

## FortiGate ile Policy Based Routing Kullanımı

Entegratör firmalar, birden fazla müşteriyle aynı anda IPsec bağlantıları oluşturmak zorunda kalabilmektedir. Bu durum özellikle aynı subnetleri paylaşan müşterilerle çalışırken büyük bir yönetim zorluğu doğurur. Bu çalışmada, Policy-Based Routing (PBR) ile IPsec yönetimi sağlayarak, overlapping subnetler arasında trafik yönlendirmenin nasıl olduğunu anlatacağım.

Ayrıca, PNETLab ortamında bir laboratuvar kurarak bu yapılandırmayı test edeceğiz.

### **Senaryo: Overlapping Subnetler ile IPsec Trafik Yönetimi**

Bir ağ ortamında, A ve B müsterisi aynı subnetleri kullanıyorsa (örneğin 172.22.10.0/24), ancak farklı cihazları farklı müşterilere yönlendirilmek istiyorsanız, Policy-Based Routing (PBR) ve IPsec VPN kombinasyonunu kullanarak yönlendirme yapabiliriz.

Örnek senaryomuz:

- A müsterisine giden trafik, 1.1.1.1 IP'sine sahip makineden çıkmalı.
- B müsterisine giden trafik, 1.1.1.5 IP'sine sahip makineden çıkmalı.
- Her iki müsterinin subneti 172.22.10.0/24 olduğu için, gelen trafigi doğru şekilde yönlendirmeliyiz.
- IP değişikliği yapılamaz, bu nedenle IPsec tünel yönlendirmesi ile çözüm üreteceğiz.

Bu noktada, Policy-Based IPsec Routing ve NAT kullanarak trafigi ayırtıracagız.

### **PNETLab Üzerinde Lab Kurulumu**

Bu senaryoyu test etmek için PNETLab ortamında bir yapı kuracağız. Kullanacağımız temel bileşenler:

- 5 adet FortiGate cihazı
- 1 adet merkezi HQ (Merkez ofis) FortiGate
- 2 adet ISP (ISP1 ve ISP2) FortiGate cihazı
- 2 müsteri (Customer A ve Customer B)
- Her müsteri için 1 adet VPC (Virtual PC)

### **Ağ Topolojisi**

1-HQ'yu ISP1 ve ISP2'ye bağla

2-HQ'nun port1'ini ISP1'in port1'ine bağla.

The screenshot shows the FortiGate interface configuration. On the left, the navigation menu includes Network, Interfaces, DNS, Packet Capture, SD-WAN, Static Routes, Policy Routes, RIP, OSPF, BGP, Routing Objects, Multicast, Policy & Objects, Security Profiles, VPN, User & Authentication, System, Security Fabric, Log & Report. A red circle labeled '1' is on the 'System' icon.

**Physical Interface (8)**

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients
fortilink	802.3ad Aggregate			Dedicated to FortiSwitch PING Security Fabric Connection	10.255
ISP (port1)	Physical Interface		10.10.10.2/255.255.255.252	PING HTTPS SSH <b>HTTP</b> FMG-Access	
<b>ISP2 (port3)</b>	Physical Interface		20.20.20.2/255.255.255.252	PING	
port2	Physical Interface		192.168.1.90/255.255.255.0	PING HTTPS <b>HTTP</b>	
port4	Physical Interface		0.0.0.0/0.0.0.0		
port5	Physical Interface		0.0.0.0/0.0.0.0		
port6	Physical Interface		0.0.0.0/0.0.0.0		
port7	Physical Interface		0.0.0.0/0.0.0.0		
port8	Physical Interface		0.0.0.0/0.0.0.0		

**Tunnel Interface (1)**

Name	Type	Members	IP/Netmask
NAT Interface (naf.root)	Tunnel Interface		0.0.0.0/0.0.0.0

3-HQ'nun port3'ünü ISP2'nin port1'ine bağla.

4-ISP1 ile Customer A bağlantısını yap

5-ISP1'in port3'ünü Customer A'nın FortiGate'ine bağla.

6-ISP2 ile Customer B bağlantısını yap

7-ISP2'nin port3'ünü Customer B'nın FortiGate'ine bağla.

8-VPC Atamaları

- HQ için 2 adet VPC atanacak.
- Customer A için 1 adet VPC atanacak.
- Customer B için 1 adet VPC atanacak.

### HQ ve ISP Cihazları Arasındaki Yönlendirme Ayarları

Şimdi HQ ile ISP1 ve ISP2 arasındaki bağlantıları yapılandıracağız. İlk olarak, HQ ve ISP1 arasındaki bağlantıyı 10.10.10.0/30 subneti üzerinden kuruyoruz. Benzer şekilde, ISP1'den Customer A'ya olan bağlantıyı 30.30.30.0/30 subneti ile sağlıyoruz.

The screenshot shows the 'Edit Interface' configuration for 'port1'. The interface is named 'port1' with an alias 'ISP'. It is a 'Physical Interface' assigned to VRF ID 0. The 'Addressing mode' is set to 'Manual' with IP/Netmask '10.10.10.2/30'. Under 'Administrative Access', 'IPv4' options like HTTPS, FMG-Access, and SSH are checked. The 'DHCP Server' option is also enabled.

The screenshot shows the list of interfaces for 'ISP1'. It includes a summary of 24 ports, a creation tool, and a detailed table. In the table, 'HQ (port1)' is highlighted with a red box. It is a 'Physical Interface' with IP '10.10.10.2/30' and administrative access including PING, HTTPS, SSH, and FMG-Access.

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Range
802.3ad Aggregate ①	802.3ad Aggregate			PING Security Fabric Connection		10.255.1.2-10.255.1.254
<b>HQ (port1)</b>	Physical Interface		10.10.10.2/30	PING HTTPS SSH <b>HTTP FMG-Access</b>		
MGT (port2)	Physical Interface		192.168.1.91/255.255.255.0	PING HTTPS <b>HTTP</b>		
port4	Physical Interface		0.0.0.0/0.0.0.0			
port5	Physical Interface		0.0.0.0/0.0.0.0			
port6	Physical Interface		0.0.0.0/0.0.0.0			
port7	Physical Interface		0.0.0.0/0.0.0.0			
port8	Physical Interface		0.0.0.0/0.0.0.0			
Tunnel Interface ①	Tunnel Interface		0.0.0.0/0.0.0.0			
NAT Interface (naf.root)	Tunnel Interface		0.0.0.0/0.0.0.0			

Ağ trafiğinin doğru şekilde yönlendirilmesi için, HQ tarafında statik route ekleyerek belirli IP bloklarına nasıl ulaşacağımızı tanımlamamız gerekiyor. HQ cihazında 30.30.30.0/30 bloğuna gidecek trafiğin ISP1 üzerinden yönlendirilmesini sağlayacağız.

