

FORTİGATE

Firewall

Policy & Objects



FortiGate cihazlarında Firewall Objects ve Policies, güvenlik duvarı yönetiminin temel yapı taşlarıdır. Bu kavramlar, ağ trafiğini kontrol etmek, yönetmek ve korumak için kullanılır. Aşağıda her iki kavramın ne olduğunu ve ne işe yaradığını detaylı bir şekilde açıklayalım:

1. Firewall Objects (Güvenlik Duvarı Nesneleri)

Firewall Objects, FortiGate cihazında belirli ağ varlıklarını tanımlayan ve yöneten öğelerdir. Bu nesneler, güvenlik duvarı politikalarının uygulanmasında kullanılan öğelerdir. Firewall objects, şu türleri içerebilir:

- **Address Objects (Adres Nesneleri):** IP adresleri veya IP adres bloklarını temsil eder. Örneğin, bir iç ağın IP aralığı veya belirli bir sunucunun IP adresi.
- **Service Objects (Hizmet Nesneleri):** Belirli bir ağ hizmetini veya protokolünü temsil eder. Örneğin, HTTP (port 80) veya HTTPS (port 443) gibi.
- **User Objects (Kullanıcı Nesneleri):** Kullanıcılar veya kullanıcı gruplarını tanımlar. Örneğin, Active Directory'den alınan kullanıcı bilgileri.
- **Schedule Objects (Zamanlama Nesneleri):** Güvenlik politikalarının hangi zaman dilimlerinde geçerli olacağını belirler. Belirli bir saatte veya günlerdeki trafik için kısıtlamalar koyulabilir.
- **Interface Objects (Arayüz Nesneleri):** Cihazın ağ arayüzlerini temsil eder. Örneğin, "wan" veya "lan" arayüzleri.
- **VPN Objects (VPN Nesneleri):** VPN bağlantılarını tanımlar, VPN trafiğini yönetmek için kullanılır.

Bu nesneler, güvenlik duvarı politikalarının daha kolay yönetilmesini sağlar ve politikaların daha esnek bir şekilde yapılandırılmasına olanak tanır.

2. Firewall Policies (Güvenlik Duvarı Politikaları)

Firewall Policies, güvenlik duvarında trafiğin nasıl yönetileceğini belirleyen kurallardır. Bu politikalar, ağın belirli bölümleri arasındaki veri trafiğini yönlendirir ve filtreler. FortiGate üzerinde güvenlik duvarı politikaları genellikle şu adımları içerir:

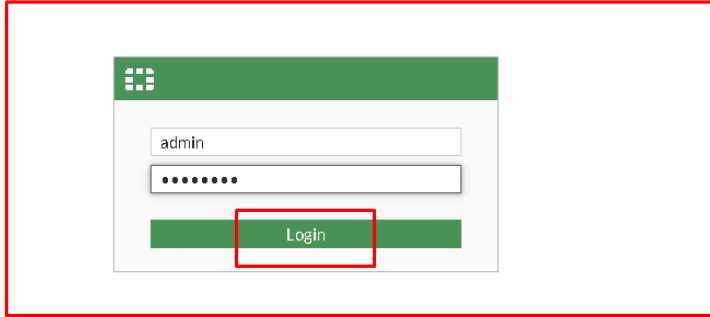
- **Source (Kaynak):** Trafiğin geldiği yer. Bu, bir IP adresi, bir kullanıcı grubu, bir ağ segmenti veya başka bir nesne olabilir.
- **Destination (Hedef):** Trafiğin hedef aldığı yer. Yine, bu da bir IP adresi, ağ veya başka bir nesne olabilir.
- **Service:** Trafiğin kullandığı hizmet veya protokol. Örneğin, HTTP, HTTPS, FTP gibi.
- **Action (Eylem):** Trafiğin nasıl işleneceği. Trafik ya allow (izin ver) ya da deny (engelle) olarak işlenebilir.
- **Log:** Trafiğin kaydını tutma. Belirli bir politika için trafik kaydının tutulup tutulmayacağını belirtir.
- **Schedule:** Trafiğin geçerli olduğu zaman dilimi. Belirli bir zaman diliminde geçerli olacak şekilde ayarlanabilir.
- **Security Profiles (Güvenlik Profilleri):** Antivirüs, web filtreleme, uygulama kontrolü gibi ek güvenlik özelliklerinin uygulanması.

Firewall Policies'in İşlevi ve Önemi

Firewall Policies, ağ trafiğinin güvenli bir şekilde yönlendirilmesi ve denetlenmesini sağlar. Bu politikalar sayesinde:

