

WINDOWS TEMELLERİ

WINDOWS DOSYA SİSTEMİ

1. PerfLogs

PerfLogs, Windows performans günlüklerini tutmak için oluşturulan bir klasördür. Günlük kaydı seçeneği varsayılan olarak kapalı olduğundan, boş bir klasör olarak bulunur.

2. ProgramData

ProgramData klasörü, Windows işletim sisteminin yüklü olduğu diskin kökünün altında gizli bir klasördür. Klasörü görebilmek için önce "Görüntüle" menüsü altında "Gizli Öğeler" seçeneği etkinleştirilmelidir. Bu klasörde, kullanıcı hesaplarından bağımsız olarak sistemde kurulu programlara ait veriler bulunmaktadır.

3. Program Files

Sistemde kurulu tüm programlar, 32 bit olarak yüklü bir Windows işletim sisteminde "Program Files" klasörü altında bulunur. 64-bit olarak yüklenen Windows işletim sistemlerinde, bu klasörün altına sadece 64-bit programlar yüklenir.

4. Program Files (x86)

Bu klasör, yalnızca "64-bit" olarak kurulu Windows işletim sistemlerinde kullanılabilir. Bu klasörün altında, sistemde yüklü olan "32-bit" programlar bulunur. "64-bit" olarak yüklenen programlar, benzer bir adla "Program Files" adlı başka bir klasörde saklanır.

5. Users

Kullanıcılar klasörü, sistemde en az bir kez oturum açan her kullanıcının kişisel klasörünü içerir. Masaüstü klasörü, indirilen dosyalar ve belgeler gibi klasörler ve belgeler, sistemdeki her kullanıcıya ait olan bu klasörün altında saklanır.

6. Windows

Windows klasörü, tüm işletim sisteminin kurulu olduğu yerdir. Kendine özgü bir yapısı vardır ve belirli bir düzende birçok sistemik bilgiyi içerir. Örneğin, kullanıcıların parolalarının tutulduğu veritabanı bu klasörün altında bulunur.

Windows Komut Satırı

1. Help

"Help", komut satırında kullanılan komutlar hakkında ayrıntılı bilgi sağlayan bir komuttur. Bilgi almak için ihtiyacımız olan komutların parametrelerini "Help" komutu ile görebiliriz.

2. Dir

"Dir", geçerli dizinin altındaki dosyaları ve klasörleri listeleyen bir komuttur.

3. Cd

"Cd", dizin geçişleri için kullanılan bir komuttur.

4. Date

"Tarih", sistemin tarih bilgilerini görüntülemek ve değiştirmek için kullanılan bir komuttur.

5. Echo

"Echo", ekrana yazdırmak için kullanılan bir komuttur.

6. Hostname

"Hostname", sistemin ana bilgisayar adı bilgilerini görmek için kullanılan bir komuttur.

7. Time

"Time", sistem saatinin gösterilmesi için kullanılan bir komuttur.

Ağ Komutları

1. "Ipconfig" Komutu

"ipconfig", sistemdeki ağ arayüzleri hakkındaki bilgileri komut satırı aracılığıyla görüntülemeye izin veren bir komuttur.

2. "Netstat" Komutu

Mevcut ağ bağlantılarını ve durumlarını komut satırı üzerinden görüntülemek mümkündür.

Komutta uygulanan parametrelerin açıklamaları aşağıdaki gibidir:

"-A" parametresi: Tüm bağlantıları ve dinleme bağlantı noktalarını görüntüler.

"-N" parametresi: Adresleri ve port numaralarını sayısal biçimde görüntüler.

"-O" parametresi: Her bağlantıyla ilişkili sahip olunan işlem kimliğini görüntüler.

3. "Nslookup" Komutu

Windows işletim sisteminde kullanılan ve bir alan adının DNS bilgilerini sorgulamak için kullanılan bir komuttur. Bu komut, belirtilen bir alan adının IP adresini çözümlmek, DNS sunucularını belirlemek veya ters DNS sorguları yapmak gibi çeşitli DNS sorgularını gerçekleştirmek için kullanılır

4. "Ping" Komutu

Aynı ağ içindeki iki farklı cihazın ağ iletişimini test etmek gerekebilir. Komut satırında "ping" komutuyla hedefe erişilip erişilmediğini bulmak mümkündür. Ağ paketleri hedefe gönderilir ve "ping" komutuyla yanıt beklenir. Bu sayede hedef adres ile ağ iletişimi olup olmadığı test edilebilir.

Not: Bir güvenlik önlemi olarak, hedef sistem, saldırganların ağ ve ana bilgisayar keşfi yapmasını önlemek için "ping" komutuna yanıt vermeyecek şekilde yapılandırılabilir.

Not: "-n" parametresi: Gönderilmesi gereken yankı isteklerinin sayısı.

5. "Systeminfo" Komutu

"systeminfo", sistem hakkında ayrıntılı bilgi sağlayan bir komuttur.

Dosya İşlemleri Komutları

1. "Type" Komutu

"type", dosya içeriğini ekrana yazdırmak için kullanılan bir komuttur.

2. "Copy" Komutu

"copy", dosya kopyalama işlemlerinde kullanılan bir komuttur. "copy" komutundaki ilk parametre kopyalanacak dosyanın yolu, ikinci parametre ise hedef yoludur.

3. "Mkdir" Komutu

"Mkdir", yeni bir dizin oluşturmak için kullanılan bir komuttur.

4. "Rename" Komutu

"rename", dosyaları yeniden adlandırma komutudur.

5. "Move" Komutu

"Move", dosyaları taşımak için kullanılan bir komuttur.

6. "Tree" Komutu

"Tree", iç içe geçmiş dizinleri tek bir komutla listelemeye izin veren bir komuttur.

7. "Rmdir" Komutu

"Rmdir", dizinleri silmek için kullanılan bir komuttur.

Microsoft Windows Komutları

SS64 Komut Referansı

Windows Users and Groups

Windows'ta kullanıcılar ve gruplar, sistem ayrıcalıkları ve görevlerinde farklılık gösterebilir. Güvenlik açısından, saldırganlar en yetkili kullanıcıyı hedefler. Windows'u hedef alan saldırganlar, komut gönderdiklerinde kullanıcı ayrıcalıklarını bilmek isterler çünkü düşük bir kullanıcı profili sınırlı işlemleri içerebilir. Savunma tarafında, analistlerin görevi, kullanıcı etkinliklerini izlemek ve şüpheli durumları kısa sürede tespit etmektir.

"Whoami" Komutu

"Whoami", sisteme hangi kullanıcı hesabının eriştiğini gösteren komuttur.

User Management Commands

"Net", kullanıcıları ve grupları yönetmek için verilen komuttur. "Net" komutundan sonraki "kullanıcı" veya "grup" parametreleri, kullanıcılar veya gruplar üzerinde bir işlemin yürütüleceğini gösterir.

1. "net user" Komutu

"Net user", sistem içindeki kullanıcı adlarını görüntüleyen komuttur.

2. "net accounts" Komutu

"net accounts" komutu, kullanıcıların sistemdeki şifre kullanımı ve oturum açma kısıtlamalarıyla ilgili yapılandırmaları görmelerini sağlar.

3. "net localgroup" Komutu

"Net localgroup", sistemdeki gruplarla ilgili işlemleri gerçekleştirmemizi sağlayan komuttur. Parametrelerle kullanılırsa gruplar üzerinde farklı işlemler yürütülebilir. Parametreler olmadan kullanıldığında, yalnızca sistemdeki grupların listesini görüntüler.