Destination	Gateway IP	Interface	Status
30.30.30.0/24	10.10.10.1	ISP (port1)	Enabled

Bunun için HQ cihazında şu yapılandırmayı yapıyoruz:

- Eğer hedef 30.30.30.0/30 ise, trafik ISP1 üzerinden yönlendirilecek. Bu
- bağlantının gateway adresi 10.10.10.1 olacak.

Bu ayarları uyguladıktan sonra, artık Customer A'dan HQ'ya giden ve HQ'dan Customer A'ya dönen trafik doğru şekilde yönlendirilecek.

The screenshot shows the Firewall Policy configuration screen. It lists three rules:

- Customer\_To\_HQ:** Source is all, Destination is all, Schedule is always, Service is ALL, Action is ACCEPT, NAT is disabled, Security Profiles is no-inspection, and Log is All.
- HQ\_TO\_CUSTOMER:** Source is all, Destination is all, Schedule is always, Service is ALL, Action is ACCEPT, NAT is disabled, Security Profiles is no-inspection, and Log is All.
- Implicit:** This rule is highlighted in blue.

The screenshot shows the "New Static Route" configuration dialog for CustomerA. The fields are as follows:

- Destination:** Subnet 0.0.0.0/0.0.0.0
- Gateway Address:** 30.30.30.1
- Interface:** ISP-1 (port1)
- Administrative Distance:** 10
- Comments:** Write a comment... (0/255)
- Status:** Enabled

On the right side, there is an "Additional Information" panel with links to API Preview, Documentation, Online Help, and Video Tutorials. At the bottom are OK and Cancel buttons.

## ISP2 Tarafının Yapılandırılması

Şimdi ISP2 bağlantılarını yapılandıracagız. Daha önce HQ tarafındaki port3'e 20.20.20.2/30 IP'sini atamıştık. Şimdi, ISP2 tarafında da uygun IP yapılandırmalarını yaparak HQ ile bağlantıyı tamamlayacağız.

The screenshot shows the FortiGate VM64-KVM interface configuration. It displays two main sections: ISP2 (top) and CustomerB (bottom). Both sections show a summary of interface types and configurations.

**ISP2 Summary:**

- 802.3ad Aggregate:** fortalink (Type: 802.3ad Aggregate, Dedicated to FortiSwitch, Members: 1-23, IP/Netmask: 10.255.1.2-10.255.1.254)
- Physical Interface:**
  - CustomerB (port3): Physical Interface, IP/Netmask: 40.40.1/255.255.255.252 (Access: PING, HTTPS, SSH, HTTP, FMC-Access)
  - HQ (port1): Physical Interface, IP/Netmask: 20.20.20.1/255.255.255.252 (Access: PING, HTTPS, SSH, HTTP, FMC-Access)
  - port2: Physical Interface, IP/Netmask: 192.168.1.92/255.255.255.0 (Access: PING, HTTPS, SSH, HTTP, FMC-Access)
  - port4: Physical Interface, IP/Netmask: 0.0.0.0/0.0.0.0
  - port5: Physical Interface, IP/Netmask: 0.0.0.0/0.0.0.0
  - port6: Physical Interface, IP/Netmask: 0.0.0.0/0.0.0.0
  - port7: Physical Interface, IP/Netmask: 0.0.0.0/0.0.0.0
  - port8: Physical Interface, IP/Netmask: 0.0.0.0/0.0.0.0
- Tunnel Interface:** NAT interface (naf.root) (Type: Tunnel Interface, IP/Netmask: 0.0.0.0/0.0.0.0)

**CustomerB Summary:**

- 802.3ad Aggregate:** fortalink (Type: 802.3ad Aggregate, Dedicated to FortiSwitch, Members: 1-23, IP/Netmask: 10.255.1.2-10.255.1.254)
- Physical Interface:**
  - ISP2 (port1): Physical Interface, IP/Netmask: 40.40.2/255.255.255.252 (Access: PING, HTTPS, SSH, HTTP, FMC-Access)
  - port2: Physical Interface, IP/Netmask: 192.168.1.94/255.255.255.0 (Access: PING, HTTPS, SSH, HTTP, FMC-Access)
  - port3: Physical Interface, IP/Netmask: 0.0.0.0/0.0.0.0
  - port4: Physical Interface, IP/Netmask: 0.0.0.0/0.0.0.0
  - port5: Physical Interface, IP/Netmask: 0.0.0.0/0.0.0.0
  - port6: Physical Interface, IP/Netmask: 0.0.0.0/0.0.0.0
  - port7: Physical Interface, IP/Netmask: 0.0.0.0/0.0.0.0
  - port8: Physical Interface, IP/Netmask: 0.0.0.0/0.0.0.0
- Tunnel Interface:** NAT interface (naf.root) (Type: Tunnel Interface, IP/Netmask: 0.0.0.0/0.0.0.0)

This screenshot is identical to the one above, showing the FortiGate VM64-KVM interface configuration for ISP2 and CustomerB. The interface types, configurations, and access details are the same as described in the first screenshot.

Bu aşamada, ISP2 üzerinden Customer B'ye yönlendirme yapacağız. Customer B için 40.40.40.0/30 subnetini kullanarak, tüm bilinmeyen istekleri ISP2'ye yönlendiren bir statik route ekleyeceğiz. Böylece, Customer B'den gelen trafigin ISP2 üzerinden HQ'ya ulaşmasını sağlayacağız.

The screenshot shows the 'Static Routes' section of the CustomerB configuration. A single static route is listed:

Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	40.40.40.1	ISP2 (port1)	Enabled	

Aynı mantıkla HQ cihazında bir statik route ekleyerek 40.40.40.0/30 bloğuna giden trafiğin ISP2 üzerinden yönlendirilmesini sağlayacağız.

The screenshot shows the 'Static Routes' section of the HQ configuration. A new static route is being created with the following details:

Destination	Subnet	Comments	Additional Information
40.40.40.0/24	Internet Service	Write a comment... / 0/255	API Preview Documentation Online Help Video Tutorials
Gateway Address	20.20.20.1		
Interface	ISP2 (port3)		
Administrative Distance	10		
Status	<input checked="" type="button"/> Enabled	<input type="button"/> Disabled	

At the bottom right are 'OK' and 'Cancel' buttons.

Bu noktada, her iki müşteri cihazı da kendi ISP'leri üzerinden HQ ile iletişim kurabilir hale gelecek.

## Software Switch Kullanarak Aynı IP Bloğunu Paylaşırma

Şimdi HQ cihazında bir Software Switch oluşturacağız. Software Switch, iki fiziksel portu birleştirerek aynı IP subnetini kullanmalarını sağlar. Bu yöntem, aynı IP bloğuna sahip olan cihazları tek bir ağa birleştirmek için kullanılır.

The screenshot shows the FortiGate VM64-KVM interface configuration. On the left sidebar, under 'Network' > 'Interfaces', 'Software Switch' is selected. The main pane displays a table of interfaces. A red box highlights the 'Software Switch' section, which contains one entry: 'LOCAL' (Type: Software Switch) with ports 'port4' and 'port5' assigned to it, and an IP address of 5.5.5.5/255.255.255.0.

