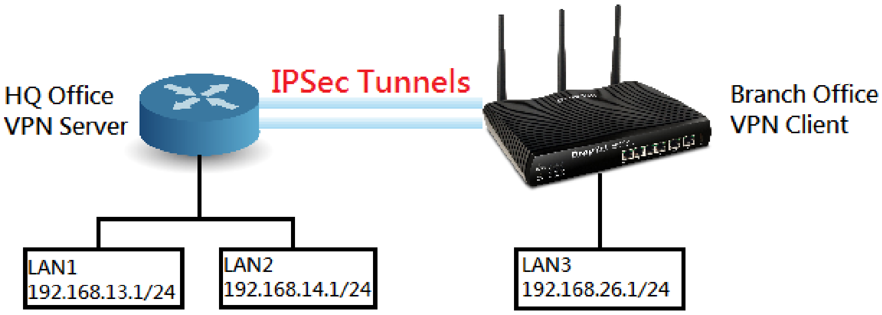
Bir VPN Profilinde IPsec Tünelinin Birden Fazla Subnet’i Bağlaması İçin Birden Fazla Phase 2 SA Oluşturmak

Bir IPsec VPN üzerinden birden fazla LAN ağına bağlanırken Vigor Router, aynı IPsec tüneli üzerinde ek Route kurallarına izin vermek için IPsec “birden çok" Remote Subnet özelliğine sahiptir, bu nedenle ek ağlar için birden fazla IPsec SA (Güvenlik Birliği(Security Association)) gerekli değildir. Ancak, bu mekanizma sadece DrayTek Vigor Router'lar arasında çalışır. DrayTek olmayan bir VPN sunucusuna bağlanırken, LAN to LAN VPN istemcisi olarak Vigor Router, bir VPN profilinde her bir subnete birden fazla IPsec tüneli oluşturmak için IKE Phase 2'deki IPsec SA'larını görüşmeyi destekler. Ve bu belge, bir VPN profili üzerinden birden fazla remote subnete erişmek için IPsec Multiple SA özelliğinin nasıl kullanılacağını tanıtmaktadır.

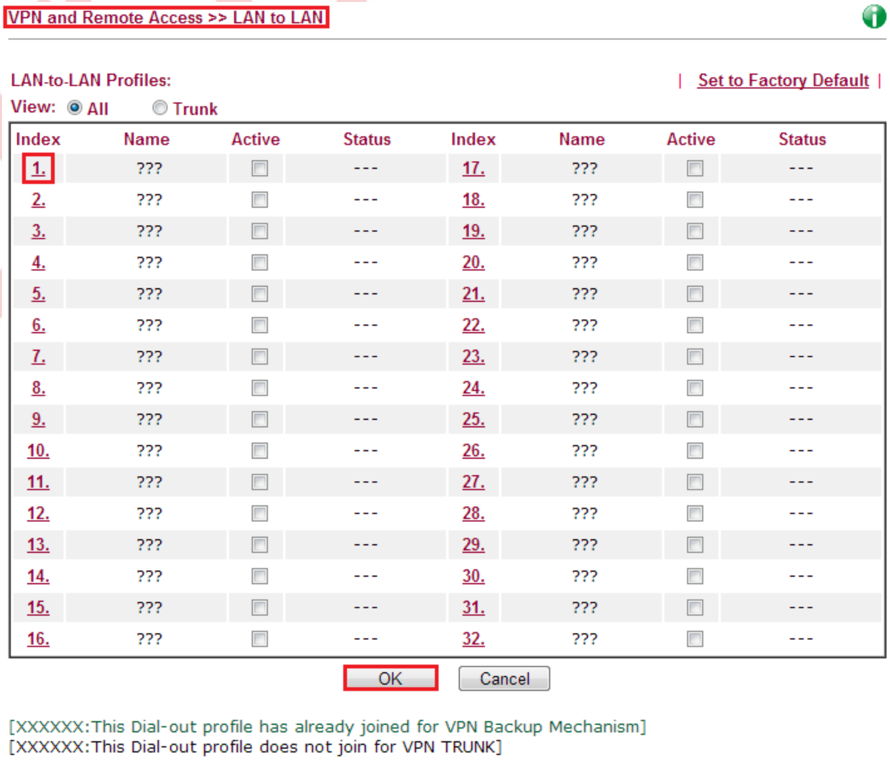
DrayOS



Hem VPN sunucusu hem de VPN istemcisi DrayTek routerları olduğunda, "More" seçeneğini kullanarak da amacımıza ulaşabileceğimizi unutmayın. Bu durumda, "Create Phase2 SA for each subnet (IPSec)” gerekli değildir ve etkinleştirilmemelidir.

Draytek Router’ı VPN Client Olarak Yapılandırma

1. **VPN and Remote Access** >> **LAN to LAN** sayfasına gidin ve yeni bir IPsec profili oluşturmak için bir index numarasına tıklayın.



