêu cầu bài Lab

- Cấu hình VPN để kết nối 2 site A và site B sao cho những máy trong nội bộ site A có thể truy cập được những trong nội bộ site B

### d. Cấu hình

- Để cấu hình VPN lan to lan cho 2 thiết bị thì sẽ có 1 router đóng vai trò là Dial-in (VPN server), Dial-out (VPN client)
- Site A đóng vai trò là Dial-in, Site B là Dial-out

**Lưu ý:** Do trong môi trường bài Lab nên các bạn có thể lựa chọn router nào làm Dial-in cũng được, nhưng ngoài thực tế thiết bị làm Dial-in nên có IP Wan tĩnh, hoặc sử dụng tên miền động (dynamic DNS)

- Trong bài hướng dẫn này sẽ giới thiệu cấu hình với giao thức phổ biến nhất là IPsec khi VPN lan to lan

🔗 Cấu hình router site A (Dial-in)

- Cấu hình Key VPN: Vào VPN and Remote Access >>> IPsec General setup

- Pre-Shared Key: điền key VPN
- Confirm Pre-Shared Key: điền lại đúng key đã điền ở Pre-shared Key

VPN and Remote Access >> IPsec General Setup

VPN IKE/IPsec General Setup  
Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

**IKE Authentication Method**

Certificate for Dial-in: None ▼

**Pre-Shared Key**

Pre-Shared Key: .....

Confirm Pre-Shared Key: .....

**IPsec Security Method**

☒ Medium (AH)  
Data will be authentic, but will not be encrypted.

High (ESP) ☒ DES ☒ 3DES ☒ AES  
Data will be encrypted and authentic.

OK Cancel

- Cấu hình profile VPN: Vào VPN and Remote Access >>> Lan to Lan >>> chọn Index 1



## LAN-to-LAN Profiles:

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

Index	Name	Active	Status	Index	Name	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](#) >>

OK

Cancel

- Mục 1: Common Setting
  - Profile Name: đặt tên profile
  - Chọn Enable this profile
  - Call Direction: chọn Dial-in
  - Idle Timeout: chỉnh về 0

Profile Index : 1

**1. Common Settings**

Profile Name <input type="text" value="to_site_b"/> <input checked="" type="checkbox"/> Enable this profile VPN Dial-Out Through <input type="text" value="WAN1 First"/> Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)	Call Direction <input type="radio"/> Both <input type="radio"/> Dial-Out <input checked="" type="radio"/> Dial-in Tunnel Mode <input type="radio"/> GRE Tunnel <input type="checkbox"/> Always on Idle Timeout <input type="text" value="0"/> second(s) <input type="checkbox"/> Enable PING to keep IPsec tunnel alive PING to the IP <input type="text"/>
---	--

- Mục 2: Dial out settings sẽ không cấu hình vì hiện tại đang cấu hình cho Dial In nên ta chuyển sang mục 3
- Mục 3: Dial-In settings
  - Chọn IPsec Tunnel

**3. Dial-In Settings**

<b>Allowed Dial-In Type</b> <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/> <input type="checkbox"/> SSL Tunnel  <input type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP <input type="text"/> or Peer ID <input type="text"/>	Username <input type="text" value="???"/> Password(Max 11 char) <input type="text"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off  <b>IKE Authentication Method</b> <input checked="" type="checkbox"/> Pre-Shared Key <input type="checkbox"/> Digital Signature(X.509) <input type="text" value="None"/> Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First  <b>IPsec Security Method</b> <input checked="" type="checkbox"/> Medium(AH) High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
---	--

- Mục 4: GRE setting sẽ không cấu hình
- Mục 5: TCP/IP Network settings
  - Remote Network IP: điền địa lớp mạng của site B. Theo bài lab, ta điền: 192.168.12.0
  - Remote Network Mask: điền subnet mask của lớp mạng bên site B. Theo bài lab, ta điền: 255.255.255.0

- Local Network IP: điền địa chỉ lớp mạng của site A. Theo bài lab, ta điền: 192.168.11.0
- Local Network Mask: điền subnet mask của lớp mạng bên site A. Theo bài lab, ta điền: 255.255.255.0
- Nhấn OK

4. GRE Settings

☐ Enable IPsec Dial-Out function GRE over IPsec
 ☐ Logical Traffic
 My GRE IP
 Peer GRE IP

5. TCP/IP Network Settings

My WAN IP0.0.0.0
Remote Gateway IP0.0.0.0
Remote Network IP192.168.12.0
Remote Network Mask255.255.255.0
Local Network IP192.168.11.0
Local Network Mask255.255.255.0
More

RIP DirectionDisable
From first subnet to remote network, you have to do
Route
☐ IPsec VPN with the Same Subnets
☐ Change default route to this VPN tunnel ( Only single WAN supports this )

OKClearCancel

### Cấu hình router site B (Dial-out)

- Cấu hình Profile VPN: Cấu hình profile VPN: Vào VPN and Remote Access >>> Lan to Lan >>> chọn Index 1



## LAN-to-LAN Profiles:

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

Index	Name	Active	Status	Index	Name	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](#) >>

OK

Cancel

- Mục 1: Common Setting
  - Profile Name: đặt tên profile
  - Chọn Enable this profile
  - Call Direction: chọn Dial-out
  - Chọn Always on

