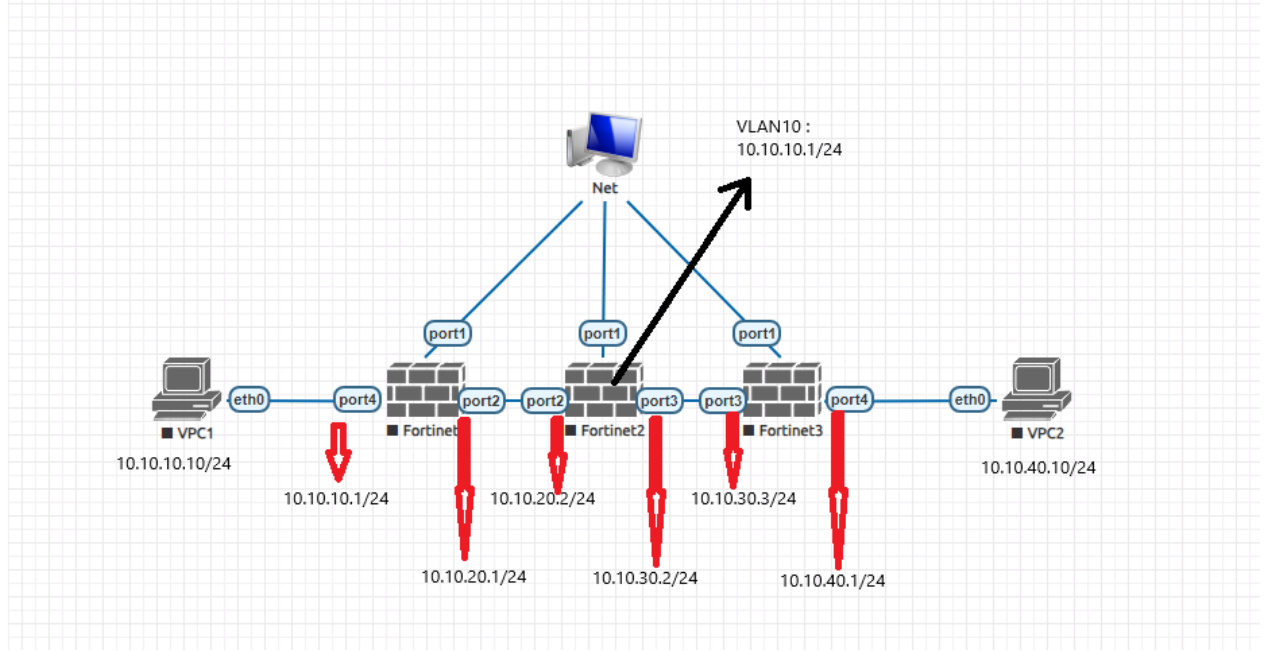


NAT

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

Fortigate üzerinde NAT teknolojisinin nasıl uygulandığı aşağıdaki topoloji üzerinden açıklanmaya çalışacaktır. Aşağıdaki topolojiye bakıldığında 3 adet Fortigate üzerindeki VLAN tanımları görülmektedir. VPC1'nin VPC2'ye erişebilmesi gerekiyor. Buradaki sorun ise VPC1'in kullandığı ip bloğunun Fortigate2 üzerinde de VLAN 10 için kullanılıyor olmasıdır. Fortigate1'den gönderilen 10.10.10.1/24 networküne ait trafik Fortigate2 üzerinden geçmek istediğinde Fortigate2 kendisine gelen paketdeki hedef ip adresi kendi üzerinde tanımlı olduğunu görüp paketi Fortigate3'e göndermek yerine kendi üzerindeki VLAN10 arayüzüne yönlendirecektir. Dolayısıyla VPC1 VPC2'ye erişemeyecektir.

VPC1'in VPC2'ye erişebilmesi için trafiğin Fortigate1'den Fortigate2'ye gönderilirken DNAT veya SNAT uygulanması gerekmektedir. Bu süreçte sadece VPC1'den VPC2'ye erişim istendiği için DNAT konfigürasyonu yapmak yeterli olacaktır. Konfigürasyonlara ilgili VLAN tanımlarının Fortigate'ler üzerinde tanımlı olduğu varsayılarak başlanacaktır.




