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

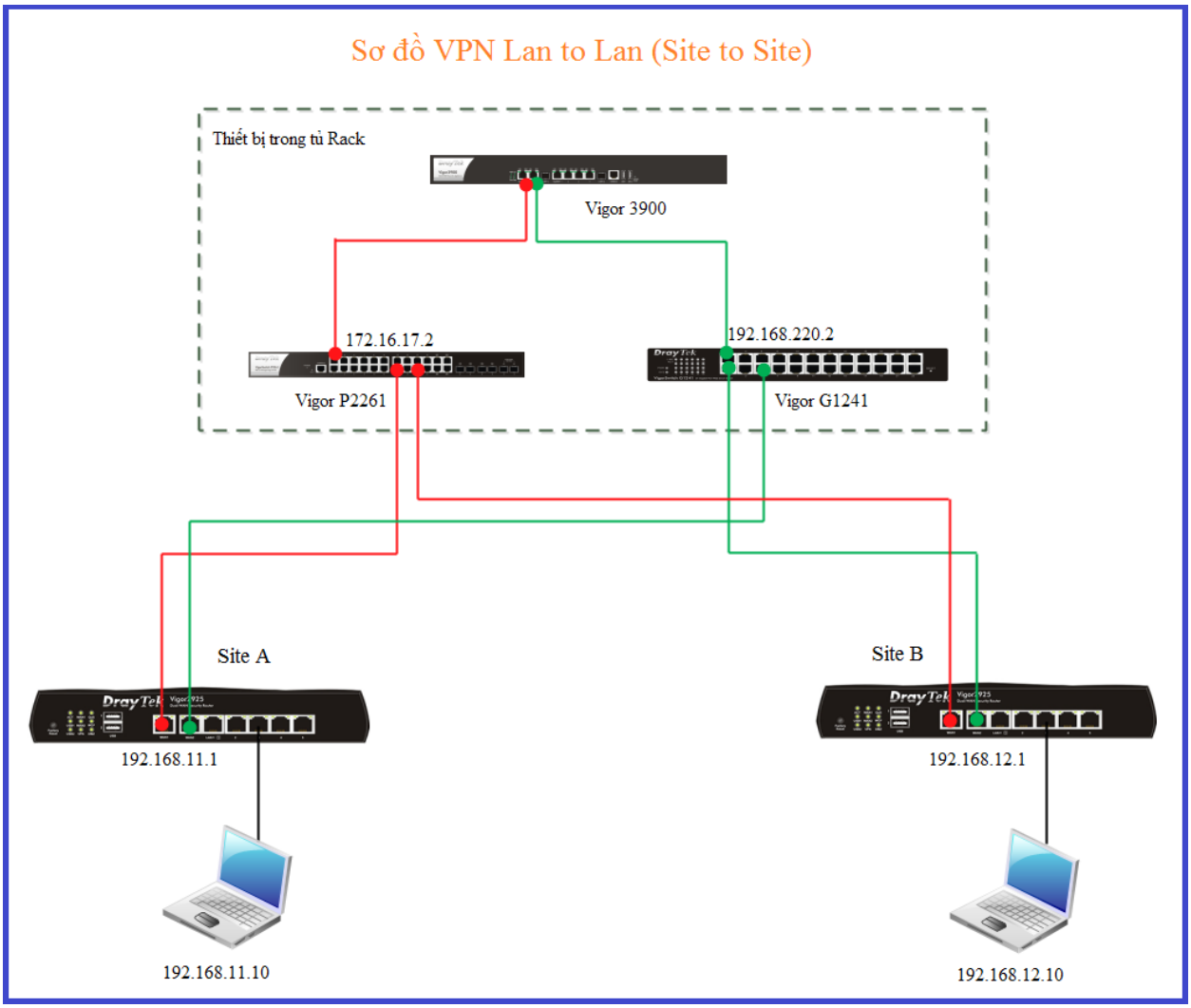
- Nối Wan 1 của router vào cổng bất kì trên switch P2261, nối Wan 2 của router vào cổng bất kì trên switch G1241