User and Group Management via Graphical User Interface (GUI)

Windows'ta kullanıcı ve grup yönetimi çoğunlukla Grafiksel Kullanıcı Arayüzü (GUI) ile yapılabilmektedir. Bu GUI üzerinden "Yerel Kullanıcılar ve Gruplar" uygulamasını

kullanarak sistemdeki kullanıcıları ve grupları yönetebiliriz. Uygulamaya "Windows + R" tuş kombinasyonu ile "Run" uygulamasını açarak "lusrmgr.msc" yazarak erişebiliriz.

Uygulama açıldığında, sol gezinme panelinde "Kullanıcılar"ı seçerek sistemdeki kullanıcıları görüntüleyebilir ve yeni kullanıcılar ekleyebiliriz. Aynı şekilde, "Gruplar" sekmesi altında grupları yönetebilir ve yeni gruplar oluşturabiliriz.

Bu uygulamada her bir kullanıcı ve grup için detaylı bilgiye çift tıklayarak ulaşabiliriz.

Permissions Management on Windows

İzin yönetimi, genel işletim sistemi güvenliğini sağlamak için en önemli konulardan biridir. Sistemin izin yönetimi dikkatli bir şekilde yapılandırılmalıdır. Her sistemin kendi izin yönetim yapılandırması vardır. Windows'un kendi izin yönetimi özellikleri de vardır.

File and Folder Permissions

Her kullanıcının dosyalara/klasörlere yetkisiz erişimi önlemek için kendi profili ve izinleri vardır. Normalde, her dosya/klasör izinlerini Windows ortamındaki üst klasörden alır. Bu hiyerarşi sabit sürücünün kök dizinine kadar devam eder. Bir kullanıcının bir dosya üzerinde çalışma yeteneği, verilen izinler tarafından yönetilir.

Viewing File permissions

Dosya izinleri, Grafiksel Kullanıcı Arayüzü (GUI) kullanılarak kolayca yapılandırılabilir. Örneğin, "file.txt" adlı bir dosyanın sahibi "sefa123" kullanıcısı olsun. Dosyaya sağ tıklayarak "özellikler" penceresini açın ve "güvenlik" sekmesine gidin. Bu pencerede, kullanıcıların ve grupların listesini göreceksiniz ve seçilen kullanıcı/grup için belirli izinleri gösterir. Eğer onay işareti gri renkteyse, dosya izinleri başka bir klasörden devralınmış demektir. İzinler manuel olarak değiştirilirse, onay işareti siyah renkte olacaktır.

Permissions Types

Dosya izinlerini yönetirken 6 farklı izin türü vardır: Tam Kontrol, Değiştirme, Okuma ve Yürütme, Okuma, Yazma ve Özel izinler.

Changing file permissions

Dosya izinlerini değiştirmek, dosyanın sahibi olmayı gerektirir. Örneğin, "file.txt" dosyasının sahibini görmek için dosyaya sağ tıklayıp "özellikler"e gidip "güvenlik" sekmesinde "gelişmiş"e tıklayabiliriz. Dosyanın sahibi "sefa123" kullanıcısı

olduğunda, bu kullanıcı olarak giriş yaptığımızda izinleri değiştirebiliriz. Örneğin, dosyanın içeriğini okuma yeteneklerini kısıtlamak için "reddet" seçeneğini kullanabiliriz.

Bu tür izin değişiklikleri yapıldığında, dosyaya erişim izni olmayan bir kullanıcı, dosyayı açmaya çalıştığında hata alır. Aynı şekilde, farklı bir kullanıcı hesabının birbirine ait olmayan bir dizine erişmeye çalıştığında da hata alır. Örneğin, "user2" hesabıyla "user1" dizinine erişmeye çalıştığında hata alır ve bu dizine erişim için yönetici kimlik bilgileri gerekir.

Dosya izinleri yönetimi, güvenlik açısından kritik öneme sahiptir. Saldırganlar, yetkili kullanıcı hesaplarına sızarak hedef dosya veya klasörlere erişmeye çalışabilirler. Bu nedenle, SOC analistleri bu tür faaliyetleri izlemeli ve ihlalleri zamanında tespit etmelidir.

User Account Control (UAC)

Kullanıcı Hesabı Kontrolü (UAC), Windows işletim sistemlerinde yetkisiz erişimi önlemek için bir güvenlik özelliğidir. Belirli değişiklikler ve işlemler, yönetici izni olmadan yapılamaz. Bu özellik, sistem güvenliğini artırsa da, zaman zaman saldırganlar tarafından atlanabilir ve ihlal edilebilir. "Kullanıcı Hesabı Kontrolü" yapılandırmaları, sistemin güvenlik güçlendirmesi yapılırken dikkatlice ve doğru bir şekilde uygulanmalıdır.

1. Her zaman bildir (Always notify):

- Uygulamalar ve kullanıcılar, yönetici izinleri gerektiren değişiklikler yapmadan önce bilgilendirilir. En güvenli ve en dikkat çekici seviye.

2. Yalnızca uygulamalar bilgisayarım üzerinde değişiklik yapmaya çalıştığında bildir (varsayılan) (Notify me only when apps try to make changes to my computer - default):

- UAC yalnızca programlar yönetici izinleri gerektiren değişiklikler yapmaya çalıştığında sizi bilgilendirir. İlk seviyeden daha az güvenli, çünkü kötü amaçlı programlar, kullanıcı tarafından yapılan eylemleri taklit etmek için oluşturulabilir.

3. Yalnızca uygulamalar bilgisayarım üzerinde değişiklik yapmaya çalıştığında bildir (Notify me only when apps try to make changes to my computer):

- Bu seviye, bir UAC isteği gösterildiğinde masaüstünün soluk olmaması dışında önceki seviye ile aynıdır. Daha az güvenli, çünkü UAC istemine müdahale eden

kötü amaçlı programlar için daha uygun bir ortam sağlar.

4. Hiç bildirimde bulunma (Never notify):

- UAC kapatılır ve yetkisiz sistem değişikliklerine karşı herhangi bir koruma sağlanmaz. Güvenlik yazılımınız yoksa, cihazınız açısından risklidir. UAC kapalıyken, kötü amaçlı yazılımların Windows'a bulaşması ve kontrolü ele geçirmesi daha kolaydır.

Windows Process Management

Process Nedir?

Bir süreç, aktif bir programın yürütüldüğü birimdir. İşlemler, işletim sisteminde çalışan komutların veya programların birimleridir. Bellek analizi genellikle süreçlerin analizi anlamına gelir. Her işlemin kendi kimlik numarası olan "İşlem Kimliği" (PID) vardır ve bu bilgi her işlemde kaydedilir.

Process Tree

Bir programın çalıştırılması bir süreçtir ve bu süreçten başka süreçler türetebilir. İki süreç arasında ebeveyn-çocuk ilişkisi bulunur.

- **Süreç:** Aktif bir programın yürütüldüğü birim.
- **Ana Süreç:** Bir veya daha fazla alt süreç oluşturmuş bir süreç.
- **Alt Süreç:** Başka bir süreç tarafından oluşturulan bir süreç. Her çocuk süreci yalnızca bir ebeveyn sürecine aittir.

