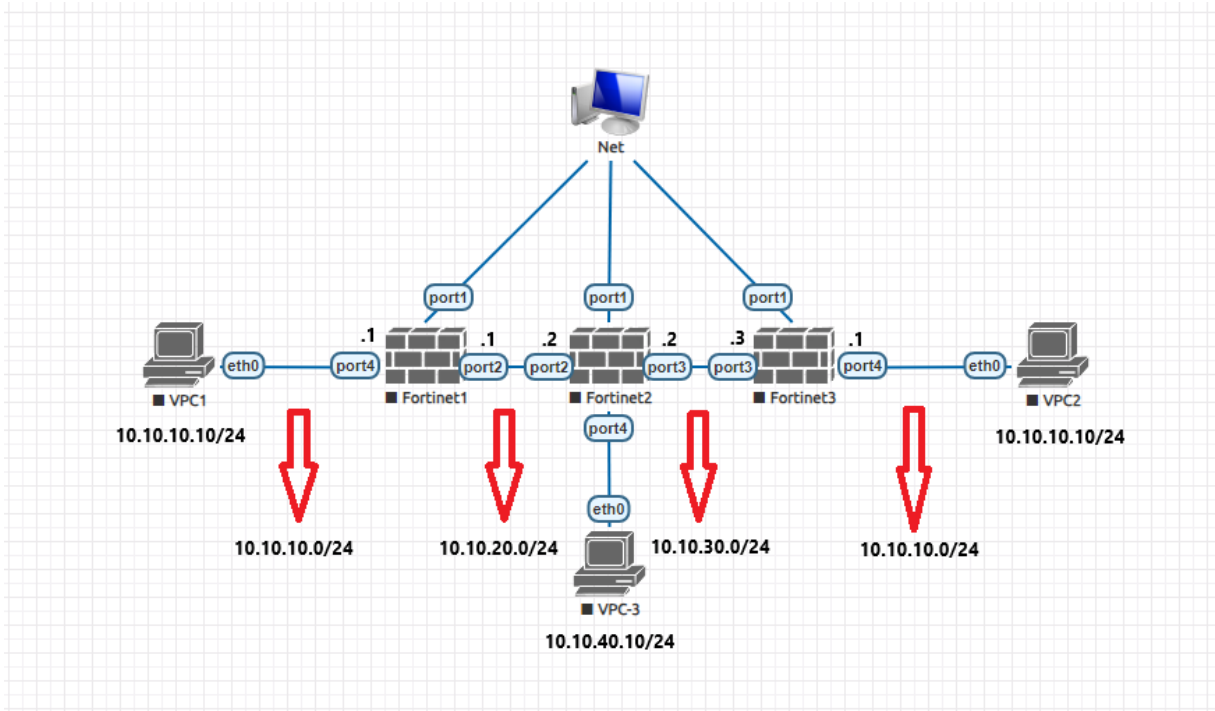


IP-Port Forwarding

Network üzerinde kullanılan ip bloklarının çoğu zaman çakışması/kullanılıyor olması gibi durumlarda Dynmic NAT (NAT/PAT) ve IP/Port Forwarding teknolojilerine ihtiyaç duyuluyor. Bu yazıda Fortigate üzerinde IP/Port Forwarding işleminin nasıl gerçekleştirildiği açıklanmaya çalışılacaktır.

Fortigate üzerinde IP/Port Forwarding teknolojisinin nasıl uygulandığı aşağıdaki topoloji üzerinden açıklanmaya çalışacaktır. Aşağıdaki topolojiye bakıldığında 3 adet Fortigate üzerindeki network tanımları görülmektedir. VPC3'ün, VPC1 ve VPC2'ye erişebilmesi gerekiyor. Buradaki sorun ise VPC1 ve VPC2'nin kullandığı ip bloğunun ve üzerlerindeki ip adreslerinin aynı olmasıdır. Bu durumda VPC3, VPC1 ve VPC2'ye aynı anda erişim sağlayamayacaktır.