- 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

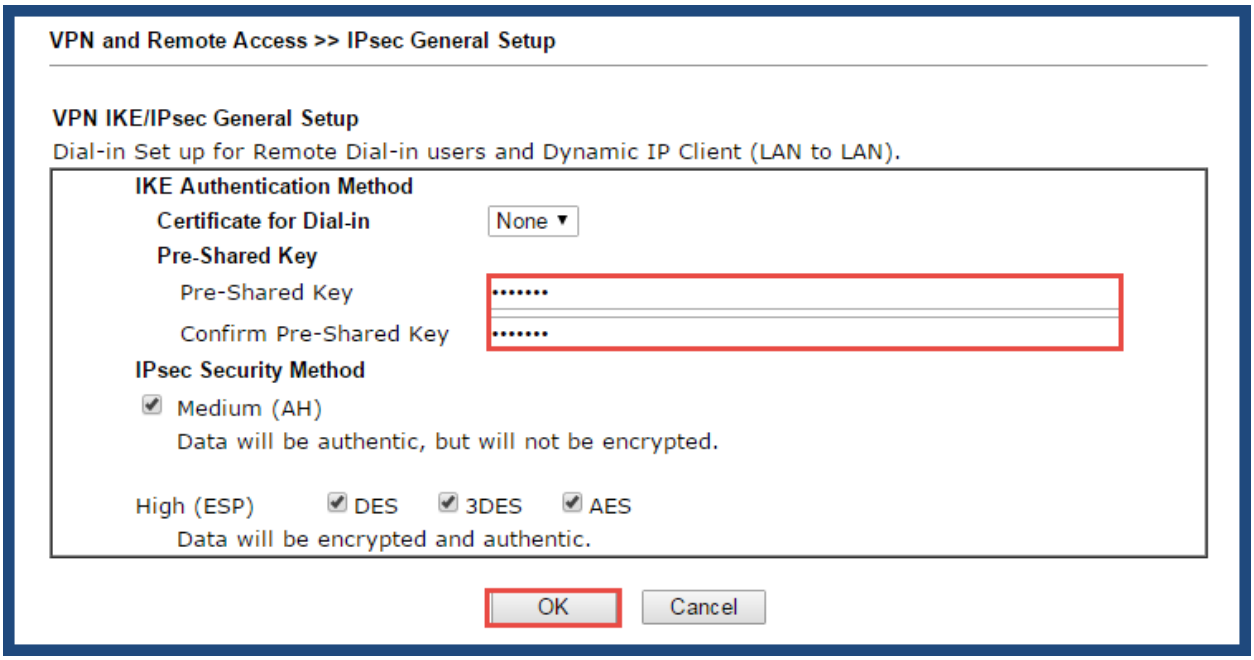
Lưu ý: Do trong môi trường bài Lab nên các bạn có thể lựa chọn router nào làm Dial-in cũng được, nhưng ngoài thực tế thiết bị làm Dial-in nên có IP Wan tĩnh, hoặc sử dụng tên miền động (dynamic DNS)

