



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.



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

VPN and Remote Access >> LAN to LAN

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

LAN-to-LA	N Profiles:					Set to	Factory D
View: •	All © Tru	nk	C ()				C (1)
Index	Name	Active	Status	Index	Name	Active	Statu
1.				<u>17.</u>			
<u>2.</u>	???			<u>18.</u>	???		
<u>3.</u>	???			<u>19.</u>	???		
<u>4.</u>	???			<u>20.</u>	???		
<u>5.</u>	???			<u>21.</u>	???		
<u>6.</u>	???			<u>22.</u>	???		
<u>7.</u>	???			<u>23.</u>	???		
<u>8.</u>	???			<u>24.</u>	???		
<u>9.</u>	???			<u>25.</u>	???		
<u>10.</u>	???			<u>26.</u>	???		
<u>11.</u>	???			<u>27.</u>	???		
<u>12.</u>	???			<u>28.</u>	???		
<u>13.</u>	???			<u>29.</u>	???		
<u>14.</u>	???			<u>30.</u>	???		
<u>15.</u>	???			<u>31.</u>	???		
<u>16.</u>	???			<u>32.</u>	???		

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

 	tt-	-t			
ne		SL	(0)	00.	
			~~		

0





- 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.

Profile Index : 1		
1. Common Settings a		
Brofile Name bronch1	Call Direction Roth Dial-Out Dial-in	
Enable this profile	Idla Timoout	
VRN Dial-Out Through WAN1 Firet	Tale Timeout	
Nathias Namine Deslute O Dess. O Diseli	Enable PING to keep alive	
Netbios Naming Packet Pass Block	PING to the IP	
(for some IGMP.IP-Camera.DHCP Relayetc.)		
2. Dial-Out Settings		
Type of Server I am calling	Ucompanya 222	
IPsec Tunnel C.	Password(Max 15 char)	
1 2TP with IPsec Policy None	PPP Authentication	
Server IP/Host Name for VPN.	VJ Compression I On Off	
(such as draytek.com or 123.45.67.89)	IKE Authentication Method e.	
118.160.99.68 d.	Pre-Shared Key	
	IKE Pre-Shared Key	
	Digital Signature(X.509)	
	Peer ID None 👻	
	Local ID	
	Alternative Subject Name First Alternat	
	Subject Name First	
	Local Certificate None 👻	
	IPsec Security Method	
	Medium(AH) High(ESB) 2DES with Authentication	
	High(ESP) JDES with Automitication	
	Advanced	
	Index(1-15) in Schedule Setup:	
3. Dial-In Settings		
Allowed Dial-In Type		
	Username 222	
PPTP	Username ???	
PPTP IPsec Tunnel	Username ??? Password(Max 11 char)	
PPTP IPsec Tunnel L2TP with IPsec Policy None	Username ??? Password(Max 11 char) VJ Compression © On © Off	
☑ PPTP ☑ IPsec Tunnel ☑ L2TP with IPsec Policy None	Username ??? Password(Max 11 char) VJ Compression © Off IKE Authentication Method	
PPTP Prsec Tunnel L2TP with IPsec Policy None Specify Remote VPN Gateway	Username ??? Password(Max 11 char) VJ Compression © On © Off IKE Authentication Method © Pre-Shared Key	
☑ PPTP ☑ IPsec Tunnel ☑ L2TP with IPsec Policy None ☑ Specify Remote VPN Gateway Peer VPN Server IP	Username ??? Password(Max 11 char) VJ Compression On Off IKE Authentication Method Ø Pre-Shared Key IKE Pre-Shared Key	
☑ PPTP ☑ IPsec Tunnel ☑ L2TP with IPsec Policy None ■ Specify Remote VPN Gateway Peer VPN Server IP	Username ??? Password(Max 11 char) VJ Compression On Off IKE Authentication Method Pre-Shared Key IKE Pre-Shared Key Digital Signature(X,509)	
✓ 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	
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 v Local ID	
♥ 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 [KE Pre-Shared Key [KE Pre-Shared Key] [Digital Signature(X.509) None [] Local ID @ Alternative Subject Name First	
♥ 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 [KE Pre-Shared Key] Digital Signature(X.509) None Local ID @ Alternative Subject Name First © Subject Name First	
♥ PPTP ♥ IPsec Tunnel ♥ L2TP with IPsec Policy None ● Specify Remote VPN Gateway Peer VPN Server IP ●	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 Other Alternative Subject Name First Subject Name First	
