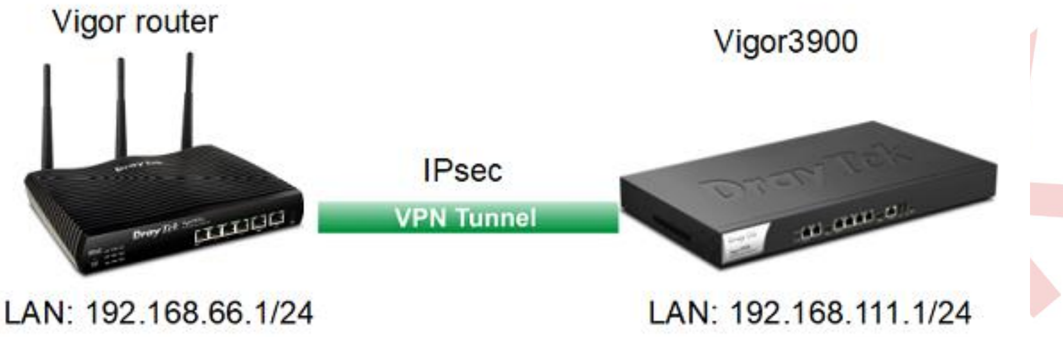
DRAYOS ROUTER VE VIGOR3900/VIGOR2960 ARASINDA IPSEC VPN

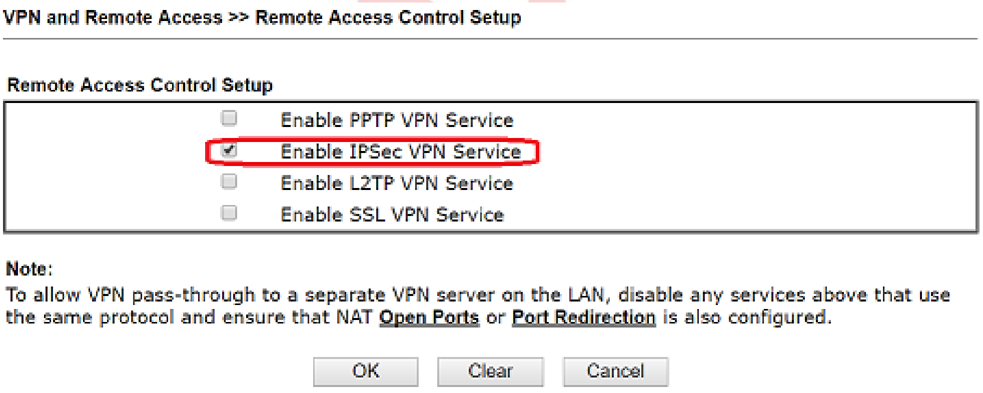
Bu makale, bir DrayOS router ile Vigor3900 / 2960 arasındaki LAN to LAN IPsec VPN'i göstermektedir. Ağ topolojisi aşağıda gösterilmiştir. Bunlardan birini VPN sunucusu olarak kullanırken, DrayOS Router ve Vigor3900 / 2960 arasında IPsec VPN bağlantısının nasıl kurulacağını göstermek için bu makaleyi iki bölüme ayırdık.



Bölüm A: DrayOS Router'ı VPN sunucusu olarak alın

DrayOS Dial-In ayarları

1. IPsec Service'nin etkin olup olmadığını **VPN and Remote Access** >> **Remote Access Control** sayfasından kontrol edin.



VPN and Remote Access >> Remote Access Control Setup

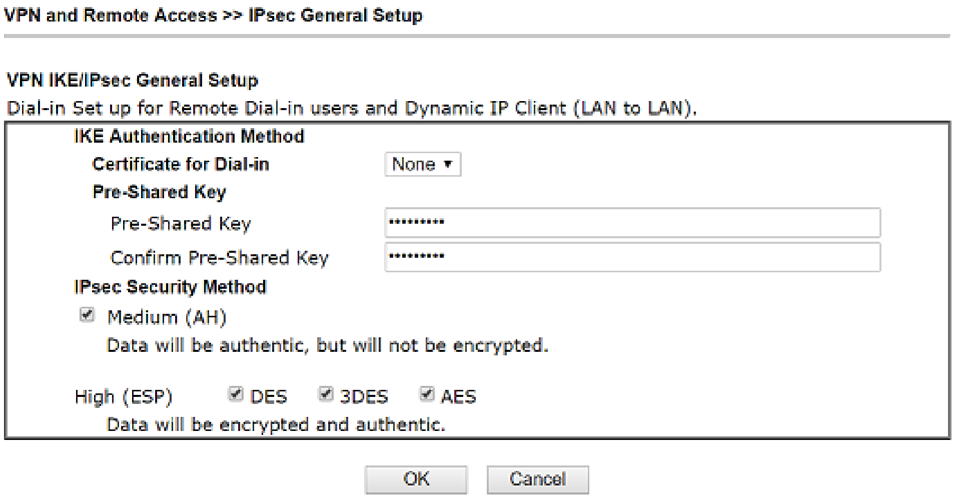
Remote Access Control Setup

☐ Enable PPTP VPN Service
☑ Enable IPSec VPN Service
☐ Enable L2TP VPN Service
☐ Enable SSL VPN Service

Note:
To allow VPN pass-through to a separate VPN server on the LAN, disable any services above that use the same protocol and ensure that NAT Open Ports or Port Redirection is also configured.