VPC3'ün VPC1 ve VPC2'ye aynı anda (Tek yönlü – VPC1 ve VPC2'den VPC3'e erişim sağlanması istenmiyor) erişim sağlayabilmesi için Fortigate1 veya Fortigate3 üzerinde IP/Port Forwarding tanımı yapılarak VPC1 veya VPC2'ye gönderilecek paketlerin farklı bir ip adresi üzerinden gönderilmesi sağlanmalıdır. Bu işlem için Fortigate3'e bağlı VPC2'ye paketler gönderilirken 10.10.100.10/32 ip adresi üzerinden gönderilmesi sağlanacaktır.

Topolojide öncelikle VPC3 ile VP2 arasındaki haberleşme sürecini sağlayabilmek için ilk adımda Fortigate1 üzerinde;

- Kullanılacak arayüzlere ip atamalarının yapılması gerekiyor. Bu arayüzlerde kullanılan ip adreslerini Policy tanımında kullanabilmek için Address tanımlarının yapılması gerekiyor.

port2	Physical Interface	10.10.20.1/255.255.255.0	PING
port3	Physical Interface	0.0.0.0/0.0.0.0	
port4	Physical Interface	10.10.10.1/255.255.255.0	PING

 VPC1_Addr	10.10.10.10/32		Address	1
 VPC3_Addr	10.10.40.10/32		Address	1

```

FortiGate # config system interface
FortiGate (interface) # edit port2
FortiGate (port2) # set mode static
FortiGate (port2) # set ip 10.10.20.1 255.255.255.0
FortiGate (port2) # set allowaccess ping
FortiGate (port2) # next
FortiGate (interface) # edit port4
FortiGate (port4) # set mode static
FortiGate (port4) # set ip 10.10.10.1 255.255.255.0
FortiGate (port4) # set allowaccess ping
FortiGate (port4) # end

FortiGate # config firewall address
FortiGate (address) # edit VPC1_Addr
new entry 'VPC1_Addr' added
FortiGate (VPC1_Addr) # set type ipmask
FortiGate (VPC1_Addr) # set subnet 10.10.10.10/32
FortiGate (VPC1_Addr) # next
FortiGate (address) # edit VPC3_Addr
new entry 'VPC3_Addr' added
FortiGate (VPC3_Addr) # set type ipmask
FortiGate (VPC3_Addr) # set subnet 10.10.40.10/32
FortiGate (VPC3_Addr) # end

```














- Arayüz ve Address tanımları yapıldıktan sonra Fortigate2 üzerinden gelecek 10.10.40.0/24 networküne ait trafiği 10.10.10.0/24 networküne yönlendirilebilmesi için Policy tanımı yapılması gerekiyor.
- Policy tanımı yapıldıktan sonra 10.10.40.0/24 networkünden gelen paketlere yanıt dönülebilmesi için 10.10.40.10/24 networküne doğru Static Route tanımı yapılması gerekiyor. Static Route tanımından sonra Fortigate2 üzerinde tanımlamalara geçilebilir.

```

FortiGate # config firewall policy
FortiGate (policy) # edit 10
new entry '10' added
FortiGate (10) # set name VPC3_to_VPC1
FortiGate (10) # set srcintf port2
FortiGate (10) # set dstintf port4
FortiGate (10) # set srcaddr VPC3_Addr
FortiGate (10) # set dstaddr VPC1_Addr
FortiGate (10) # set action accept
FortiGate (10) # set schedule always
FortiGate (10) # set service ALL
FortiGate (10) # end

FortiGate # config router static
FortiGate (static) # edit 1
new entry '1' added
FortiGate (1) # set dst 10.10.40.0/24
FortiGate (1) # set gateway 10.10.20.2
FortiGate (1) # set device port2
FortiGate (1) # end

```

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
VPC3_to_VPC1	 port2	 port4	 VPC3_Addr	 VPC1_Addr	 always	 ALL	 ACCEPT	 Disabled
Implicit Deny	<input type="checkbox"/> any	<input type="checkbox"/> any	 all	 all	 always	 ALL	 DENY	