♥ 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 © Medimic (H)	
♥ 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 U Local ID O Alternative Subject Name First Subject Name First IPsec Security Method Medium(AH) Medium(AH)	
PPTP IPsec Tunnel L2TP with IPsec Policy None Specify Remote VPN Gateway Peer VPN Server IP or Peer ID GRE over IPsec Settions	Username ??? Password(Max 11 char) VJ Compression On Off IKE Authentication Method Pre-Shared Key IKE Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.509) None U Local ID Alternative Subject Name First Subject Name First IPsec Security Method Medium(AH) High(ESP) DES 3DES AES	
PPTP IPsec Tunnel L2TP with IPsec Policy None Specify Remote VPN Gateway Peer VPN Server IP or Peer ID A. GRE over IPsec Settings Enable Reser Dial-Out function CPE over Toose	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	
PPTP IPsec Tunnel L2TP with IPsec Policy None Specify Remote VPN Gateway Peer VPN Server IP or Peer ID decode the set of t	Username ??? Password(Max 11 char) VJ Compression © On © Off IKE Authentication Method © Pre-Shared Key [KE Pre-Shared Key [KE Pre-Shared Key] [Digital Signature(X.509) None Local ID © Alternative Subject Name First © Subject Name First [Psec Security Method © Medium(AH) High(ESP) © DES © 3DES © AES	
	Username ??? Password(Max 11 char) VJ Compression On Off IKE Authentication Method Pre-Shared Key KE Pre-Shared Key Digital Signature(X.509) None Local ID Alternative Subject Name First Subject Name First Paec Security Method Medium(AH) High(ESP) DES 3DES AES	
	Username ??? Password(Max 11 char) VJ Compression On Off IKE Authentication Method Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.509) None U Local ID Alternative Subject Name First Subject Name First IPsec Security Method Medium(AH) High(ESP) DES 3DES AES	
Ø PPTP Ø IPsec Tunnel Ø L2TP with IPsec Policy None Specify Remote VPN Gateway Peer VPN Server IP or Peer ID Benable IPsec Settings Enable IPsec Dial-Out function GRE over IPsec Logical Traffic My WAN IP 0 0.0.0	Username ??? Password(Max 11 char) VJ Compression • On • Off IKE Authentication Method Pre-Shared Key IKE Pre-Shared Key ID Digital Signature(X.509) None Local ID • Alternative Subject Name First • Subject Name First IPsec Security Method Ø Medium(AH) High(ESP) Ø DES Ø 3DES Ø AES Peer GRE IP Peer GRE IP	
IPsec Tunnel IPsec Tunnel L2TP with IPsec Policy None Specify Remote VPN Gateway Peer VPN Server IP or Peer ID Image: Specify Remote VPN Gateway Image: Specify Remote VPN Gateway Peer VPN Server IP Image: Specify Remote VPN Gateway Image: Specify	Username ??? Password(Max 11 char) VJ Compression On Off IKE Authentication Method Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.509) None U Local ID Alternative Subject Name First Subject Name First IPsec Security Method Medium(AH) High(ESP) DES 3DES AES Peer GRE IP Peer GRE IP Prom first subnet to remote network, you have to do	
Image: Property of the second seco	Username ??? Password(Max 11 char) VJ Compression On Off IKE Authentication Method Pre-Shared Key IKE Pre-Shared Key ID Digital Signature(X.509) None Local ID O Alternative Subject Name First Subject Name First IPsec Security Method Medium(AH) High(ESP) DES 3DES AES Peer GRE IP Peer GRE IP RIP Direction Disable From first subnet to remote network, you have to do	