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

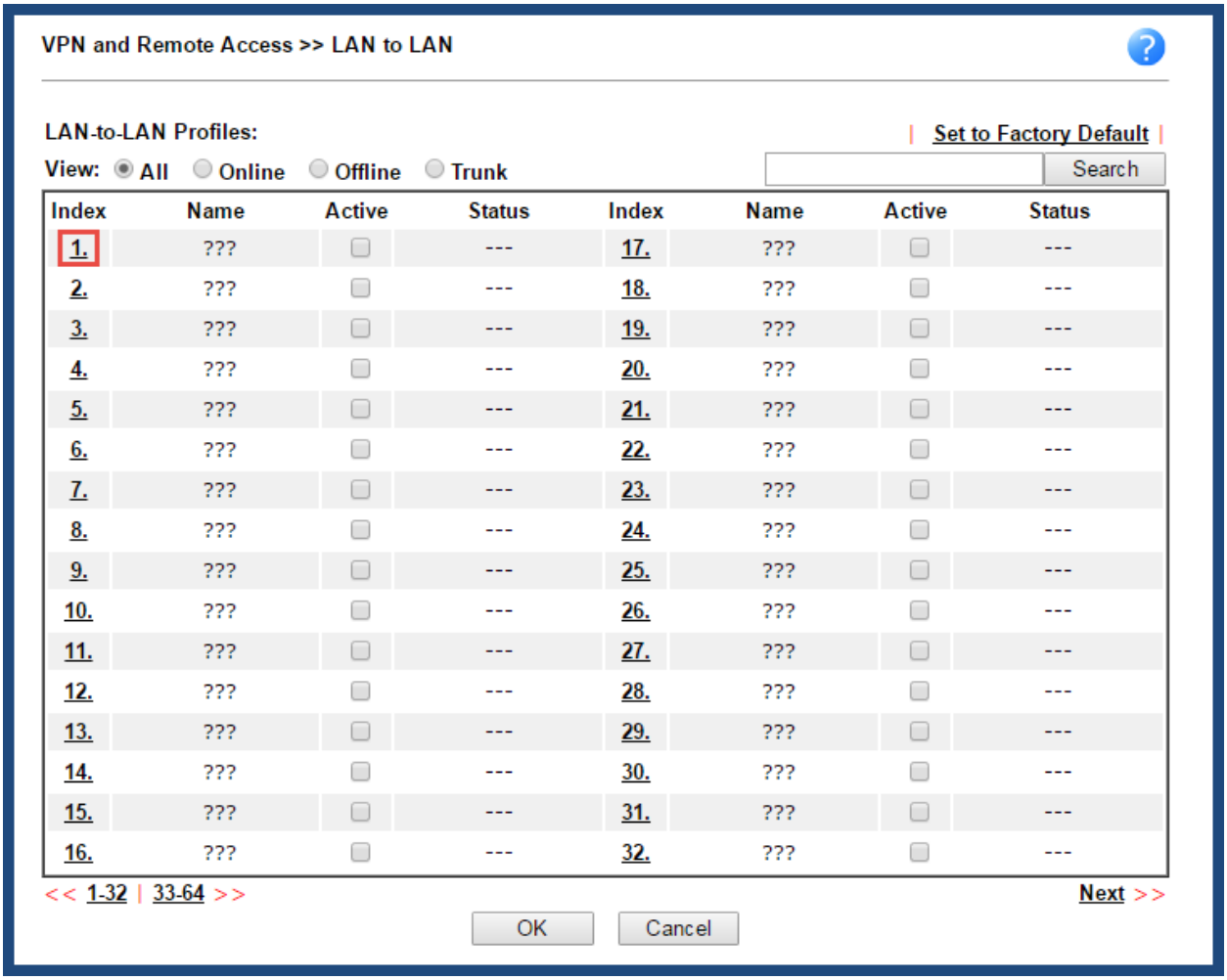
- Cấu hình router site A (Dial-in)

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

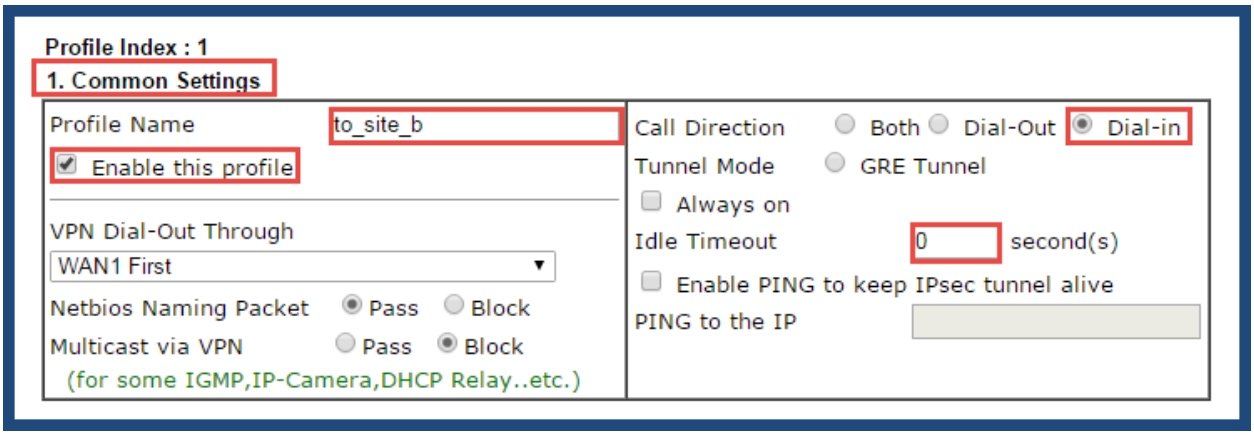
- Pre-Shared Key: điền key VPN
- Confirm Pre-Shared Key: điền lại đúng key đã điền ở Pre-shared Key