+ Create New

Edit

Clone

Delete

Search

Destination	Gateway IP	Interface	Status
10.10.40.0/24	10.10.20.2	 port2	 Enabled










- Fortigate1 üzerindeki tanımlamalar yapıldıktan sonra Fortigate1'e uygulanan konfigürasyonların karşılığı Fortigate2 üzerinde de tanımlanmalıdır. Bu süreçte kullanılacak arayüzlere ip adresleri tanımlandıktan sonra Address tanımları aşağıdaki gibi olmalıdır. Burada Fortigate3 üzerindeki 10.10.10.0/24 (VPC2_Addr) networkündeki istemciye 10.10.100.0/24 adres aralığıyla erişileceği için tanımlarında da 10.10.100.0/24 adresi kullanılacaktır.




```

FortiGate2 # config system interface
FortiGate2 (interface) # edit port2
FortiGate2 (port2) # set mode static
FortiGate2 (port2) # set ip 10.10.20.2 255.255.255.0
FortiGate2 (port2) # set allowaccess ping
FortiGate2 (port2) # next
FortiGate2 (interface) # edit port3
FortiGate2 (port3) # set mode static
FortiGate2 (port3) # set ip 10.10.30.2 255.255.255.0
FortiGate2 (port3) # set allowaccess ping
FortiGate2 (port3) # next
FortiGate2 (interface) # edit port4
FortiGate2 (port4) # set mode static
FortiGate2 (port4) # set ip 10.10.40.1 255.255.255.0
FortiGate2 (port4) # set allowaccess ping
FortiGate2 (port4) # end

FortiGate2 # config firewall address
FortiGate2 (address) # edit VPC1_Addr
new entry 'VPC1_Addr' added
FortiGate2 (VPC1_Addr) # set type ipmask
FortiGate2 (VPC1_Addr) # set subnet 10.10.10.10/32
FortiGate2 (VPC1_Addr) # next
FortiGate2 (address) # edit VPC3_Addr
new entry 'VPC3_Addr' added
FortiGate2 (VPC3_Addr) # set type ipmask
FortiGate2 (VPC3_Addr) # set subnet 10.10.40.10/32
FortiGate2 (VPC3_Addr) # next
FortiGate2 (address) # edit VPC2_Addr
new entry 'VPC2_Addr' added
FortiGate2 (VPC2_Addr) # set type ipmask
FortiGate2 (VPC2_Addr) # set subnet 10.10.100.10/32
FortiGate2 (VPC2_Addr) # end

```

 port2	 Physical Interface	10.10.20.2/255.255.255.0	 PING
 port3	 Physical Interface	10.10.30.2/255.255.255.0	 PING
 port4	 Physical Interface	10.10.40.1/255.255.255.0	 PING

















 VPC1_Addr	10.10.10.10/32	Address	1
 VPC2_Addr	10.10.100.10/32	Address	1
 VPC3_Addr	10.10.40.10/32	Address	2

- Arayüz ve Address tanımları yapıldıktan sonra Policy tanımına geçilebilir. Burada yine paketleri VPC2'ye gönderebilmek için 10.10.100.0/24 networkü kullanılacaktır. Bu adres Fortigate3 üzerinde tanım yaparken ilgili ip adresine Forward edilecektir. Bu nedenle paketler Fortigate3 üzerine gelene kadar 10.10.100.0/24 networküne erişmek üzere gönderilecektir.

```

FortiGate2 # config firewall policy
FortiGate2 (policy) # edit 10
new entry '10' added
FortiGate2 (10) # set name VPC3_to_VPC1
FortiGate2 (10) # set srcintf port4
FortiGate2 (10) # set dstintf port2
FortiGate2 (10) # set srcaddr VPC3_Addr
FortiGate2 (10) # set dstaddr VPC1_Addr
FortiGate2 (10) # set action accept
FortiGate2 (10) # set schedule always
FortiGate2 (10) # set service ALL
FortiGate2 (10) # next
FortiGate2 (policy) # edit 11
new entry '11' added
FortiGate2 (11) # set name VPC3_to_VPC2
FortiGate2 (11) # set srcintf port4
FortiGate2 (11) # set dstintf port3
FortiGate2 (11) # set srcaddr VPC3_Addr
FortiGate2 (11) # set dstaddr VPC2_Addr
FortiGate2 (11) # set action accept
FortiGate2 (11) # set schedule always
FortiGate2 (11) # set service ALL
FortiGate2 (11) # end