Bu hiyerarşik temsil "İşlem Ağacı" olarak adlandırılır. İşlem Ağacını görüntülemek için "Süreç Hacker" gibi araçlar kullanılabilir. "Süreç Hacker," Windows'ta çalışan işlemleri gerçek zamanlı olarak izleyen ücretsiz ve açık kaynaklı bir araçtır.

İşlem Hacker: [Process Hacker](#)

Windows Legitimate Processes

Windows'ta farklı görevlere sahip birçok yerel işlem bulunmaktadır. Güvenlik açısından önemli olan ve içerdikleri kullanıcı ve sistem bilgilerini görmemiz gereken bazı süreçlere odaklanalım.

wininit.exe

"Wininit.exe," "Windows Initialization Process" olarak bilinir. Bu işlem, Hizmet Kontrol Yöneticisi (services.exe), Yerel Güvenlik Otoritesi süreci (lsass.exe), ve Yerel Oturum

Yöneticisi (lsn.exe) gibi önemli süreçleri başlatma sorumluluğundadır.

"C:\Windows\System32" klasöründe bulunur, sistem önyüklemesi sırasında oluşturulur ve en yetkili kullanıcı olan NT AUTHORITY\SYSTEM ayrıcalıklarıyla çalışır.

services.exe

"Services.exe," hizmetleri başlatma ve durdurma işleminden sorumlu olan bir süreçtir.

"svchost.exe," "dllhost.exe," "taskhost.exe," ve "spoolsv.exe" gibi alt süreçleri yönetir.

"C:\Windows\System32" klasöründe bulunur, NT AUTHORITY\SYSTEM ayrıcalıklarıyla çalışır. Normal koşullarda işlem ağacında yalnızca bir "services.exe" işlemi bulunmalıdır.

svchost.exe

"Svchost.exe," dinamik bağlantı kitaplıklarından çalışan hizmetler için genel bir ana

bilgisayar işlemidir. "Services.exe"nin alt sürecidir ve "C:\Windows\System32"

klasöründe bulunur. NT AUTHORITY\NETWORK SERVICE veya NT AUTHORITY\SYSTEM ayrıcalıklarıyla çalışır.

lsass.exe

"Lsass.exe" (Local Security Authority Subsystem Service), kullanıcıların oturum açma sırasında şifre onayı gibi kritik güvenlik işlemlerinden sorumlu olan bir süreçtir.

"C:\Windows\System32" klasöründe bulunur ve NT AUTHORITY\SYSTEM ayrıcalıklarıyla çalışır. Saldırganlar, bu süreç üzerinden kullanıcı şifrelerine erişmeye çalışabilir.

winlogon.exe

"Winlogon.exe," kullanıcı oturum açma ve çıkış işlemlerini yöneten bir süreçtir.

"C:\Windows\System32" klasöründe bulunur ve NT AUTHORITY\SYSTEM ayrıcalıklarıyla çalışır.

explorer.exe

"Explorer.exe," grafiksel kullanıcı arayüzünü sağlayan ana süreçtir. "C:\Windows\" klasöründe bulunur ve oturum açmış kullanıcının ayrıcalıklarıyla çalışır.

Task Manager

"Görev Yöneticisi," Windows işletim sistemindeki işlemleri görüntülemeyi ve yönetmeyi sağlayan bir uygulamadır. Süreçleri grafiksel bir kullanıcı arayüzü (GUI) ile görüntüleyebilir ve sonlandırabilirsiniz.

Process Operations Commands

Windows işlemleri genellikle GUI üzerinden yönetilir, ancak bazı durumlarda komut satırı kullanılabilir. İşlemleri listelemek için "Tasklist" komutu, işlemleri sonlandırmak için ise "Taskkill" komutu kullanılır.

Tasklist command:

```
tasklist
```

Taskkill command:

```
taskkill /PID <PID_Value>
```

Windows Services

Hizmetler Nedir?

Hizmetler, arka planda çalışan programlardır ve kullanıcı etkileşimi olmadan çalışabilirler. Windows'ta çalışan hizmetler güvenlik açısından önemlidir. Saldırganlar, hizmetleri kullanarak sistem bilgisi toplayabilir veya sızma girişimlerinde bulunabilirler. Hizmetler, olay günlükleri aracılığıyla izlenmeli ve şüpheli etkinlikler tespit edilmelidir.

Managing Windows Services with a Graphical User Interface (GUI)

Windows hizmetlerini grafik kullanıcı arayüzü (GUI) üzerinden görüntülemek ve yönetmek mümkündür. "services.msc" komutu ile "Hizmetler" uygulamasını açarak hizmetler hakkında detaylı bilgiler alabilir ve yönetebilirsiniz.

Managing Windows Services with Command Line

Windows hizmetlerini komut satırından yönetmek için "sc" komutunu kullanabilirsiniz.

Display all running services:

```
sc query
```

View all services:

```
sc query type=service state=all
```

Get information about the service

Hizmet bilgilerini tek bir pencerede görüntülemek karmaşık olabilir, bu nedenle yalnızca belirli bir hizmet hakkında bilgi almak isteyebiliriz. Örneğin, "Windows Güncelleme Hizmeti" için bilgi almak için aşağıdaki komutu kullanabiliriz:

```
sc query wuauerv
```

Starting and Stopping the Service

Hizmetleri komut satırı üzerinden başlatıp durdurabiliriz. Örneğin, "Windows Güncelleme Hizmeti"ni başlatmak için aşağıdaki komutu kullanabiliriz:

```
sc start wuauerv  
sc stop wuauerv
```

Task Scheduler Windows

Zamanlanmış görev nedir?

Zamanlanmış görev, belirli işlemlerin sistemde belirli zaman aralıklarında veya belirli zamanlarda yürütülmesidir. Saldırganlar, erişimlerini kalıcı hale getirmek için zamanlanmış görevleri kullanabilirler.

Managing Scheduled Tasks with the GUI

Zamanlanmış görevleri GUI kullanarak görüntülemek ve yönetmek mümkündür. "taskschd.msc" komutu ile "Görev Zamanlayıcı" programını açarak zamanlanmış görevleri görebiliriz. Yeni bir zamanlanmış görev eklemek için "Görev Oluştur" düğmesine tıklayabiliriz. Oluşturduğumuz görevi çalıştırmak için sağ tıklayıp "Çalış" seçeneğini kullanabiliriz.

Managing Scheduled Tasks with Command Line

Zamanlanmış görevleri komut satırı üzerinden yönetmek için "schtasks" komutu kullanılır.

View scheduled tasks

"Schtasks" komutu parametre olmadan kullanıldığında, tüm zamanlanmış görevleri gösterir. Örneğin:

```
schtasks
```

Getting information about the scheduled task

"Schtasks" komutu parametrelerle kullanıldığında belirli zamanlanmış görevler hakkında bilgi alabiliriz. Örneğin:

```
schtasks /Query /TN TrainingTask
```

Enable the Scheduled Task

Devre dışı bırakılmış zamanlanmış görevler "schtasks" komutuyla etkinleştirilebilir. Örneğin:

```
schtasks /Change /ENABLE /TN TrainingTask
```

Running the scheduled task via command line

Zamanlanmış görevler "schtasks" komutuyla çalıştırılabilir. Örneğin:

```
schtasks /Run /TN TrainingTask
```

Terminating the scheduled task via the command line

Planlanmış görevler "schtasks" komutuyla sonlandırılabilir. Örneğin:

```
schtasks /End /TN TrainingTask
```

Deleting scheduled task via command line

Zamanlanmış görevler "schtasks" komutuyla silinebilir. Örneğin:

```
schtasks /Delete /TN TrainingTask
```

Windows Registry

Windows Kayıt Defteri Nedir?

