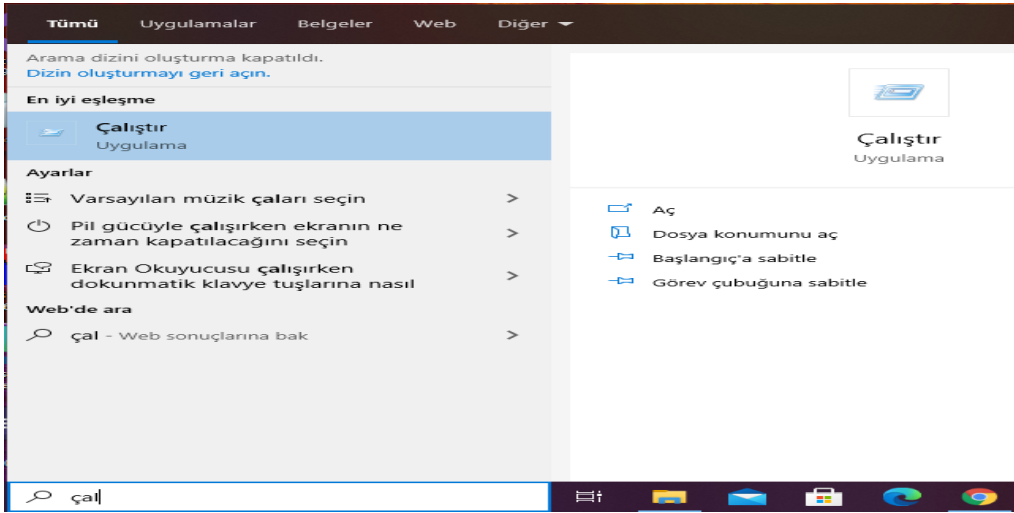


Windows 10 İşletim Sisteminin Güvenlik Duvarında IP Adresi Engelleme

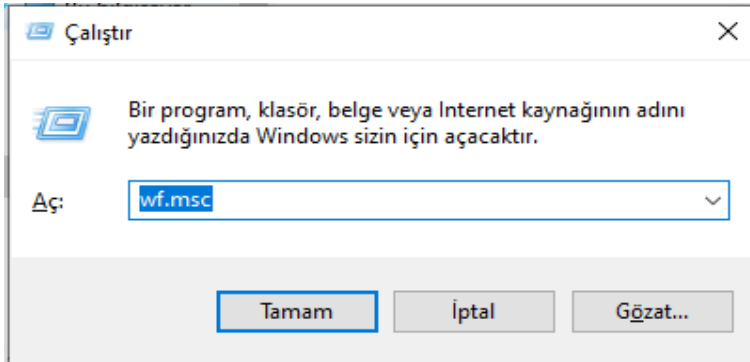
Yakın zamanda internetimde yavaşlamalar gerçekleştiğini fark ettim. Bunun üzerine bilgisayarımda ağ protokol analiz aracı olan Wireshark uygulamasını açtığımda dikkatimi kendi bilgisayarımın bir IP adresinin 80 portuna sürekli TCP bağlantı istekleri gönderdiğim dikkatimi çekti. Bu trafikte herhangi bir veri aktarmaksızın TCP oturumları açılıp sonlandırılıyordu. Bunun önüne geçebilmek adına bilgisayarımın interneti kullanan uygulamaları kapatarak bu oturumun tek IP adresinden mi yoksa farklı IP adreslerine de gönderilip gönderilmediğini gözlemledim. Gördüğüm kadarıyla tek IP adresine gönderiliyordu. Bunun üzerine Windows işletim sisteminin kendi güvenlik duvarında bu IP adresinden giden paketleri engelleyebileceğim bir kural tanımlamaya karar verdim. BU yazımda sizlere Windows işletim sistemindeki güvenlik duvarında nasıl IP adresinden veya IP adres aralığından gelen paketleri engelleyebileceğinizi anlatmaya çalışacağım.