```

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
VPC3_to_VPC2	 port4	 port3	 VPC3_Addr	 VPC2_Addr	 always	 ALL	✓ ACCEPT	✗ Disabled
VPC3_to_VPC1	 port4	 port2	 VPC3_Addr	 VPC1_Addr	 always	 ALL	✓ ACCEPT	✗ Disabled
Implicit Deny	<input type="checkbox"/> any	<input type="checkbox"/> any	 all	 all	 always	 ALL	✗ DENY	

- Policy tanımı yapıldıktan sonra son olarak Static Route tanımını yapıldığında Fortigate2 üzerinde uygulanması gereken konfigürasyonlar tamamlanacaktır. Bu tanımlamalar sonucunda PC3'den PC1'te erişilebilmesi gerekmektedir.

```

FortiGate2 # config system interface
FortiGate2 (interface) # edit port2
FortiGate2 (port2) # set mode static
FortiGate2 (port2) # set ip 10.10.20.2 255.255.255.0
FortiGate2 (port2) # set allowaccess ping
FortiGate2 (port2) # next
FortiGate2 (interface) # edit port3
FortiGate2 (port3) # set mode static
FortiGate2 (port3) # set ip 10.10.30.2 255.255.255.0
FortiGate2 (port3) # set allowaccess ping
FortiGate2 (port3) # next
FortiGate2 (interface) # edit port4
FortiGate2 (port4) # set mode static
FortiGate2 (port4) # set ip 10.10.40.1 255.255.255.0
FortiGate2 (port4) # set allowaccess ping
FortiGate2 (port4) # end

```

Destination	Gateway IP	Interface	Status
10.10.10.0/24	10.10.20.1	port2	Enabled
10.10.100.0/24	10.10.30.3	port3	Enabled

```

VPC-3
VPCS> trace 10.10.10.10
trace to 10.10.10.10, 8 hops max, press Ctrl+C to stop
 1  10.10.40.1  0.463 ms  0.360 ms  0.354 ms
 2  10.10.20.1  1.221 ms  0.462 ms  0.405 ms
 3  *10.10.10.10  0.894 ms (ICMP type:3, code:3, Destination port unreachable)
VPCS>

```

- VP3'den VPC1'ye doğru erişim sağlandıktan sonra artık VPC2'ye erişilebilmesi için Fortigate3 üzerindeki konfigürasyonlara başlanabilir. Fortigate3 üzerinde de kullanılacak arayüzlere ip atamaları ve adres tanımlamaları yapılmalıdır. Address tanımı yapılırken Fortigate2 üzerinden VPC2'ye gönderilen paketlerin hedef ip adresi 10.10.100.0/24 netwürlünden olacağı için burada gelen trafiklerin 10.10.10.0/24 networküne yönlendirilmesi gerekiyor. Bu işlem için Virtual IPs (IP/Port Forwarding) tanımı yapılmalıdır.

```

FortiGate3 # config system interface
FortiGate3 (interface) # edit port3
FortiGate3 (port3) # set mode static
FortiGate3 (port3) # set ip 10.10.30.3 255.255.255.0
FortiGate3 (port3) # set allowaccess ping
FortiGate3 (port3) # next
FortiGate3 (interface) # edit port4
FortiGate3 (port4) # set mode static
FortiGate3 (port4) # set ip 10.10.10.1 255.255.255.0
FortiGate3 (port4) # set allowaccess ping
FortiGate3 (port4) # end

FortiGate3 # config firewall address
FortiGate3 (address) # edit VPC3_Addr
new entry 'VPC3_Addr' added
FortiGate3 (VPC3_Addr) # set type ipmask
FortiGate3 (VPC3_Addr) # set subnet 10.10.40.10/32
FortiGate3 (VPC3_Addr) # end

```

port3	Physical Interface	10.10.30.3/255.255.255.0	PING
port4	Physical Interface	10.10.10.1/255.255.255.0	PING

VPC3_Addr	10.10.40.10/32	Address	1
-----------	----------------	---------	---

- Virtual IP tanımı için “**Policy&Objects -> Virtual IPs -> Create New**” yolu takip edilmelidir. Burada temel anlamda seçilmesi gereken kısımlara bakıldığında;
 - o Interface, istek gelecek arayüzün (dış bacak) belirtilmesi için kullanılıyor.
 - o External IP Address/Range, istek gelecek paketlerde bulunması beklenen hedef ip adresini belirtmek için kullanılıyor.
 - o Map to, dışarıdan gelmesi beklenen ip adresinin LAN içerisinde yönlendirileceği hedef ip adresini belirtmek için kullanılıyor.