OK Clear Cancel

2. **VPN and Remote Access Control** >> **IPsec General Setup** sayfasına gidin. **Pre-Shared Key** girin ve kaydetmek için **OK**'a tıklayın.



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).

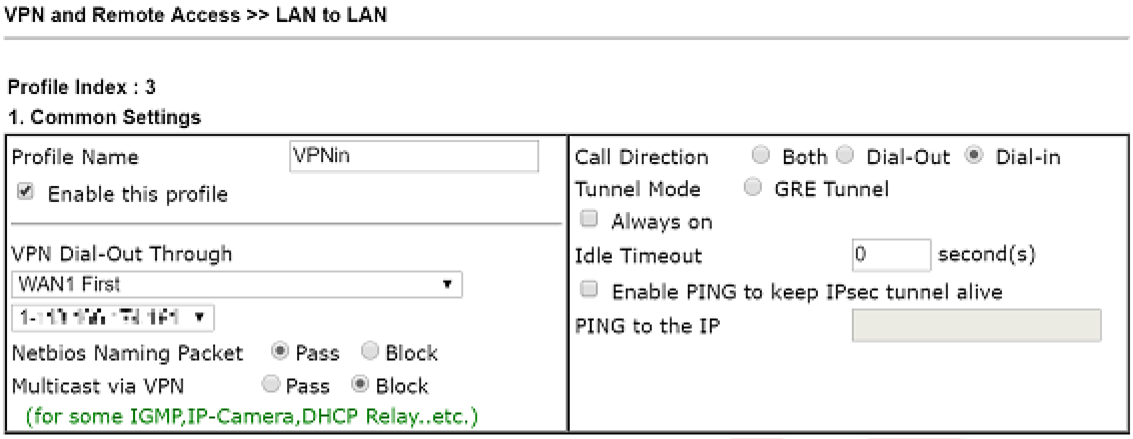
IKE Authentication Method
Certificate for Dial-in: None ▾
Pre-Shared Key
Pre-Shared Key: •••••••••
Confirm Pre-Shared Key: •••••••••

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

3. **VPN and Remote Access Control** >> **LAN to LAN** sayfasına gidin. Ve uygun bir indexe tıklayın. Common Settings'de:
   a. **Profile name** girin.
   b. Profili etkinleştirin.
   c. **Call Direction** için "Dial-in" seçeneğini seçin.



VPN and Remote Access >> LAN to LAN

Profile Index : 3

1. Common Settings

Profile Name: VPNin

☑ Enable this profile

VPN Dial-Out Through: WAN1 First ▾

[redacted] ▾

Netbios Naming Packet: ● Pass ○ Block

Multicast via VPN: ○ Pass ● Block

(for some IGMP,IP-Camera,DHCP Relay..etc.)

Call Direction: ○ Both ○ Dial-Out ● Dial-in

Tunnel Mode: ○ GRE Tunnel

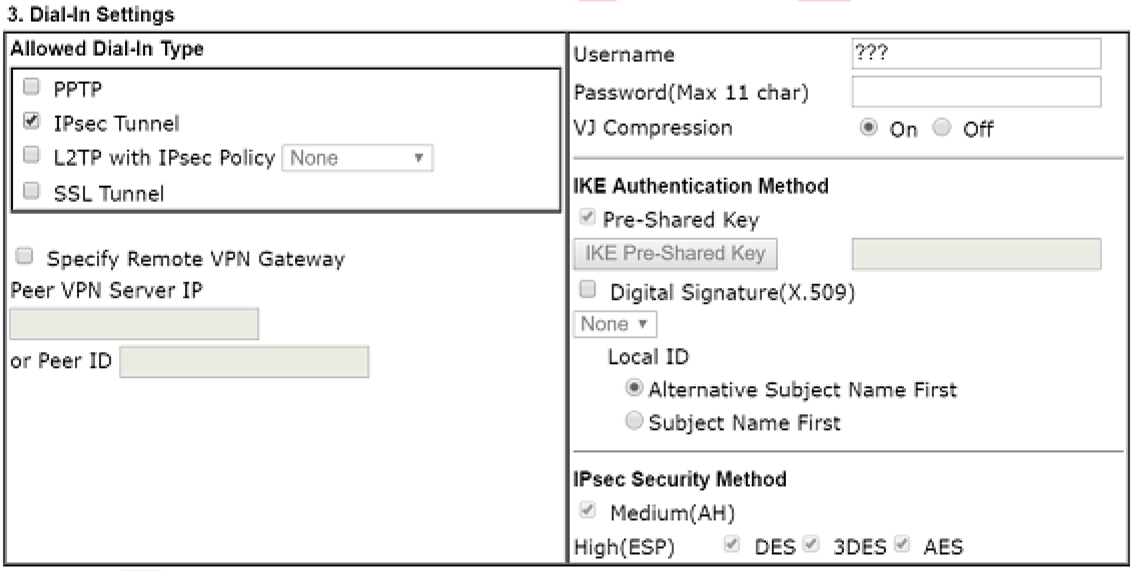
□ Always on

Idle Timeout: 0 second(s)

□ Enable PING to keep IPsec tunnel alive

PING to the IP:

4. Dial-In Settings'de **IPsec** aramaya izin verin.



3. Dial-In Settings

Allowed Dial-In Type

□ PPTP

☑ IPsec Tunnel

□ L2TP with IPsec Policy: None ▾

□ SSL Tunnel

□ Specify Remote VPN Gateway

Peer VPN Server IP:

or Peer ID:

Username: ???