VPN and Remote Access >> LAN to LAN

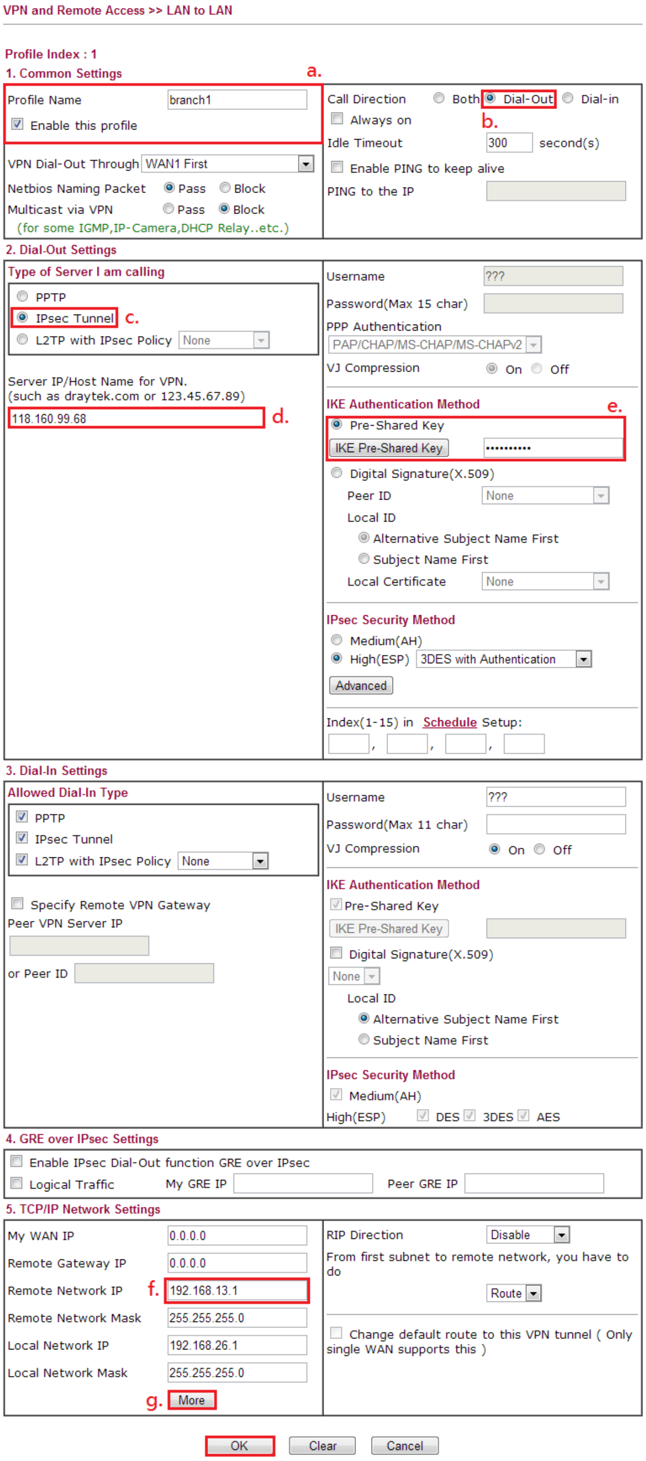
LAN-to-LAN Profiles: | Set to Factory Default |

View: ● All ○ Trunk

Index	Name	Active	Status	Index	Name	Active	Status
1.	???	□	---	17.	???	□	---
2.	???	□	---	18.	???	□	---
3.	???	□	---	19.	???	□	---
4.	???	□	---	20.	???	□	---
5.	???	□	---	21.	???	□	---
6.	???	□	---	22.	???	□	---
7.	???	□	---	23.	???	□	---
8.	???	□	---	24.	???	□	---
9.	???	□	---	25.	???	□	---
10.	???	□	---	26.	???	□	---
11.	???	□	---	27.	???	□	---
12.	???	□	---	28.	???	□	---
13.	???	□	---	29.	???	□	---
14.	???	□	---	30.	???	□	---
15.	???	□	---	31.	???	□	---
16.	???	□	---	32.	???	□	---

[XXXXXX:This Dial-out profile has already joined for VPN Backup Mechanism]
[XXXXXX:This Dial-out profile does not join for VPN TRUNK]

2. IPsec profil yapılandırmalarını ayarlayın.
    a. Profil adı girin ve **Enable this profile**'ı etkinleştirin.
    b. **Dail-Out**'u seçin.
    c. **Type of Server** için "IPsec Tunnel" i seçin.
    d. **Server IP**'i girin.
    e. **Pre-Shared Key** girin.
    f. **Remote Network IP** girin.
    g. **More**'a tıklayın.



VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name: branch1
☑ Enable this profile
VPN Dial-Out Through: WAN1 First
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
□ Always on
Idle Timeout: 300 second(s)
□ Enable PING to keep alive
PING to the IP

2. Dial-Out Settings

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

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)
118.160.99.68

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): 3DES with Authentication
Advanced

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

3. Dial-In Settings

Allowed Dial-In Type
☑ PPTP
☑ IPsec Tunnel
☑ L2TP with IPsec Policy: None

□ 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

4. GRE over IPsec Settings

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

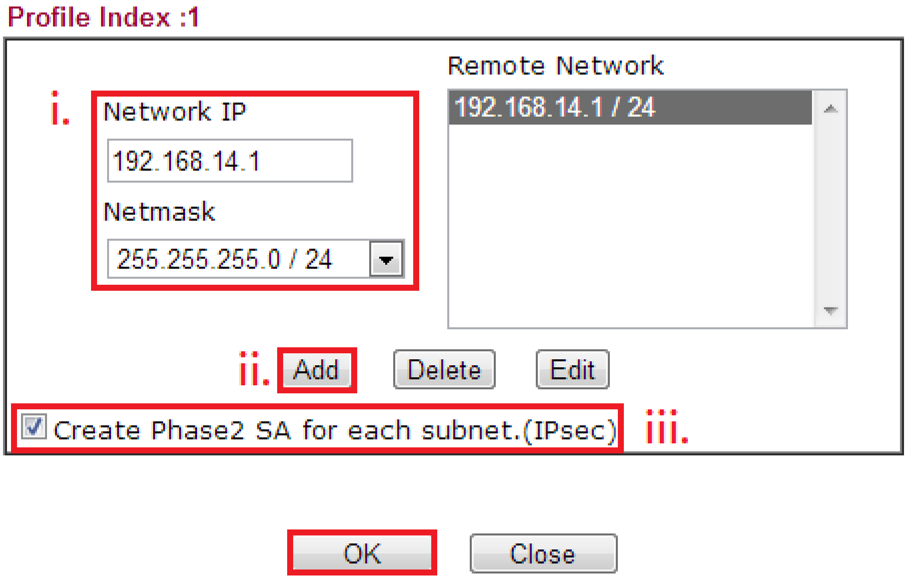
5. TCP/IP Network Settings

My WAN IP: 0.0.0.0
Remote Gateway IP: 0.0.0.0
Remote Network IP: 192.168.13.1
Remote Network Mask: 255.255.255.0
Local Network IP: 192.168.26.1
Local Network Mask: 255.255.255.0
More