Bu süreçte;

- DNAT konfigürasyonu için ilk adımda NAT işleminin belirli bir ip aralığına mı yoksa trafiğin Fortigate üzerinden çıkış yapacağı arayüzünde kullanılan/tanımlanan ip adresine mi NAT yapılacağı belirlenmelidir.
- **Trafik Fortigate üzerinde çıkış yapacağı arayüzün ip adresine NAT'lanacak ise** herhangi bir ek ayar yapılmasına ihtiyaç yoktur.
 - o Bu seçeneğin kullanım yerine örnek olarak Internete çıkış yapılabilmesi için internete çıkış yapacak bütün trafiğin Public IP adreslerine NAT'lanarak internet ortamına çıkarılması verilebilir. Örnekten de anlaşılacağı üzere bu seçenekte bir grup ip adresleri çıkış yapılacak arayüze atanan tek bir ip adresine NAT/PAT yapılmaktadır.

- **Trafikler belirli bir formatta NAT'lanmak isteniyorsa** bu durumda Policy tanımına geçilmeden önce **"Policy&Ojects -> Ip Pools -> Create New"** yolu izlenerek IP Pool tanımı yapılması gerekiyor. IP Pool tanımı için kullanılabilecek 4 farklı seçenek bulunuyor;
 - o **Overload**, bu tanım tipinde Policy tanımında belirtilen kaynak ip adreslerinin tamamının burada belirtilen aralıktaki ip adreslerine NAT/PAT yapılması için kullanılmaktadır. Burada NAT/PAT işlemi için oluşturulacak IP havuzunun başlangıç ve bitiş aralığını belirtmek yeterlidir. Tek bir ip adresine NAT/PAT yapılacak ise tanımda başlangıç adresi olarak da bitiş adresi olarak da aynı ip adresini yazmak gerekiyor.
 - Ip adresinin kısıtlı olduğu networklerde veya WAN çıkışlarında LAN'daki istemcilerin kısıtlı Public ip adresi üzerinden internete çıkarmak gibi durumlarda kullanılıyor.
 - Burada IPv4 adreslerin IPv6 adreslerle haberleşebilmesi isteniyorsa **"NAT64"** seçeneği devreye alınmalıdır.

```
FortiGate1 # config firewall ippool
FortiGate1 (ippool) # edit Overload-1
new entry 'Overload-1' added
FortiGate1 (Overload-1) # set type overload
FortiGate1 (Overload-1) # set startip 192.168.10.250
FortiGate1 (Overload-1) # set endip 192.168.10.254
FortiGate1 (Overload-1) # end
```

Edit Dynamic IP Pool

Name	Overload-1
Comments	Write a comment... 0/255
Type	Overload
External IP address/range 	192.168.10.250-192.168.10.254
NAT64	<input type="checkbox"/>
ARP Reply	<input checked="" type="checkbox"/>

OK

Cancel

- o **One-to-One**, bu tanım Policy tanımında belirtilen kaynak ip adreslerinin tamamının burada belirtilen ip aralığına sadece NAT'lanması için kullanılmaktadır. PAT yapılmamaktadır. Dolayısıyla IP Pool tanımında tanımlanan ip adresi tükendiği takdirde yeni isteklere NAT işlemi uygulanamayacaktır.
 - Bu tanım için de NAT'lanacak ip aralığının belirtilmesi yeterlidir. Kullanımına örnek olarak buradaki tanım WAN bacağına doğru uygulandığında IP Pool tanımında belirtilen ip adreslerini LAN içerisindeki hangi istemciler kullanıyorsa kullandığı süre zarfında internet üzerinden erişilebilir olacaktır (Örnek olarak Reverse DNS aramalarını düzgün bir şekilde çözme ihtiyacı duyan bir posta sunucusunun her zaman belirli bir IP adresi kullanması gerekir).

```

FortiGate1 # config firewall ippool

FortiGate1 (ippool) # edit One-to-One-1
new entry 'One-to-One-1' added

FortiGate1 (One-to-One-1) # set type one-to-one


FortiGate1 (One-to-One-1) # set startip 192.168.20.250

FortiGate1 (One-to-One-1) # set endip 192.168.20.254

FortiGate1 (One-to-One-1) # end