Image: Program in the second state of the second state	Username ??? Password(Max 11 char) VJ Compression On Off IKE Authentication Method Pre-Shared Key KE Pre-Shared Key Digital Signature(X.509) None Local ID O Alternative Subject Name First Subject Name First IPsec Security Method Medium(AH) High(ESP) DES 3DES AES RIP Direction Disable F From first subnet to remote network, you have to do Route F	
PPTP IPsec Tunnel L2TP with IPsec Policy None Specify Remote VPN Gateway Peer VPN Server IP or Peer ID Image: Specify Remote VPN Gateway Peer VPN Server IP Image: Specify Remote VPN Gateway Peer VPN Server IP Image: Specify Remote VPN Gateway Peer VPN Server IP Image: Specify Remote VPN Gateway Peer VPN Server IP Image: Specify Remote VPN Gateway Peer VPN Server IP Image: Specify Remote VPN Gateway Per VPN Server IP Image: Specify Remote VPN Gateway Image: Specify Remot	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 Peer GRE IP Peer GRE IP Peer GRE IP RIP Direction Disable • From first subnet to remote network, you have to Change default route to this VPN tunnel (Only	
Ø PPTP Ø IPsec Tunnel Ø L2TP with IPsec Policy None Specify Remote VPN Gateway Peer VPN Server IP or Peer ID Image: Specify Remote VPN Gateway Peer VPN Server IP Image: Specify Remote VPN Gateway Peer VPN Server IP Image: Specify Remote VPN Gateway Peer VPN Server IP Image: Specify Remote VPN Gateway Image: Specify Remote VPN Gateway <td>Username ??? Password(Max 11 char) VJ Compression • On • Off IKE Authentication Method Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.509) None U Local ID • Alternative Subject Name First • Subject Name First IPsec Security Method Ø Medium(AH) High(ESP) Ø DES Ø 3DES Ø AES 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)</td> <td></td>	Username ??? Password(Max 11 char) VJ Compression • On • Off IKE Authentication Method Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.509) None U Local ID • Alternative Subject Name First • Subject Name First IPsec Security Method Ø Medium(AH) High(ESP) Ø DES Ø 3DES Ø AES 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)	
PPTP PrpP PrpP Psec Tunnel L2TP with IPsec Policy None Specify Remote VPN Gateway Peer VPN Server IP or Peer ID Image: Specify Remote VPN Gateway Peer VPN Server IP Image: Specify Remote VPN Gateway Or Peer ID Image: Specify Remote VPN Gateway Or Peer ID Image: Specify Remote VPN Gateway Image: S	Username ??? Password(Max 11 char) VJ Compression • On Off IKE Authentication Method Pre-Shared Key IKE Pre-Shared Key ID gital Signature(X.509) None • Local ID • Alternative Subject Name First • Subject Name First IPsec Security Method Ø Medium(AH) High(ESP) Ø DES Ø 3DES Ø AES RIP Direction Disable • Peer GRE IP Peer GRE IP RIP Direction Disable • Route • Change default route to this VPN tunnel (Only single WAN supports this)	
IPPTP IPsec Tunnel L2TP with IPsec Policy None Specify Remote VPN Gateway Peer VPN Server IP or Peer ID Image: Specify Remote VPN Gateway Peer VPN Server IP Image: Specify Remote VPN Gateway Peer VPN Server IP Image: Specify Remote VPN Gateway Peer VPN Server IP Image: Specify Remote VPN Gateway Peer VPN Server IP Image: Specify Remote VPN Gateway Image: Specify Remote Settings My WAN IP Remote Gateway IP Image: Specify Remote Network Mask 255:255:255:0 Image: Specify Remote Network Mask 255:255:25:0	Username ??? Password(Max 11 char) VJ Compression On Off IKE Authentication Method Pre-Shared Key IKE Pre-Shared Key ID gigtal Signature(X.509) None Local ID Alternative Subject Name First Subject Name First IPsec Security Method Alternative Subject Name First IPsec Security Method Medium(AH) High(ESP) DES 3DES AES Peer GRE IP Peer GRE IP 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)	