RIP Direction: Disable
From first subnet to remote network, you have to do
Route
□ Change default route to this VPN tunnel (Only single WAN supports this)

OK   Clear   Cancel

3. Açılır Pencerede
   i. Remote’da ikinci **Network IP** ve **Netmask**’ı girin.
   ii. **Add**’e tıklayın.
   iii. **Create Phase2 SA for each subnet (IPSec)**’i işaretleyin.
   iv. Pencereyi kapatmak için **OK**’a tıklayın ve ardından kaydetmek için **OK**’a tıklayın.



Profile Index :1

i. Network IP: 192.168.14.1

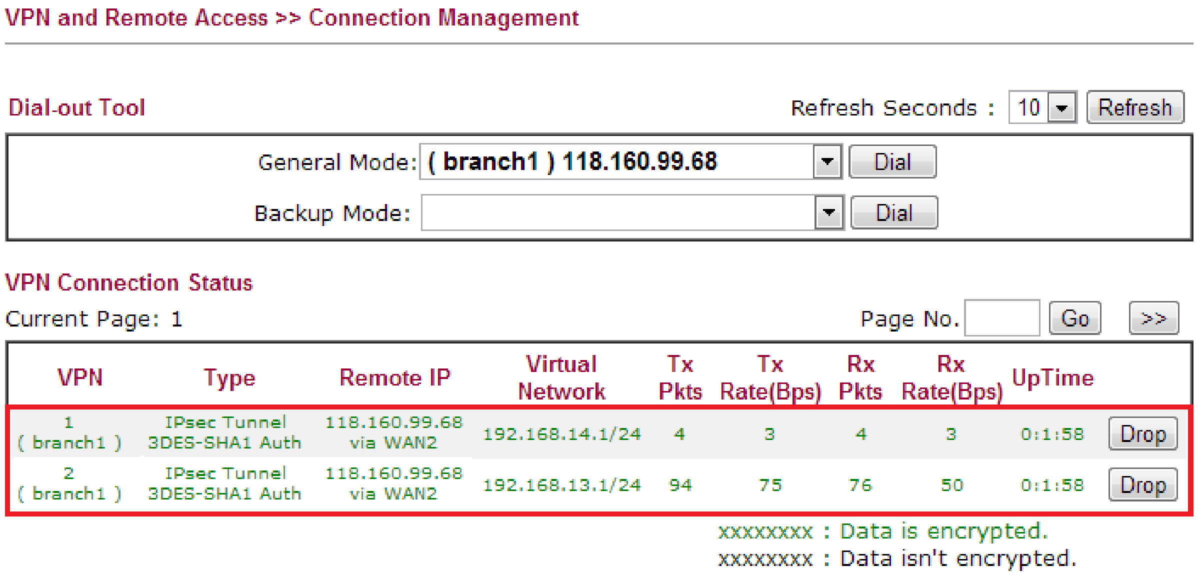
Netmask: 255.255.255.0 / 24

Remote Network: 192.168.14.1 / 24

iii. ☑ Create Phase2 SA for each subnet.(IPsec)

VPN Bağlantısını Kontrol Edin

VPN bağlatışını kontrol etmek için **VPN and Remote Access >> Connection Management** sayfasına gidin. Gördüğünüz gibi iki IPsec tüneli kuruldu.



VPN and Remote Access >> Connection Management

Dial-out Tool

Refresh Seconds : 10

General Mode: (branch1) 118.160.99.68

Backup Mode:

VPN Connection Status

Current Page: 1

Page No.

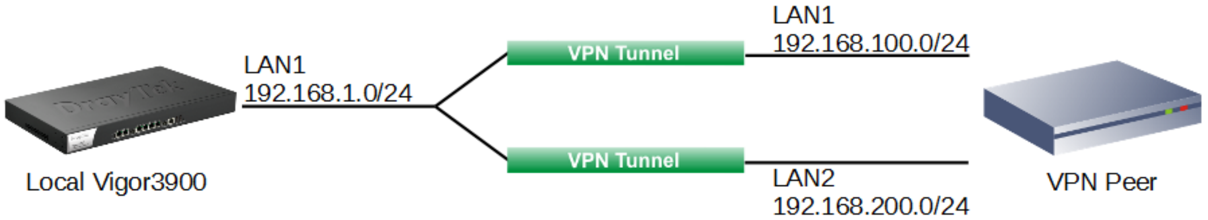
VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime	
1 (branch1)	IPsec Tunnel 3DES-SHA1 Auth	118.160.99.68 via WAN2	192.168.14.1/24	4	3	4	3	0:1:58	Drop
2 (branch1)	IPsec Tunnel 3DES-SHA1 Auth	118.160.99.68 via WAN2	192.168.13.1/24	94	75	76	50	0:1:58	Drop