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP F
802.3ad Aggregate	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection		10.255.1.2-1
Physical Interface	Physical Interface					
ISP (port1)	Physical Interface		10.10.10.2/255.255.255.252	PING HTTPS SSH HTTP FMG-Access		
ISP2 (port3)	Physical Interface		20.20.20.2/255.255.255.252	PING		
port2	Physical Interface		192.168.1.90/255.255.255.0	PING HTTPS HTTP		
port6	Physical Interface		0.0.0.0/0.0.0.0			
port7	Physical Interface		0.0.0.0/0.0.0.0			
port8	Physical Interface		0.0.0.0/0.0.0.0			
Software Switch	Software Switch	port4 port5	5.5.5.5/255.255.255.0	PING		5.5.5.2-5.5.5.
Tunnel Interface	Tunnel Interface		0.0.0.0/0.0.0.0			
NAT interface (naf.root)	Tunnel Interface					

Örneğin, port4 ve port5'in aynı IP aralığını kullanmasını istiyoruz. Bu yüzden Software Switch oluşturarak 5.5.5.0/24 subnetini atayacağız.

FortiGate üzerinde Software Switch oluşturmak için şu adımları takip ediyoruz:

1. FortiGate arayüzüne girin ve sol üst köşedeki "+" butonuna tıklayın.
2. Yeni bir arayüz eklerken "Type" olarak "Software Switch" seçin.
3. Port4 ve Port5'i Software Switch içeresine dahil edin.
4. Yeni Software Switch'e 5.5.5.0/24 subnetini atayın.

Bu yapılandırma sayesinde, bu iki portu kullanan cihazlar aynı IP bloğunu paylaşacak ve aynı ağ içerisinde haberleşebilecek.

## FortiGate ile IPsec VPN, Statik Yönlendirme ve Trafik Yönetimi

Müşteri lokasyonlarıyla merkez ofis (HQ) arasında güvenli bağlantı sağlamak için IPsec VPN tünelleri, statik yönlendirme ve firewall kuralları ile doğru trafik yönetimi gereklidir. Bu yapılandırmada, Customer A ve Customer B ile HQ arasındaki iletişim güvenli hale getireceğiz ve istemcilerin doğru şekilde çalışmasını sağlayacağız.

## Customer A İçin IPsec VPN, Statik Route ve Firewall Yapılandırması

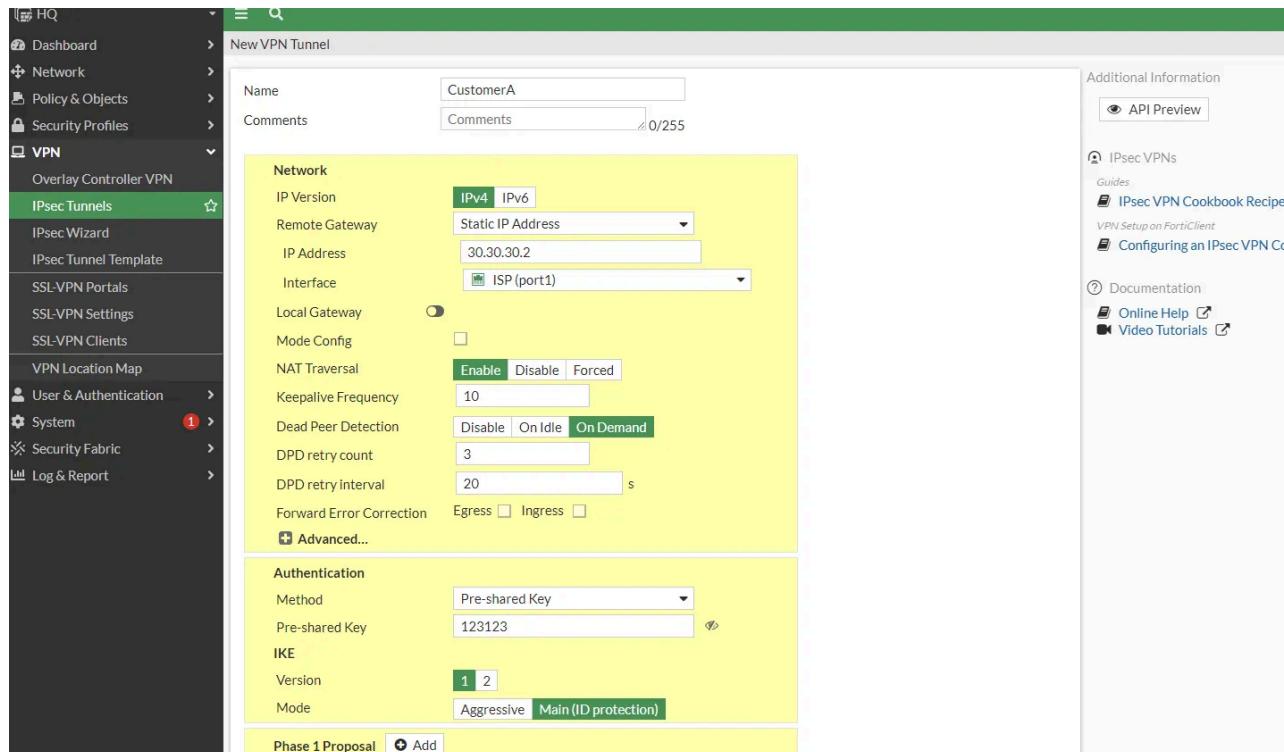
## IPsec VPN Tünelinin Oluşturulması (HQ Tarafında)

Öncelikle Customer A için bir IPsec tüneli oluşturacağız. Bu tünelin amacı, HQ ile Customer A arasındaki trafiği güvenli bir şekilde yönlendirmek ve Customer A'ya giderken 30.30.30.2 IP adresinin kullanılmasını sağlamaktır.

### Adımlar:

HQ tarafında yeni bir IPsec tüneli oluşturun.

- Tünele bir isim verin (örneğin, CustomerA\_Tunnel ).
- Customer A'nın dış IP adresini Remote Gateway olarak girin.
- Kimlik doğrulama yöntemi olarak Pre-Shared Key belirleyin.
- Şifreleme için AES-256 ve SHA256 kullanın.
- Local Subnet olarak HQ tarafından aldığı (5.5.5.0/24), Remote Subnet olarak Customer A'nınliğini (172.22.10.0/24) belirleyin.



