**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;

diyagram, çizgi, metin, öykü gelişim çizgisi; kumpas; grafiğini çıkarma içeren bir resim

Yapay zeka tarafından oluşturulan içerik yanlış olabilir.

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.

metin, ekran görüntüsü, sayı, numara, çizgi içeren bir resim

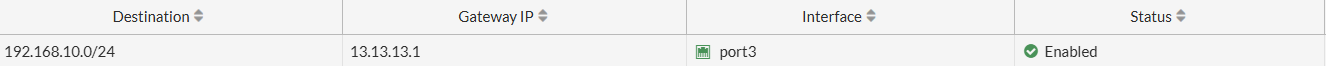
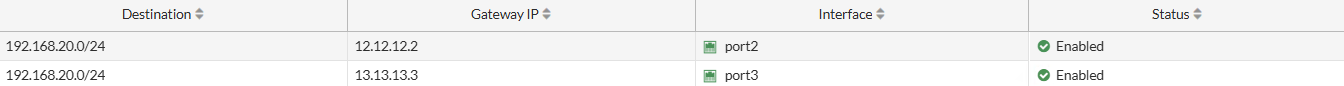
Yapay zeka tarafından oluşturulan içerik yanlış olabilir.

metin, ekran görüntüsü, yazı tipi içeren bir resim

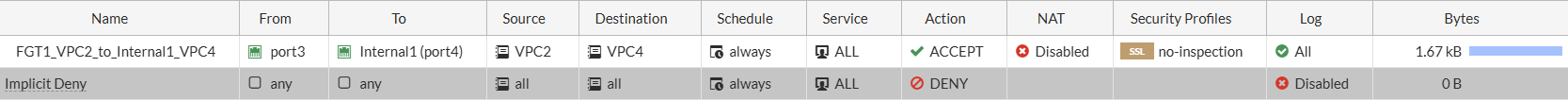
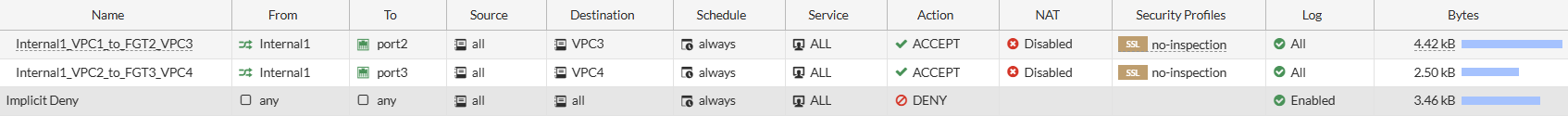
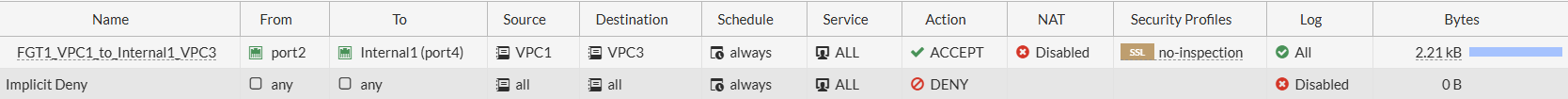
Yapay zeka tarafından oluşturulan içerik yanlış olabilir.metin, ekran görüntüsü, çizgi, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulan içerik yanlış olabilir.

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



* 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.



* 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.

metin, yazı tipi, ekran görüntüsü içeren bir resim

Yapay zeka tarafından oluşturulan içerik yanlış olabilir.

* + 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.

metin, ekran görüntüsü, yazılım, multimedya yazılımı içeren bir resim

Yapay zeka tarafından oluşturulan içerik yanlış olabilir.

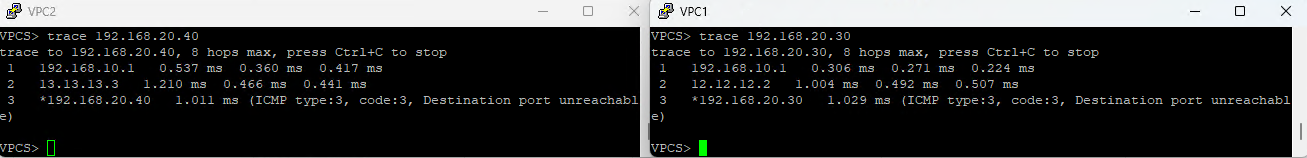
* Erişimi sağlayabilmek için PBR tanımında belirli bir kaynaktan gelip belirli bir hedefe giden trafiğin hangi Gateway’i kullanacağını belirlemek üzere PBR tanımı yapılması gerekmektedir. Aşağıdaki görselden de anlaşılacağı üzere paketlerin hangi **Interface üzerinden geleceği**, **hangi Interface üzerinde 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.

metin, ekran görüntüsü, yazılım, sayı, numara içeren bir resim

Yapay zeka tarafından oluşturulan içerik yanlış olabilir. metin, ekran görüntüsü, yazılım, sayı, numara içeren bir resim

Yapay zeka tarafından oluşturulan içerik yanlış olabilir.

* 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.