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

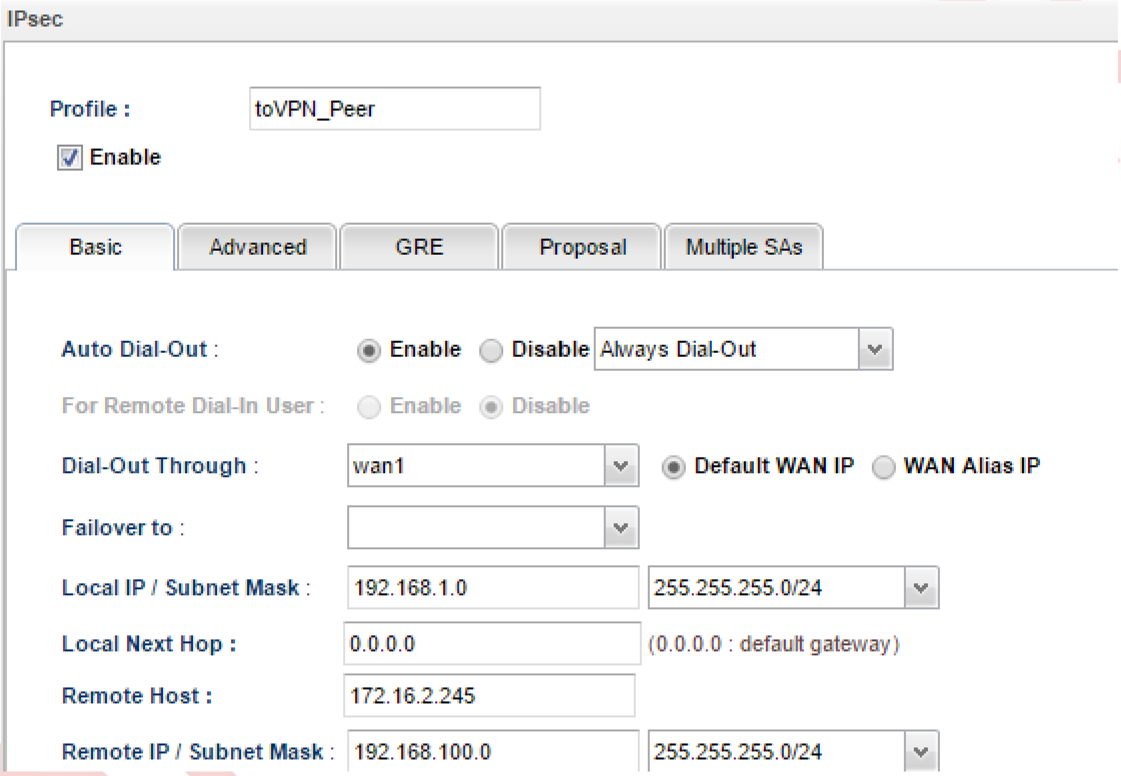
Linux

Durum 1: Vigor3900’de bir local ağ varken VPN Peer’de iki local ağ bulunmaktadır

Bu örnekte, Vigor3900'ün LAN ağı 192.168.1.0/24'tür. VPN Peer'in LAN1 ağı 192.168.100.0/24 ve LAN2 ise 192.168.200.0/24'tür.



1. Basic sekmesinde, Vigor3900'ün LAN ağını (192.168.1.0/24) Local IP / Subnet Mask’ı ve VPN Peer'ın LAN1 ağı (192.168.100.0/24) Remote IP / Subnet Mask’ı olarak yapılandırabiliriz.



Profile : toVPN_Peer

☑ Enable

Auto Dial-Out : ● Enable ○ Disable Always Dial-Out

For Remote Dial-In User : ○ Enable ● Disable

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

Failover to :

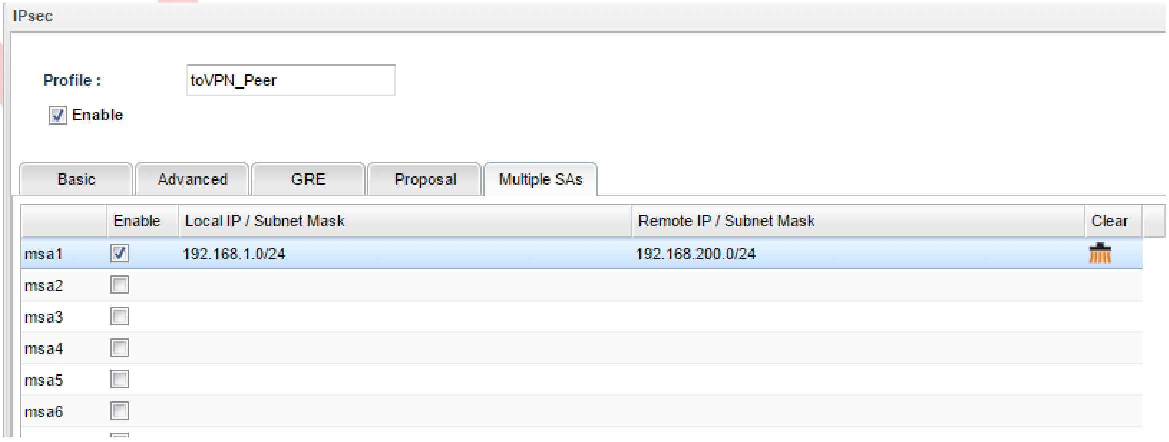
Local IP / Subnet Mask : 192.168.1.0 255.255.255.0/24

Local Next Hop : 0.0.0.0 (0.0.0.0 : default gateway)

Remote Host : 172.16.2.245

Remote IP / Subnet Mask : 192.168.100.0 255.255.255.0/24

2. Multiple SAs sekmesinde, Vigor3900'ün Local IP / Subnet Mask’ı için LAN ağını tekrar ve VPN Peer'ın Remote IP / Subnet Mask’ı için LAN2 ağını girin.