```

Edit Dynamic IP Pool

Name	<input type="text" value="One-to-One-1"/>
Comments	<input type="text" value="Write a comment..."/> 0/255
Type	<input type="text" value="One-to-One"/>
External IP address/range 	<input type="text" value="192.168.20.250-192.168.20.254"/>
ARP Reply	<input checked="" type="checkbox"/>

OK

Cancel

- **Fixed Port Range**, bu tanım tipi Policy tanımında belirtilen kaynak ip adreslerinin belirli bir kısmının NAT'lanması istendiği durumlarda kullanılmaktadır. Bu tanım için NAT'lanacak ip adres (Internal Ip Address) aralığının ve NAT için kullanılacak (External Ip Address) ip adres aralığının tanımlanması yeterlidir.
 - İsteğe bağlı olarak **"Ports Per User"** seçeneği seçilerek kullanıcı başına oluşturulabilecek Session miktarı da sınırlandırılabilir.

```

FortiGate1 # config firewall ippool

FortiGate1 (ippool) # edit Fixed-Prt-Rng-1

FortiGate1 (Fixed-Prt-Rng-1) # set type fixed-port-range

FortiGate1 (Fixed-Prt-Rng-1) # set startip 192.168.30.250

FortiGate1 (Fixed-Prt-Rng-1) # set endip 192.168.30.254

FortiGate1 (Fixed-Prt-Rng-1) # set source-startip 1.1.1.1

FortiGate1 (Fixed-Prt-Rng-1) # set source-endip 1.1.1.1

FortiGate1 (Fixed-Prt-Rng-1) # set port-per-user 500

FortiGate1 (Fixed-Prt-Rng-1) # end

```

Edit Dynamic IP Pool

Name	Fixed-Prt-Rng-1
Comments	Write a comment... 0/255
Type	Fixed Port Range
External IP address/range ⓘ	192.168.30.250-192.168.30.254
Internal IP Range ⓘ	1.1.1.1-1.1.1.1
Ports Per User	<input checked="" type="checkbox"/> 500
ARP Reply	<input checked="" type="checkbox"/>

OK

Cancel

- **Port Block Allocation**, bu tanım tipi Policy tanımında belirtilen kaynak ip adresleri için dinamik olarak belirli bir port aralığının tahsis edilmesini sağlamak için kullanılıyor. Yani Policy tanımında belirtilen kaynak ip adreslerini NAT/PAT işlemine tabi tutuyor ama her kullanıcı için bunu sınırlandırma imkânı sunuyor. Her kaynak ip adresi kendisine tahsis edilen port miktarı kadar NAT/PAT işlemi gerçekleştirebiliyor. Tanımında sadece toplamda kullanılacak port boyutunun ve her kullanıcı/kaynak ip adresi için kaç adet port kullanılacağını belirtmesi gerekmektedir.

```
FortiGate1 # config firewall ippool
FortiGate1 (ippool) # edit Prt-Blk-All-1
new entry 'Prt-Blk-All-1' added

FortiGate1 (Prt-Blk-All-1) # set type port-block-allocation
FortiGate1 (Prt-Blk-All-1) # set startip 192.168.40.250
FortiGate1 (Prt-Blk-All-1) # set endip 192.168.40.254
FortiGate1 (Prt-Blk-All-1) # set block-size 4096
FortiGate1 (Prt-Blk-All-1) # set num-blocks-per-user 8
FortiGate1 (Prt-Blk-All-1) # end
```

Edit Dynamic IP Pool



Name	Prt-Blk-All-1
Comments	Write a comment... 0/255
Type	Port Block Allocation
External IP address/range ⓘ	192.168.40.250-192.168.40.254
Block Size	4096
Blocks Per User	8
ARP Reply	<input checked="" type="checkbox"/>