New VPN Tunnel

**Diffie-Hellman Groups**

- 32
- 31
- 30
- 29
- 28
- 27
- 26
- 25
- 24
- 23
- 22
- 21
- 20
- 19
- 18
- 17
- 16
- 15
- 14
- 5
- 2
- 1

Key Lifetime (seconds): 86400

Local ID:

**XAUTH**

Type: Disabled

**Phase 2 Selectors**

Name	Local Address	Remote Address
CustomerA	0.0.0.0/0.0.0	0.0.0.0/0.0.0

**New Phase 2**

Name: CustomerA

Comments: Comments

Local Address: Subnet 0.0.0.0/0.0.0

Remote Address: Subnet 0.0.0.0/0.0.0

**Advanced...**

Phase 2 Proposal: **Add**

Encryption: DES Authentication: MD5

Enable Replay Detection:

Enable Perfect Forward Secrecy (PFS):

Diffie-Hellman Group:  32  31  30  29  28  27  
 26  25  24  5  2  1

Local Port: All

Remote Port: All

Protocol: All

Auto-negotiate:

Autovpn Keep Alive:

Customer A tarafında aynı ayarlarla bir IPsec tüneli oluşturun.

### Phase 2 ayarlarını yapın:

- Local Subnet: 172.22.10.0/24
- Remote Subnet: 5.5.5.0/24

New VPN Tunnel

**Network**

Name: HQ

Comments: Comments /255

IP Version: IPv4

Remote Gateway: Static IP Address

IP Address: 10.10.10.2

Interface: ISP-1 (port1)

Local Gateway:

Mode Config:

NAT Traversal: Enable

Keepalive Frequency: 10

Dead Peer Detection: On Demand

DPD retry count: 3

DPD retry interval: 20 s

Forward Error Correction: Egress  Ingress

**Advanced...**

**Authentication**

Method: Pre-shared Key

Pre-shared Key: \*\*\*\*\*

**IKE**

Version: 1 2

Mode: Aggressive Main (ID protection)

**Phase 1 Proposal**: **Add**

Encryption: DES Authentication: MD5

Diffie-Hellman Group:  32  31  30  29  28  27

## Statik Yönlendirme (Static Route) Tanımları

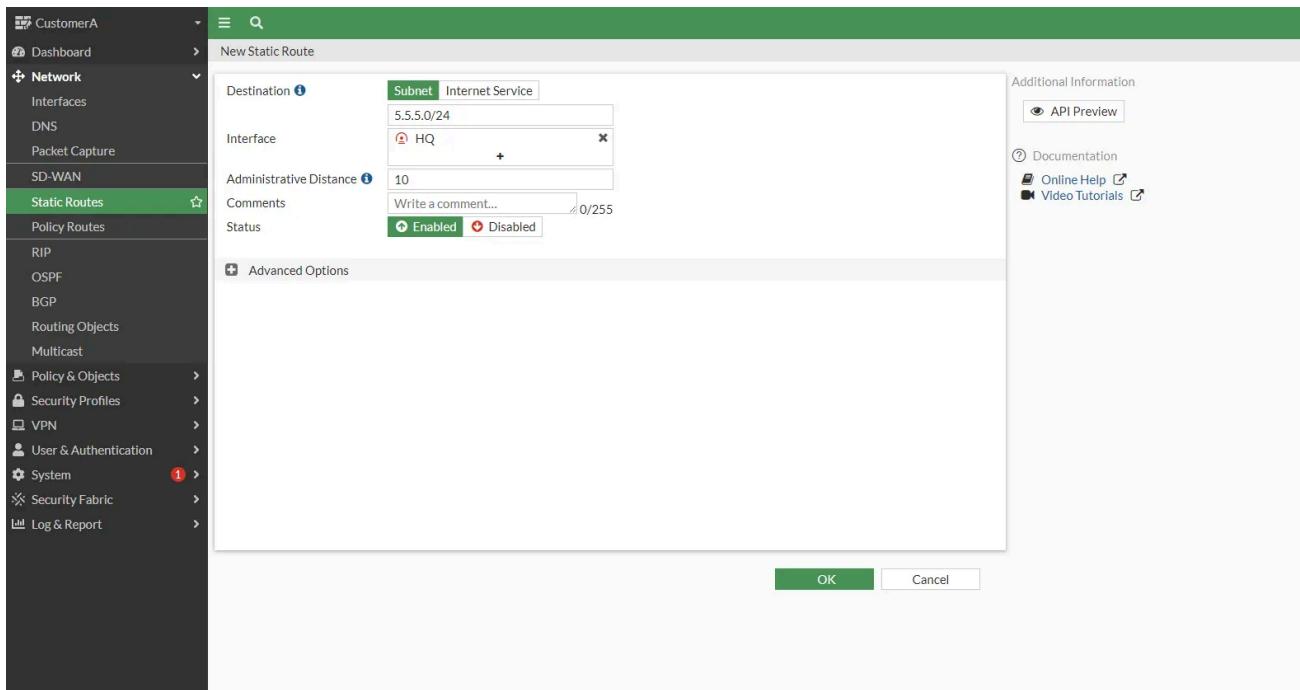
VPN tünelinin çalışabilmesi için statik route eklememiz gerekiyor. Bu yönlendirme, Customer A'dan gelen trafiğin tünel üzerinden yönlendirilmesini sağlayacaktır.

**HQ Tarafında:**

- 172.22.10.0/24 ağına giden trafiğin CustomerA\_Tunnel üzerinden gitmesini sağlayacak bir statik route eklenir.

**Customer A Tarafında:**

- 5.5.5.0/24 ağına giden trafiğin CustomerA\_Tunnel üzerinden gitmesi için statik route tanımlanır.



Bu ayarlar sayesinde, Customer A ile HQ arasındaki trafik doğru şekilde yönlendirilecektir.

## Firewall Kurallarının Eklenmesi

HQ tarafında Customer A için bir firewall kuralı oluşturulur:

- 5.5.5.0/24'ten 172.22.10.0/24 ağına giden trafiğe izin verilir.
- Güvenli bağlantının çalışabilmesi için tüm hizmetler açık olmalıdır.

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
CustomerA → LOCAL	all	all	always	ALL	✓ ACCEPT	✗ Disabled	ssl no-inspection	✓ All	0B
CustomerB → LOCAL	all	all	always	ALL	✓ ACCEPT	✗ Disabled	ssl no-inspection	✓ All	0B
LOCAL → CustomerA	all	all	always	ALL	✓ ACCEPT	✗ Disabled	ssl no-inspection	✓ All	0B
LOCAL → CustomerB	all	all	always	ALL	✓ ACCEPT	✗ Disabled	ssl no-inspection	✓ All	0B
Implicit									

Customer A tarafında da aynı şekilde bir kural oluşturulur:

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
HQ → port3	all	all	always	ALL	✓ ACCEPT	✗ Disabled	ssl no-inspection
port3 → HQ	all	all	always	ALL	✓ ACCEPT	✗ Disabled	ssl no-inspection
Implicit							

- 172.22.10.0/24'ten 5.5.5.0/24 ağına giden trafiğe izin verilir.

Bu kurallar, VPN bağlantısının her iki yönlü çalışmasını sağlar.