Profile : toVPN_Peer

☑ Enable

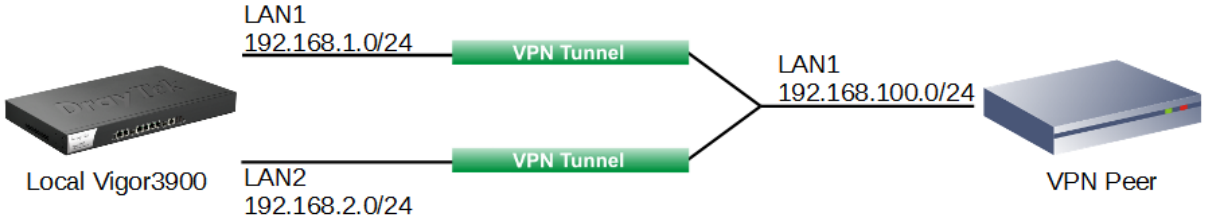
	Enable	Local IP / Subnet Mask	Remote IP / Subnet Mask	Clear
msa1	☑	192.168.1.0/24	192.168.200.0/24	
msa2	☐			
msa3	☐			
msa4	☐			
msa5	☐			
msa6	☐			

3. Benzer şekilde Multiple SA ayarını yapılandırmamız veya Vigor3900 Remote noktasındaki iki IPsec VPN Dial-in profil oluşturmamız gerekiyor.

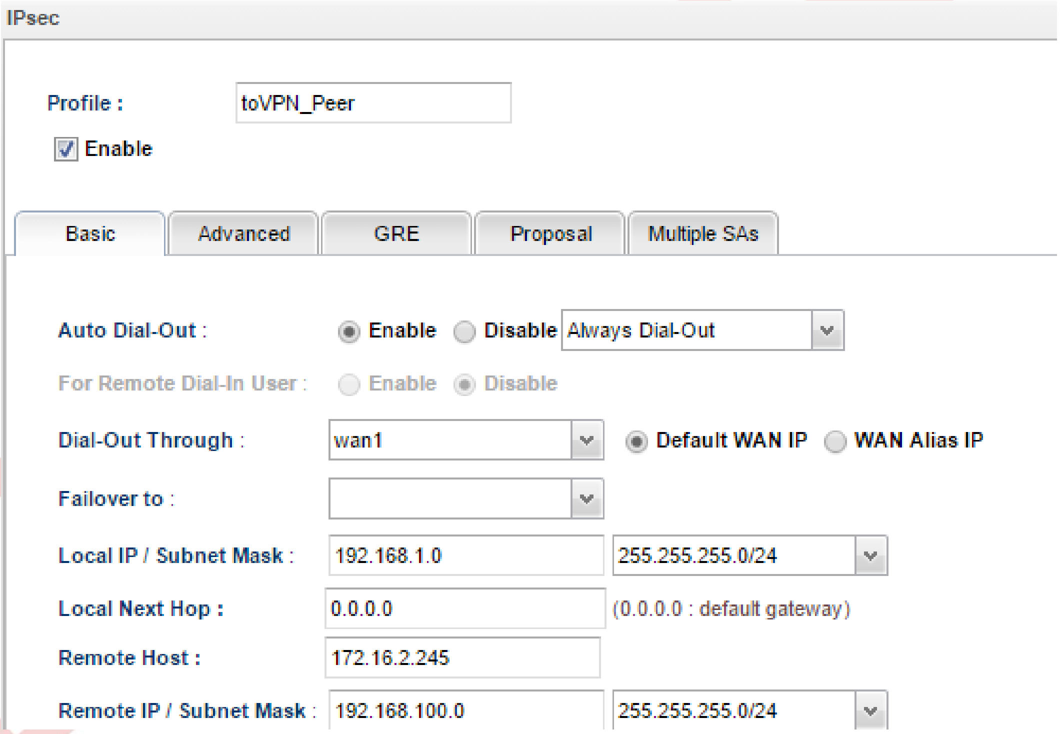
4. IPsec bağlantısı kurulurken, Vigor3900 iki IPsec SA oluşturacaktır. Bunlardan biri, 192.168.1.0/24 ve 192.168.100.0/24 ağı arasındaki verileri şifrelemek. Diğer ise 192.168.1.0/24 ve 192.168.200.0/24 ağı arasındaki verileri şifrelemek.

Durum 2: Vigor3900'de iki local ağ varken VPN Peer'de bir local ağ bulunmaktadır

Bu örnekte, Vigor3900'ün LAN1 ağı 192.168.1.1/24 ve LAN2 192.168.2.1/24'tür. VPN Peer'in LAN ağı 192.168.100.1/24'tür.



1. Basic sekmesinde, Vigor3900'ün LAN1 ağını Local IP / Subnet Mask'ı ve VPN Peer'ın LAN ağını (192.168.100.0/24) Remote IP / Subnet Mask'ı olarak yapılandırabiliriz.


IPsec

Profile : toVPN_Peer

☑ Enable

Auto Dial-Out : ● Enable ○ Disable Always Dial-Out

For Remote Dial-In User : ○ Enable ● Disable

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

Failover to :

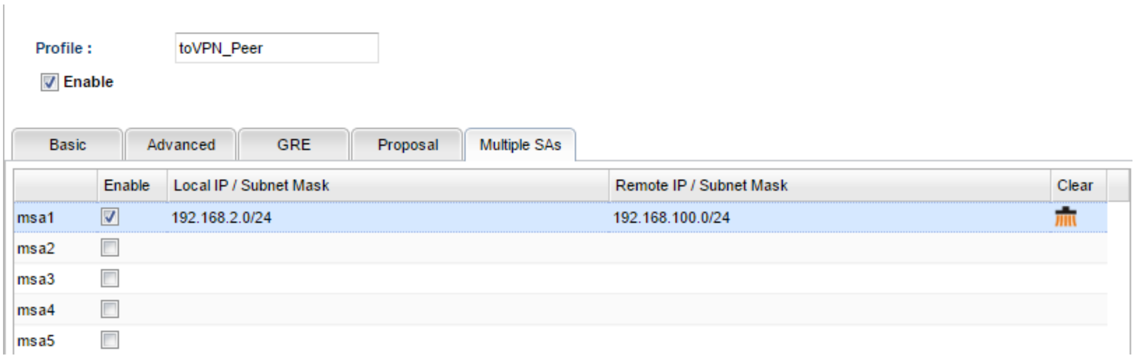
Local IP / Subnet Mask : 192.168.1.0 255.255.255.0/24