OK

Cancel

- Bu uygulamamız için çıkış arayüzünde kullanılmayan ip aralığı olan 10.10.100.1-10.10.100.254 arasında NAT/PAT işlemi yapılmasını sağlayacağız (normalde doğrudan çıkış arayüzüne atanan ip adresine (10.10.20.1/24) NAT yaparak da bu işlem gerçekleştirilebilir. Burada sadece örnek uygulama olması için IP Pool tanımı yapılıyor). Bunun için Overload tipinde IP Pool tanımı oluşturulması gerekiyor.











```
FortiGate1 # config firewall ippool
FortiGate1 (ippool) # edit VPC2NAT
FortiGate1 (VPC2NAT) # set type overload
FortiGate1 (VPC2NAT) # set startip 10.10.100.1
FortiGate1 (VPC2NAT) # set endip 10.10.100.254
FortiGate1 (VPC2NAT) # end
```

 VPC2NAT | 10.10.100.1 - 10.10.100.254 | Overload |  Enabled | 1

- IP Pool tanımı yapıldıktan sonra artık Policy tanımına geçilebilir. Policy tanımında NAT özelliğini devreye alıp “**Use Dynamic IP Pool**” seçeneğinde oluşturulan IP Pool tanımının seçilmesi yeterlidir. Policy tanımında kaynak ip kısmında belirtilen adreslerin çıkış arayüzünde tanımlı ip adresine NAT/PAT yapılarak gönderilmesi isteniyor ise burada “**Use Outgoing Interface Address**” seçeneğinin seçilmesi yeterli olacaktır.

```
FortiGate1 # config firewall address
FortiGate1 (address) # edit VPC1_Addr
new entry 'VPC1_Addr' added
FortiGate1 (VPC1_Addr) # set type ipmask
FortiGate1 (VPC1_Addr) # set subnet 10.10.10.10/32
FortiGate1 (VPC1_Addr) # next
FortiGate1 (address) # edit VPC2_Addr
new entry 'VPC2_Addr' added
FortiGate1 (VPC2_Addr) # set type ipmask
FortiGate1 (VPC2_Addr) # set subnet 10.10.40.10/32
FortiGate1 (VPC2_Addr) # end
```

```
FortiGate1 # config firewall policy
FortiGate1 (policy) # edit 10
new entry '10' added
FortiGate1 (10) # set name VPC1_to_VPC2
FortiGate1 (10) # set srcintf port4
FortiGate1 (10) # set dstintf port2
FortiGate1 (10) # set srcaddr VPC1_Addr
FortiGate1 (10) # set dstaddr VPC2_Addr
FortiGate1 (10) # set action accept
FortiGate1 (10) # set schedule always
FortiGate1 (10) # set service ALL
FortiGate1 (10) # set nat enable
FortiGate1 (10) # set ippool enable
FortiGate1 (10) # set poolname VPC2NAT
FortiGate1 (10) # end
```

Name	From	To	Source	Destination	Schedule	Service
VPC1_to_VPC2	 port4	 port2	 VPC1_Addr	 VPC2_Addr	 always	 ALL
Implicit Deny	<input type="checkbox"/> any	<input type="checkbox"/> any	 all	 all	 always	 ALL

- Policy tanımı yapıldıktan sonra son olarak Static route tanımı yapılarak Fortigate1 üzerinde uygulanması gereken konfigürasyonlar tamamlanıyor.

```
FortiGate1 # config router static
FortiGate1 (static) # edit 1
new entry '1' added
FortiGate1 (1) # set dst 10.10.40.0/24
FortiGate1 (1) # set gateway 10.10.20.2
FortiGate1 (1) # set device port2
FortiGate1 (1) # end
```

Edit Static Route

Automatic gateway retrieval ☐

Destination

Subnet
Internet Service

10.10.40.0/255.255.255.0

Gateway Address

10.10.20.2

Interface

port2

Administrative Distance

10

Comments

Write a comment...