Password(Max 11 char):

VJ Compression: ● On ○ Off

IKE Authentication Method

☑ Pre-Shared Key

IKE Pre-Shared Key

□ Digital Signature(X.509)

None ▾

Local ID

● Alternative Subject Name First

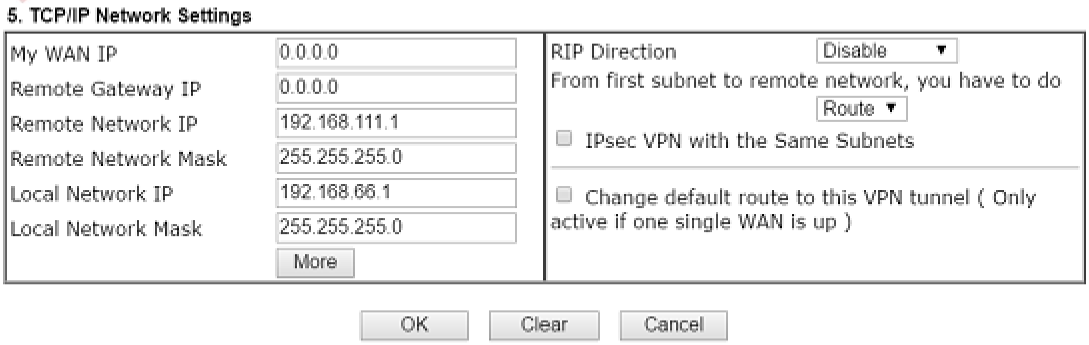
○ Subject Name First

IPsec Security Method

☑ Medium(AH)

High(ESP): ☑ DES ☑ 3DES ☑ AES

5. TCP/IP Network Settings'de **Remote Network IP/Mask**'da Vigor Router'ın LAN'ını girin. Ardından **OK**'a tıklayın.



5. TCP/IP Network Settings

My WAN IP	0.0.0.0
Remote Gateway IP	0.0.0.0
Remote Network IP	192.168.111.1
Remote Network Mask	255.255.255.0
Local Network IP	192.168.66.1
Local Network Mask	255.255.255.0

More

RIP Direction: Disable ▾

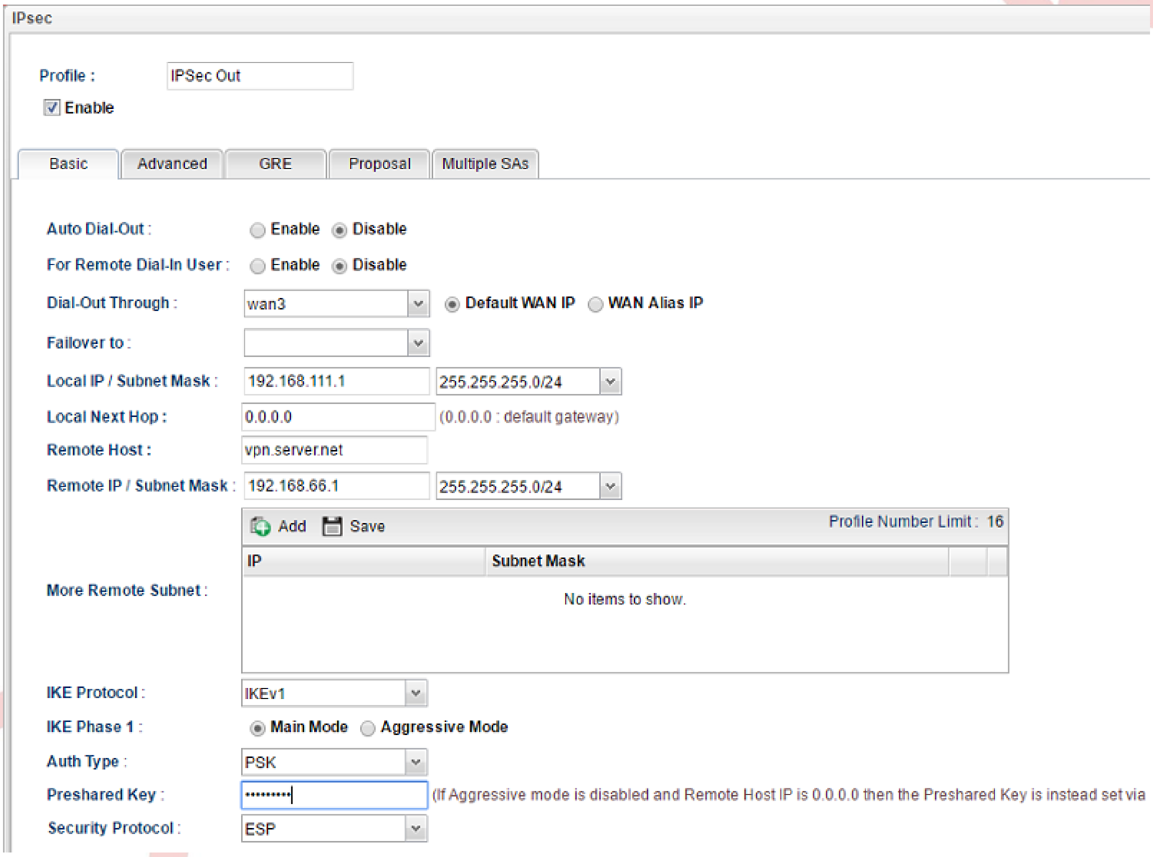
From first subnet to remote network, you have to do: Route ▾