Local Next Hop : 0.0.0.0 (0.0.0.0 : default gateway)

Remote Host : 172.16.2.245

Remote IP / Subnet Mask : 192.168.100.0 255.255.255.0/24

2. Ardından Multiple SAs sekmesinde, Vigor3900'ün LAN2 ağını ve VPN Peer's LAN ağını girin.


Profile : toVPN_Peer

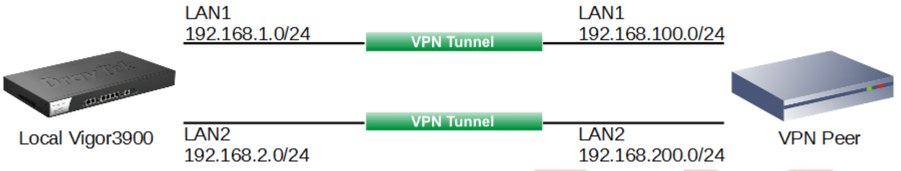
☑ Enable

	Enable	Local IP / Subnet Mask	Remote IP / Subnet Mask	Clear
msa1	☑	192.168.2.0/24	192.168.100.0/24	
msa2	□			
msa3	□			
msa4	□			
msa5	□			

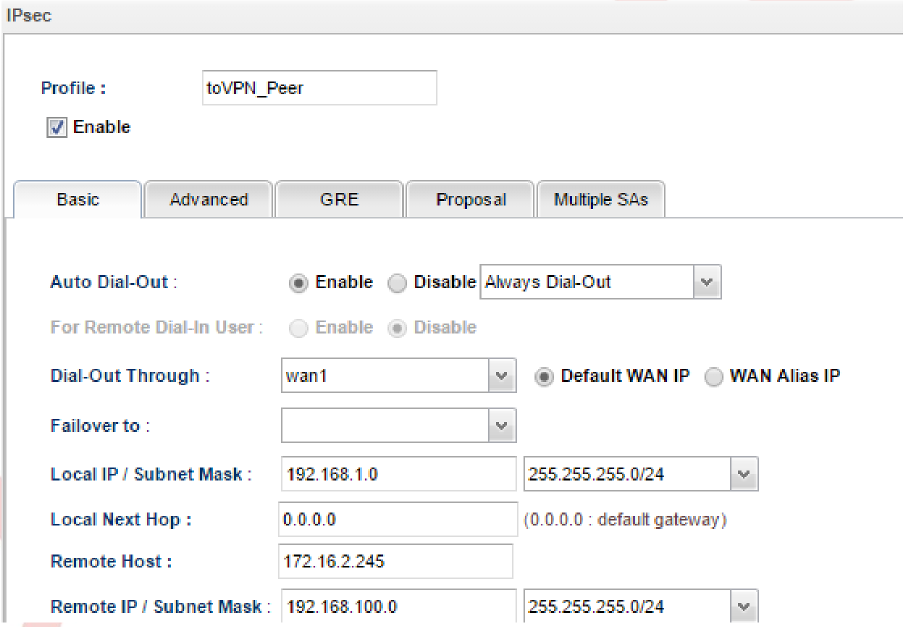
3. Benzer şekilde Multiple SA ayarını yapılandırmamız veya Vigor3900 Remote noktasındaki iki IPsec VPN Dial-in profil oluşturmamız gerekiyor.
4. IPsec bağlantısı kurulurken, Vigor3900 iki IPsec SA oluşturacaktır. Bunlardan biri, 192.168.1.0/24 ve 192.168.100.0/24 ağı arasındaki verileri şifrelemek. Diğeri, 192.168.2.0/24 ve 192.168.100.0/24 ağı arasındaki verileri şifrelemek içindir.

Durum 2: Hem Vigor3900 hem de VPN Peer'ın iki Local ağı bulunmaktadır

Bu örnekte, Vigor3900'ün LAN1 ağı 192.168.1.0/24 ve LAN2 192.168.2.0/24'tür. VPN Peer'in LAN1 ağı 192.168.100.0/24 ve LAN2 ağı 192.168.200.0/24'tür.



1. Basic sekmesinde, Vigor3900'ün LAN1 ağını Local IP / Subnet Mask'ı ve VPN Peer'ın LAN1 ağını (192.168.100.0/24) Remote IP / Subnet Mask'ı olarak yapılandırabiliriz.


IPsec

Profile : toVPN_Peer

☑ Enable

Auto Dial-Out : ● Enable ○ Disable Always Dial-Out

For Remote Dial-In User : ○ Enable ● Disable

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

Failover to :

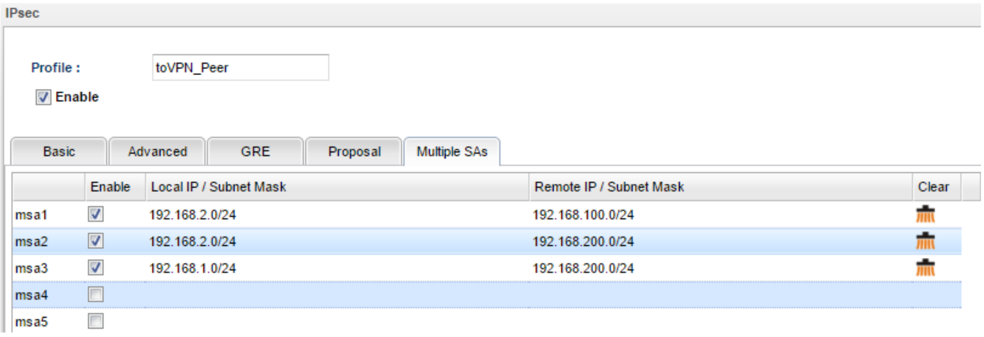
Local IP / Subnet Mask : 192.168.1.0 255.255.255.0/24