Windows Kayıt Defteri, sistemde yüklü programlarla ilgili işletim sistemini ve sistem yapılandırmalarını içeren hiyerarşik bir veritabanıdır. Program ve donanım bilgilerini bu veritabanında saklar. Örneğin, bir program Windows'ta yüklendiğinde, program lisansının son kullanma tarihini Windows Kayıt Defteri'nde tutabilir.

Windows Kayıt Defteri, saldırganlar için önemli bir hedeftir. İçerdiği bilgiler, sistemdeki programlar ve yapılandırmalar hakkında detaylı bilgiler içerir. Saldırganlar, bu bilgileri kullanarak sistemdeki zayıf noktaları belirleyebilir ve daha fazla ayrıcalığa sahip hesapları ele geçirme amacıyla saldırılarını planlayabilirler.

Kayıt Defteri'ne Erişim

Kayıt defteri dosyalarına metin tabanlı olmadıkları için özel bir yazılım kullanmak gerekir. "Kayıt Defteri Düzenleyicisi" gibi araçlar, kayıt defteriyle ilgili işlemleri gerçekleştirmek için kullanılır.

Kayıt Defteri Yapısı

Windows Kayıt Defteri girdileri "%SystemRoot%\System32\Config" konumunda bulunur.

Kayıt defteri iki temel unsur içerir: "anahtarlar" ve "değerler". Kayıt defteri anahtarları, kapsayıcı nesnelerdir, değerler ise dosyalara benzer, kapsayıcı olmayan nesnelerdir. Anahtarlar, değerler ve alt anahtarlar içerebilir.

Örneğin, HKEY_LOCAL_MACHINE\Software\Microsoft\Windows, HKEY_LOCAL_MACHINE kök anahtarının "Software" alt anahtarının "Microsoft" alt anahtarının "Windows" alt anahtarını ifade eder.

Yedi ön tanımlı kök anahtar vardır:

- HKEY_LOCAL_MACHINE veya HKLM

- HKEY_CURRENT_CONFIG veya HKCC
- HKEY_CLASSES_ROOT veya HKCR
- HKEY_CURRENT_USER veya HKCU
- HKEY_USERS veya HKU
- HKEY_PERFORMANCE_DATA (yalnızca Windows NT'de)
- HKEY_DYN_DATA (yalnızca Windows 9x'te)

HKEY_LOCAL_MACHINE veya HKLM

Bilgisayara özel donanım ve yazılım yapılandırmalarını içerir. Önemli alt anahtarlar arasında DONANIM, SAM, GÜVENLİK, YAZILIM ve SİSEM bulunur.

HKEY_CURRENT_CONFIG veya HKCC

Sistemin çalışma sırasındaki donanım yapılandırmalarını içerir.

HKEY_CLASSES_ROOT veya HKCR

Yazılım ayarları, kısayollar ve kullanıcı arayüzü ile ilgili bilgileri içerir.

HKEY_USERS veya HKU

Sisteme kayıtlı tüm kullanıcıların yapılandırmalarını içerir.

Reg Uzantılı Dosyalar

"Reg" uzantılı dosyalar, kayıt defteri işlemlerini dışa aktarırken kullanılan dosya biçimidir. Bu metin tabanlı dosya yapısı aşağıdaki gibidir:

```
[HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Control\\ComputerName\\ComputerName]
"ComputerName"="BilgisayarAdi"
```

Örneğin, "Bilgisayar Adı"nı kayıt defterinden "reg" uzantılı dosya olarak dışa aktaralım ve ardından bu dosyayı açarak içeriğini not defteri ile inceleyelim. Bu işlemi gerçekleştirdiğimizde, kaydedilen dosyadaki bilgisayar adını başarıyla okuyabiliriz.

Komut Satırında Kayıt Defteri İşlemleri

Kayıt defteri düzenleyici programındaki birçok işlem, komut satırında da gerçekleştirilebilir. Kayıt defteri anahtarlarını ve değerlerini okuma, yeni değerler ekleme, anahtarları dışa aktarma ve içe aktarma gibi işlemler komut satırı kullanılarak yapılabilir. Örneğin, önceki örnekte dosyaya kaydettiğimiz bilgisayar adını komut satırı kullanarak kayıt defterinden okuyalım:

```
reg query HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Control\\ComputerName\\ComputerName
```

Windows Firewall

Yukarıdaki ekran görüntüsünde görüldüğü gibi, bu komut ile bilgisayar adı başarıyla kayıt defterinden okundu. Komut satırında kayıt defteri üzerinde gerçekleştirilebilecek diğer işlemlerle ilgili daha fazla bilgiye [bu bağlantıdan](#) ulaşabilirsiniz.

Windows Güvenlik Duvarı nedir?

Windows Güvenlik Duvarı, ağ trafiğini belirli kurallar çerçevesinde kontrol etme yeteneğine sahip bir güvenlik aracıdır. Gelen ve giden ağ paketlerini denetler, bu sayede oluşturulan kurallara uygun olanları izin verir veya engeller. Kötü niyetli bağlantıları engelleme konusunda etkilidir ve doğrulanmış güvenli hedeflere izin verilen bağlantıları ekleyerek güvenliğini artırabilir.

Windows Güvenlik Duvarı, sistem güvenliği için temel bir savunma yöntemidir. Oluşturulan kurallar sayesinde dışarıdan gelen tehditlere karşı etkili bir koruma sağlar. Saldırganlar genellikle güvenlik duvarını atlamaya çalışır veya devre dışı bırakmaya odaklanır. Ancak, bu yöntemleri tespit edebilmek adına güvenlik duvarı kurallarını düzenli olarak izlemek ve değişiklikleri kontrol etmek önemlidir. Güvenlik duvarının devre dışı bırakılmadığından emin olmak da kritiktir.

Güvenlik Duvarı Kuralı nedir?

Güvenlik Duvarı Kuralı: Windows Defender Güvenlik Duvarı'nda bir ağ paketinin güvenlik duvarından geçmesine izin verilip verilmediğini belirlemek için kullanılan bir dizi koşul içeren bir kural.

(Kaynak: microsoft.com)

