PALO ALTO FIREWALL NAT

Hazırlayan : Mehmet Emin DOĞAN | Sistem Mühendisi

PALO ALTO FIREWALL NAT KAVRAMI VE KONFİGÜRASYONU

Bu makaleyi PAN web sayfasındaki dökümandan faydalanarak yazacağımı bildirmek isterim.

Palo Alto işletim sistemi Source IP/Port ve Destination IP/Port olmak üzere her iki translate işlemini de yapar. Bu işlemi yapmak için bazı kurallar kullanır. Bu kurallar

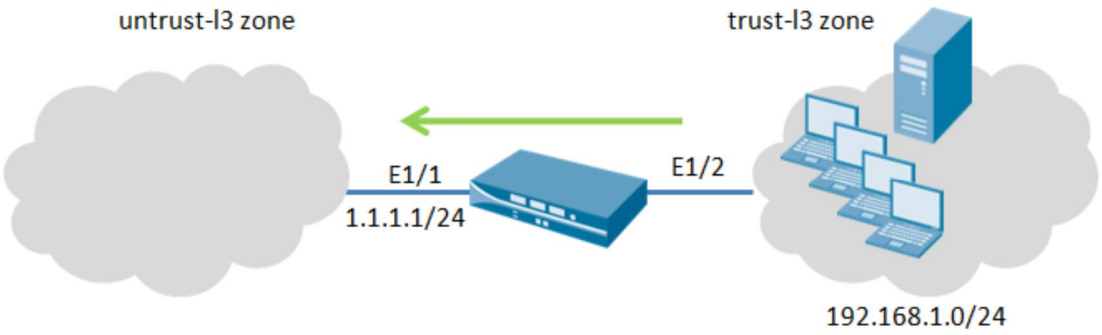
- Source (kaynak) ve Destination (hedef) zone
- Destination Interface (isteğe bağlı)
- Source ve Destination Adres
- Servis

kullanılarak dizayn edilir. Birden fazla NAT kuralı yazılabilir ve bu kurallar yukarıdan aşağıya doğru değerlendirilir. Yukarıdan aşağı doğru gelirken paket herhangi bir NAT kuralı ile eşleşirse diğer tüm kurallar ignore edilir. Bundan dolayı özel bir NAT kuralımız varsa en başa koyarız.

	Source				Destination						
Name	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
rule1	trust-l3	any	any	any	untrust-l3	any	any	any		none	

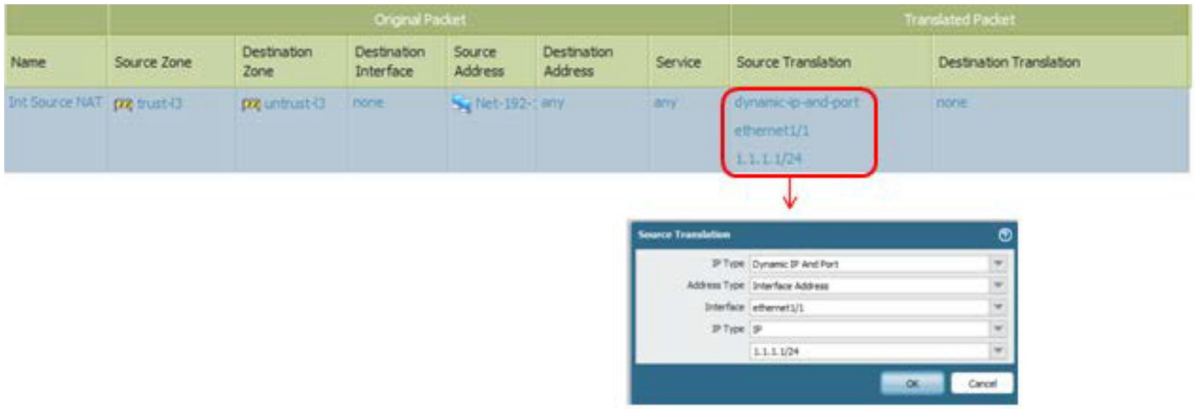
Source NAT

Örnekler üzerinden anlatacağım birkaç case olacak. Topolojimiz aşağıda görüldüğü gibidir.



192.168.1.0/24 subnetindeen gelen büm trafik dış interface'imiz olan E1/1'in IP adresine yani 1.1.1.1/24 subnetinteki adreslere çevriliyor.