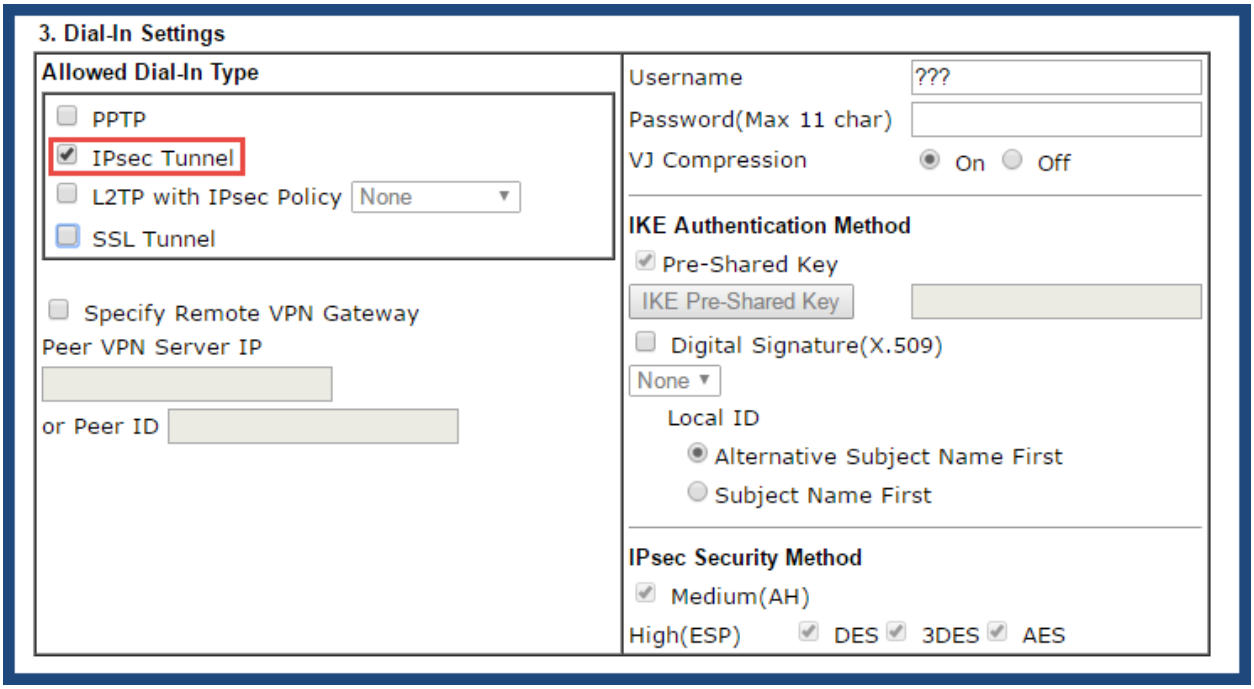
- Cấu hình profile VPN: Vào VPN and Remote Access >>> Lan to Lan >>> chọn Index 1



