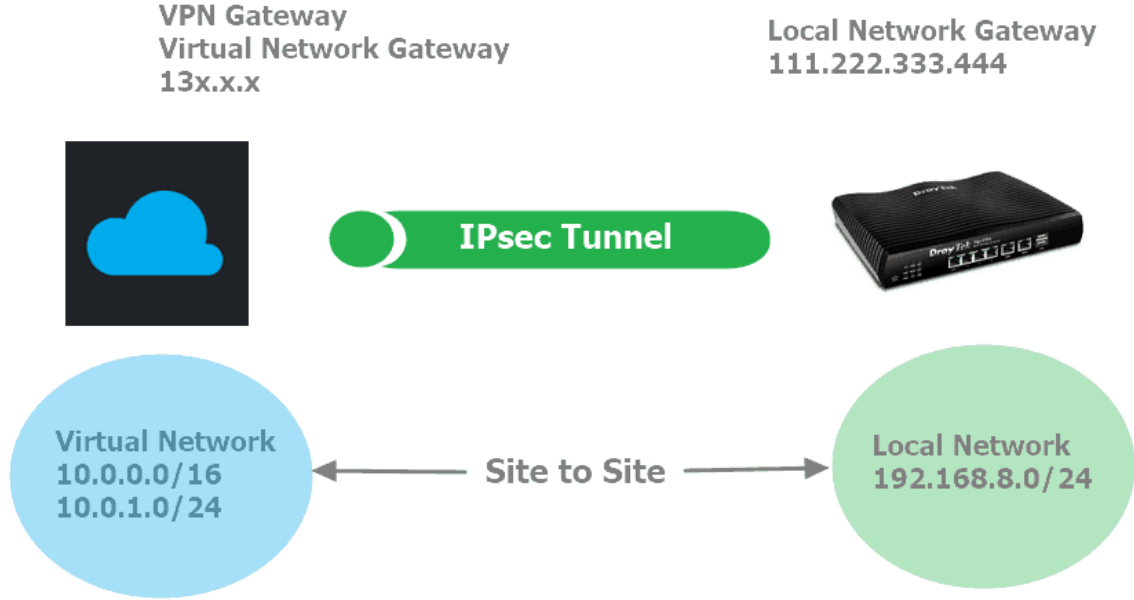


MICROSOFT AZURE VE VIGOR ROUTER ARASINDA IKEv2 VPN

Bu makalede, Microsoft Azure Server ve Vigor Router arasında Dynamic Routing modunda IPsec tünelinin nasıl kurulacağı gösterilmektedir. Ağ topolojisi aşağıda verilmektedir.



Microsoft Azure Server Kurulumu

1. **All Services >> Networking** altında **Virtual Networks** 'e tıklayarak yeni sanal ağlar oluşturabilir veya arama yapabilirsiniz.

All services By category ▼ Collapse all | Expand all

NETWORKING (20)

Virtual networks	★	Virtual networks (classic)	★
Load balancers	★	Application gateways	★
Virtual network gateways	★	Local network gateways	★

2. Sanal Ağları oluşturmak için **Add**'e tıklayın ardından gereken ayarları girin:

- **Name** girin.
- **Address Space** için örneğin 10.0.0.0/16 girin.
- **Source Group** için "Create new" seçeneğini seçin.
- Router'unuza yakın bir **Location** seçin.
- Subnet ayarlarını default olarak ayarlayın. (Azure Subnet'i otomatik olarak oluşturacaktır.)
- **Create** 'e tıklayın.

Virtual networks
預設目錄

+ Add Edit columns More

Filter by name...

NAME ↑↓

* Name
VNet ✓

* Address space ⓘ
10.0.0.0/16
10.0.0.0 - 10.0.255.255 (65536 addresses)