Adımlar:

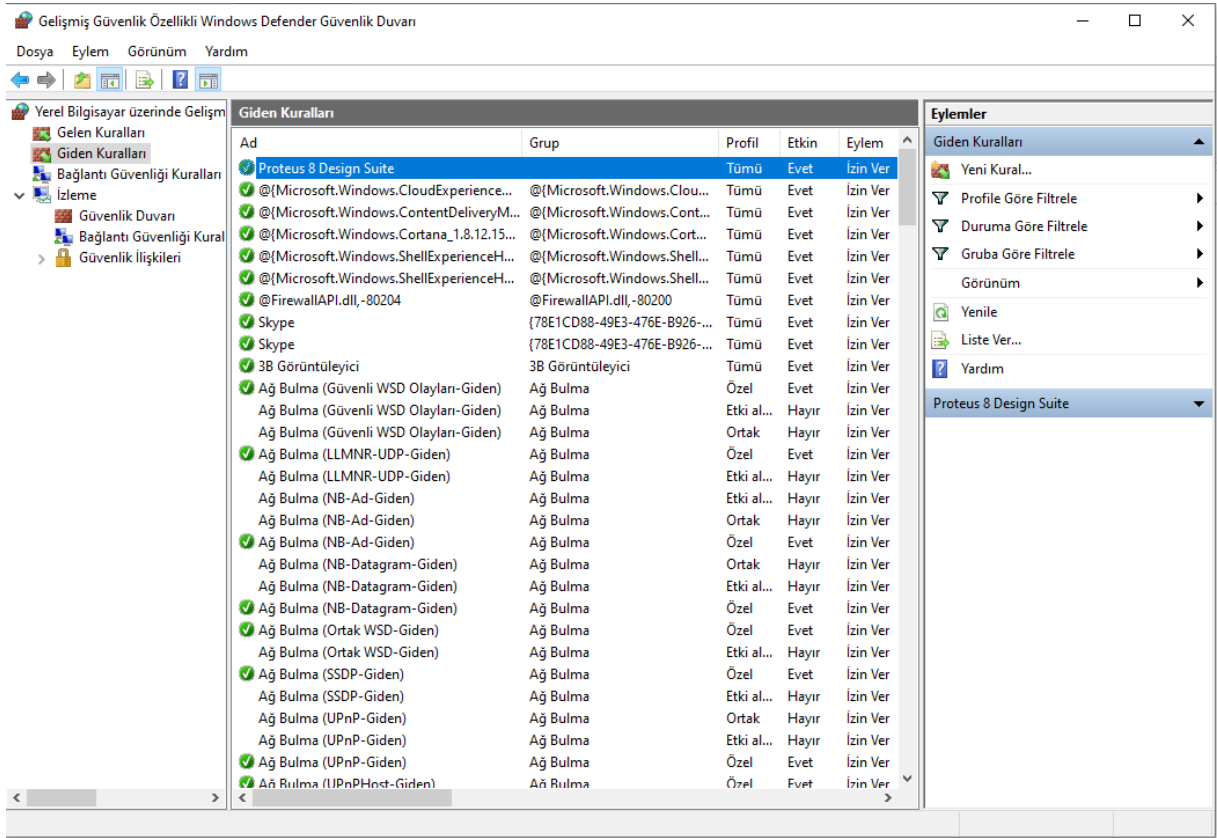
1-Bilgisayarın arama kısmına işletim sisteminin Türkçe kullanıyorsanız “çalıştır” İngilizce kullanıyorsanız “run” yazarak açılan pencereyi açıyoruz.



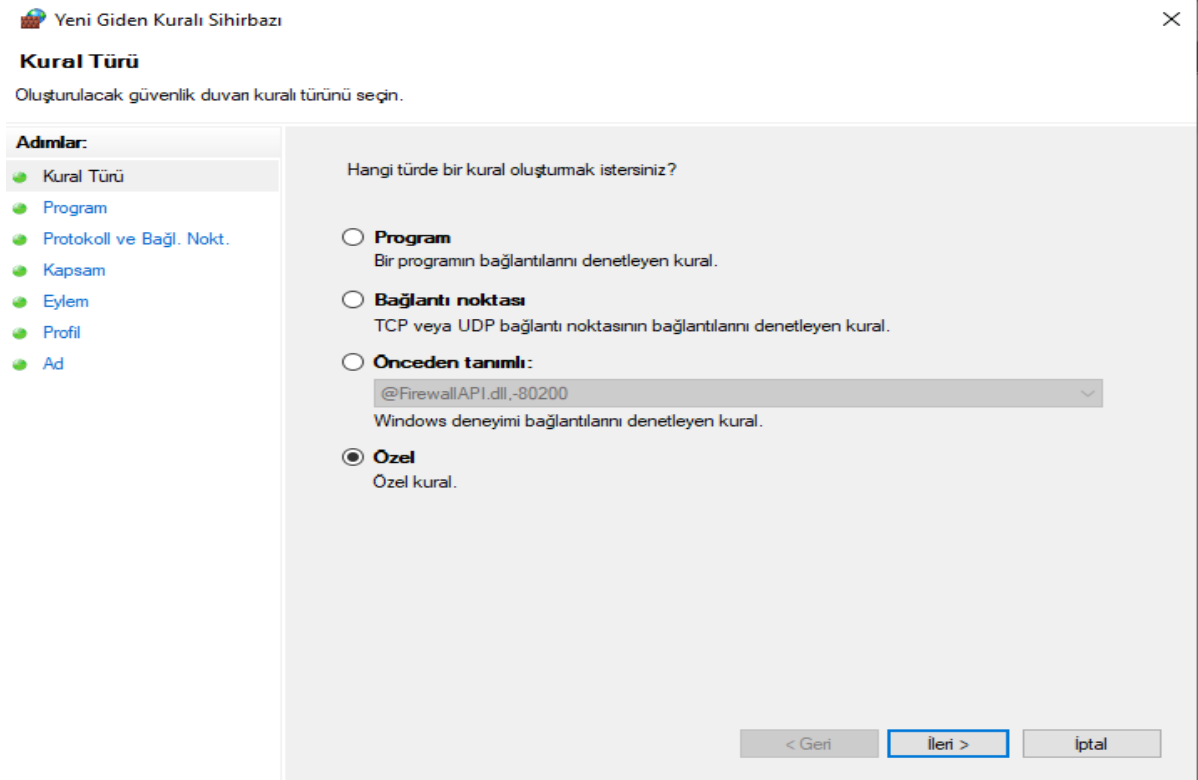
2- Açılan pencerede “wf.msc” yazarak gelişmiş güvenlik özellikli Windows güvenlik duvarı penceresini açıyoruz.