□ IPsec VPN with the Same Subnets

□ Change default route to this VPN tunnel (Only active if one single WAN is up)

Vigor3900 Dial-out Ayarları

6. **VPN and Remote Access >> VPN Profiles** sayfasına gidin. IPsec sekmesinde **Add**’e tıklayın. Common Settings’de:
   a. **Profile name** girin ve profili etkinleştirin.
   b. **Dial Out** için kullanılan **WAN interface’**yi seçin.
   c. **Local IP/Subnet Mask’**da Vigor300’ün LAN’ını girin.
   d. **Server IP/Host Name**’de DrayOS Router’ın WAN IP’si ya da domain adını girin.
   e. **Remote IP/Subnet Mask**’da DrayOS Router’ın LAN’ını girin.
   f. 2.adımda girilen **Preshared Key** değerini girin.
   g. **Apply**’a tıklayın.


IPsec

Profile : IPSec Out

☑ Enable

Auto Dial-Out : ○ Enable ● Disable

For Remote Dial-In User : ○ Enable ● Disable

Dial-Out Through : wan3 ● Default WAN IP ○ WAN Alias IP

Failover to :

Local IP / Subnet Mask : 192.168.111.1 255.255.255.0/24

Local Next Hop : 0.0.0.0 (0.0.0.0 : default gateway)

Remote Host : vpn.server.net

Remote IP / Subnet Mask : 192.168.66.1 255.255.255.0/24

More Remote Subnet :

Profile Number Limit : 16

IP	Subnet Mask

No items to show.

IKE Protocol : IKEv1

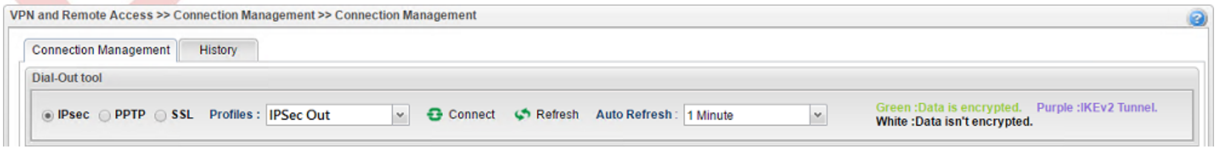
IKE Phase 1 : ● Main Mode ○ Aggressive Mode

Auth Type : PSK

Preshared Key : ••••••••• (If Aggressive mode is disabled and Remote Host IP is 0.0.0.0 then the Preshared Key is instead set via

Security Protocol : ESP

Şimdi VPN’i aramak için **VPN and Remote Access >> Connection Management** sayfasına gidebiliriz.


VPN and Remote Access >> Connection Management >> Connection Management

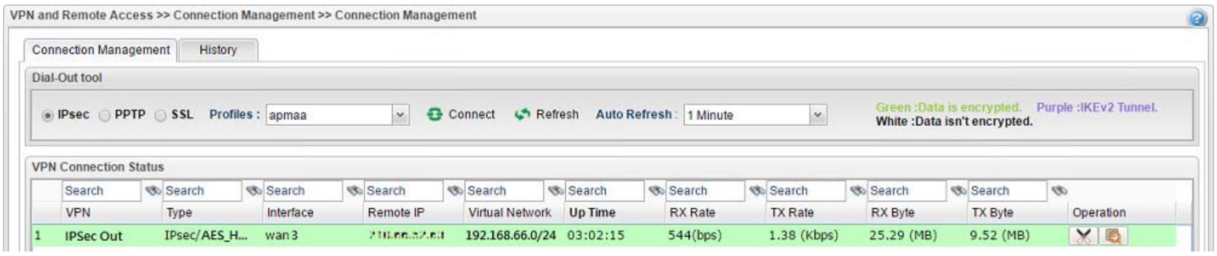
Dial-Out tool

● IPsec ○ PPTP ○ SSL Profiles : IPSec Out

Auto Refresh : 1 Minute

Green :Data is encrypted. Purple :IKEv2 Tunnel.
White :Data isn't encrypted.

VPN başarıyla bağlandıktan sonra, aşağıdaki durumu görebiliriz.


VPN and Remote Access >> Connection Management >> Connection Management

Dial-Out tool

● IPsec ○ PPTP ○ SSL Profiles : apmaa

Auto Refresh : 1 Minute

Green :Data is encrypted. Purple :IKEv2 Tunnel.
White :Data isn't encrypted.