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

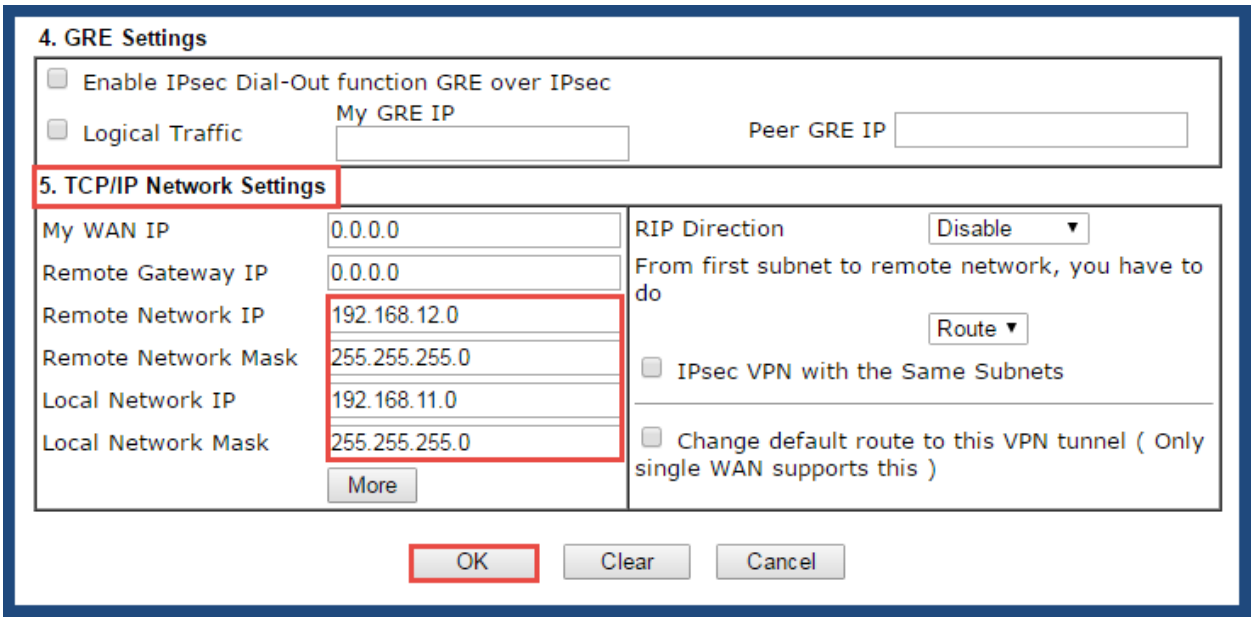


- Mục 2: Dial out settings sẽ không cấu hình vì hiện tại đang cấu hình cho Dial In nên ta chuyển sang mục 3
- Mục 3: Dial-In settings
    - Chọn IPsec Tunnel



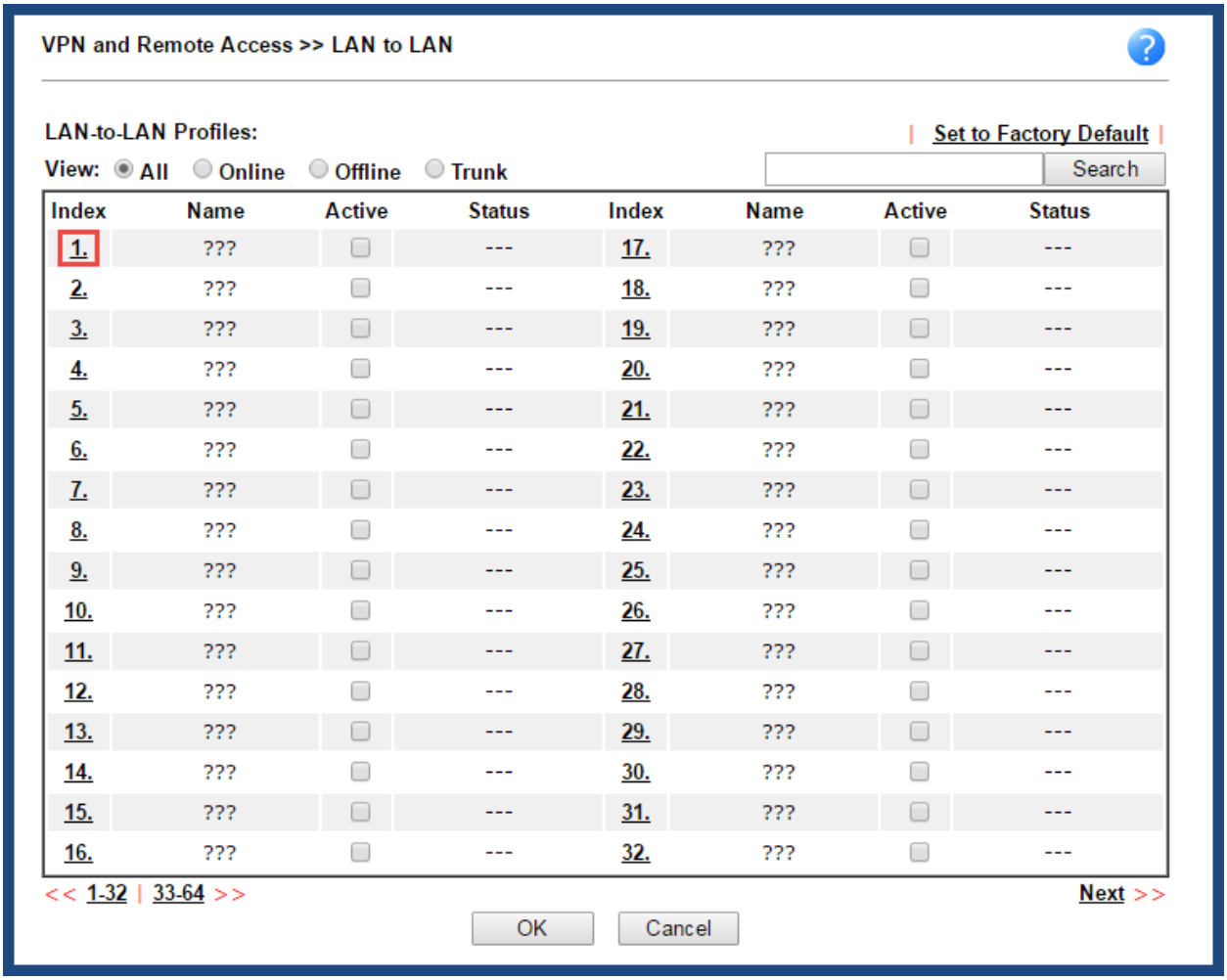
- Mục 4: GRE setting sẽ không cấu hình
- Mục 5: TCP/IP Network settings
    - Remote Network IP: điền địa lớp mạng của site B. Theo bài lab, ta điền: 192.168.12.0
    - Remote Network Mask: điền subnet mask của lớp mạng bên site B. Theo bài lab, ta điền: 255.255.255.0