## Customer B İçin IPsec VPN, Statik Route ve Firewall Yapılandırması IPsec

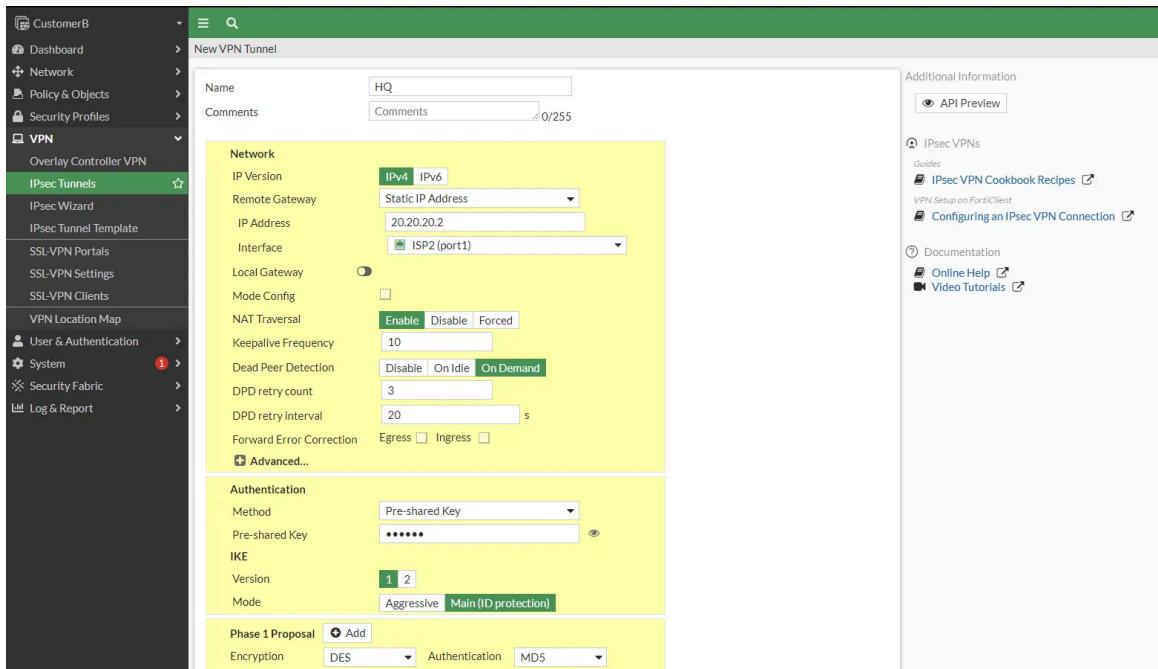
### VPN Tünelinin Oluşturulması (HQ Tarafında)

Customer B için oluşturulacak VPN tüneli, ISP2 üzerinden çalışacak ve HQ tarafında 40.40.40.2 IP adresi kullanılacaktır.

#### Adımlar:

HQ tarafında yeni bir IPsec tüneli oluşturun.

- Tünele CustomerB\_Tunnel adını verin.
- Customer B'nin dış IP adresini Remote Gateway olarak girin.
- Kimlik doğrulama olarak Pre-Shared Key belirleyin.
- Şifreleme olarak AES-256 ve SHA256 kullanın.
- Local Subnet olarak HQ tarafından ağı (5.5.5.0/24), Remote Subnet olarak Customer B'nin ağını (172.22.10.0/24) belirleyin.



Customer B tarafında aynı ayarlarla bir IPsec tüneli oluşturun.

Phase 2 ayarlarını tamamlayın:

- Local Subnet: 172.22.10.0/24
- Remote Subnet: 5.5.5.0/24

## Statik Yönlendirme (Static Route) Tanımları

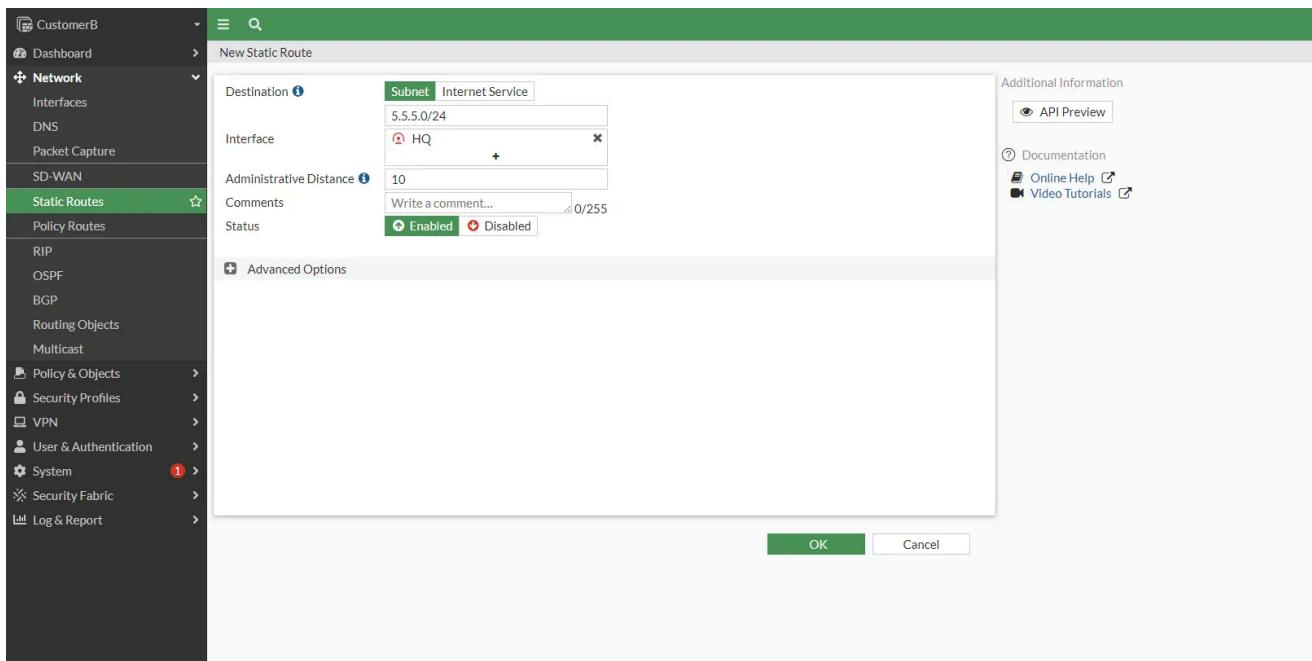
VPN bağlantısının çalışabilmesi için HQ ve Customer B tarafında statik yönlendirmeler yapılmalıdır.

**HQ Tarafında:**

- 172.22.10.0/24 ağına giden trafik CustomerB\_Tunnel üzerinden yönlendirilir.

**Customer B Tarafında:**

- 5.5.5.0/24 ağına giden trafik CustomerB\_Tunnel üzerinden yönlendirilir.



Bu yapılandırma ile Customer B, HQ ile sorunsuz bir şekilde haberleşecektir.

## Firewall Kurallarının Eklenmesi

HQ tarafında Customer B için bir firewall kuralı oluşturulur:

- 5.5.5.0/24'ten 172.22.10.0/24 ağına giden trafiğe izin verilir.