* Subscription
免費試用版 ✓

* Resource group
 Create new Use existing
VNet ✓

* Location
East Asia ✓

Subnet

* Name
default

* Address range ⓘ

Create Automation options

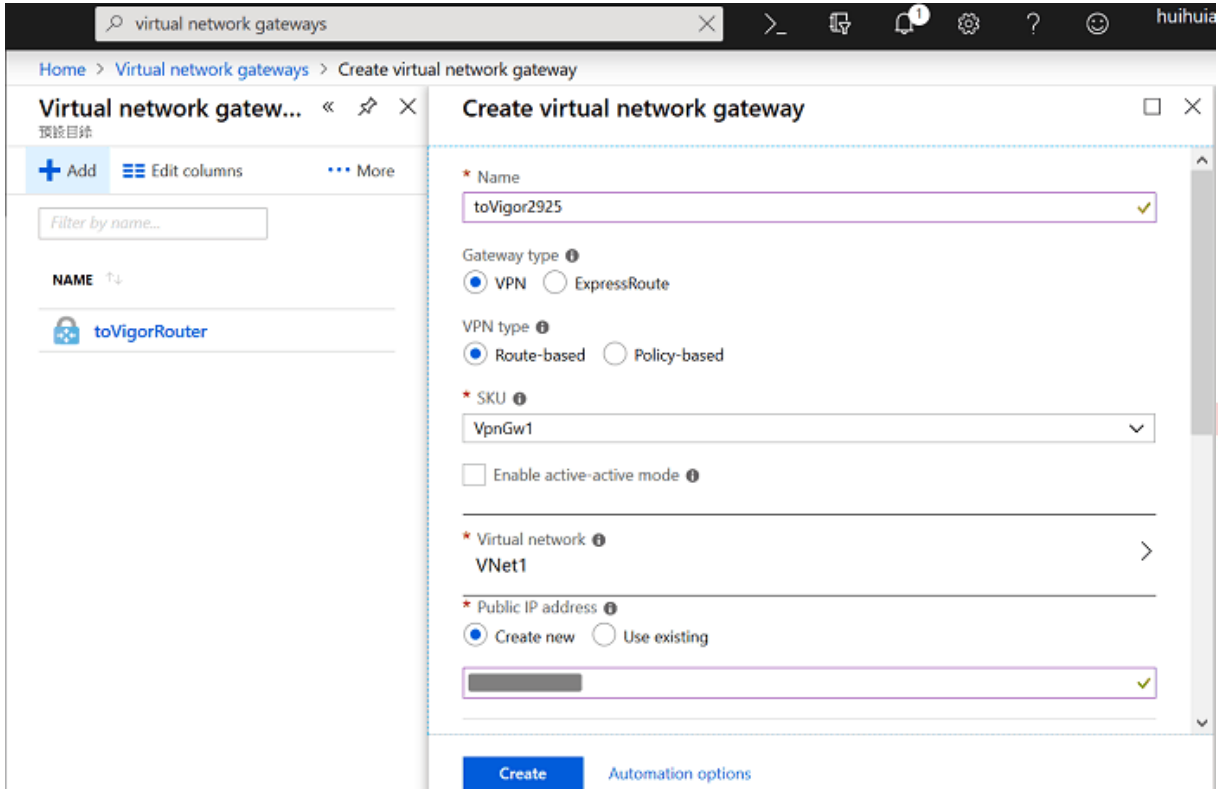
3. **All Services** >> **Networking** altında Virtual Network Gateways'e tıklayarak sanal gateway oluşturun. Bu adımda Azure, VPN Service için Public bir IP tahsis edecektir.

All services Filter By category Collapse all Expand all

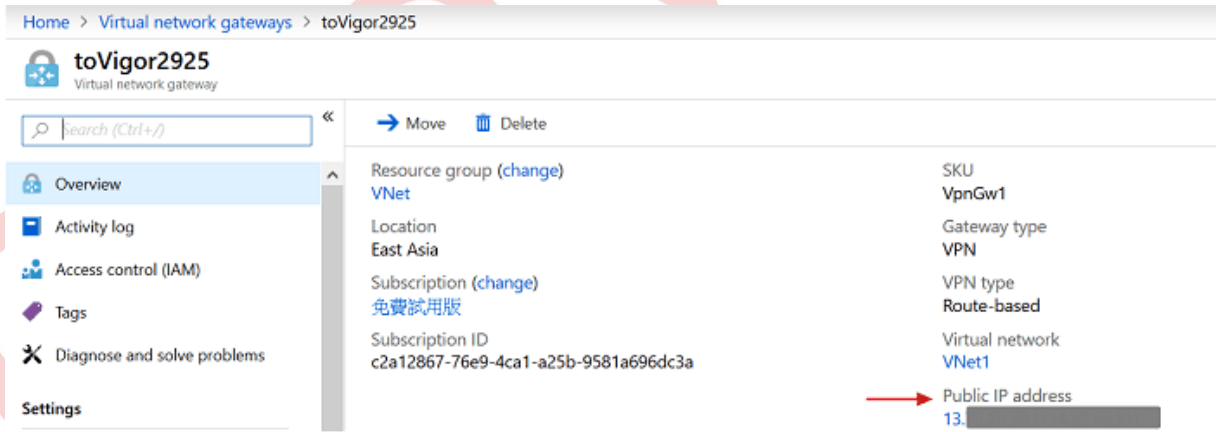
NETWORKING (20)

