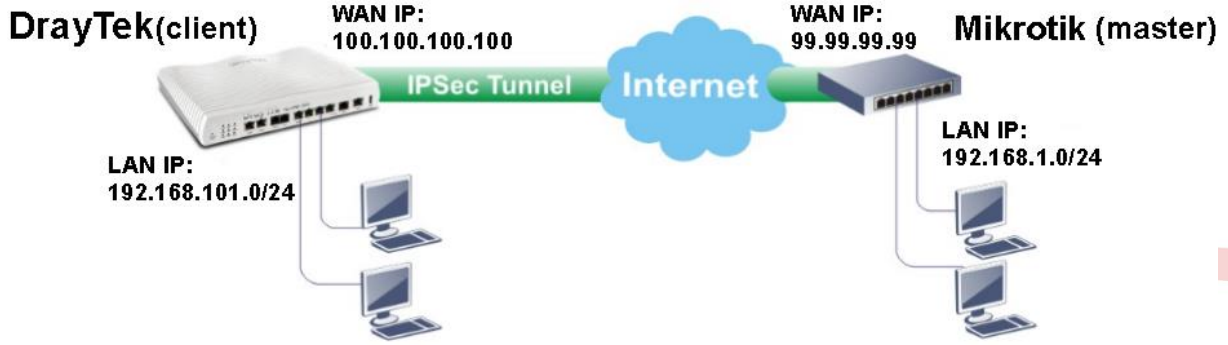


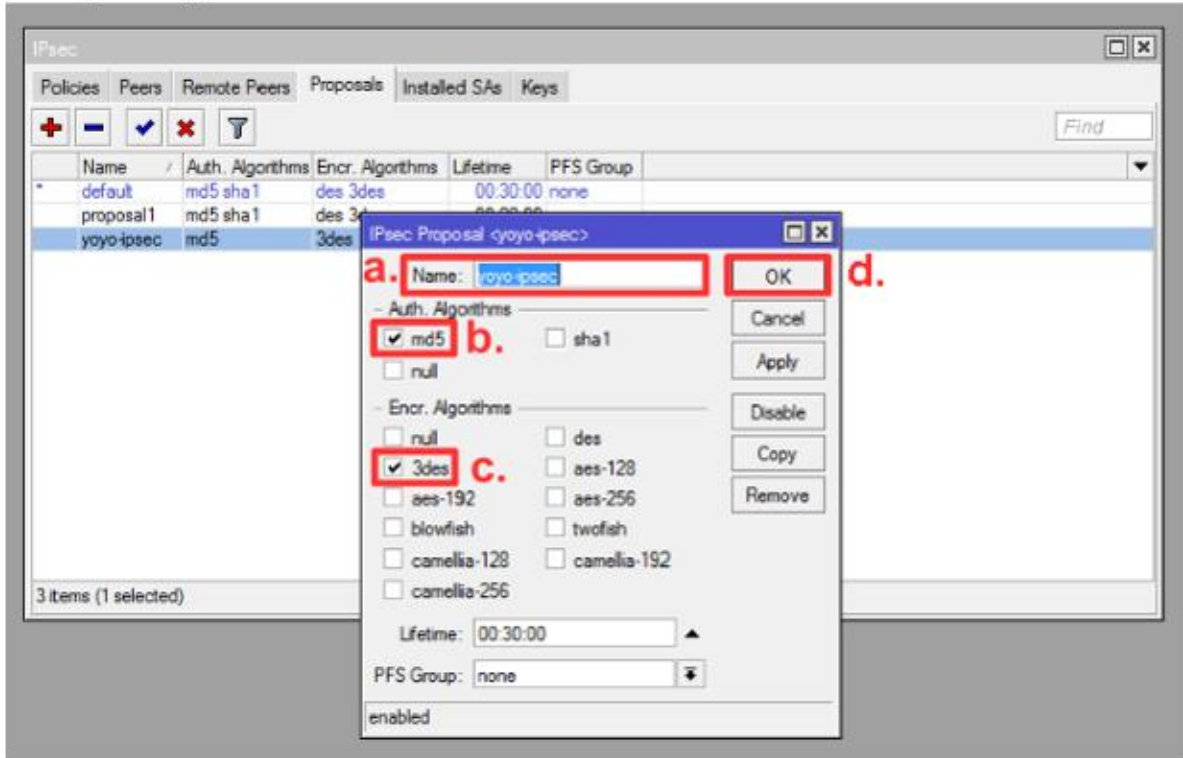
MIKROTIK VE VIGOR ROUTER ARASINDA IPSEC VPN

Bu makale, bir Mikrotik router ve bir DrayTek Vigor Router arasında IPsec LAN to LAN ayarlarının nasıl yapıldığını göstermektedir.



Mikrotik Router Yapılandırması

1. Yeni bir IPsec Proposal oluşturun: **IPsec >> Proposal**'a gidin ve yeni bir tane ekleyin.
 - a. **Name** girin.
 - b. Auth. Algorithms için **md5** seçin.
 - c. Encr. Algorithms için **3des** seçin.
 - d. Konfigürasyonu kaydetmek için **OK**'a tıklayın.