Önce NAT kuralımıza bir isim veriyoruz. Source Zone olarak trust olarak isim verdiğimiz iç networkümüzde bulunan zone'u seçiyoruz. Destination Zone bizim untrust dediğimiz dış dünyaya çıkacak alanımız oluyor bunu seçiyoruz. Özellikle seçilmek istenen bir source adress varsa seçiyoruz. Daha sonra Source Translation kısmında dynamic-ip-and-port seçilip, adres tipi interface adres, intereface : dış interface IP tipi IP olarak seçiliyor.



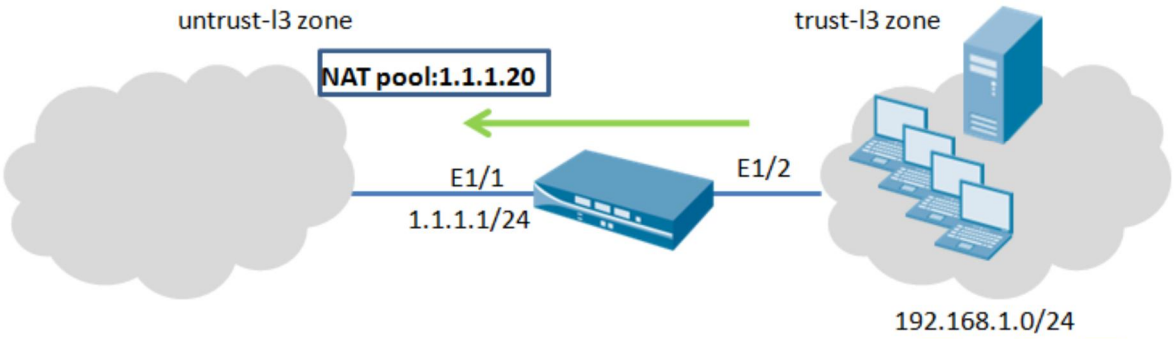
NAT kuralının çalışıp çalışmadığını anlamak için, "show session all" komutunu CLI ekranında çalıştırırsak bize var olan session bilgilerini getirecektir.

```
admin@PA-5060> show session all
--------------------------------------------------------------------------------
ID Application State Type Flag Src[Sport]/Zone/Proto (translated IP[Port])
Vsys Dst[Dport]/Zone (translated IP[Port])
--------------------------------------------------------------------------------
2359304 ssh ACTIVE FLOW NS 192.168.1.250[59534]/trust-l3/6 (1.1.1.1[50219])
vsys1 1.1.1.10[22]/untrust-l3 (1.1.1.10[22])
2359303 ssh ACTIVE FLOW NS 192.168.1.100[50034]/trust-l3/6 (1.1.1.1[51650])
vsys1 1.1.1.10[22]/untrust-l3 (1.1.1.10[22])
admin@PA-5060>
```

Herhangi bir session''un detaylı bilgisini de görmek istersek " show session id 2359304 komutunu kullanabiliriz.

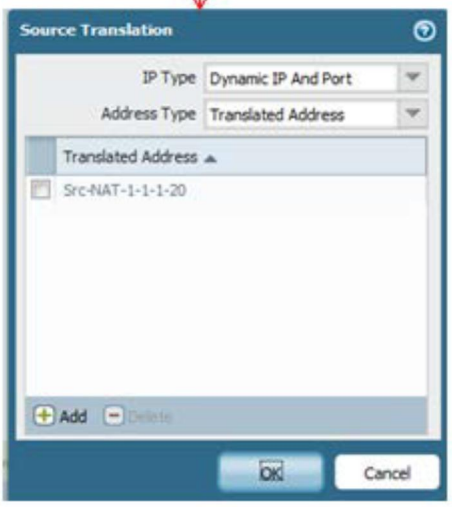
```
admin@PA-5060> show session id 2359304
Session 2359304
c2s flow:
source: 192.168.1.250 [trust-l3]
dst: 1.1.1.10
proto: 6
sport: 59534 dport: 22
state: ACTIVE type: FLOW
src user: unknown
dst user: unknown
s2c flow:
source: 1.1.1.10 [untrust-l3]
dst: 1.1.1.1
proto: 6
sport: 22 dport: 50219
state: ACTIVE type: FLOW
src user: unknown
dst user: unknown
start time : Fri Apr 8 10:26:33 2011
timeout : 432000 sec
time to live : 431845 sec
total byte count : 5686
```