Local Next Hop : 0.0.0.0 (0.0.0.0 : default gateway)

Remote Host : 172.16.2.245

Remote IP / Subnet Mask : 192.168.100.0 255.255.255.0/24

2. Multiple SAs sekmesinde, aşağıdaki üç ayarı girin:
   - Vigor3900'ün LAN2 ağı - VPN Peer'ın LAN1 ağına
   - Vigor3900'ün LAN2 ağı VPN Peer'ın LAN2 ağına
   - Vigor3900'ün LAN1 ağı - VPN Peer'ın LAN2 ağına

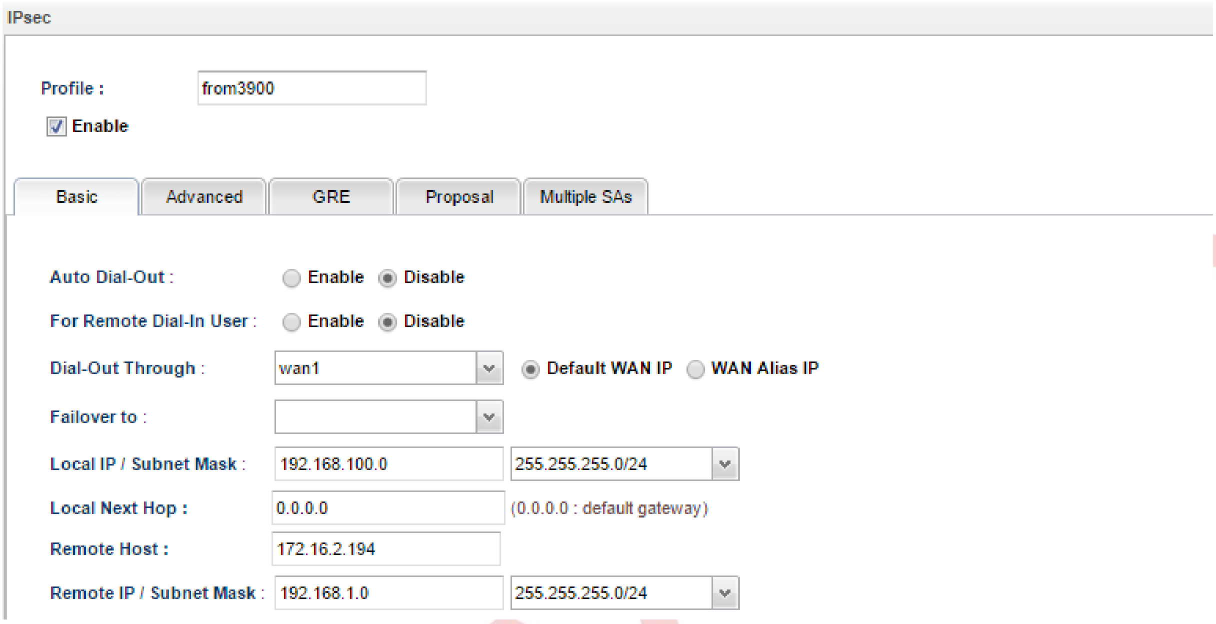

IPsec

Profile : toVPN_Peer

☑ Enable

	Enable	Local IP / Subnet Mask	Remote IP / Subnet Mask	Clear
msa1	☑	192.168.2.0/24	192.168.100.0/24	
msa2	☑	192.168.2.0/24	192.168.200.0/24	
msa3	☑	192.168.1.0/24	192.168.200.0/24	
msa4	□			
msa5	□			

3. IPsec bağlantı kuruluşu sırasında Vigor3900, 4 IPsec SA oluşturacaktır. Bunlardan biri, 192.168.1.0/24 ve 192.168.100.0/24 ağı arasındaki verileri şifrelemek ve bunların geri kalanı, 192.168.1.0/24 ve 192.168.200.0/24 ağı, 192.168.2.0/24 ve 192.168.100.0/24 ağı ile 192.168.2.0/24 ağı ile 192.168.200.0/24 ağı arasındaki verileri şifrelemek içindir.



Profile : from3900

☑ 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 :

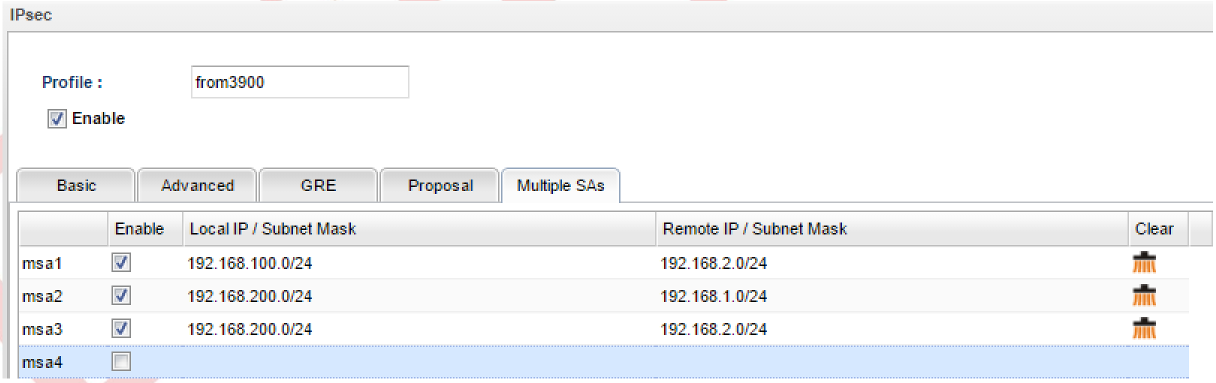
Local IP / Subnet Mask : 192.168.100.0 255.255.255.0/24

Local Next Hop : 0.0.0.0 (0.0.0.0 : default gateway)