www.netfast.com.tr





- 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			
	Ren	note Network		
i.	Network IP 192	. 168.14.1 / 24	~	
	192.168.14.1			
	Netmask			
	255.255.255.0 / 24 💌			
			-	
	Add Delete	Edit		
🗹 Cre	eate Phase2 SA for each subne	et.(IPsec)		

OK	Close

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

	Gene	eral Mode: (bra	anch1)118.160	.99.68	3 •	- D	ial	
	Back		D	ial				
Current Dag	o: 1					Da		Go
Current Pag	je: 1 Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Pa Rx Pkts	ge No. Rx Rate(Bps)	Go UpTime
VPN	rype Type IPsec Tunnel 3DES-SHA1 Auth	Remote IP 118.160.99.68 via WAN2	Virtual Network	Tx Pkts 4	Tx Rate(Bps) 3	Pag Rx Pkts 4	ge No. Rx Rate(Bps) 3	Go UpTime 0:1:58
VPN (branch1) 2 (branch1)	IPsec Tunnel 3DES-SHA1 Auth IPsec Tunnel 3DES-SHA1 Auth	Remote IP 118.160.99.68 via WAN2 118.160.99.68 via WAN2	Virtual Network 192.168.14.1/24 192.168.13.1/24	Tx Pkts 4 94	Tx Rate(Bps) 3 75	Pa Rx Pkts 4 76	ge No. Rx Rate(Bps) 3 50	Go UpTime 0:1:58 0:1:58

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	
Basic Advanced	GRE Proposa	Multiple SAs
Auto Dial-Out :	Enable Disable Ah	ways Dial-Out
For Remote Dial-In User	O Enable	
Dial-Out Through :	wan1 🗸	Oefault 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 👻

 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.

Psec							
Profile	e: nable	toVPN_Peer					
Basi	c Ad	lvanced	GRE	Proposal	Multiple SAs		
	Enable	Local IP / Sub	net Mask			Remote IP / Subnet Mask	Clear
msa1	V	192.168.1.0/24	4			192.168.200.0/24	πι
msa2							
msa3							
msa4							
msa5							
msa6							

3. Benzer şekilde Multiple SA ayarını yapılandırmamız veya Vigor3900 Remote noktasındaki iki IPsec VPN Dialin 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.

IPse	ec						
	Profile :	toVPN_P	eer				
ſ	Basic	Advanced	GRE	Proposal	Multiple SAs		
	Auto Dial-O)ut :	Enable	Disable Alwa	ays Dial-Out	¥	
	For Remote	Dial-In User :	Enable Disable				
	Dial-Out Th	rough :	wan1	~	Default WAN	IP 🔵 WAN Alias IP	
	Failover to :			*			
	Local IP / Se	ubnet Mask :	192.168.1.0		255.255.255.0/24	*	
	Local Next Hop :		0.0.0.0		(0.0.0.0 : default gateway)		
	Remote Ho	st:	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 : Enal Basic	ble	toVPN_Peer	Proposal Mr	ultiple SAs			
	Enable	Local IP / Subnet Mask			Remote IP / Subnet Mask	CI	lear
msa1	V	192.168.2.0/24			192.168.100.0/24	л	π
msa2							
msa3							
msa4							
msa5							





- 3. Benzer şekilde Multiple SA ayarını yapılandırmamız veya Vigor3900 Remote noktasındaki iki IPsec VPN Dialin 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.

