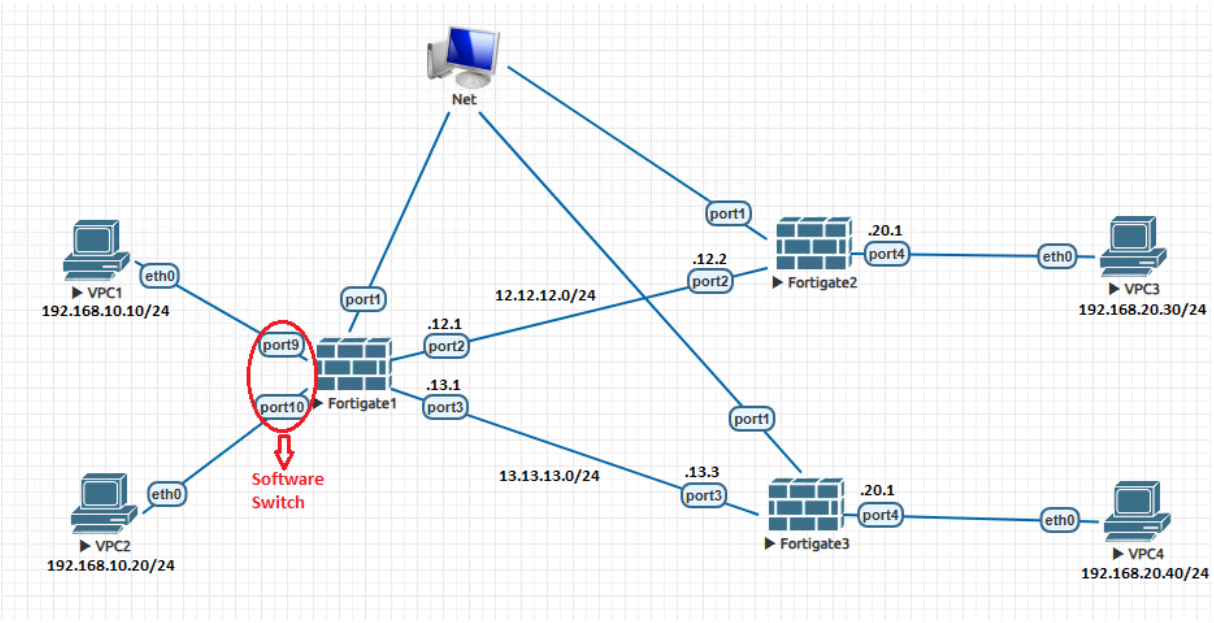
PBR (Policy Based Routing)

L3 cihazlar üzerinde yapılan yönlendirme sürecine müdahale edilmesi gereken durumlarla karşılaşılabiliyor. Örnek olarak bir kaynağa iki farklı erişim seçeneği bulunabilir ve bazı istemcilerin (tüm protokoller için veya sadece belirli protokoller için) ikinci rotayı tercih ederek ulaşması istenebilir. Bu gibi durumlarda PBR (Policy Based Routing) özelliğine ihtiyaç duyulmaktadır.

PBR (Policy Based Routing), bir trafiğin sadece hedef ip adresine bakılarak yönlendirilmesini sağlamak yerine, belirli bir kaynak ip, protokol türü, uygulama, kullanıcı, port numarasını göz önünde bulundurup belirli bir hedefe yönlendirilmesini sağlamak için kullanılan özelliktir. Bu özelliği aşağıdaki örnek topoloji üzerinden açıklamak gerekirse;



Topolojiye genel olarak bakıldığında Fortigate2 ve Fortigate3 cihazlarının Internal portlarında 192.168.20.0/24 networkü kullanılıyor. Fortigate1'e bağlı VPC1 cihazının VPC3'e, VPC2 cihazının VPC4'e erişmesi gerekiyor. Bu durumda uygulanabilecek iki seçenek bulunuyor.

- İlk seçenek NAT uygulanarak VPC1 ve VPC2'nin farklı bir ip bloğu üzerinden VPC3 ve VPC4'e erişmesi sağlanabilir.
    - Burada ek olarak NAT üzerine PBR uygulanarak VPC1 ve VPC2'nin belirli portlar için Fortigate2 üzerindeki Internal networküne, belirli portlar için Fortigate3 üzerindeki Internal networküne erişmesi de sağlanabilir.
- İkinci seçenek olarak doğrudan PBR uygulanarak VPC1 istemcisinin VPC3'e erişimi için Fortigate2'yi, VPC2 istemcisinin VPC4'e erişmesi için Fortigate3'ü tercih etmesi sağlanabilir. Bu uygulama da bu erişim için konfigürasyon yapılacaktır.