Virtual networks	★	Virtual networks (classic)	★
Load balancers	★	Application gateways	★
Virtual network gateways	★	Local network gateways	★

4. Sanal gateway oluşturmak için **Add**'e tıklayın ardından gereken ayarları girin.
- **Name** girin.
 - **Gateway type** için "VPN" seçeneğini seçin.
 - **VPN type** için "Route-Based" seçeneğini seçin.
 - **SKU** için "VpnGw1" seçeneğini seçin.
 - **Virtual Network** için VNet1'i seçin. (VNet1 1.adımda oluşturduğumuz sanal ağ)
 - **Public IP** için "Create New" i seçin ve herhangi bir IP'yi girin. (Azure'un neden bir IP adresi girmek istediğinden emin değiliz.)
 - **Create**'e tıklayın.



5. Azure'un VPN Gateway'i için Public IP'yi ayarlaması biraz zaman alabilir. Tamamlandıktan sonra Public IP'yi aynı sayfada görebilirsiniz.



6. Azure'da **Local Network Gateway** oluşturun. . Bu adımda Vigor Router'ın Internet IP'sini ve Local ağını girmemiz gerekiyor ve Vigor Router, bir NAT aygıtının arkasına doğrudan bağlanmamalı, doğrudan internete bağlanmalıdır. Local Network Gateway oluşturmak için **Add**'e tıklayın ardından gereken ayarları girin.
- **Name** girin.
 - **IP Address** için Vigor Router'un WAN IP'sini girin.
 - **Address Space** için Vigor Router'un LAN ağını girin. Örnekte 192.168.8.0/24.
 - **Resource Group** için "Use Existing" e tıklayın ve VNet seçeneğini seçin.
 - **Create**'e tıklayın.

Home > Local network gateways > Create local network gateway

Local network gateways

預設目錄

+ Add Edit columns More

Filter by name...

NAME ↑↓

Create local network gate...

* Name
site8 ✓

* IP address ⓘ
[Redacted] ✓

Address space ⓘ
192.168.8.0/24 ...
Add additional address range ...

Configure BGP settings

* Subscription
免費試用版

* Resource group ⓘ
 Create new Use existing

VNet

Create Automation options

1. Birkaç dakika bekleyin; aynı sayfada oluşturulan Local Network Gateway profilini göreceğiz. Azure ile Vigor Router arasındaki VPN bağlantısını yapılandırmak için Connections'a tıklayın.

Home > Local network gateways > site8

site8

Local network gateway

Search (Ctrl+)

Move Delete

Resource group (change)
VNet

Location
East Asia

Subscription (change)
免費試用版

Subscription ID
c2a12867-76e9-4ca1-a25b-9581a696dc3a

Tags (change)
Click here to add tags

IP address
[Redacted]

Address space
192.168.8.0/24

Overview

Activity log

Access control (IAM)

Tags

Settings

Configuration

Connections

Properties

2. Azure'da VPN bağlantısı oluşturun ve gerekli ayarları girin.

- Connection Type'ı Site-to-Site (IPsec) olarak ayarlayın.
- 3. Adımda oluşturduğumuz Azure VPN Public IP'si olarak **Virtual Gateway**'i seçin.
- 5. Adımda oluşturduğumuz Azure VPN Router'unun Public IP ve ağı olan **Local Network Gateway**'ini seçin.
- **Pre-Shared Key** girin.
- **Resource Group** için VNet seçeneğini seçin.
- **OK**'a tıklayın.

Home > Local network gateways > site8 - Connections > Add connection

Add connection site8

* Name
VPN-Vigor2925 ✓

Connection type ⓘ
Site-to-site (IPsec) ▾

* Virtual network gateway ⓘ
toVigor2925 >

* Local network gateway ⓘ
site8 🔒

* Shared key (PSK) ⓘ
1qaz2wsx ✓

Subscription ⓘ
免費試用版 ▾

Resource group ⓘ
VNet 🔒

OK

Azure'daki VPN yapılandırmalarını tamamladık sonra Vigor Router'da VPN profilini ayarlayacağız.