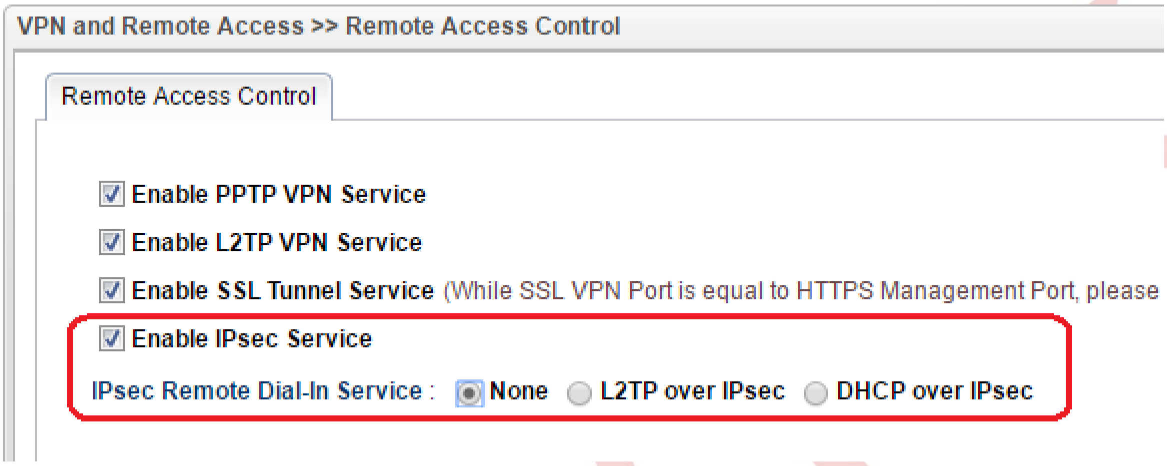
VPN Connection Status

	VPN	Type	Interface	Remote IP	Virtual Network	Up Time	RX Rate	TX Rate	RX Byte	TX Byte	Operation
	Search	Search	Search	Search	Search	Search	Search	Search	Search	Search	
1	IPSec Out	IPsec/AES_H...	wan3	[redacted]	192.168.66.0/24	03:02:15	544(bps)	1.38 (Kbps)	25.29 (MB)	9.52 (MB)	

Bölüm B: Vigor3900'ü VPN Server olarak alın

Vigor3900 Dial-in Ayarları

1. IPsec Service'nin etkin olup olmadığını **VPN and Remote Access** >> **Remote Access Control** sayfasından kontrol edin.



VPN and Remote Access >> Remote Access Control

Remote Access Control

☑ Enable PPTP VPN Service

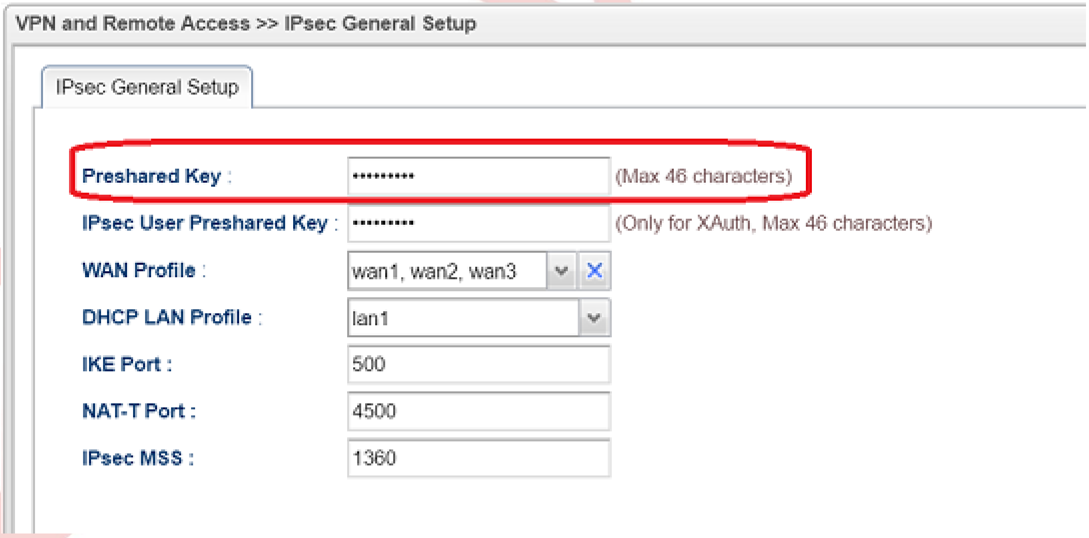
☑ Enable L2TP VPN Service

☑ Enable SSL Tunnel Service (While SSL VPN Port is equal to HTTPS Management Port, please

☑ Enable IPsec Service

IPsec Remote Dial-In Service : ● None ○ L2TP over IPsec ○ DHCP over IPsec

2. **VPN and Remote Access Control** >> **IPsec General Setup** sayfasına gidin**. Pre-Shared Key** girin ve kaydetmek için OK'a tıklayın.