- 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

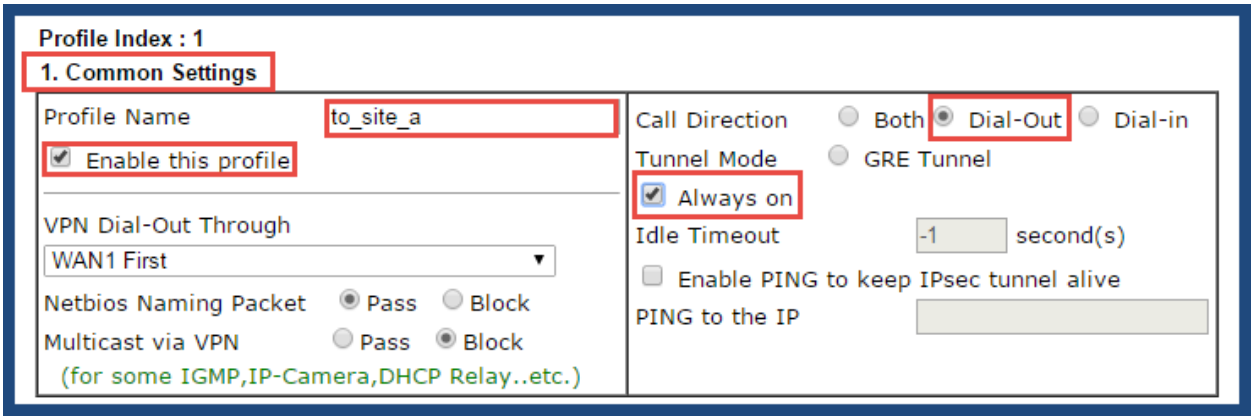


- Cấu hình router site B (Dial-out)

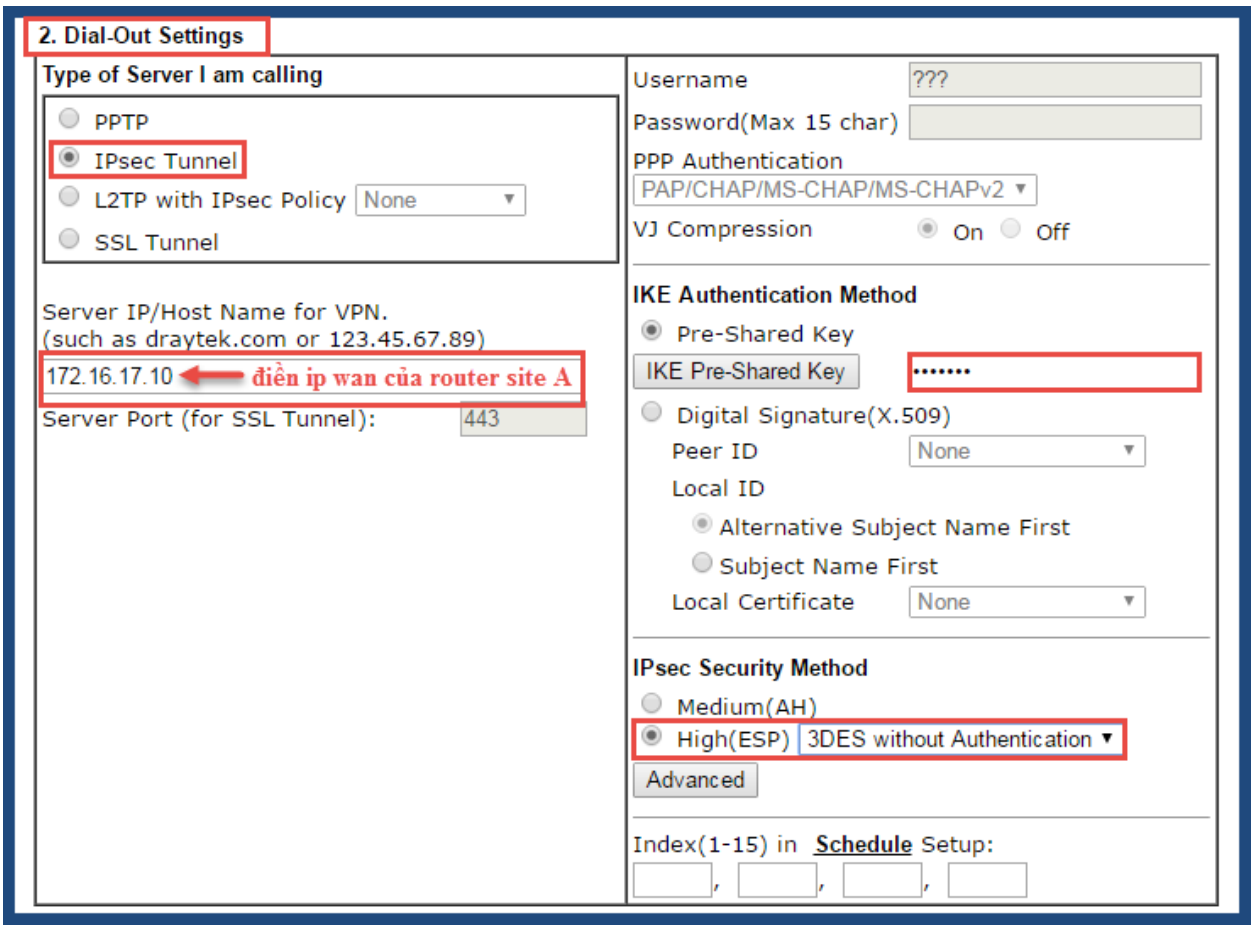
- Cấu hình Profile VPN: Cấu hình profile VPN: Vào VPN and Remote Access >>> Lan to Lan >>> chọn Index 1