Customer B tarafında da benzer bir firewall kuralı oluşturulur:

- 172.22.10.0/24'ten 5.5.5.0/24 ağına giden trafiğe izin verilir.

Bu ayarlar sayesinde Customer B ile HQ arasında güvenli bir bağlantı sağlanır.

Name	Source	Destination	Schedule	Action	NAT	Security Profiles	Log
Port3_To_HQ	all	all	always	ALL	ACCEPT	Disabled	no-inspection UTM
port3→HQ	all	all	always	ALL	ACCEPT	Disabled	no-inspection UTM
HQ_To_Port3	all	all	always	ALL	ACCEPT	Disabled	no-inspection UTM

## VPC, DHCP Yapılandırması ve İstemcilerin Bağlanması

Müşteri tarafındaki istemcilerin IP alabilmesi ve IPsec tünel üzerinden trafigin yönlendirilmesi için DHCP yapılandırmasını tamamlamamız gereklidir.

### Customer A Tarafında:

The screenshot shows the FortiGate UI under the 'Network' > 'Interfaces' section. The interface 'Client (port3)' is selected. The configuration includes:

- Name:** Client (port3)
- Alias:** Client
- Type:** Physical Interface
- VRF ID:** 0
- Role:** Undefined
- Address:**
  - Addressing mode:** Manual (selected)
  - IP/Netmask:** 172.22.10.1/255.255.255.0
  - Secondary IP address:** (disabled)
- Administrative Access:**
  - IPv4:**
    - HTTPS
    - PING
    - SSH
    - SNMP
    - RADIUS Accounting
    - Security Fabric Connection
  - Receive LLDP:** Use VDOM Setting (selected), Enable (selected)
  - Transmit LLDP:** Use VDOM Setting (selected), Enable (selected)
- DHCP Server:**
  - DHCP status:** Enabled (selected)
  - Address range:** 172.22.10.2-172.22.10.254
  - Netmask:** 255.255.255.0
  - Default gateway:** Same as Interface IP (selected)

### Customer B Tarafında:

172.22.11.1/24 subnetini port 3 kısmına vermek yeterlidir

VPC de ip alımı için dhcp veya ip dhcp yazmak yeterlidir.

### Policy-Based Routing (PBR) ile Trafik Yönlendirme ve Ağ Yönetimi

Customer B'nin zaman zaman 40.40.40.4 ile ISP2 üzerinden, bazen de 30.30.30.4 ile ISP1 üzerinden HQ'ya yönlendirildiğini fark ettim. Aynı şekilde, HQ'dan 5.5.5.x IP bloğundan ping attığımızda trafigin bazen ISP1, bazen ISP2 üzerinden gittiğini gördük. Bu durum, trafigin belirli bir düzen içinde yönlendirilmesini ve stabil bir yapı oluşturulmasını engelliyordu.

Bu noktada PBR (Policy-Based Routing) kullanarak her trafigin belirli bir ISP üzerinden yönlendirilmesini sağladık. Ancak, yönlendirme kurallarının eski bağlantılar üzerinde etkili olabilmesi için öncelikle aktif bağlantıları sıfırlamamız gerekiyor.

### Bağlantıların Sıfırlanması ve Yeni Yönlendirme Kurallarının Etkinleştirilmesi

Öncelikle, firewall üzerinde daha önce açılmış bağlantıları kapatarak eski yönlendirme tablolarının devre dışı kalmasını sağladık. Bunun için:

- “diagnose sys session clear” komutunu kullanarak mevcut oturumları sıfırladık.

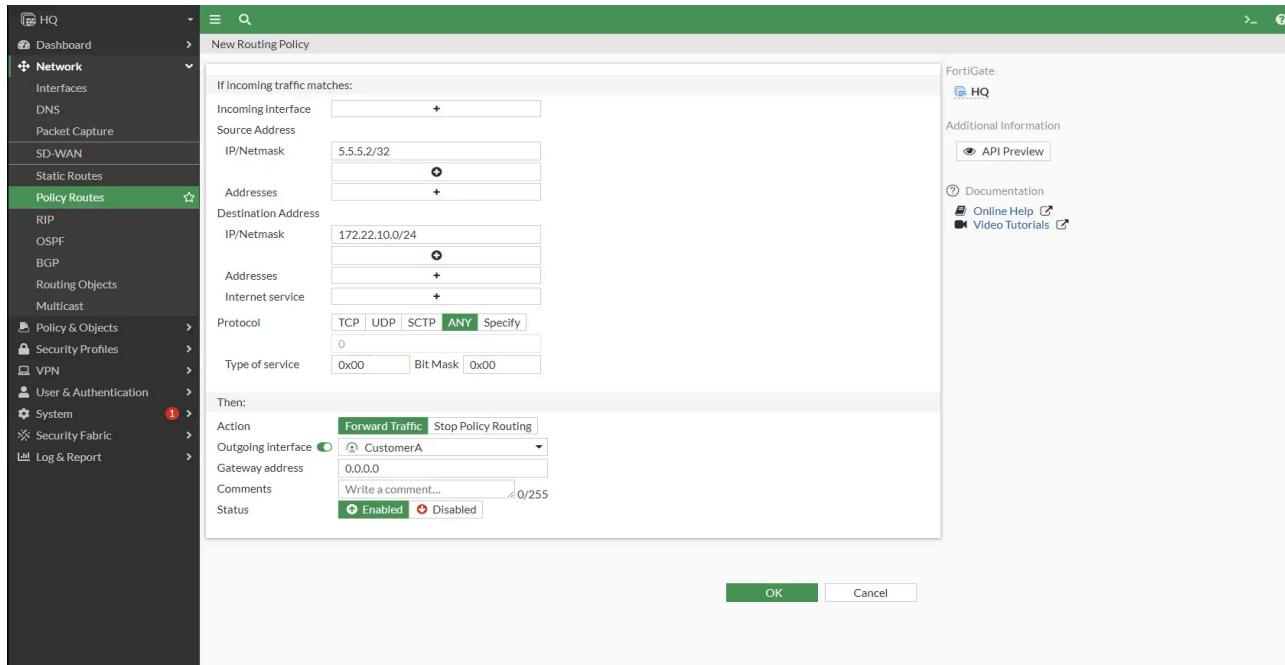
- “diagnose sys filter clear” ile aktif bağlantıları temizleyerek, yönlendirme kurallarının yeniden yüklenmesini sağladık.

Bu adımlar, firewall’ın PBR kurallarına uygun yeni oturumları oluşturmasını ve mevcut yönlendirme çıkışmalarının önüne geçilmesini sağladı.