ÖRNEK 2 HERHANGİ BİR ADRESİ NAT TRANSLATİON İÇİN KULLANMAK

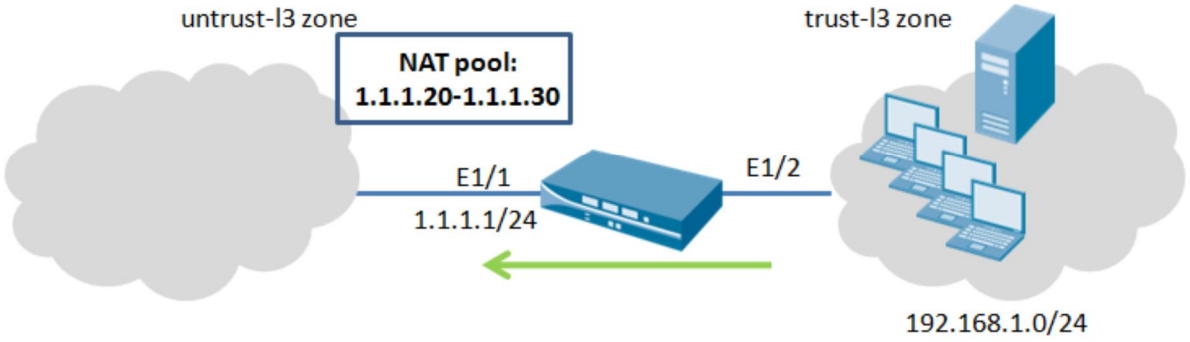


Burda Source translation olarak dynamic-ip-and-port seçtikten sonra Adres tipini Translated Adress olarak seçip daha önce oluşturduğumuz bir adres objesini translated adres olarak seçiyoruz.

	Original Packet						Translated Packet	
Name	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
Int Source NAT	trust-l3	untrust-l3	none	Net-192-	any	any	dynamic-ip-and-port Src-NAT-1-1-1-20	none



ÖRNEK 3 SOURCA NAT IP ADRESS TRANSLATİON



Sadece Source IP adreslerimizi NAT işlemine tabi tutarken Source Translation kısmında dynamic-ip kısmını seçip daha önce belirlediğimiz bir IP havuzunu Translated Address olarak belirliyoruz.

Destination NAT

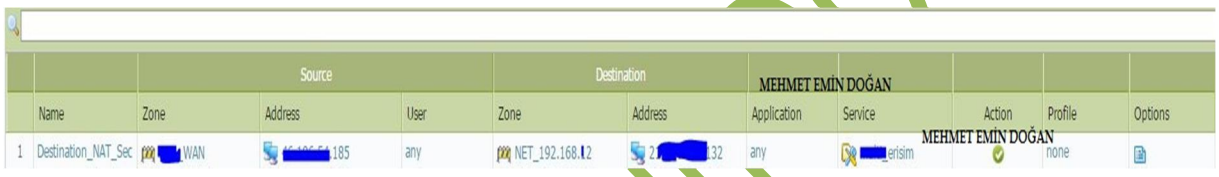
Destinatio NAT hedef ip adreslerini ve portlarını translate etmek için kullanılır. Aynı zamanda tek bir IP adresini birden fazla iç IP adresine çevirmek için de kullanılır. Destination Port numaraları da destination host'ları tanımlamak için kullanılır.

Bu örnekte daha önce bazı testler yapmak iiçin kullandığım NAT kuralını ve politikasını sizlerle paylaşacağım.

Sms Kimlik doğrulama sistemi için yaptığımız testi kısaca şöyle açıklayacağım. Palo Alto Firewall üzerinde kimlik doğrulama profili olarak bir sms authentication ürününü seçtik. Dışarıdan bir IP'ye bu testi gerçekleştirmesi için NAT kuralı ve NAT politikası yazılması gerekir.