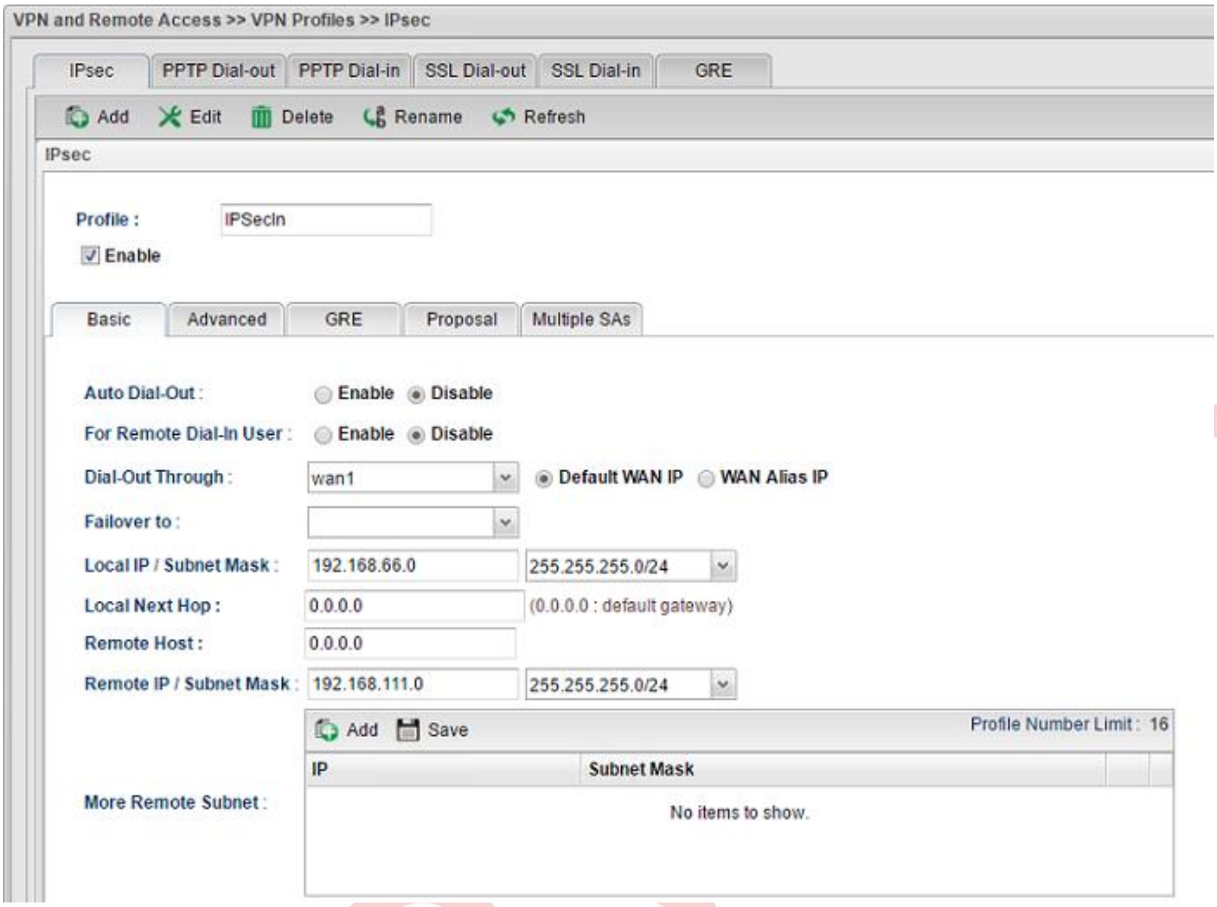


VPN and Remote Access >> IPsec General Setup

IPsec General Setup

Preshared Key :	••••••••••	(Max 46 characters)
IPsec User Preshared Key :	•••••••••	(Only for XAuth, Max 46 characters)
WAN Profile :	wan1, wan2, wan3	
DHCP LAN Profile :	lan1	
IKE Port :	500	
NAT-T Port :	4500	
IPsec MSS :	1360	

3. **VPN and Remote Access** >> **VPN Profiles** sayfasına gidin. IPsec sekmesinde **Add'**e tıklayın.
   a. **Profile name** girin ve profili etkinleştirin.
   b. **Local IP/Subnet Mask**'da Vigor300'ün LAN'ını girin.
   c. **Remote IP/Subnet Mask**'da DrayOS Router'ın LAN'ını girin.
   d. **Apply**'a tıklayın.



VPN and Remote Access >> VPN Profiles >> IPsec

IPsec

Profile : IPSecIn

☑ Enable

Auto Dial-Out : ○ Enable ● Disable

For Remote Dial-In User : ○ Enable ● Disable

Dial-Out Through : wan1 ● Default WAN IP ○ WAN Alias IP

Failover to :

Local IP / Subnet Mask : 192.168.66.0 255.255.255.0/24

Local Next Hop : 0.0.0.0 (0.0.0.0 : default gateway)