Doldurulması gereken zorunlu alanlar dışında Virtual IP tanımını özelleştirmek için;

- “Optimal Filters -> Source Address” kısmında gelmesi beklenen paketlerin hedef ip adreslerinin yanında kaynak ip adreslerinin de kontrol edilerek Forward edilmesi sağlanabiliyor. Bu sayede IP/Port Forwarding işlemine belirli bir grubun erişmesi sağlanabiliyor.
- “Optimal Filters -> Services” kısmıyla paketleri LAN içerisindeki ilgili ip adresine yönlendirme işlemi sadece belirli servisler üzerinden erişim sağlanmak istendiğinde yapılması sağlanabiliyor.

```
FortiGate3 # config firewall vip
FortiGate3 (vip) # edit ToPort4VIP
new entry 'ToPort4VIP' added

FortiGate3 (ToPort4VIP) # set extip 10.10.100.10
FortiGate3 (ToPort4VIP) # set extintf port3
FortiGate3 (ToPort4VIP) # set mappedip 10.10.10.10
FortiGate3 (ToPort4VIP) #
FortiGate3 (ToPort4VIP) # set src-filter 10.10.40.10
FortiGate3 (ToPort4VIP) # set service ALL
FortiGate3 (ToPort4VIP) #
FortiGate3 (ToPort4VIP) # #set portforward enable
FortiGate3 (ToPort4VIP) # #set protocol icmp
FortiGate3 (ToPort4VIP) # #set extport 9999
FortiGate3 (ToPort4VIP) # #set mappedport 8080
FortiGate3 (ToPort4VIP) # #set portmapping-type 1-to-1
FortiGate3 (ToPort4VIP) # end
```

Edit Virtual IP

VIP type: IPv4

Name: ToPort4VIP

Comments: Write a comment... 0/255

Color: Change

Network

Interface: port3

Type: Static NAT

External IP address/range: 10.10.100.10

Map to

IPv4 address/range: 10.10.10.10

☒ Optional Filters

Source address: ☒ 10.10.40.10

Services: ☒ ALL

☐ Port Forwarding

FortiGate

FortiGate3

Statistics (since last reset)

ID	
Last used	N/A
First used	N/A
Hit count	0

Clear Counters

Additional Information

API Preview

References

Edit in CLI

Documentation

Online Help

Video Tutorials

OK Cancel

- “Port Forwarding -> Protocol” kısmıyla belirli protokoller üzerinden istek gönderildiği takdirde IP/Port Forwarding işlemi yapılması sağlanabiliyor. Yani bu özellikte bir ip adresini tek bir ip adresine Forward etmek yerine port bilgilerini kullanarak birden fazla ip adresine Forward edilebilmektedir. Bir anlamda PAT işlemi gibi görülebilir.
- “Port Forwarding -> Port Mapping Type” kısmıyla Forward edilmek üzere gönderilen paketlerde kullanılan port bilgileri değerlendirilirken belirli bir port aralığının tek bir porta mı yoksa eşleniği genişlikteki bir port aralığını bire bir mi Forward edileceğini belirlemek için kullanılıyor. Örnek olarak
 - One to One -> hedef port bilgisi 10-100 arasında olan paketler LAN içerisindeki ilgili ip adresinin sadece 9000 portuna Forward edilir.

☒ Port Forwarding

Protocol	TCP	UDP	SCTP	ICMP
Port Mapping Type	One to one	Many to many		
External service port ⓘ	10 - 100			
Map to IPv4 port	9000			

- 9090

- Many-to-Many -> hedef port bilgisi 10-100 arasında olan paketler LAN içerisindeki ilgili ip adresine hedef port bilgisi 9000-9090 arasında Forward edilir.