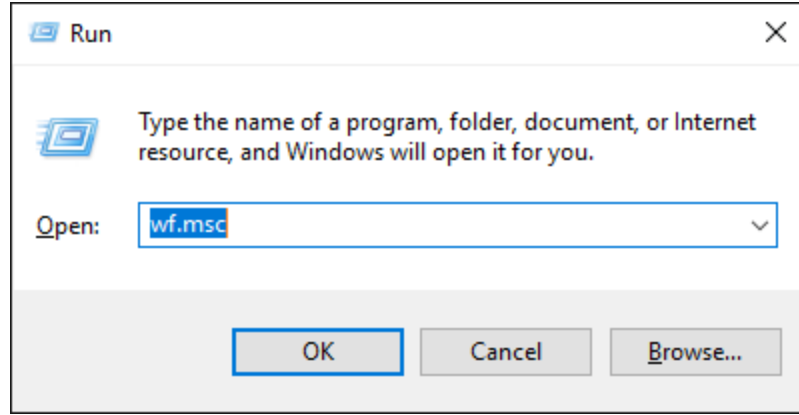
Gelen Ve Giden Kurallar

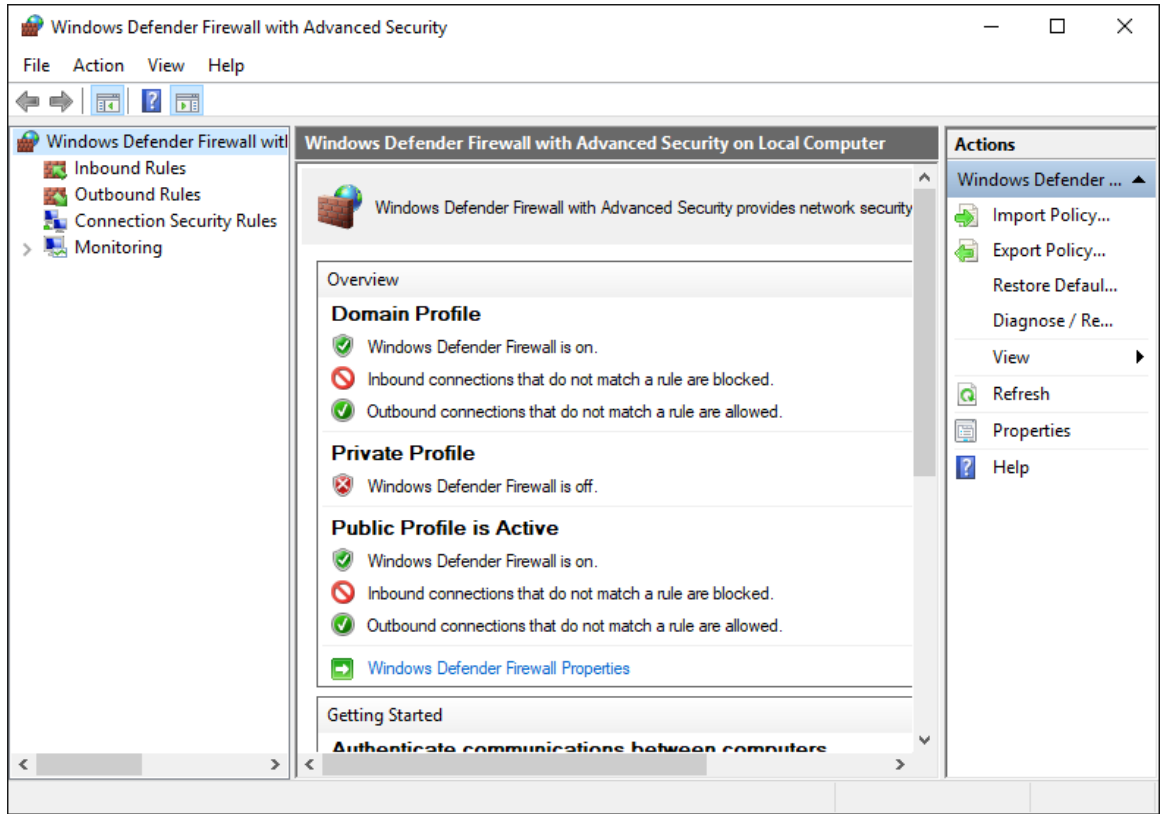
Gelen kuralı, kuralların parametrelerine göre bir ağdan yerel bir bilgisayara geçen trafiği filtreler. Giden kurallar için yerel bilgisayarlardan ağa gönderilen trafik filtreleme kurallarına göre filtrelenebilir.

(Source: nstec.com)

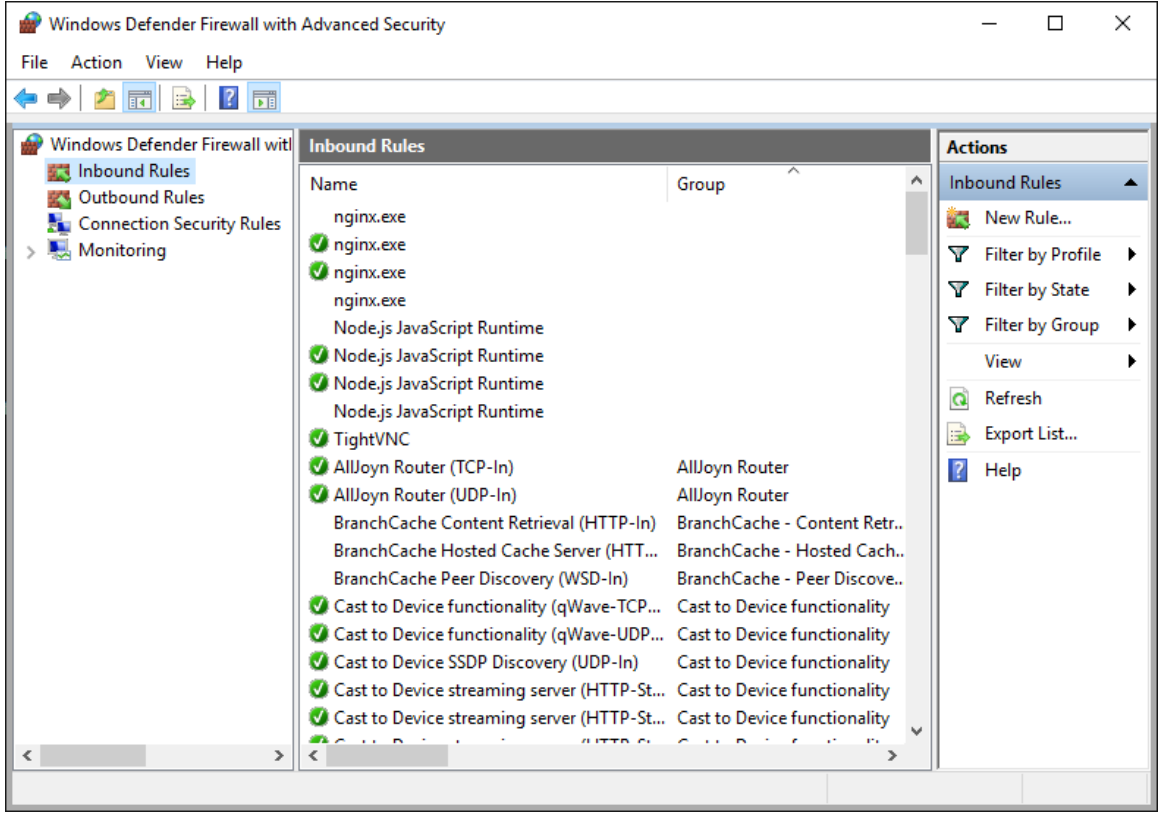
Grafiksel Kullanıcı Arayüzü (GUI) ile Güvenlik Duvarı Kuralları Yönetimi

Windows güvenlik duvarı uygulaması, Windows güvenlik duvarı kurallarını yönetmek için kullanılabilir. Grafik kullanıcı arayüzü üzerinden kural yönetimi rahatlıkla yapılabilir. Örneğin, Windows güvenlik duvarı uygulamasını açalım:

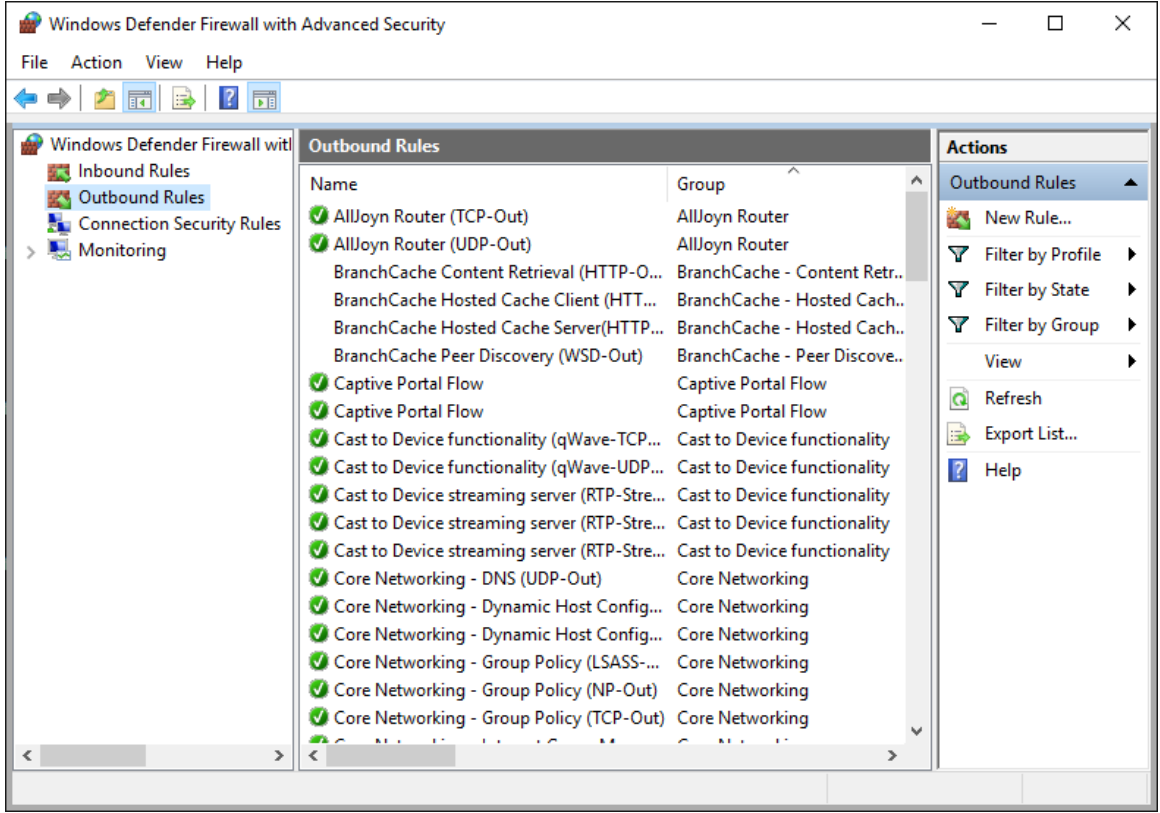




Windows güvenlik duvarı ilk kez açıldığında, yukarıdakine benzer bir pencere belirir. Bu pencerede sol menüden gelen ve giden kuralları ayrı olarak görebiliriz:



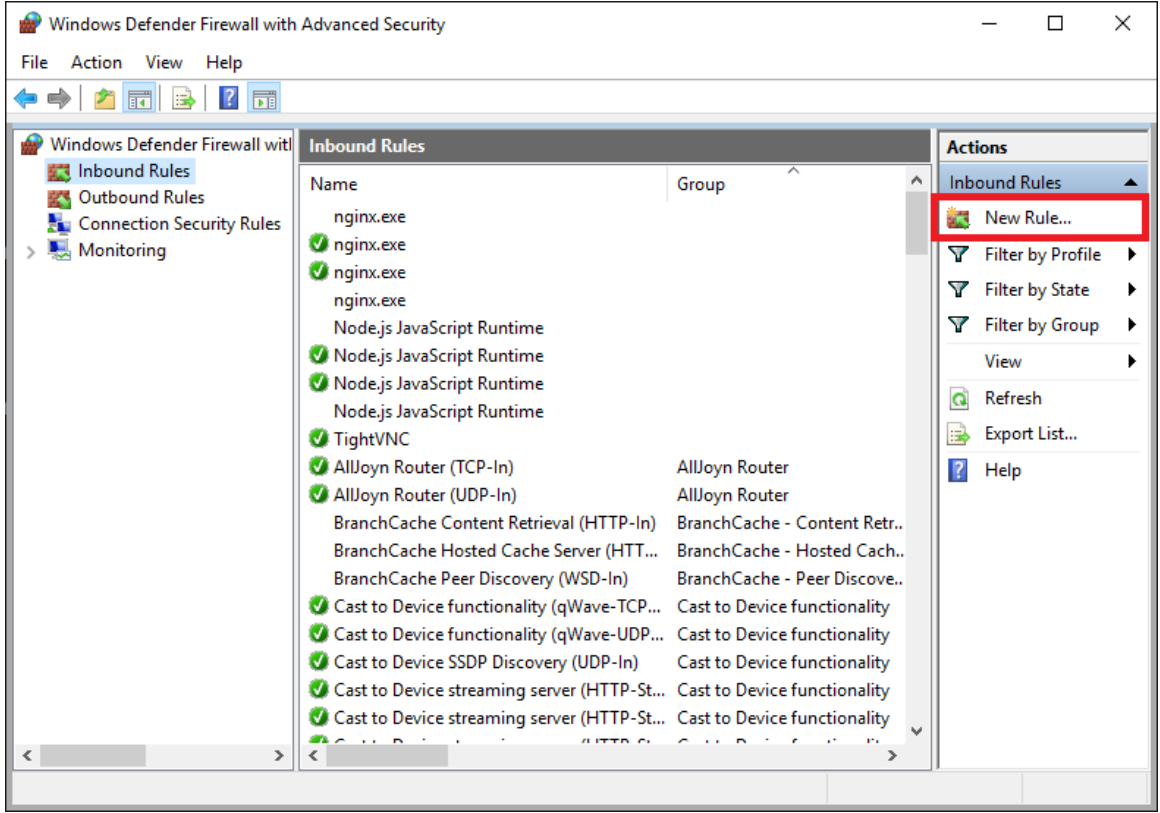
Yukarıdaki ekran görüntüsünde görüldüğü gibi, gelen trafiği yönetmek için yazılan kurallarla ilgili ayrıntılar başarıyla görüntülendi.



Yukarıdaki ekran görüntüsünde görüldüğü gibi, giden trafiği yönetmek için yazılan kurallarla ilgili ayrıntılar başarıyla görüntülenmiştir.

Yeni bir güvenlik duvarı kuralı oluşturma

Windows Güvenlik Duvarı uygulamasında yeni bir kural oluşturmak oldukça kolaydır. Bunun için uygulamanın sağ kısmındaki "New Rule" seçeneği kullanılır. Örneğin, gelen trafik kuralı olarak "TCP 4444" bağlantı noktasındaki tüm gelen paketleri engelleyen bir kural ekleyelim. Her şeyden önce, soldaki menüden "Inbound Rules" bölümüne gitmeli, ardından "New Rule" düğmesiyle adımları sırayla uygulamalısınız:



"New Rule" seçeneğine tıkladıktan sonra sırasıyla gerekli yapılandırma yapılır.

New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

☐ **Program**
Rule that controls connections for a program.

☒ **Port**
Rule that controls connections for a TCP or UDP port.

☐ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

☐ **Custom**
Custom rule.

< Back Next > Cancel

Bu bölümde kural türü "Port" olarak tanımlanmalıdır.