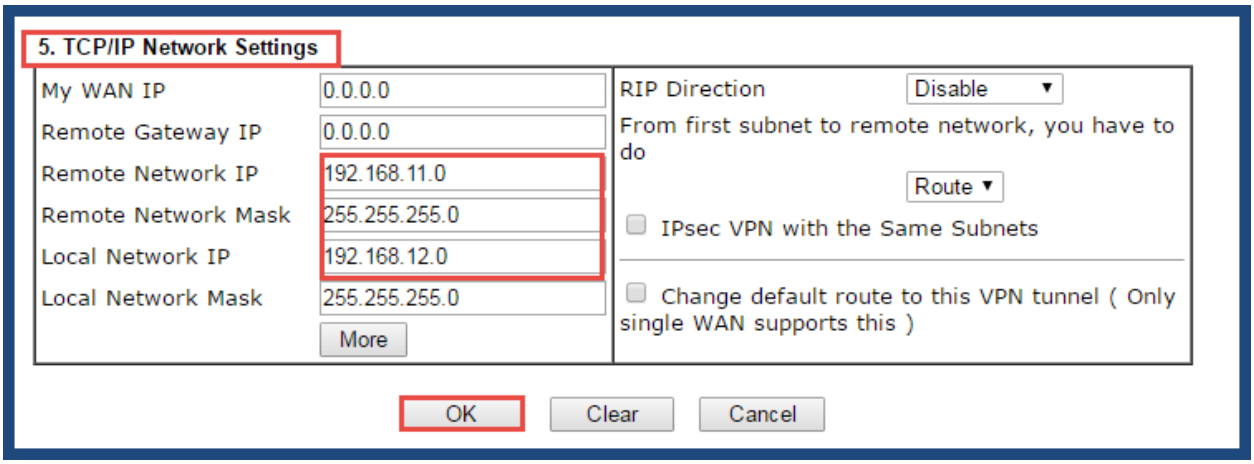
- Mục 1: Common Setting
  - Profile Name: đặt tên profile
  - Chọn Enable this profile
  - Call Direction: chọn Dial-out
  - Chọn Always on



- 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 sercurity Method: Chọn High (ESP)