PBR kullanarak VPC1'in VPC3'e, VPC2'nin VPC4'e erişebilmesi için;

- FW'lar üzerinde Software Switch tanımı ve sırasıyla FGT1, FGT2, FGT3 üzerindeki ilgili portlara ip atamaları yapılarak Ping paketlerine izin verilmiştir.

Physical Interface 8							
port1	Physical Interface		192.168.1.36/255.255.255.0	PING HTTPS SSH HTTP			0
port2	Physical Interface		12.12.12.1/255.255.255.0	PING			4
port3	Physical Interface		13.13.13.1/255.255.255.0	PING			4
port4	Physical Interface		0.0.0.0/0.0.0.0				0
port5	Physical Interface		0.0.0.0/0.0.0.0				0
port6	Physical Interface		0.0.0.0/0.0.0.0				0
port7	Physical Interface		0.0.0.0/0.0.0.0				0
port8	Physical Interface		0.0.0.0/0.0.0.0				0
Software Switch 1							
Internal1	Software Switch	port9 port10	192.168.10.1/255.255.255.0	PING			4

Physical Interface 4							
Internal1 (port4)	Physical Interface		192.168.20.1/255.255.255.0	PING			1
port1	Physical Interface		192.168.1.37/255.255.255.0	PING HTTPS SSH HTTP			0
port2	Physical Interface		12.12.12.2/255.255.255.0	PING Security Fabric Connection			2

Physical Interface 4							
Internal1 (port4)	Physical Interface		192.168.20.1/255.255.255.0	PING			1
port1	Physical Interface		192.168.1.38/255.255.255.0	PING HTTPS SSH HTTP			0
port2	Physical Interface		0.0.0.0/0.0.0.0				0
port3	Physical Interface		13.13.13.3/255.255.255.0	PING			2

- Interface tanımları yapıldıktan sonra sırasıyla FGT1, FGT2 ve FGT3 için Static Route tanımları yapıldı.

Destination	Gateway IP	Interface	Status
192.168.20.0/24	12.12.12.2	port2	Enabled
192.168.20.0/24	13.13.13.3	port3	Enabled

Destination	Gateway IP	Interface	Status
192.168.10.0/24	12.12.12.1	port2	Enabled

Destination	Gateway IP	Interface	Status
192.168.10.0/24	13.13.13.1	port3	Enabled

- Static Route tanımlarından sonra sırasıyla FGT1, FGT2 ve FGT3 için Policy tanımları da (tek yönlü tanımlandı) yapılarak VPC1'den VPC3'e erişim ve VPC2'den VPC4'e erişim test edildi.
    - Burada unutulmamalıdır ki, VPC3'Ün de VPC4'ün de ip adresi 192.168.20.0/24 bloğuna dahil edilmiştir. Eğer ki her iki cihazın da ip adresi aynı verilmiş olunsaydı bu durumda NAT kullanmak zorunda kalınacaktır.
    - Farklı bir bakış açısıyla 192.168.10.0/24 networkündeki bütün cihazların hem Fortigate2 hem de Fortigate3 üzerindeki 192.168.20.0/24 networküne

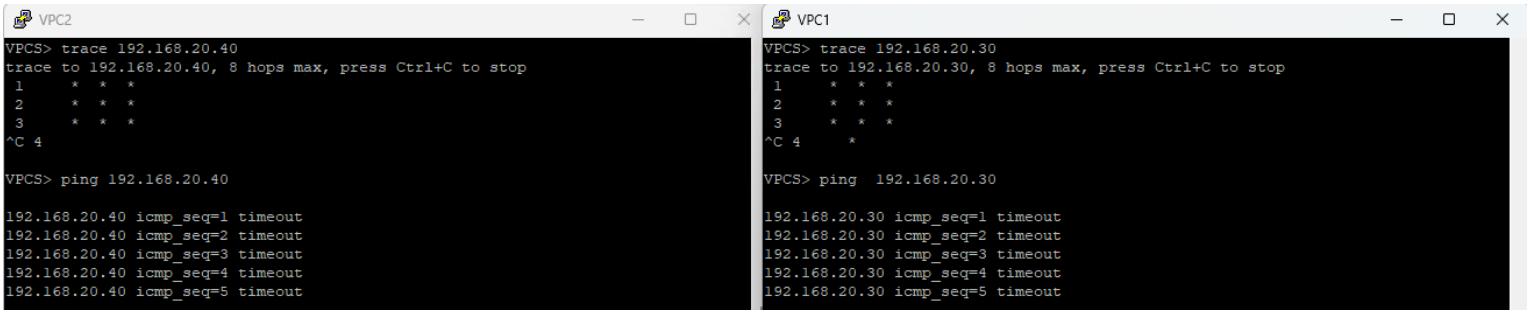
erişmesi istenseydi NAT teknolojisi kullanılmak zorunda kalınacaktı. PBR kullanımını irdelemek adına farklı istemcilerin farklı hedeflere erişmesi üzerine konfigürasyon yapılıyor.

Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
FGT1_VPC1_to_Internal1_VPC3	port2	Internal1 (port4)	VPC1	VPC3	always	ALL	ACCEPT	Disabled	SSL no-inspection	All	2.21 kB
Implicit Deny	any	any	all	all	always	ALL	DENY			Disabled	0 B

Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
Internal1_VPC1_to_FGT2_VPC3	Internal1	port2	all	VPC3	always	ALL	ACCEPT	Disabled	SSL no-inspection	All	4.42 kB
Internal1_VPC2_to_FGT3_VPC4	Internal1	port3	all	VPC4	always	ALL	ACCEPT	Disabled	SSL no-inspection	All	2.50 kB
Implicit Deny	any	any	all	all	always	ALL	DENY			Enabled	3.46 kB

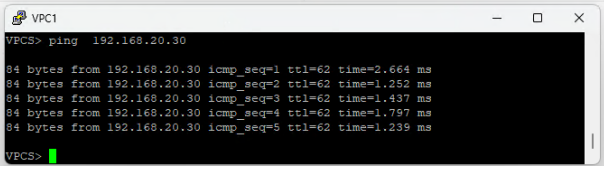
Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
FGT1_VPC2_to_Internal1_VPC4	port3	Internal1 (port4)	VPC2	VPC4	always	ALL	ACCEPT	Disabled	SSL no-inspection	All	1.67 kB
Implicit Deny	any	any	all	all	always	ALL	DENY			Disabled	0 B

- Policy tanımları yapıldıktan erişimler test edildiğinde çıktıları aşağıdaki gibi görünmektedir.
    - Burada Policy tanımlanırken kaynak ip adreslerini “all” yerine farklı spesifik olarak VPC1 ve VPC2 belirtilse dahi paketler hedefine ulaşmayacaktır.