New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Protocol and Ports**
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

☒ TCP
☐ UDP


Does this rule apply to all local ports or specific local ports?

☐ All local ports
☒ Specific local ports:

Example: 80, 443, 5000-5010

< Back Next > Cancel

Bu bölümde, "TCP" seçeneğini işaretleyelim ve bağlantı noktası bilgilerini "4444" olarak yazalım.

 New Inbound Rule Wizard ✕

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

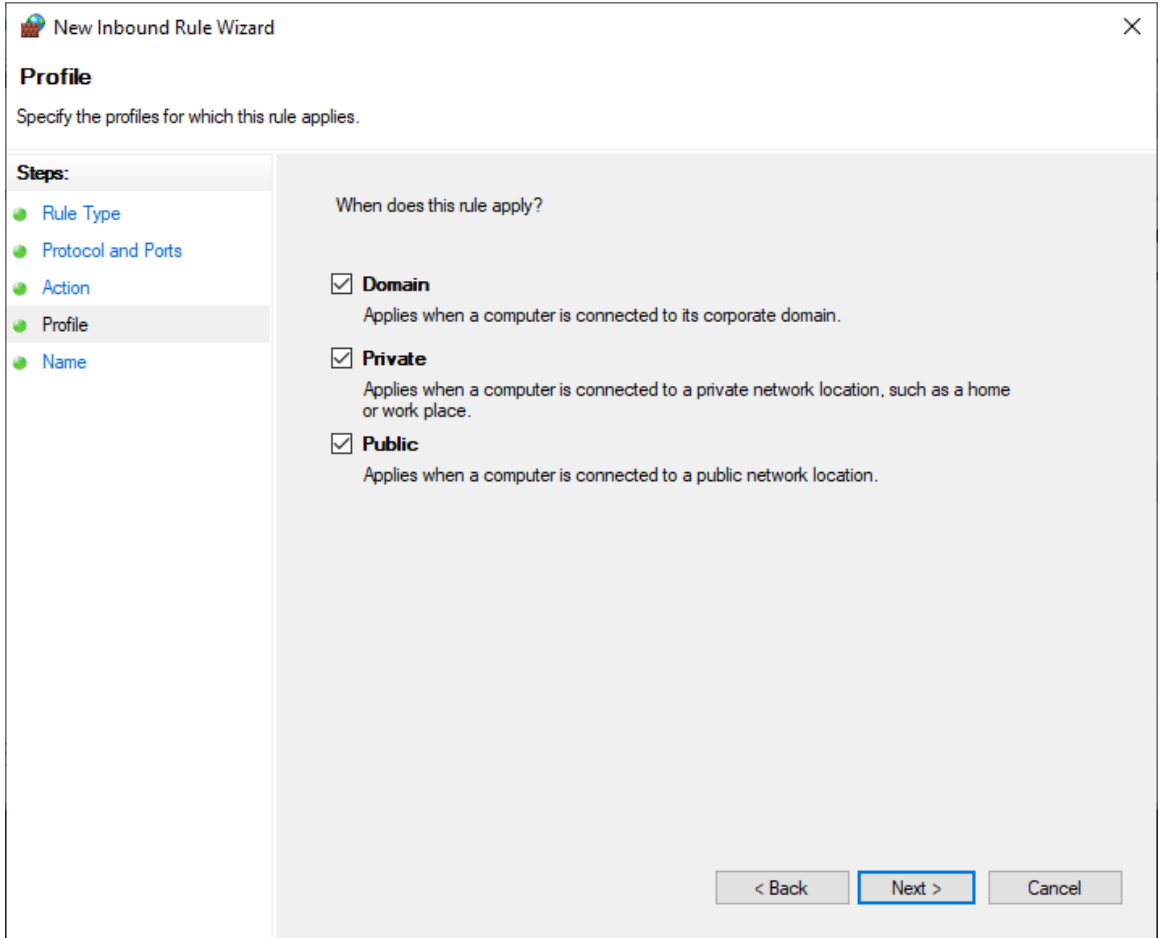
☐ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
[Customize...](#)

☒ **Block the connection**

[< Back](#) [Next >](#) [Cancel](#)

Bu bölüm "Bağlantayı engelle" seçeneğini seçerek devam eder.



Bu bölümde kuralın uygulanacağı profilleri doğrulamamız gerekiyor. Tüm seçilenlerle devam edelim.

New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name**

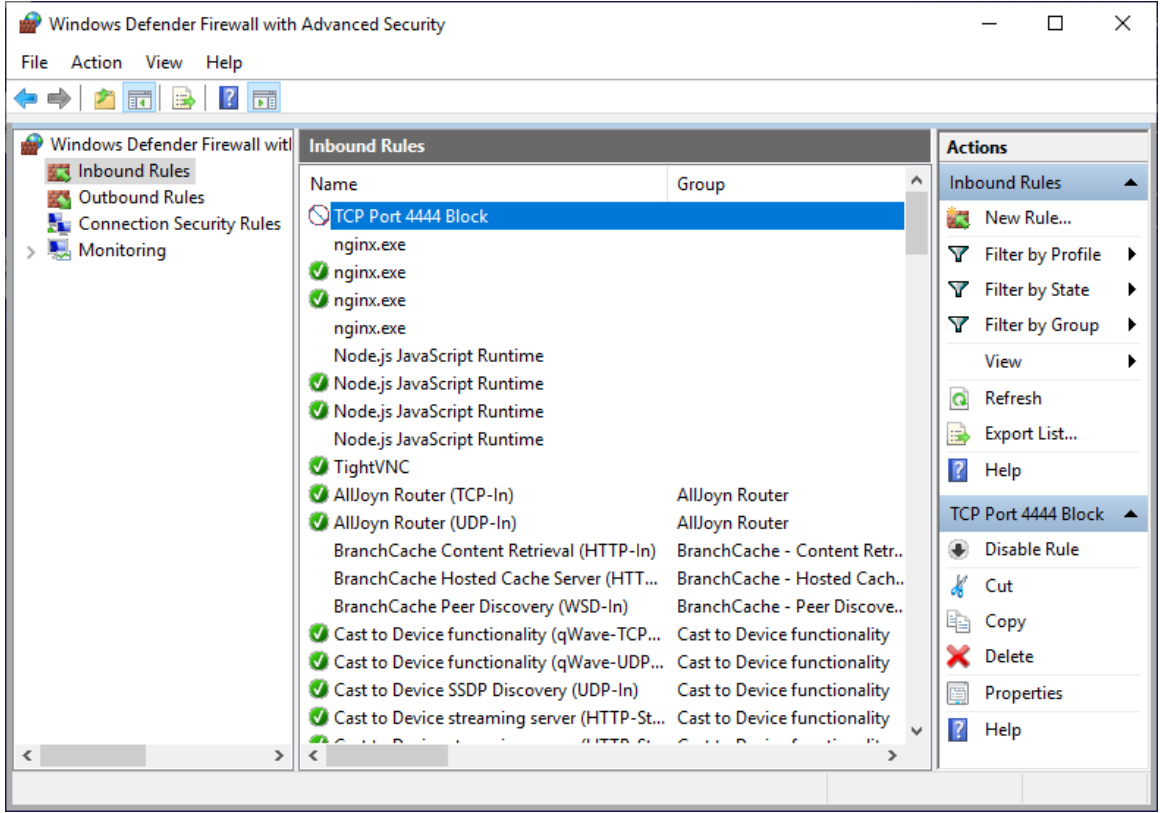
Name:

TCP Port 4444 Block

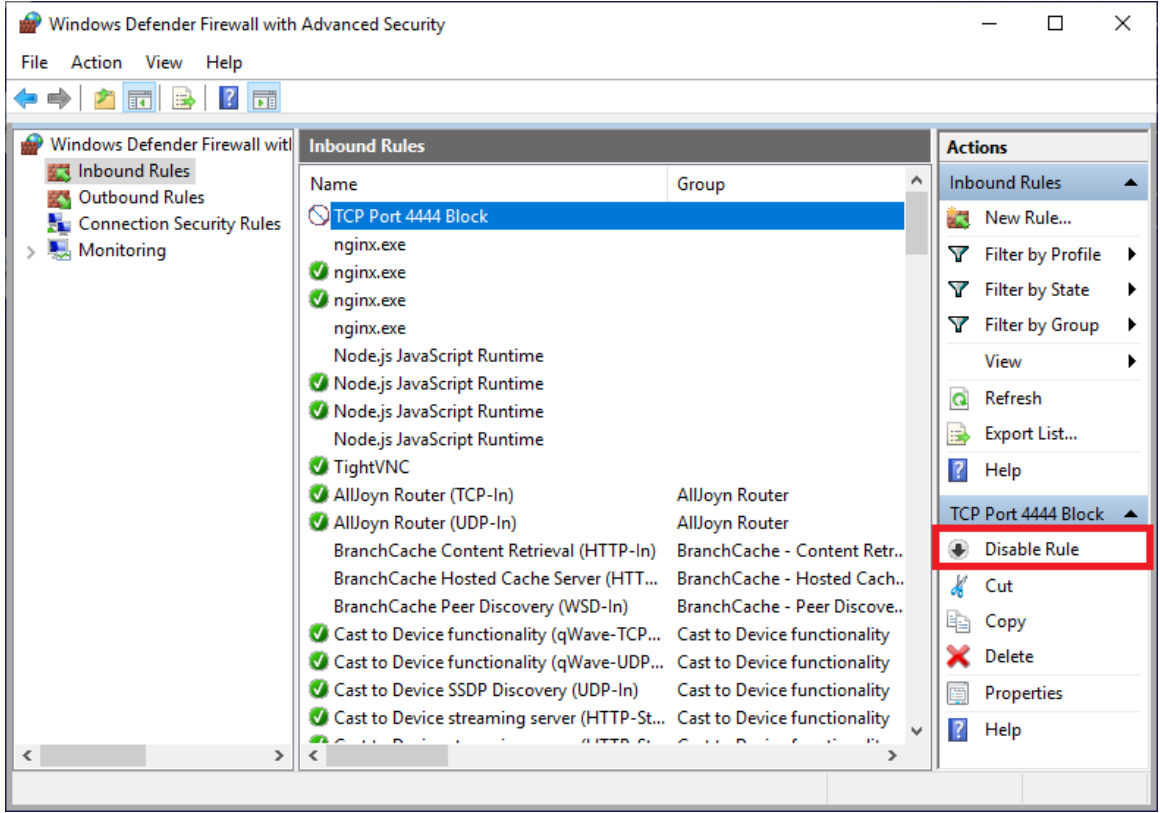
Description (optional):

< Back Finish Cancel

Bu bölümde kuralın adı girilmeli, kuralı "TCP Port 4444 Block" olarak adlandırılmalı ve devam edelim.



Yukarıdaki ekran görüntüsünde görüldüğü gibi, güvenlik duvarı kuralı başarıyla eklendi. Kural oluşturulduğunda etkinleştirilir ve gerekirse uygulama penceresinin sağ alt bölümünden devre dışı bırakılabilir.



Komut Satırı ile Güvenlik Duvarı Kuralları Yönetimi

Windows güvenlik duvarı kurallarının yönetimi de komut satırı üzerinden yapılabilir. Bunun için "netsh" komutu kullanılır. Örneğin, tüm güvenlik duvarı kurallarını "netsh advfirewall firewall show rule name=all" komutuyla listeleyelim:

```
PS C:\Users\sefa123> netsh advfirewall firewall show rule name=all
```

Rule Name:	TCP Port 4444 Block
------------	---------------------

Enabled:	Yes
Direction:	In
Profiles:	Domain,Private,Public
Grouping:	
LocalIP:	Any
RemoteIP:	Any
Protocol:	TCP
LocalPort:	4444
RemotePort:	Any
Edge traversal:	No
Action:	Block

Rule Name:	Microsoft Edge (mDNS-In)
------------	--------------------------

Enabled:	Yes
Direction:	In
Profiles:	Domain,Private,Public
Grouping:	Microsoft Edge
LocalIP:	Any
RemoteIP:	Any
Protocol:	UDP
LocalPort:	5353
RemotePort:	Any
Edge traversal:	No
Action:	Allow

Güvenlik duvarı kuralının bilgilerini görüntüleme

Komut çıktıları uzun olduğunda çıktıyı sınırlamak için komut satırı üzerinden gerçekleştirilen işlemlerde daha kısa çıktılar üreten komutlar uygulanabilir.

Örneğin, bir önceki örnekte ekrandaki tüm kuralları yazdırmak yerine, sadece adı geçen kuralın bilgilerini görmek mümkündür. Bunun için uygulanacak komut şu şekildedir: “netsh advfirewall firewall show rule name=”TCP Port 4444 Block””

Bu komutu uygulayarak daha önce oluşturduğumuz Windows güvenlik duvarı kuralı hakkındaki bilgileri görelim:

```
PS C:\Users\sefa123> netsh advfirewall firewall show rule name="TCP Port 4444 Block"

Rule Name:                                TCP Port 4444 Block
-----
Enabled:                                    Yes
Direction:                                In
Profiles:                                  Domain,Private,Public
Grouping:
LocalIP:                                    Any
RemoteIP:                                  Any
Protocol:                                  TCP
LocalPort:                                 4444
RemotePort:                                Any
Edge traversal:                             No
Action:                                     Block
Ok.
```

Bir güvenlik duvarı kuralını silme

Güvenlik duvarı kuralını komut satırı üzerinden silmek mümkündür. Örneğin, "netsh advfirewall firewall delete rule name="TCP Port 4444 Block" komutuyla komut satırı aracılığıyla grafik arayüzden oluşturduğumuz kuralı silelim:

```
Ok.

PS C:\Users\sefa123> netsh advfirewall firewall delete rule name="TCP Port 4444 Block"

Deleted 1 rule(s).
Ok.
```

Yukarıdaki resimde görüldüğü gibi, güvenlik duvarı kuralı başarıyla silindi.

Not: Komut satırındaki güvenlik duvarı kuralını silerken, komut satırı yönetici haklarıyla çalıştırılmalıdır, aksi takdirde komut çalışmaz.

Komut satırı üzerinden güvenlik duvarı kurallarına birçok farklı değişiklik uygulanabilir. Örneğin, güvenlik duvarı kuralını devre dışı bırakın/etkinleştirin, yeni bir güvenlik duvarı kuralı ekleyin veya yalnızca gelen/giden güvenlik duvarı kurallarını listeleyin. Bu işlemler için komutta uygulanan parametrelerin değiştirilmesi gerekir. Aşağıdaki adres, "netsh" komutu ve kullanımı hakkında daha detaylı bilgi almak için kullanılabilir.

Netsh Command: <https://ss64.com/nt/netsh.html>