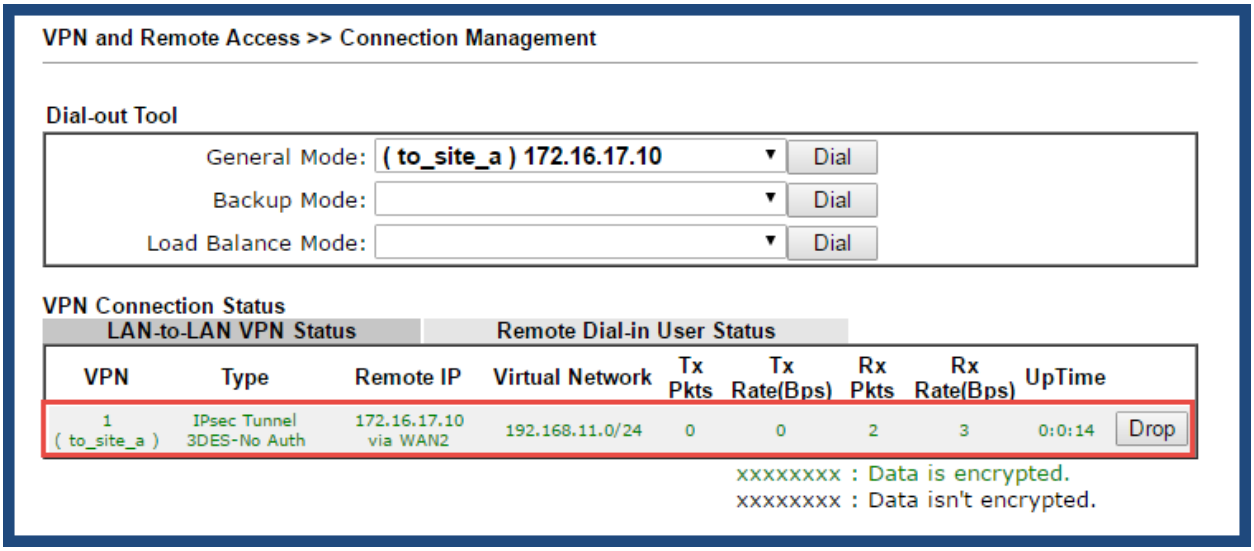
- Mục 3: Dial in settings sẽ không cấu hình vì hiện tại đang cấu hình cho Dial out
- Mục 4: GRE setting sẽ không cấu hình
- Mục 5: TCP/IP Network settings
    - Remote Network IP: điền địa lớp mạng của site A. Theo bài lab, ta điền: 192.168.11.0
    - Remote Network Mask: điền subnet mask của lớp mạng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



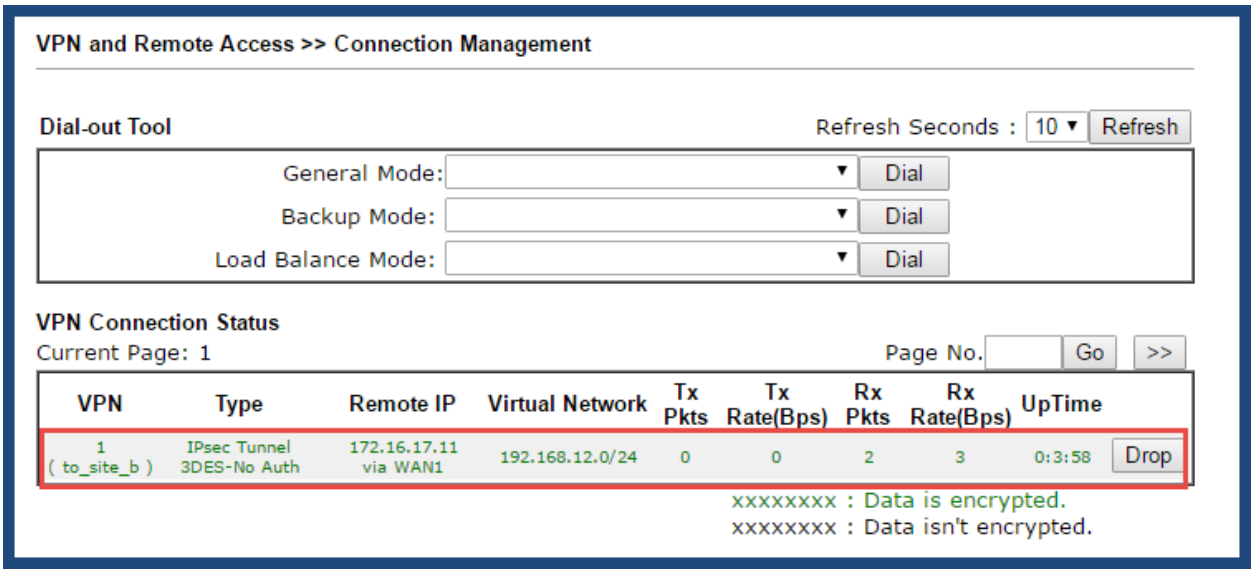
- Kiểm tra kết nối VPN

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

- Hiển thị kết nối VPN trên router Dial out



- Hiển thị kết nối trên router Dial in



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