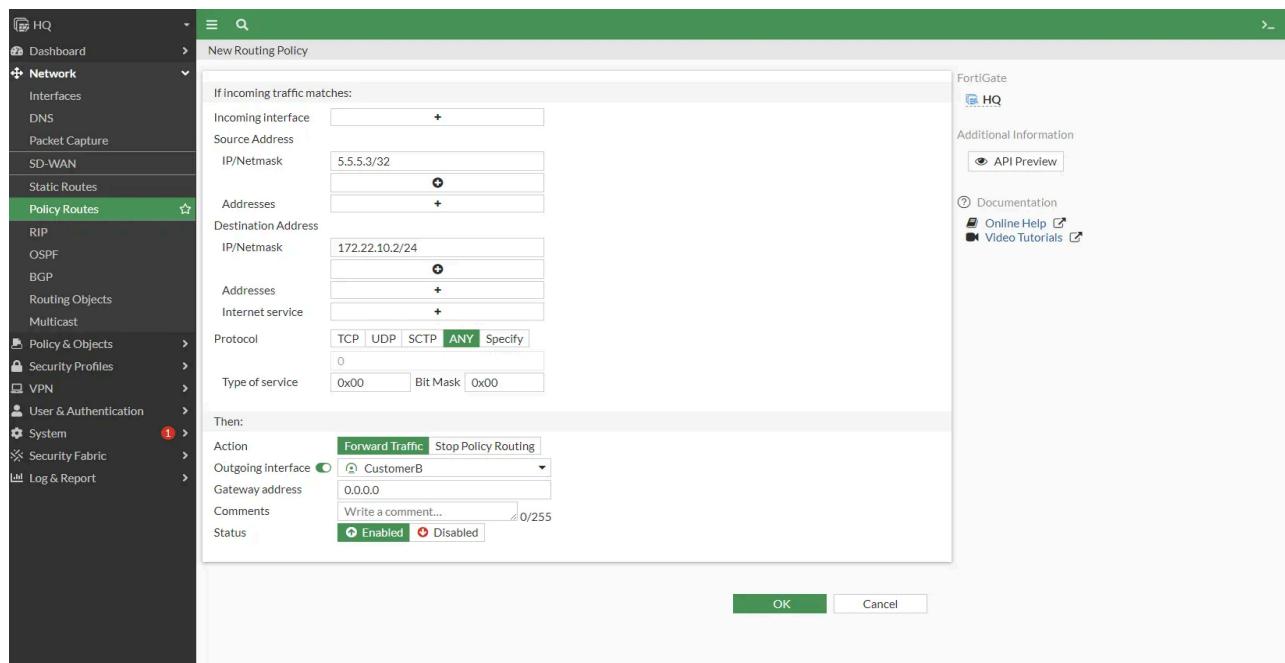
## Policy-Based Routing (PBR) ile Trafik Yönetimi

PBR kullanarak, Customer A ve Customer B trafiğinin doğru ISP üzerinden yönlendirilmesini sağladık.

- 5.5.5.2 IP’sine sahip istemcinin Customer A’ya erişirken ISP1 (30.30.30.2) üzerinden gitmesini zorunlu hale getirdik.



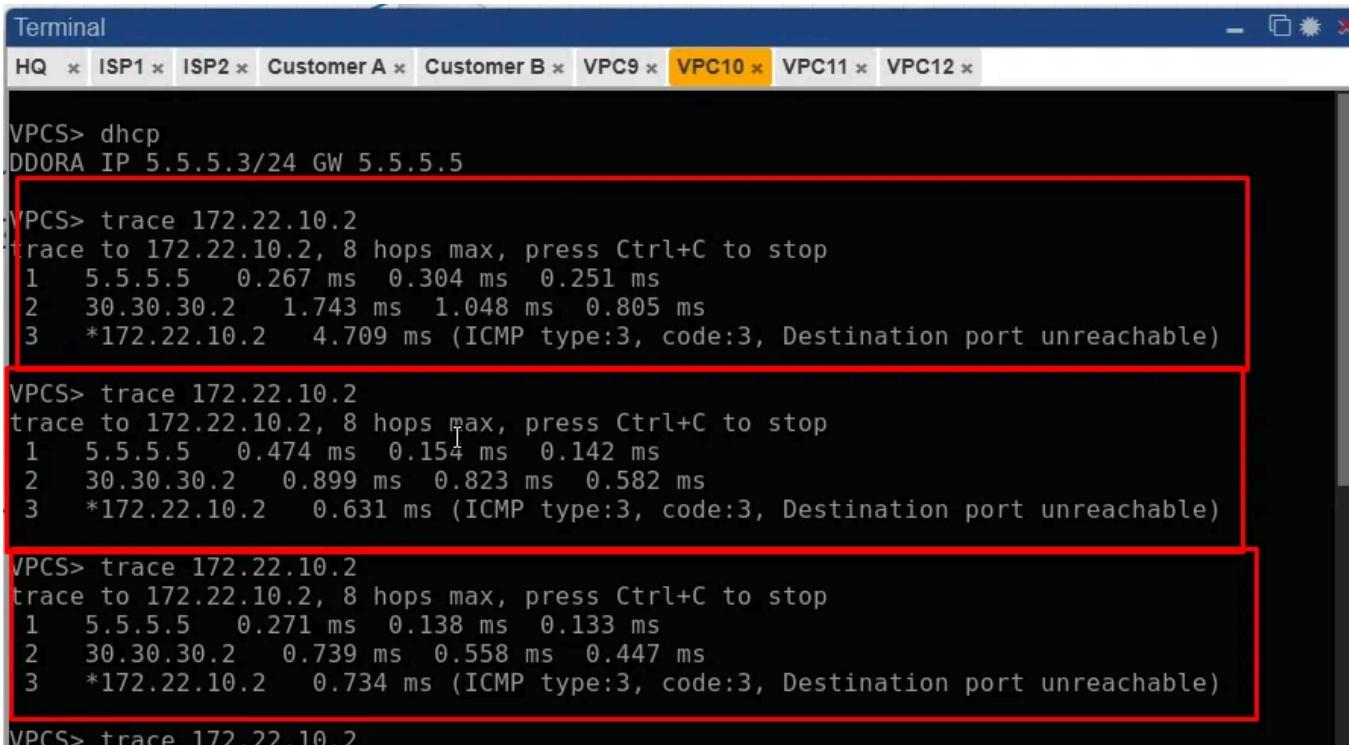
- 5.5.5.3 IP’sine sahip istemcinin Customer B’ye erişirken ISP2 (40.40.40.2) üzerinden çıkışmasını sağladık.



Bunu yaparken PBR'nin statik route'ları geçersiz kılabileceğini ve aşırı kullanımın ağ trafiginde beklenmeyen yönlendirmelere sebep olabileceğini göz önünde bulundurduk. Bu yüzden sadece zorunlu trafikler için PBR kuralları ekledik ve gereksiz yönlendirmelerden kaçındık.

Bu yapılandırma ile artık:

- 5.5.5.2 → Customer A → ISP1 üzerinden çıkacak.
- 5.5.5.3 → Customer B → ISP2 üzerinden çıkacak.