2. Peer yapılandırması: **IPsec >> Peer**'e gidin ve yeni bir tane ekleyin.
 - a. **Address** için DrayTek'in WAN IP'sini girin.
 - b. **Pre shared key** için Auth. Method seçeneğini seçin ve **Secret** girin.
 - c. Hash Algorithm'e **md5**, Encryption Algorithm'e **3des** girin.
 - d. Konfigürasyonu kaydetmek için **OK**'a tıklayın.

3. Policy yapılandırması: **IPsec >> Policy**'e gidin ve yeni bir tane ekleyin. General sekmesinde:
- Src. Address** için Mikrotik'in LAN IP'sini girin.
 - Dst. Address** için DrayTek'in LAN IP'sini girin.

4. Action sekmesinde:
- Tunnel**'i işaretleyin.
 - SA Src. Address** için Mikrotik'in WAN IP'sini girin.
 - SA Dst. Address** için DrayTek'in WAN IP'sini girin.
 - Proposal** için daha önce oluşturduğumuz Proposal'ı seçin.

- g. Konfigürasyonu kaydetmek için **OK**'a tıklayın.

5. NAT yapılandırması: **Firewall** >> **NAT**'a gidin ve yeni bir kural ekleyin. (Not: Bu kural NAT Rules'da ilk kural olmalıdır.) General sekmesinde,
- Chain için **srcnat** seçeneğini seçin.
 - Hedef networkünüzün aralığını **Dst. Address**'e girin.
 - Out. Interface** için WAN Interface'inizi girin burada ether1'i kullanıyoruz.

6. Action sekmesinde:
- Action'ı **accept** olarak ayarlayın.
 - Konfigürasyonu kaydetmek için **OK**'a tıklayın.

Vigor Router Yapılandırması

1. LAN to LAN profil oluşturun: **VPN and Remote Access >> LAN to LAN** sayfasına gidin. Profil eklemek için bir indexe tıklayın.
 - a. Profil adı girin ve **Enable this profile**'ı etkinleştirin.
 - b. Call Direction için **Dial-out** seçeneğini seçin.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

a. Profile Name Enable this profile

Call Direction Both Dial-Out Dial-in

Always on

Idle Timeout second(s)

Enable PING to keep alive

PING to the IP

VPN Dial-Out Through

Netbios Naming Packet Pass Block

Multicast via VPN Pass Block
(for some IGMP,IP-Camera,DHCP Relay..etc.)

2. Dial-Out Settings'de:

- c. Type of Sever I am calling için IPsec Tunnel seçeneğini seçin.
- d. Mikrotik Server'ın IP veya Hostname 'ini girin.
- e. IKE Authentication Method için **Pre-Shared Key**'i seçin ve key girin.
- f. IPSEC Security Method için **High(ESP)** seçeneğinde **3DES with Authentication** seçeneğini seçin.
- g. Gelişmiş ayarlar için **Advanced**'a tıklayın.

2. Dial-Out Settings

Type of Server I am calling

PPTP

c. IPsec Tunnel

L2TP with IPsec Policy

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)

d.

Username Password(Max 15 char)

PPP Authentication

VJ Compression On Off

IKE Authentication Method

e. Pre-Shared Key

IKE Pre-Shared Key

Digital Signature(X.509)

Peer ID

Local ID

Alternative Subject Name First

Subject Name First

Local Certificate

IPsec Security Method

Medium(AH)

f. High(ESP)

g.

Index(1-15) in **Schedule** Setup:

, , ,

3. IKE Advanced settings'de: IKE Phase 2 proposal için **3DES_MD5** ayarlayın ve **OK**'a tıklayın.
4. TCP/IP Network Settings'de:
 - a. **Remote Network IP**'ye Mikrotik'in LAN IP'sini girin.
 - b. Konfigürasyonu kaydetmek için **OK**'a tıklayın.

IKE advanced settings

IKE phase 1 mode: Main mode Aggressive mode

IKE phase 1 proposal: Auto

IKE phase 2 proposal: **3DES_MD5**

IKE phase 1 key lifetime: 28800 (800 ~ 38400)

IKE phase 2 key lifetime: 3600 (500 ~ 3600)

Perfect Forward Secret: Disable Enable

Local ID:

Note: If you select 'Auto' in IKE phase 1 proposal, the router will send the following proposals to negotiate with the remote site. The proposals include: DES_(MD5/SHA)_G1, 3DES_MD5_G1, 3DES_MD5_G2, 3DES_(MD5/SHA)_G5, AES128_MD5_(G2/G5), AES256_SHA_(G2/G5), AES256_SHA_G14

OK Close

Yukarıdaki konfigürasyondan sonra, VPN otomatik olarak kurulacaktır. VPN bağlantısı durumunu kontrol etmek için, **VPN and Remote Access >> Connection Management** sayfasına gidin.

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Seconds : 10 Refresh

General Mode: **(IPsec-out) 99.99.99.99** Dial

Backup Mode: Dial

Load Balance Mode: Dial

VPN Connection Status Page No. Go >>

Current Page: 1

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime
1 (IPsec-out)	IPsec Tunnel 3DES-MD5 Auth	99.99.99.99 via WAN1	192.168.1.0/24	1779	7	1929	3	1:55:39 Drop