Remote Host : 0.0.0.0

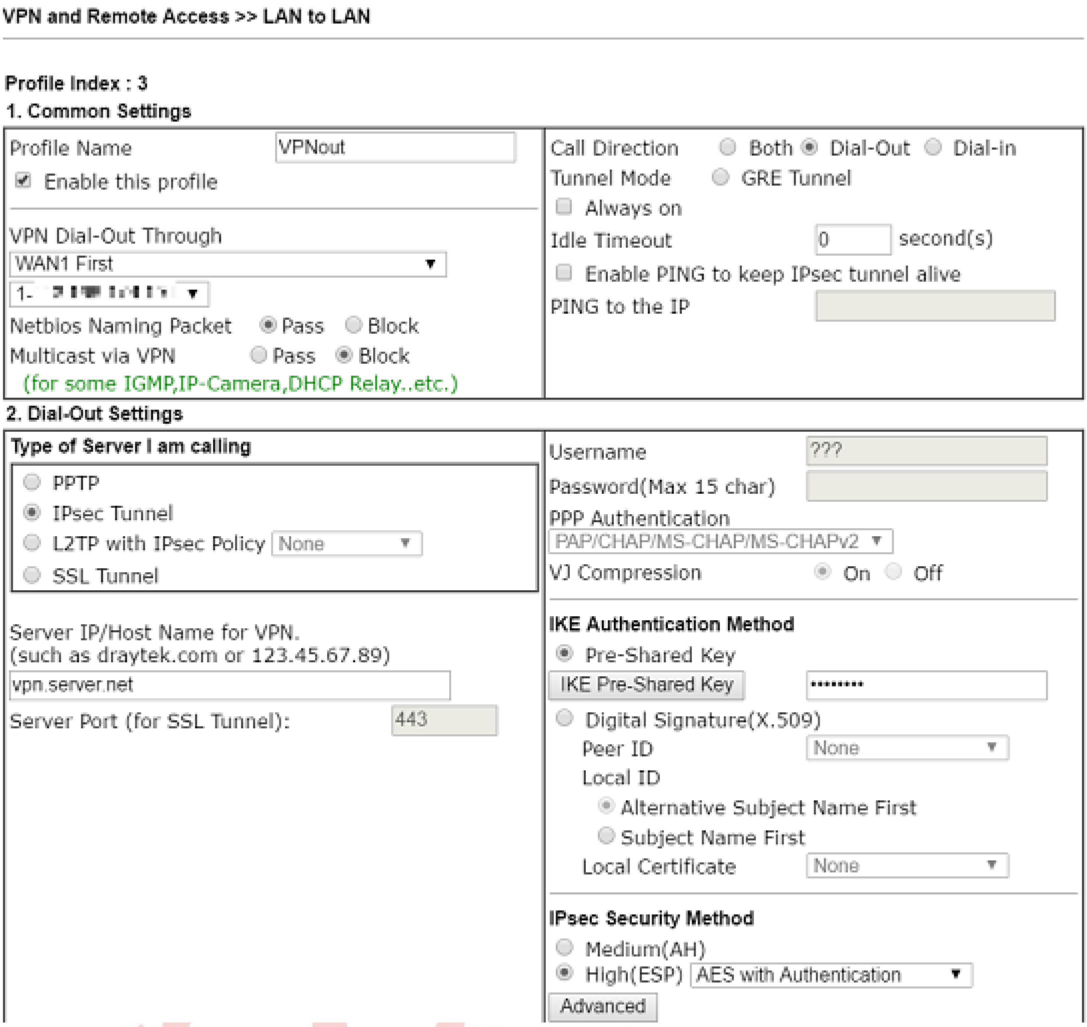
Remote IP / Subnet Mask : 192.168.111.0 255.255.255.0/24

More Remote Subnet : Profile Number Limit : 16

IP	Subnet Mask
No items to show.	

DrayOS Router Dial-Out Ayarları

4. **VPN and Remote Access Control** >> **LAN to LAN** sayfasına gidin. Ve uygun bir indexe tıklayın.
    a. **Profile name** girin ve profili etkinleştirin.
    b. **Call Direction** için “Dial-Out” seçeneğini seçin.
    c. Dial-Out settings’de **dial-out type**’ı IPsec olarak seçin.
    d. **Server IP/Host Name**’de Vigor3900’ün WAN IP’sini veya domain adını girin.
    e. 2.adımda girilen **Preshared Key**’e girin.
    f. **IPSec Security Method** için High(ESP)’de AES with Authentication seçeneğini seçin.



VPN and Remote Access >> LAN to LAN

Profile Index : 3

1. Common Settings

Profile Name: VPNout
☑ Enable this profile

VPN Dial-Out Through
WAN1 First ▼
1- [redacted] ▼

Netbios Naming Packet ● Pass ○ Block
Multicast via VPN ○ Pass ● Block
(for some IGMP,IP-Camera,DHCP Relay..etc.)

Call Direction ○ Both ● Dial-Out ○ Dial-in
Tunnel Mode ○ GRE Tunnel
□ Always on
Idle Timeout: 0 second(s)
□ Enable PING to keep IPsec tunnel alive
PING to the IP:

2. Dial-Out Settings

Type of Server I am calling
○ PPTP
● IPsec Tunnel
○ L2TP with IPsec Policy: None ▼
○ SSL Tunnel