The terminal window shows the following session:

```

Terminal
HQ * ISP1 * ISP2 * Customer A * Customer B * VPC9 * VPC10 * VPC11 * VPC12 *
VPCS> dhcp
DDORA IP 5.5.5.3/24 GW 5.5.5.5
VPCS> trace 172.22.10.2
trace to 172.22.10.2, 8 hops max, press Ctrl+C to stop
1 5.5.5.5 0.267 ms 0.304 ms 0.251 ms
2 30.30.30.2 1.743 ms 1.048 ms 0.805 ms
3 *172.22.10.2 4.709 ms (ICMP type:3, code:3, Destination port unreachable)

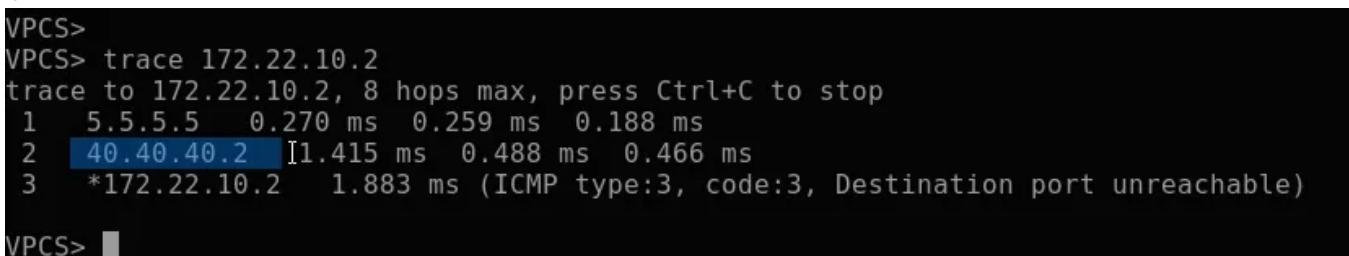
VPCS> trace 172.22.10.2
trace to 172.22.10.2, 8 hops max, press Ctrl+C to stop
1 5.5.5.5 0.474 ms 0.154 ms 0.142 ms
2 30.30.30.2 0.899 ms 0.823 ms 0.582 ms
3 *172.22.10.2 0.631 ms (ICMP type:3, code:3, Destination port unreachable)

VPCS> trace 172.22.10.2
trace to 172.22.10.2, 8 hops max, press Ctrl+C to stop
1 5.5.5.5 0.271 ms 0.138 ms 0.133 ms
2 30.30.30.2 0.739 ms 0.558 ms 0.447 ms
3 *172.22.10.2 0.734 ms (ICMP type:3, code:3, Destination port unreachable)

VPCS> trace 172.22.10.2

```

Böylece her istemci yalnızca tanımlanan ISP'yi kullanarak çıkış yapacak ve yanlış yönlendirme sorunu ortadan kalkmış olacak.



The terminal window shows the following session:

```

VPCS>
VPCS> trace 172.22.10.2
trace to 172.22.10.2, 8 hops max, press Ctrl+C to stop
1 5.5.5.5 0.270 ms 0.259 ms 0.188 ms
2 40.40.40.2 1.415 ms 0.488 ms 0.466 ms
3 *172.22.10.2 1.883 ms (ICMP type:3, code:3, Destination port unreachable)

VPCS>

```

## Policy-Based Routing'in Ağa Etkisi ve Olası Riskler

PBR kullanmanın avantajları olduğu kadar, dikkat edilmesi gereken bazı önemli noktalar da bulunuyor.

PBR, statik route'ları geçersiz kılar.

- Eğer bir hedef için hem statik route hem de PBR tanımlandıysa, PBR öncelikli olur ve statik route çalışmaz.

- Bu yüzden PBR ile statik route'ların çakışmaması için yönlendirme tablosunu iyi kontrol etmek gerekir.

PBR fazla kullanılırsa yönetimi zorlaştırır.

- Her yeni PBR kuralı yönlendirme tablosuna ek bir yük getirir ve işlem maliyetini artırır.
- Ańska çok fazla PBR kuralı olması, trafiğin beklenmeyen şekillerde yönlendirilmesine neden olabilir.

PBR, failover mekanizması içermez.

- Örneğin, ISP1 çökerse, PBR kuralı nedeniyle trafik ISP2'ye otomatik olarak yönlendirilmez.
- Bu gibi durumlar için SD-WAN veya dinamik yönlendirme protokoller (BGP, OSPF) kullanılması daha mantıklı olabilir.

Bu nedenlerden dolayı PBR kullanımını sadece belirli trafik senaryolarında önerilir ve mümkün olduğunda fazla kural eklenmemelidir.

### **Gerçek Hayatta Karşılaşılan Bir Senaryo**

Sektörde çalışırken benzer bir durumla karşılaştım. Bir müşteri, bilgisayarının Türk Telekom ISP'den çıkışmasını, ancak telefonunun Superonline ISP üzerinden çıkışmasını istedi.

Bunun nedeni şuydu:

- Bilgisayarın güvenlik kontrolü için Türk Telekom interneti session yükü fazla olduğu için kısıtlama getirildiği için,
- Ancak mobil cihazların bu güvenlik filtresine ihtiyacı yoktu ve doğrudan Superonline'dan çıkıştı daha hızlıydı.

Bunu yapmak için PBR kullanarak şu yönlendirme kurallarını oluşturduk:

- Bilgisayarın trafiğini Türk Telekom ISP'ye yönlendirdik.
- Telefonun internet trafiğini Superonline ISP'ye yönlendirdik.

Ancak burada bir önemli sorun ortaya çıktı:

- Eğer T ISP çökerse, bilgisayar otomatik olarak Superonline'a geçemeyecekti.

- Bunu yapmak için SD-WAN veya dinamik yönlendirme sistemleri kullanmak daha mantıklıydı.

Sonuç olarak, PBR, belirli yönlendirme senaryoları için faydalı olsa da, dinamik değişikliklere uyum sağlayamadığı için büyük ölçekli ağlarda SD-WAN gibi çözümler daha iyi sonuç verebilir.

## **Sonuç: Hangi Yöntemi Kullanmalıyız?**

- Eğer ağınız küçükse ve tek ISP kullanıyorsanız, Statik Route yeterlidir.
- Belirli cihazların belirli ISP'lerden çıkışını istiyorsanız, PBR kullanılabilir ancak fazla kural eklememelisiniz.
- Ağınız büyüyorsa, yedekli bağlantılarınız varsa ve otomatik failover istiyorsanız, SD-WAN en iyi çözümüdür.

Bu yapılandırma ile Customer A ve Customer B'nin doğru ISP'den çıkış yapmasını sağladık, yönlendirme hatalarını düzelttik ve ağın stabil çalışmasını garanti altına aldık.

Ancak bu sistem daha da büyürse, statik yönlendirme yerine SD-WAN veya dinamik yönlendirme protokollerini (BGP, OSPF) kullanmanın daha mantıklı olacağını söyleyebiliriz.

Sonuç olarak, ağın ölçegine ve ihtiyaçlarına bağlı olarak en uygun yönlendirme yöntemini seçmek, sistemin performansını ve güvenliğini artırmak açısından büyük önem taşır.

Bir başka çalışmada görüşmek üzere.