Status

☒ Enabled
☐ Disabled

+ Advanced Options

- Fortigate1 üzerindeki konfigürasyonlar tamamlandıktan sonra Fortigate2 üzerindeki tanımlamalara başlanabilir. **Fortigate2 üzerinde normal tanımdan farklı olarak Fortigate1 üzerinden gelecek trafiğin NAT'lanarak geleceği düşünülerek tanımlar 10.10.100.0/24 bloğu üzerinden yapılması gerekiyor.** Özetle 10.10.100.0/24 bloğuna gelecek trafiklerin 10.10.20.1 adresine gönderilmesi gerekecektir. Bunun için ilk adımda Policy tanımı yapılabilir.

```
FortiGate2 # config firewall address
FortiGate2 (address) # edit VPC1_NAT_Addr
new entry 'VPC1_NAT_Addr' added
FortiGate2 (VPC1_NAT_Addr) # set type ipmask
FortiGate2 (VPC1_NAT_Addr) # set subnet 10.10.100.1/24
FortiGate2 (VPC1_NAT_Addr) # next
FortiGate2 (address) # edit VPC2_Addr
new entry 'VPC2_Addr' added
FortiGate2 (VPC2_Addr) # set type ipmask
FortiGate2 (VPC2_Addr) # set subnet 10.10.40.10/32
FortiGate2 (VPC2_Addr) # end
```

```
FortiGate2 # config firewall policy
FortiGate2 (policy) # edit 10
new entry '10' added
FortiGate2 (10) # set name VPC1_to_VPC2
FortiGate2 (10) # set srcintf port2
FortiGate2 (10) # set dstintf port3
FortiGate2 (10) # set srcaddr VPC1_NAT_Addr
FortiGate2 (10) # set dstaddr VPC2_Addr
FortiGate2 (10) # set action accept
FortiGate2 (10) # set schedule always
FortiGate2 (10) # set service ALL
FortiGate2 (10) # end
```

Name	From	To	Source	Destination	Schedule	Service
VPC1_to_VPC2	port2	port3	VPC1_NAT_Addr	VPC2_Addr	always	ALL
Implicit Deny	<input type="checkbox"/> any	<input type="checkbox"/> any	all	all	always	ALL

- Son olarak 10.10.40.10/32 adresinden gelen trafiklerin 10.10.100.1/24 bloğuna ve 10.10.100.1/24 subnetinden gelen trafiklerin 10.10.40.0/24 networküne iletilebilmesi için Static route tanımlarının yapılması yeterli olacaktır.

Destination	Gateway IP	Interface	Status	Comments
10.10.100.0/24	10.10.20.1	port2	Enabled	
10.10.40.0/24	10.10.30.3	port3	Enabled	











```
FortiGate2 # config router static
FortiGate2 (static) # edit 1
new entry '1' added
FortiGate2 (1) # set dst 10.10.100.1/24
FortiGate2 (1) # set gateway 10.10.20.1
FortiGate2 (1) # set device port2
FortiGate2 (1) # next
```

```
FortiGate2 (static) # edit 2
new entry '2' added
FortiGate2 (2) # set dst 10.10.40.0/24
FortiGate2 (2) # set gateway 10.10.30.3
FortiGate2 (2) # set device port3
FortiGate2 (2) # end
```