Profile :	toVPN_	Peer			
Enable					
Basic	Advanced	GRE	Proposal	Multiple SAs	
Auto Dial-Out	:	Enable) Disable Alwa	ays Dial-Out	~
For Remote Di	ial-In User :	🔵 Enable 🌘	Disable		
Dial-Out Throu	ugh :	wan1	~	Default WAN	I IP 🔵 WAN Alias I
Failover to :			~]	
Local IP / Subr	net Mask :	192.168.1.0		255.255.255.0/24	~
Local Next Ho	р:	0.0.0.0		(0.0.0.0 : default g	ateway)
Remote Host :		172.16.2.245			

- 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	e: nable	toVPN_Pe	eer						
Basi	c Ad	vanced	GRE	Proposal	Multiple SAs				
	Enable	Local IP / S	Subnet Mask			Remote IP / Subne	t Mask	C	lear
msa1	V	192.168.2.	0/24			192.168.100.0/24		m	π
msa2	V	192.168.2.	0/24			192.168.200.0/24		m	π
msa3	\checkmark	192.168.1.	0/24			192.168.200.0/24		m	π
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.

IPsec		
Profile : from3900)	
Basic Advanced	GRE Proposal	Multiple SAs
Auto Dial-Out : For Remote Dial-In User : Dial-Out Through : Failover to :	Enable Disable Enable Disable wan1 v	Default WAN IP WAN Alias IP
Local IP / Subnet Mask :	192.168.100.0	255.255.255.0/24 🗸
Local Next Hop :	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 🗸

- 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:

sec						
Profile	:	from3900				
🗸 En	able					
)(
Basic	c Ad	dvanced GRE	Proposal	Multiple SAs		
Basic	c Ac Enable	dvanced GRE Local IP / Subnet Mask	Proposal	Multiple SAs	Remote IP / Subnet Mask	Clear
Basik nsa1	c Ac Enable	Ivanced GRE Local IP / Subnet Mask 192.168.100.0/24	Proposal	Multiple SAs	Remote IP / Subnet Mask 192.168.2.0/24	Clear mt
Basik msa1 msa2	c Ac Enable V	Ivanced GRE Local IP / Subnet Mask 192.168.100.0/24 192.168.200.0/24	Proposal	Multiple SAs	Remote IP / Subnet Mask 192.168.2.0/24 192.168.1.0/24	Clear
Basik msa1 msa2 msa3	C Ad Enable	Interference GRE Local IP / Subnet Mask 192.168.100.0/24 192.168.200.0/24 192.168.200.0/24	Proposal	Multiple SAs	Remote IP / Subnet Mask 192.168.2.0/24 192.168.1.0/24 192.168.2.0/24	Clear m m m

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

Con	nection Management His	tory																	
Dial	-Out tool																		
۲	IPsec OPPTP OSSL	Prof	iles :			~	Conne	ct	📢 Refresh 🛛 Auto F	Refr	esh : 1 Minut	e		۷			Green : White :E	Data Data	a is encrypted. isn't encrypted.
VPN	Connection Status																		
	Search	1	Search	1	Search	1	Search	1	Search	1	Search	1	Search	1	Search	3	Search	1	Search
	VPN		Туре		Interface		Remote IP		Virtual Network		Up Time		RX Rate		TX Rate		RX Byte		TX Byte
1	toVPN_Peer##msa3		IPsec/AES_	н	wan1		172.16.2.24	45	192.168.200.0/24		00:23:36		O(bps)		O(bps)		O(Byte)		0(Byte)
2	toVPN_Peer##msa2		IPsec/AES_	н	wan1		172.16.2.24	45	192.168.100.0/24		00:23:37		O(bps)		O(bps)		O(Byte)		O(Byte)
3	toVPN_Peer##msa1		IPsec/AES_	н	wan1		172.16.2.24	45	192.168.200.0/24		00:23:38		480(bps)		960(bps)		2.40 (KB)		4.80 (KB)
4	toVPN_Peer		IPsec/AES_	н	wan1		172.16.2.24	45	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!

Basi	ic	Advanced	GRE	Proposal	Multiple SAs		
	Enabl	e Local IP	/ Subnet Mask			Remote IP / Subnet Mask	Clear
isa1	1	192.168.2	2.0/24			192.168.100.0/24	M IL
isa2	×	192.168.2	2.0/24			192.168.200.0/24	ли
isa3	v	192.168.1	1.0/24			192.168.200.0/24	T
isa4							
				2			