Remote Host : 172.16.2.194

Remote IP / Subnet Mask : 192.168.1.0 255.255.255.0/24

4. Tabi ki, VPN Peer uygun konfigürasyonlara sahip olmalıdır. Örneğin VPN Peer olarak çalışan başka bir Vigor3900 atın. Basic sekmesinde, LAN ağını (192.168.100.0/24) Local IP / Subnet Mask'ı ve diğer Vigor3900'ün LAN ağını (192.168.1.0/24) Remote IP / Subnet Mask'ı olarak yapılandırabiliriz.
5. Sonra Multiple SAs sekmesinde, aşağıdaki üç ayarı girin:

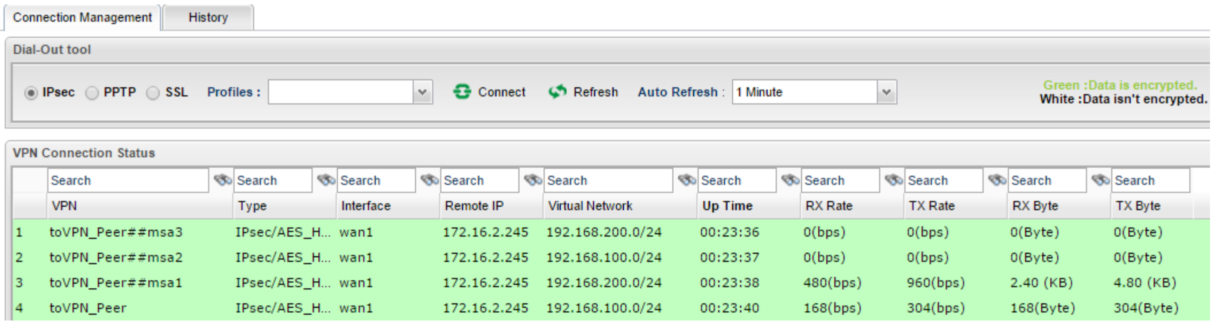


Profile : from3900

☑ Enable

	Enable	Local IP / Subnet Mask	Remote IP / Subnet Mask	Clear
msa1	☑	192.168.100.0/24	192.168.2.0/24	
msa2	☑	192.168.200.0/24	192.168.1.0/24	
msa3	☑	192.168.200.0/24	192.168.2.0/24	
msa4	☐			

6. Yukarıdaki yapılandırmalardan sonra, iki router arasında 4 IPsec bağlantısı görmeliyiz. Farklı ağlar arasında aktarılan veriler dört farklı IPsec SA tarafından şifrelenir.

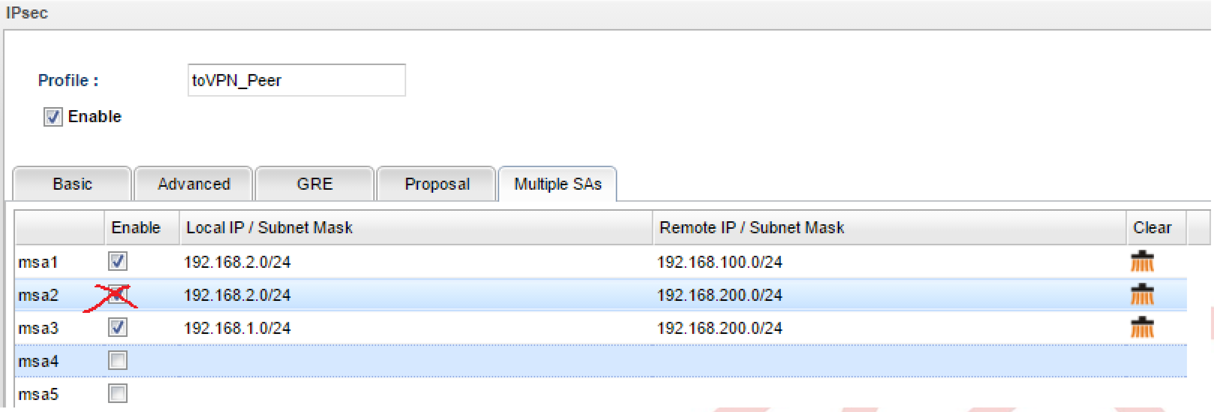


● IPsec ○ PPTP ○ SSL Profiles : Auto Refresh : 1 Minute

Green :Data is encrypted.
White :Data isn't encrypted.

	VPN	Type	Interface	Remote IP	Virtual Network	Up Time	RX Rate	TX Rate	RX Byte	TX Byte
1	toVPN_Peer##msa3	IPsec/AES_H...	wan1	172.16.2.245	192.168.200.0/24	00:23:36	0(bps)	0(bps)	0(Byte)	0(Byte)
2	toVPN_Peer##msa2	IPsec/AES_H...	wan1	172.16.2.245	192.168.100.0/24	00:23:37	0(bps)	0(bps)	0(Byte)	0(Byte)
3	toVPN_Peer##msa1	IPsec/AES_H...	wan1	172.16.2.245	192.168.200.0/24	00:23:38	480(bps)	960(bps)	2.40 (KB)	4.80 (KB)
4	toVPN_Peer	IPsec/AES_H...	wan1	172.16.2.245	192.168.100.0/24	00:23:40	168(bps)	304(bps)	168(Byte)	304(Byte)

7. Local ağın 192.168.2.0/24 remote ağa 192.168.200.0/24 erişimini istemiyorsak ne yapabiliriz? Birden çok SAs sekmesinde msa2'yi kaldırmanız yeterli!



IPsec

Profile : toVPN_Peer

☑ Enable

	Enable	Local IP / Subnet Mask	Remote IP / Subnet Mask	Clear
msa1	☑	192.168.2.0/24	192.168.100.0/24	
msa2	☒	192.168.2.0/24	192.168.200.0/24	
msa3	☑	192.168.1.0/24	192.168.200.0/24	
msa4	□			
msa5	□			