3- Bu pencerede engellemek istediğimiz IP adresinin durumuna göre bilgisayarımızdan istek gönderilmesini istediğimiz veya istemediğimiz IP adresleri için “Giden Kuralları” kısmını seçiyoruz. Bilgisayarımıza istek gönderilmesini istemediğimiz IP adreslerine işlem yapmak istiyorsak “Gelen Kuralları” kısmını seçiyoruz. Ben kendi bilgisayarımdan istek gönderildiği için “Giden Kuralları” kısmı seçiyorum. “Eylemler” kısmında “Yeni Kural” kısmına tıklıyoruz.



4- Açılan pencerede IP adresi engelleme kuralı oluşturmak için kural türünü “Özel” olarak seçiyoruz ve “İleri” butonuna tıklıyoruz.



5- Burada “Tüm Programlar” seçerek devam ediyoruz.

 Yeni Giden Kuralı Sihirbazı

Program

Bu kuralın eşleştiği programın tam yolunu ve yürütülebilir dosyasının adını belirtin.

Adımlar:

Kural Türü

Program

Protokoll ve Bağl. Nokt.

Kapsam

Eylem

Profil

Ad

Bu kural tüm programlara mı yoksa belirli bir programı mı uygulanacak?

☒ Tüm programlar

Kural, bilgisayar üzerindeki, diğer kural özellikleriyle eşleşen tüm bağlantılara uygulanır.

☐ Bu programın yolu:

Gözet...

Ömek: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

Hizmetler

Bu kuralın uygulanacağı hizmetleri belirtin.


Özelleştir...

< Geri

İleri >

İptal

6- Burada herhangi bir değişiklik yapmadan “ileri” butonuna tıklayarak devam ediyoruz.

 Yeni Giden Kuralı Sihirbazı

Protokoll ve Bağl. Nokt.

Bu kuralın uygulandığı protokolleri ve bağlantı noktalarını belirtin.

Adımlar:

Kural Türü

Program

Protokoll ve Bağl. Nokt.

Kapsam

Eylem

Profil

Ad

Bu kural hangi bağlantı noktaları ve protokoller için geçerlidir?

Protokol türü:

Herhangi

Protokol numarası:

0

Yerel bağlantı noktası:

Tüm bağlantı noktaları

Ömek: 80, 443, 5000-5010

Uzak bağlantı noktası:

Tüm bağlantı noktaları

Ömek: 80, 443, 5000-5010

İnternet Denetim İletisi Protokolü (ICMP) ayarları:

Özelleştir...

< Geri

İleri >

İptal

7- Açılan pencerede ise kapsamı belirlemek için girilecek IP adreslerinin yerel ağdan gelecek IP adresleri ise “yerel IP adresine uygulanıyor” kısmına , global bir IP adresinden gelecek IP adresleri için engelleme yapacaksanız “uzak IP adreslerine uygulanıyor” kısmına yazacağız. Belirli IP adreslerini engelleyebilmek için “Bu IP adresleri” radio butonunu seçerek metin alanının yan tarafından bulunan “Ekle” butonuna tıklıyoruz.