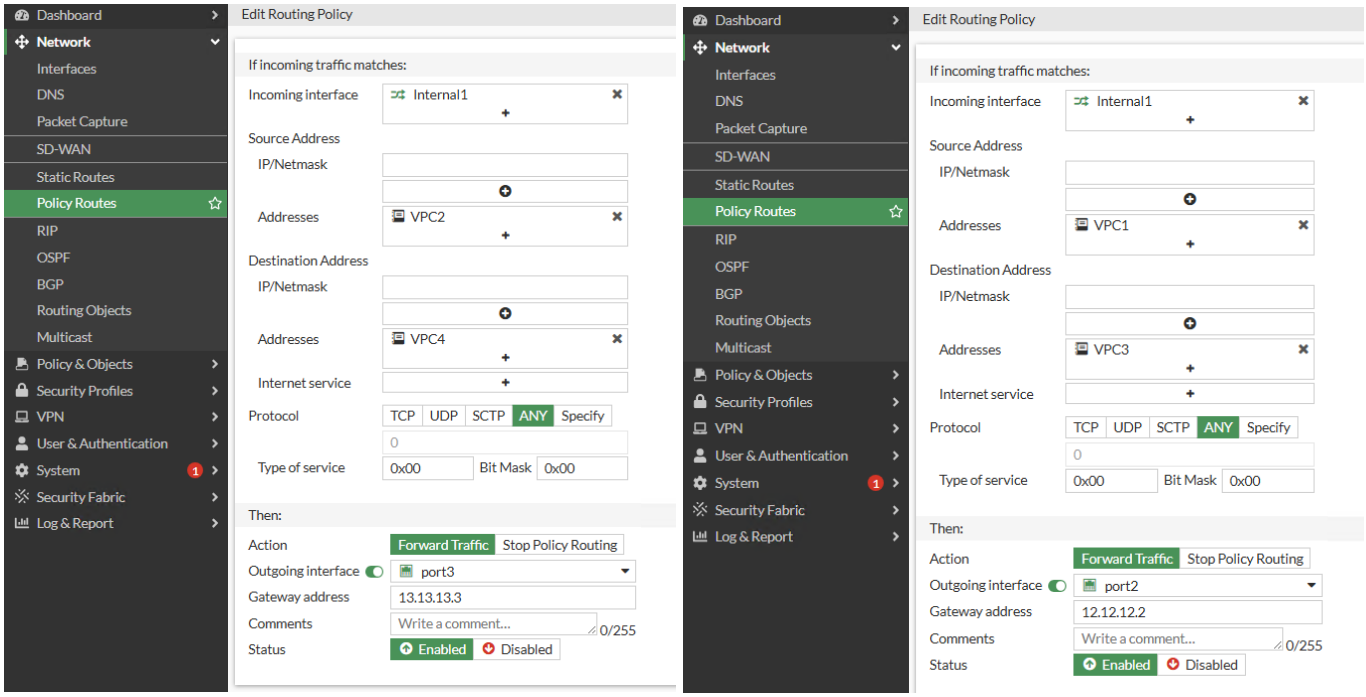
    - İstemcilerin hedefe erişememsinin nedeni Static Route kısmında 192.168.20.0/24 networkü için iki farklı Static Route tanımının bulunmasıdır. Bunu Static Route tanımlarından birisini Disable’a çekip aktif olan Static Route için erişimi test ederek görebilirsin. Bu durumda aktif olan Static Route tanımını için erişim sağlanabilecektir.

Destination	Gateway IP	Interface	Status
192.168.20.0/24	12.12.12.2	port2	Enabled
192.168.20.0/24	13.13.13.3	port3	Disabled

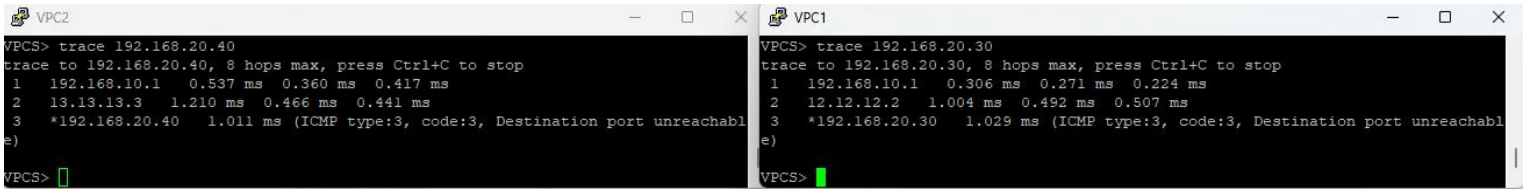


- Erişimi sağlayabilmek için PBR tanımında belirli bir kaynaktan gelip belirli bir hedefe giden trafiğin hangi Gateway’i kullanacağını belirlemek üzere PBR tanımı yapılması gerekmektedir. Aşağıdaki görselden de anlaşılacağı üzere paketlerin hangi **Interface üzerinden geleceği**, **hangi Interface üzerinde çıkarılacağı**, **kaynak ve hedef ip adresleri** (bir ip bloğu olabileceği gibi belirli ip adresleri de eklenebiliyor), **hangi protokole sahip paketler olacağı** ve **QoS uygulanıp uygulanmayacağı** gibi parametreler burada tanımlanıyor.

- Gateway adresi olarak Next Hop ip adresinin yazıldığına dikkat edilmelidir.
- Action kısmında anlaşılacağı üzere, paketler Policy tabanlı yönlendirilebileceği gibi engellenmesi/bloklanması da sağlanabiliyor.



- PBR tanımları yapıldıktan sonra her iki istemcinin de hedeflerine erişebildiği görülebilmektedir.



Notlar

- PBR konfigürasyonuyla bir hat üzerindeki L3 bağlantının kesilmesi sonucunda FW üzerinde çeşitli aksiyonların alınması (farklı bir hat üzerinden trafiğin devam etmesinin sağlanması, HA'in pasif durumdaki FW'a geçmesi gibi) da sağlanabiliyor. Bu gibi pek çok çözümde kullanılabiliyor.