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

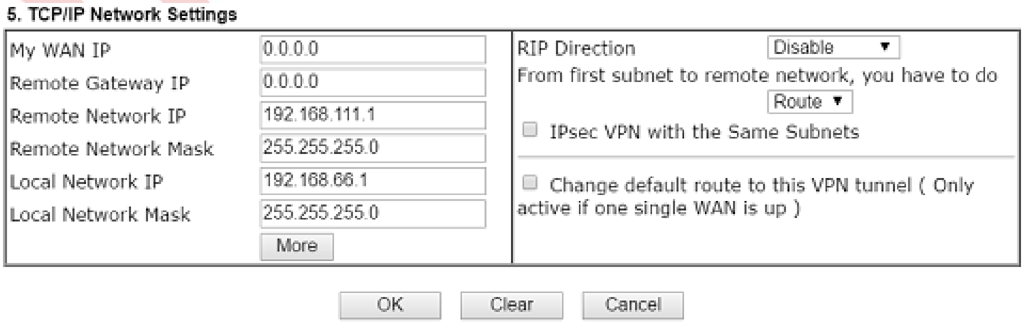
Server Port (for SSL Tunnel): 443

Username: ???
Password(Max 15 char):
PPP Authentication: PAP/CHAP/MS-CHAP/MS-CHAPv2 ▼
VJ Compression ● On ○ Off

IKE Authentication Method
● Pre-Shared Key
IKE Pre-Shared Key: ••••••••
○ Digital Signature(X.509)
Peer ID: None ▼
Local ID
● Alternative Subject Name First
○ Subject Name First
Local Certificate: None ▼

IPsec Security Method
○ Medium(AH)
● High(ESP): AES with Authentication ▼
Advanced

1. TCP/IP Network Settings'de **Remote Network IP/Mask**'da Vigor3900'üz LAN'ını girin. Ardından **OK**'a tıklayın.



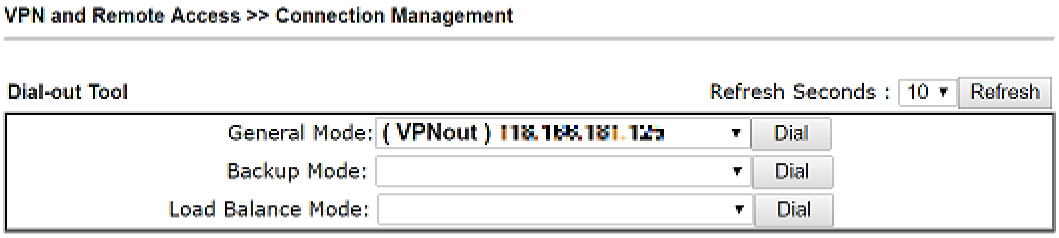
5. TCP/IP Network Settings

My WAN IP: 0.0.0.0
Remote Gateway IP: 0.0.0.0
Remote Network IP: 192.168.111.1
Remote Network Mask: 255.255.255.0
Local Network IP: 192.168.66.1
Local Network Mask: 255.255.255.0
More

RIP Direction: Disable ▼
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 active if one single WAN is up)

OK Clear Cancel

Şimdi VPN'i aramak için **VPN and Remote Access** >> **Connection Management** sayfasına gidebiliriz.



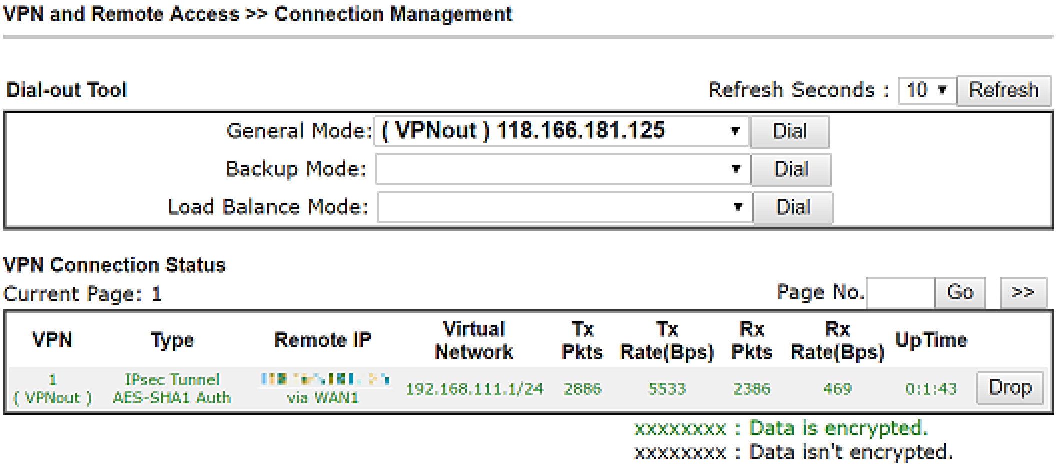
VPN and Remote Access >> Connection Management

Dial-out Tool

Refresh Seconds : 10 ▼ Refresh

General Mode: (VPNout) [redacted] ▼ Dial
Backup Mode: ▼ Dial
Load Balance Mode: ▼ Dial

VPN başarıyla bağlandıktan sonra, aşağıdaki durumu görebiliriz.



VPN and Remote Access >> Connection Management

Dial-out Tool

Refresh Seconds : 10 ▾ Refresh

General Mode:	(VPNout) 118.166.181.125 ▾	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 (VPNout)	IPsec Tunnel AES-SHA1 Auth	[redacted] via WAN1	192.168.111.1/24	2886	5533	2386	469	0:1:43	Drop

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