Profile Index : 1

**1. Common Settings**

Profile Name <input type="text" value="to_site_a"/> <input checked="" type="checkbox"/> Enable this profile VPN Dial-Out Through <input type="text" value="WAN1 First"/> Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)	Call Direction <input type="radio"/> Both <input checked="" type="radio"/> Dial-Out <input type="radio"/> Dial-in Tunnel Mode <input type="radio"/> GRE Tunnel <input checked="" type="checkbox"/> Always on Idle Timeout <input type="text" value="-1"/> second(s) <input type="checkbox"/> Enable PING to keep IPsec tunnel alive PING to the IP <input type="text"/>
---	--

- Mục 2: Dial out setting
  - Chọn IPsec Tunnel
  - Server IP/Host Name for VPN: điền địa chỉ IP wan của router Dial in (router site A).
  - Pre-Shared Key: điền key VPN đã cấu hình ở router Dial in
  - IPsec security Method: Chọn High (ESP)

**2. Dial-Out Settings**

Type of Server I am calling <input type="radio"/> PPTP <input checked="" type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy <input type="text" value="None"/> <input type="radio"/> SSL Tunnel  Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) <input type="text" value="172.16.17.10"/> ← điền ip wan của router site A Server Port (for SSL Tunnel): <input type="text" value="443"/>	Username <input type="text" value="???"/> Password(Max 15 char) <input type="text"/> PPP Authentication <input type="text" value="PAP/CHAP/MS-CHAP/MS-CHAPv2"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off  <b>IKE Authentication Method</b> <input checked="" type="radio"/> Pre-Shared Key <input type="text" value="IKE Pre-Shared Key"/> <input type="text" value="....."/> <input type="radio"/> Digital Signature(X.509) Peer ID <input type="text" value="None"/> Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First Local Certificate <input type="text" value="None"/>  <b>IPsec Security Method</b> <input type="radio"/> Medium(AH) <input checked="" type="radio"/> High(ESP) <input type="text" value="3DES without Authentication"/> <input type="button" value="Advanced"/>  Index(1-15) in <u>Schedule</u> Setup: <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>
--	--



- Mục 3: Dial in settings sẽ không cấu hình vì hiện tại đang cấu hình cho Dial out
- Mục 4: GRE setting sẽ không cấu hình
- Mục 5: TCP/IP Network settings
  - Remote Network IP: điền địa lớp mạng của site A. Theo bài lab, ta điền: 192.168.11.0
  - Remote Network Mask: điền subnet mask của lớp mạng bên site A. Theo bài lab, ta điền: 255.255.255.0
  - Local Network IP: điền địa chỉ lớp mạng của site B. Theo bài lab, ta điền: 192.168.12.0
  - Local Network Mask: điền subnet mask của lớp mạng bên site B. Theo bài lab, ta điền: 255.255.255.0
  - Nhấn OK

5. TCP/IP Network Settings	
My WAN IP	0.0.0.0
Remote Gateway IP	0.0.0.0
Remote Network IP	192.168.11.0
Remote Network Mask	255.255.255.0
Local Network IP	192.168.12.0
Local Network Mask	255.255.255.0
<a href="#">More</a>	
RIP Direction	Disable ▼
From first subnet to remote network, you have to do	
	Route ▼
<input type="checkbox"/> IPsec VPN with the Same Subnets	
<input type="checkbox"/> Change default route to this VPN tunnel ( Only single WAN supports this )	
<div> <div>OK</div> <div>Clear</div> <div>Cancel</div> </div>	

#### Kiểm tra kết nối VPN

- Trên router site A và site B: Vào VPN and Remote Access Control >>> Connection Management

- Hiện thị kết nối VPN trên router Dial out

VPN and Remote Access >> Connection Management

---

**Dial-out Tool**

General Mode:	( to_site_a ) 172.16.17.10	Dial
Backup Mode:		Dial
Load Balance Mode:		Dial

**VPN Connection Status**

LAN-to-LAN VPN Status				Remote Dial-in User Status					
VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime	
1 ( to_site_a )	IPsec Tunnel 3DES-No Auth	172.16.17.10 via WAN2	192.168.11.0/24	0	0	2	3	0:0:14	Drop

xxxxxxx : Data is encrypted.  
xxxxxxx : Data isn't encrypted.

- Hiện thị kết nối trên router Dial in

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 ( to_site_b )	IPsec Tunnel 3DES-No Auth	172.16.17.11 via WAN1	192.168.12.0/24	0	0	2	3	0:3:58	Drop

xxxxxxx : Data is encrypted.  
xxxxxxx : Data isn't encrypted.

### e. Cách test

- Kết nối laptop vào mỗi router, và trên laptop trong site A ping hoặc truy cập qua laptop bên site B và ngược lại

### f. Bài Tập

- Cấu hình chia Vlan cho 2 router như sau
  - Router 1:
    - Lan 1: 192.168.10.x/24

- Lan 2: 192.168.11.x/24
- Router 2:
  - Lan 1: 192.168.15.x/24
  - Lan 2: 192.168.16.x/24

- Cấu hình Policy route sao cho:

- Router 1:
  - Lan 2 truy cập internet theo W2
- Router 2:
  - Truy cập trang web Https theo W1

- Cấu hình VPN lan to lan: router 1 (sử dụng lan 1) và router 2 (sử dụng lan 2) để VPN với nhau

- Trên router 1 có 1 server dữ liệu với IP 192.168.10.2

- Cấu hình firewall sao cho:

- Chỉ cho phép IP từ 192.168.16.10 đến 192.168.16.100 được phép truy cập server 192.168.10.2

- Server 192.168.10.2 thì được truy cập toàn bộ máy trong lan 2 của router 2