- Static Route tanımıyla Fortigate2 üzerindeki tanımlamaları da tamamladıktan sonra son adım olan Fortigate3 üzerinde tanımlamalara başlanabilir. Burada da Fortigate2 üzerinde uygulandığı gibi 10.10.10.0/24 subnetinden gelmesi beklenen trafiğin kaynak ip adresinin 10.10.100.1/24 subnetinden bir ip adresiyle geleceği düşünülerek tanım yapılmalıdır. Özetle yapılması gereken tanımlar aşağıdaki gibi olacaktır.


```
FortiGate3 # config firewall address
FortiGate3 (address) # edit VPC1_NAT_Addr
new entry 'VPC1_NAT_Addr' added
FortiGate3 (VPC1_NAT_Addr) # set type ipmask
FortiGate3 (VPC1_NAT_Addr) # set subnet 10.10.100.1/24
FortiGate3 (VPC1_NAT_Addr) # next
FortiGate3 (address) # edit VPC2_Addr
new entry 'VPC2_Addr' added
FortiGate3 (VPC2_Addr) # set type ipmask
FortiGate3 (VPC2_Addr) # set subnet 10.10.40.10/32
FortiGate3 (VPC2_Addr) # end
```


```
FortiGate3 # config firewall policy
FortiGate3 (policy) # edit 10
new entry '10' added
FortiGate3 (10) # set name VPC1_NAT_to_VPC2
FortiGate3 (10) # set srcintf port3
FortiGate3 (10) # set dstintf port4
FortiGate3 (10) # set srcaddr VPC1_NAT_Addr
FortiGate3 (10) # set dstaddr VPC2_Addr
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
VPC1_NAT_to_VPC2	 port3	 port4	 VPC1_NAT_Addr	 VPC2_Addr	 always	 ALL
Implicit Deny	<input type="checkbox"/> any	<input type="checkbox"/> any	 all	 all	 always	 ALL

```
FortiGate3 # config router static
FortiGate3 (static) # edit 1
new entry '1' added
FortiGate3 (1) # set dst 10.10.100.1/24
FortiGate3 (1) # set gateway 10.10.30.2
FortiGate3 (1) # set device port3
FortiGate3 (1) # end
```

Edit Static Route

Automatic gateway retrieval  ☐

Destination 



Subnet Internet Service

10.10.100.0/255.255.255.0


Gateway Address

10.10.30.2

Interface

 port3 

+

Administrative Distance 

10

Comments

Write a comment... 0/255

Status

☒ Enabled ☐ Disabled

+ Advanced Options

```
VPCS> trace 10.10.40.10
trace to 10.10.40.10, 8 hops max, press Ctrl+C to stop
 1  10.10.10.1    0.501 ms  0.398 ms  0.323 ms
 2  10.10.20.2    0.908 ms  0.643 ms  0.449 ms
 3  10.10.30.3    0.934 ms  0.709 ms  0.249 ms
 4  *10.10.40.10  1.358 ms (ICMP type:3, code:3, Destination port unreachable)
```

Unutulmamalıdır ki burada Dinamik NAT yapılmaktadır. DNAT teknolojisinde bir kaynak ip adresinden trafik oluşturulduğunda ilgili kaynak ip adresi NAT işlemine tabi tutulur ve bu işlem NAT tablosuna kayıt edilir. NAT uygulanan kaynak ip adresinin oturumu sonlandırıldığında NAT tablosunda ilgili kaynak ip adresi için oluşturulan satır silinerek kullanılan NAT adresi farklı kaynak ip adreslerinde kullanılmaya başlanacaktır. Dolayısıyla **Dynamic NAT** (DNAT) yönteminin tek yönlü erişimin sağlanması gereken durumlarda kullanılabileceğini söyleyebiliriz. VPC1-VPC2 ile arasında çift yönlü haberleşebilmesi için **Static NAT** (SNAT) konfigürasyonu yapılması gerekiyor.

SNAT konfigürasyonu üzerine örnek yapabilmek adına topolojide Fortigate2'nin 4. Portuna bağlı VPC3 eklenmiştir. Burada Fortigate1 ve Fortigate3 üzerinde aynı ip adreslerini kullanan VPC1 ve VPC2 istemcilerinin Fortigate2 üzerindeki VP3 istemcisiyle karşılıklı olarak haberleşmesi istenmektedir. Bunun için;

-

GÖRSELLER GÜNCELLENECEK VE TEK YÖNLÜ HABERLEŞME OLARAK YAZI TEKRAR DÜZENLENECEK.

ARDINDAN ÇİFT YÖNLÜ HABERLEŞME SAĞLANABİLMESİ İÇİN STATİC NAT KONFIGÜRASYONU AÇIKLANACAK

Kaynaklar

- <https://www.fortinetguru.com/2019/02/configuring-ip-pools-3/>

- <https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-configure-SNAT-with-IP-pool/ta-p/195322>
- <https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/29961/dynamic-snat>