☒ Port Forwarding

Protocol	TCP	UDP	SCTP	ICMP
Port Mapping Type	One to one	Many to many		
External service port ⓘ	10 - 100			
Map to IPv4 port	9000-9090			

- IP/Port Forwarding işlemi için Virtual IP tanımı da yapıldıktan sonra artık Policy tanımına geçilebilir. Policy tanımında kaynak ip adresi olarak Fortigate2 üzerinden gelecek paketlerin kaynak ip adresi 10.10.40.0/24 networkünden olacaktır ama hedef ip adresi kısmı için gelecek paketlerin hedef ip adresleri 10.10.100.0/24 networküne göre olacaktır. Bu nedenle hedef ip adresi 10.10.10.0/24 networküne yönlendirilebilmesi için oluşturulan Virtual IP adres tanımı seçilmelidir.

```
FortiGate3 # config firewall policy
FortiGate3 (policy) # edit 10
new entry '10' added

FortiGate3 (10) # set name VPC3_to_VPC2
FortiGate3 (10) # set srcintf port3
FortiGate3 (10) # set dstintf port4
FortiGate3 (10) # set srcaddr VPC3_Addr
FortiGate3 (10) # set dstaddr ToPort4VIP
FortiGate3 (10) # set action accept
FortiGate3 (10) # set schedule always
FortiGate3 (10) # set service ALL
FortiGate3 (10) # end
```


Name	From	To	Source	Destination	Schedule	Service	Action	NAT
VPC3_to_VPC2	port3	port4	VPC3_Addr	ToPort4VIP	always	ALL	✓ ACCEPT	✗ Disabled
Implicit Deny	<input type="checkbox"/> any	<input type="checkbox"/> any	all	all	always	ALL	✗ DENY	

- Son adımda gelecek paketlerin tekrar 10.10.40.0/24 networküne iletebilmesi için Static Route tanımını da yapılarak konfigürasyon sonlandırılabilir.

```
FortiGate3 # config router static
FortiGate3 (static) # edit 1
new entry '1' added
FortiGate3 (1) # set dst 10.10.40.0/24
FortiGate3 (1) # set gateway 10.10.30.2
FortiGate3 (1) # set device port3
FortiGate3 (1) # end
```

Destination	Gateway IP	Interface	Status
10.10.40.0/24	10.10.30.2	port3	✓ Enabled

- Artık test zamanı. Son durumda VPC3 cihazı VPC1 ve VPC2 cihazına erişilebilir durumda olmalıdır.

```
VPC-3
VPCS>
VPCS> trace 10.10.10.10
trace to 10.10.10.10, 8 hops max, press Ctrl+C to stop
 1  10.10.40.1  0.609 ms  0.502 ms  0.480 ms
 2  10.10.20.1  1.132 ms  0.773 ms  0.828 ms
 3  *10.10.10.10  1.596 ms (ICMP type:3, code:3, Destination port unreachable)

VPCS> trace 10.10.100.10
trace to 10.10.100.10, 8 hops max, press Ctrl+C to stop
 1  10.10.40.1  0.603 ms  0.485 ms  0.491 ms
 2  10.10.30.3  1.252 ms  1.195 ms  0.745 ms
 3  *10.10.30.3  0.601 ms (ICMP type:3, code:3, Destination port unreachable)
```

Unutulmamalıdır ki burada sadece VPC3 cihazı VPC1 ve VPC2 cihazına erişebilmesi için konfigürasyon yapılmıştır. Normal şartlarda Policy ve Static Route tanımları yapılarak VPC1'in VPC3 ile karşılıklı haberleşmesi sağlanabilir ama VPC2'nin VPC3'e erişebilmesi için (yani karşılıklı haberleşebilmeleri için) Fortigate3 üzerinde yeni bir Policy oluşturularak Outgoing Interface ip adresine veya farklı bir ip kullanılması isteniyorsa bir IP Pool tanımı oluşturularak VPC2 adresinin Fortigate2'ye **NAT** işlemine tabi tutularak gönderilmesi gerekiyor. Fortigate2 üzerinde de NAT uygulanan ip adresine göre Static Route ve Policy tanımları yapılması gerekmektedir.

Kaynak

- <https://community.fortinet.com/t5/FortiGate/Technical-Tip-Using-Virtual-IPs-to-configure-port-forwarding/ta-p/198195>
- <https://docs.fortinet.com/document/fortigate/6.2.16/cookbook/510402/static-virtual-ips>
- <https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-change-port-mapping-types-in-VIP/ta-p/195130>