DrayOS

1. **VPN and Remote Access >> LAN to LAN** sayfasına gidin. Profili aşağıdaki gibi ayarlamak için uygun bir index numarasına tıklayın:
 - **Enable this VPN profile**'ı etkinleştirin.
 - Azure'un Local Network Gateway'inde yapılandırılan IP'yi **Dial-Out Through**'un WAN 'ı olarak girin.
 - **Call Direction** için "Dial-Out" seçeneğini seçin.

- **Always On**'a tıklayın.
- **Dial-Out Settings**'de **IPsec Tunnel** ve **IKEv2** seçeneğini seçin.
- **Server IP/Host Name**'de Azure'un Local Network Gateway'inin Public IP adresini girin.
- Azure'un Connections yapılandırmasındaki **IKE Pre-Shared Key**'i girin.
- **IPsec Security Method** için "AES with Authentication" seçeneğini seçin.
- Proposal ve Key Lifetime ayarlarını yapılandırmak için **Advanced** butonuna tıklayın.

2. IKE gelişmiş ayarlarında,

- **IKE phase1 proposal** için "AES 256_SHA1_G2" yi seçin. (Azure VPN Server yalnızca Diffie-Helman Grup G2'yi desteklemektedir.)
- **IKE phase2 key lifetime**'ı "27000 seconds" olarak değiştirin. (Azure VPN Server Phase2 Key Lifetime için yalnızca P27000 seconds'ı desteklemektedir.)
- **OK**'a tıklayın.

IKE advanced settings

IKE phase 1 mode(IKEv1)	<input type="radio"/> Main mode	<input type="radio"/> Aggressive mode
IKE phase 1 proposal	AES256_SHA1_G2	
IKE phase 2 proposal	AES256_SHA1	
IKE phase 1 key lifetime	28800	(900 ~ 86400)
IKE phase 2 key lifetime	27000	(600 ~ 86400)
Perfect Forward Secret	<input checked="" type="radio"/> Disable	<input type="radio"/> Enable
Local ID		

3. **TCP/IP Network Settings** alanında,

- **Remote Network** ve **Mask** için Azure'un Virtual Network'ü "10.0.0.0" ve "255.255.0.0/16" girin.
- **Local Network** ve **Mask** için "192.168.8.0" ve "255.255.255.0/24" girin.
- Kaydetmek için **OK**'a tıklayın.

5. TCP/IP Network Settings

My WAN IP	0.0.0.0	RIP Direction	Disable
Remote Gateway IP	0.0.0.0	From first subnet to remote network, you have to do	Route
Remote Network IP	10.0.0.0	<input type="checkbox"/> IPsec VPN with the Same Subnets	
Remote Network Mask	255.255.0.0 / 16	<input type="checkbox"/> Change default route to this VPN tunnel (Only active if one single WAN is up)	
Local Network IP	192.168.8.0		
Local Network Mask	255.255.255.0 / 24		
	<input type="button" value="More"/>		

Bundan sonra Vigor Router'dan Azure'a VPN bağlantısı sağlanacaktır. VPN bağlantısı durumunu **VPN and Remote Access >> Connection Management** sayfasından kontrol edebiliriz . VPN bağlantısını doğrulamak için sanal makineyi Azure Sanal Ağına ping yapmaya çalışabiliriz.

VPN Connection Status

All VPN Status		LAN-to-LAN VPN Status		Remote Dial-in User Status				
VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(bps)	Rx Pkts	Rx Rate(bps)	UpTime
1 (to2952)	IPsec Tunnel DES-No Auth		192.168.0.0/24	0	0	6532	136	3:37:46
2 (toVivian)	PPTP		192.168.239.0/24	260	24	380	24	22:47:57
3 (86)	PPTP/MPPE		192.168.1.0/24	0	0	0	0	8:6:10
4 (Azure)	IKEv2 IPsec Tunnel AES-SHA1 Auth		10.0.0.0/16	15	24	37	24	0:31:37

Linux

1. **VPN and Remote Access >> VPN Profiles >> IPsec** sayfasına gidin. Profil oluşturmak için **Add**'e tıklayın. Temel ayarlarda:

- **Enable**'ı etkinleştirin.
- **Auto Dial-Out** için "Enable" ve **Always Dial-Out** seçeneklerini seçin.
- Azure'un Local Network Gateway'indeki IP'nin WAN'ını **Dial-Out Through Interface** için girin.
- Router'un Local IP'sini **Local IP/Subnet Mask**'a girin.
- **Remote Host IP**'ye Azure'un Virtual Network Gateway'inin Public IP'sini girin.
- **IKE Protocol** için "IKEv2" seçeneğini seçin. (Azure Dinamik Routing IKEv2 kullanır.)
- **Auth Type** için "PSK" seçeneğini seçin.
- Azure'un Connections ayarlarında yapılandırılan **Pre-Shared Key** 'i girin.

Profile : Azure

Enable

Basic Advanced GRE Proposal Multiple SAs

Auto Dial-Out : a. Enable Disable Always Dial-Out

For Remote Dial-In User : Enable Disable

Dial-Out Through : b. wan2 Default WAN IP WAN Alias

Failover to :

Local IP / Subnet Mask : c. 192.168.8.0 255.255.255.0/24

Local Next Hop : 0.0.0.0 (0.0.0.0 : default gateway)

Remote Host : d. Azure Virtual Gateway IP

Remote IP / Subnet Mask : 10.0.0.0 e. 255.255.0.0/16

Add Save

IP	Subnet Mask
No items to show	

More Remote Subnet :

IKE Protocol : f. IKEv2

Auth Type : g. PSK

Preshared Key : h. ****

Local ID : (optional)

Remote ID : (optional)

Security Protocol : ESP

2. Advanced sekmesine gidin. **Phase2 Key Life Time** 'ı "27000" saniye olarak ayarlayın.

Profile : Azure

Enable

Basic **Advanced** GRE Proposal Multiple SAs

Phase1 Key Life Time : 28800 seconds

Phase2 Key Life Time : 27000 seconds

Perfect Forward Secrecy Status : Enable Disable

Dead Peer Detection Status : Enable Disable

3. Proposal sekmesine gidin:

- **IKE Phase1 Proposal** için “AES 256_G2” seçeneğini seçin.
- **IKE Phase2 Proposal** için “SHA1” seçeneğini seçin.
- **IKE Phase2 Proposal** için “AES 256 with auth” seçeneğini seçin.
- **IKE Phase2 Proposal** için “SHA1” seçeneğini seçin.
- Ayarları kaydetmek için **Apply**'a tıklayın.

Profile : Azure

Enable

Basic Advanced GRE **Proposal** Multiple SAs

IKE Phase1 Proposal [Dial-Out] : AES256 G2

IKE Phase1 Authentication [Dial-Out] : SHA1

IKE Phase2 Proposal [Dial-Out] : AES256 with auth

IKE Phase2 Authentication [Dial-Out] : SHA1

Accepted Proposal [Dial-In] : acceptall

Bundan sonra Vigor Router'dan Azure'a VPN bağlantısı sağlanacaktır. VPN bağlantısı durumunu **VPN and Remote Access >> Connection Management** sayfasından kontrol edebiliriz . VPN bağlantısını doğrulamak için sanal makineyi Azure Sanal Ağına ping yapmaya çalışabiliriz.

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

Connection Management History

Dial-Out tool

IPsec PPTP SSL Profiles : Connect Refresh Auto Refresh : 1 Minute

VPN Connection Status

VPN	Type	Interface	Remote IP	Virtual Network	Up Time	RX Rate	TX Rate	RX Byte
1	draytektest	PPTP	wan2	192.168.239.12	01:15:52	1.46 (Kbps)	12.59 (Kbps)	5.41 (MB)
2	vkit80	PPTP	wan2	192.168.239.11	11:06:42	0(bps)	0(bps)	147.16 (KB)
3	v	PPTP	wan2	192.168.239...	22:45:11	0(bps)	0(bps)	1.02 (MB)
4	2952	IPsec/AES...	wan2	192.168.0.0...	16:24:18	0(bps)	0(bps)	256.32 (KB)
5	Azure	IPsec/AES...	wan2	10.0.0.0/16	20:24:37	0(bps)	0(bps)	38.34 (KB)
6	MIS3	IPsec/AES...	wan2	172.16.2.0/24	20:25:17	2.45 (Kbps)	1.56 (Kbps)	79.07 (MB)