NAT kuralımızın adını verip, Source Zone olarak WAN zone'umuzu seçiyoruz. Desstination Zone olarak da WAN alanımızı seçiyoruz (istekler dış bacağa geldiği için).Destination adres olarak WAN bacağımıza yani isteklerin dışarıdan gelirken karşılaşacağı ilk bacağıın IP adresini yazıyoruz. Eğer özel bir servis grubunuz varsa servis grup olarak ekleyip burda servis kısmına girebilirsiniz. Buraya kadar orijinal paket için konfigürasyonumuzdu. Translated paket için ise Destination Adress Translation kısmından translated adresi içerideki radius server IP adresini yani sms authentication yazılımının kurulu olduğu server'ın ip adresini veriyoruz.

Gelelim bu NAT kuralı için politika (poicy) yazmaya:

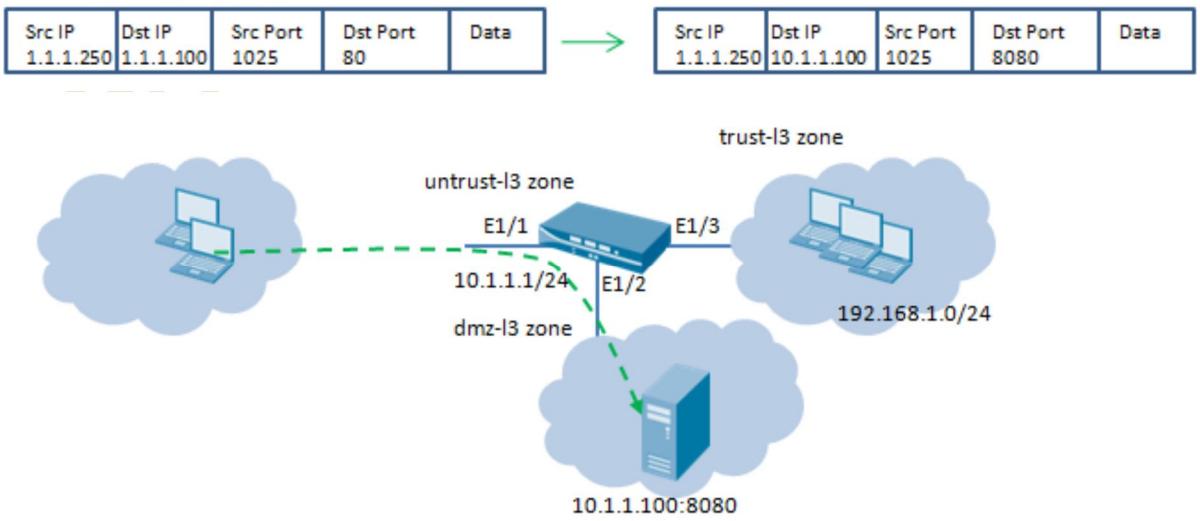


Policy ismini verdikten sonra dışarıdan şu IP adresinden gelip şu Zone'ume ulaşmaya çalışan kullanıcıya izin ver işlemini resimde görüldüğü gibi uyguluyoruz.

Destination IP & Port Translation

Bazı durumlarda Hep IP hem de Port translation gerekebilir. Aşağıdaki örnek PAN resmi sayfasından alınarak hazırlanmıştır

Topoloji :



NAT Kuralı

	Original Packet						Translated Packet	
Name	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
Dst NAT-webserv	untrust-l3	untrust-l3	none	any	Servers-public	service-http	none	address: webserver-private port: 8080

Dışarıdan untrust Zone'uma gelip serverlarıma 80 portuyla erişen kullanıcının I P adresini ve Portunu translate et.

Security Kuralı

	Source		Destination			
Name	Zone	Address	Zone	Address	Application	Service
Webserver acces	untrust-l3	any	dmz-l3	Servers-public	web-browsing	any

Dışarıdan DMZ alanıma web uygulamasını kullanarak gelenlere izin ver.

Verification

```
admin@PA-2050> show session all
--------------------------------------------------------------------------------
ID Application State Type Flag Src[Sport]/Zone/Proto (translated IP[Port])
Vsys Dst[Dport]/Zone (translated IP[Port])
--------------------------------------------------------------------------------
80 web-browsing ACTIVE FLOW ND 1.1.1.250[55077]/untrust-l3/6 (1.1.1.250[55077])
vsys1 1.1.1.100[80]/dmz-l3 (10.1.1.100[8080])
```


Soru ve önerileriniz için m.emn.dogan@gmail.com adresine yazabilirsiniz.