Yeni Giden Kuralı Sihirbazı

Kapsam

Bu kuralı uygulayan protokolü ve uzaktaki IP adreslerini belirtin.

Adımlar:

- Kural Türü
- Program
- Protokoll ve Bağlı Nokt.
- Kapsam**
- Eylem
- Profil
- Ad

Bu kural hangi yerel IP adreslerine uygulanıyor?

☒ Herhangi Bir IP Adresi

☐ Bu IP adresleri:

Ekle...
Düzenle...
Kaldır

Bu kuralın uygulandığı arabirim türlerini özelleştir: Özelleştir...

Bu kural hangi uzak IP adreslerine uygulanıyor?

☐ Herhangi Bir IP Adresi

☒ Bu IP adresleri:

Ekle...
Düzenle...
Kaldır

< Geri İleri > İptal

8- Açılan pencerede ise engellemek istediğiniz IP adreslerini yazarak “Tamam” butonuna tıklıyoruz. Eğer ki tek IP adresi yerine IP adres aralığını engellemek istiyorsak “Bu IP adres aralığı” kısmını seçerek girilecek adres aralığının ilk ve son IP adres alanlarını doldurarak engelleyebilirsiniz.

IP Adresi

Eğleştirilecek IP adreslerini belirt:

☒ Bu IP adresi veya alt ağ:

Örnekler: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112

☐ Bu IP adresi aralığı:

İlk:

Son:

☐ Önceden tanımlanan bilgisayar kümesi:

Varsayılan Ağ Geçidi

Tamam İptal

9- Engellemek istediğimiz IP adreslerini tanımladıktan sonra bu adreslere uygulanacak eylemi “Bağlantıyı engelle” olarak seçiyoruz.

Yeni Giden Kuralı Sihirbazı

Eylem

Bağlantı kuralda belirtilen koşullarla eşleştğinde yapılacak eylemi belirtin.

Adımlar:

- Kural Türü
- Program
- Protokoll ve Bağl. Nokt.
- Kapsam
- Eylem**
- Profil
- Ad

Bir bağlantı belirtilen koşulları sağladığında gerçekleştirilmesi gereken eylem nedir?

☐ **Bağlantıya izin ver**
Buna IPsec ile korunanların yanısıra korunmayan bağlantılar da dahildir.

☐ **Bağlantı güvenliyse izin ver**
Buna yalnızca IPsec kullanarak kimliği doğrulanmış bağlantılar dahildir. Bağlantıların güvenliği IPsec özelliklerindeki ayarlar ve Bağlantı Güvenliği Kuralı düğümündeki kurallar kullanılarak sağlanır.

☐ **Bağlantıyı engelle**

10- Sıradaki pencerede tanımlardan da anlaşılacağı gibi ne zaman uygulanacağını seçiyoruz. Ben ağ fark etmeksizin uygulanmasını istediğim için hepsini seçerek devam ediyorum.

Yeni Giden Kuralı Sihirbazı

Profil

Bu kuralın uygulandığı profilleri belirtin.

Adımlar:

- Kural Türü
- Program
- Protokoll ve Bağl. Nokt.
- Kapsam
- Eylem
- Profil**
- Ad

Bu kural ne zaman uygulanacak?

☒ **Etki alanı**
Bilgisayar kuruluş etki alanına bağlandığında uygulanır.

☒ **Özel**
Bilgisayar ev veya işyeri gibi bir özel ağ konumuna bağlandığında uygulanır.

☒ **Ortak**
Bilgisayar bir ortak ağ konumuna bağlandığında uygulanır.

11- Son olarak tanımladığımız kuralı belirleyecek bir “Ad” tanımlıyoruz ve kuraldaki yapılan engellemelerle ilgili açıklama eklemek istersek “Açıklama” kısmına yazabiliyoruz. “Son” butonuna tıkladıktan sonra kuralımızı oluşturmuş oluyoruz.

Artık güvenlik duvarı -> gelişmiş ayarlar -> giden kurallar (tanımlamayı yaptığınız alan bağlı olarak) kısmına giderek tanımlamış olduğunuz kuralı görebilirsiniz. Artık tanımlamış olduğunuz kuralın çalışıp çalışmadığını wireshark gibi bir ağ sniff aracı kullanarak test edebilirsiniz.

Kaynaklar:

<https://help.liquidweb.com/s/article/Blocking-IP-Addresses-Using-Windows-Firewall>

<https://superuser.com/questions/1159401/using-windows-firewall-to-block-a-specific-ip-on-windows-10>

<https://techexpert.tips/windows/windows-firewall-block-ip-address-list/>