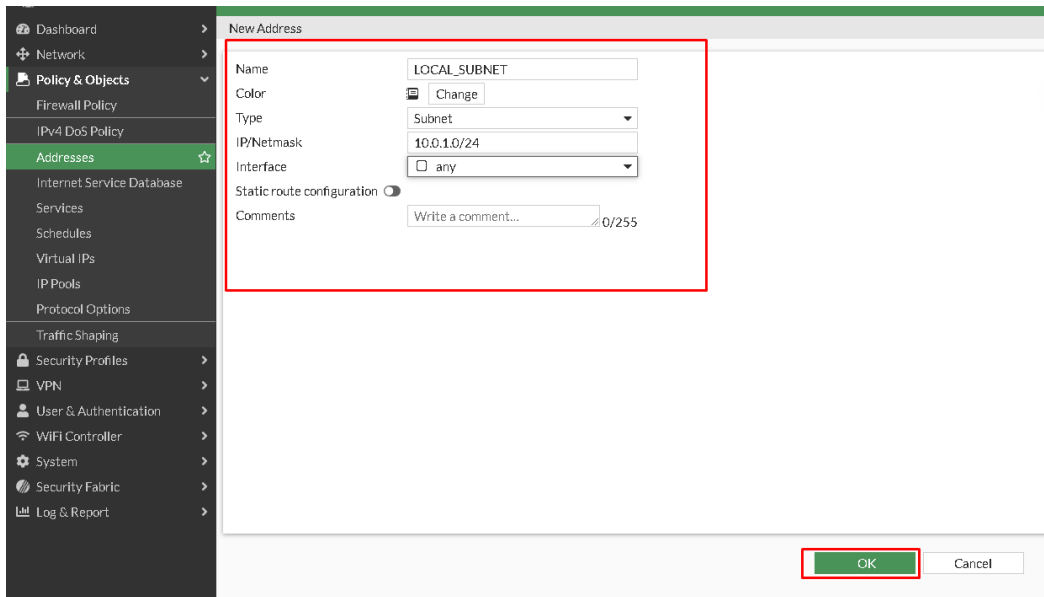
- **Ağ Güvenliği Sağlanır:** Belirli trafiği engelleyerek istenmeyen veya zararlı trafiğin ağa girmesi engellenir.
- **Erişim Kontrolü Uygulanır:** Kimlerin, hangi hizmetlere erişebileceği kontrol edilir.
- **Kritik Uygulamalar Korunur:** Önemli hizmetler ve uygulamalar korunarak, yalnızca gerekli trafiğe izin verilir.
- **Yönetilebilirlik Artar:** Nesnelerin kullanımı, ağ yöneticilerinin politikaları kolayca yapılandırmasına olanak tanır.

1- Fortigate cihazımızın arayüzüne giriş yapalım.



The image shows the Fortigate login interface. It features a green header bar with the Fortigate logo. Below the header, there is a white box containing a text input field with the username 'admin', a password input field with masked characters, and a green 'Login' button. The 'Login' button is highlighted with a red rectangle.

2- Kuralı uygulayacağımız kaynak (source) adresi belirtmek için **Policy & Objects** altında yer alan **Addresses** kısmında bir subnet oluşturalım.



The image shows the 'New Address' configuration screen in the Fortigate web interface. The left sidebar contains a menu with various options, including 'Policy & Objects' and 'Addresses'. The 'Addresses' option is selected and highlighted. The main content area shows the 'New Address' form. The form includes fields for 'Name' (LOCAL_SUBNET), 'Color' (Change), 'Type' (Subnet), 'IP/Netmask' (10.0.1.0/24), 'Interface' (any), 'Static route configuration' (unchecked), and 'Comments' (Write a comment...). The 'OK' button is highlighted with a red rectangle.

- 3- **Policy&Objects** altında yer alan **Firewall Policy** kısmında kural oluşturalım. Burada **port3** seçerek hangi ağ arayüzünden giriş yaptığımızı tanımlıyoruz. Ardından çıkış arayüzümüz olan **port1** adresinide alt kısma ekliyoruz. Oluşturduğumuz **Loca_Subnet** 'i tanımlayarak istediğimiz servisler ile devam ediyoruz.İnspection mode **flow-based** seçeneği ile isteğin **NAT** kullanılarak dışarıya çıkmasını sağlıyoruz. Aşağıda NAT ve Inspection mode hakkında gerekli açıklamalar mevcuttur.

Flow-based inspection, trafiği akış (flow) seviyesinde analiz eden ve güvenlik denetimlerini gerçek zamanlı olarak uygulayan bir yöntemdir. Bu mod, hızlı performans sağlar ve düşük gecikme süresi gerektiren senaryolarda tercih edilir.

Proxy-based inspection, trafiği cihaz üzerinde bir ara sunucu (proxy) gibi durdurarak analiz eder. Bu mod, daha derinlemesine güvenlik denetimi sağlar, ancak performans açısından daha yoğun kaynak kullanır.

NAT (Network Address Translation), ağ cihazlarının, genellikle bir yönlendiricinin (router), bir ağdaki özel IP adreslerini başka bir ağdaki (genellikle internet) genel IP adreslerine çevirme işlemidir. Bu mekanizma, hem ağ güvenliğini artırır hem de IP adreslerinin verimli kullanılmasını sağlar.

The screenshot displays the configuration for a Firewall Policy named "Internet_Access". The settings are as follows:

- Name:** Internet_Access
- Incoming Interface:** port3
- Outgoing Interface:** port1
- Source:** LOCAL_SUBNET
- Destination:** all
- Schedule:** always
- Service:** ALL_ICMP, DNS, HTTP, HTTPS, SSH
- Action:** ACCEPT
- Inspection Mode:** Flow-based
- Firewall/Network Options:**
 - NAT:** ☒
 - IP Pool Configuration:** Use Outgoing Interface Address
 - Preserve Source Port:** ☐
 - Protocol Options:** default
- Security Profiles:**

- 4- Herhangi bir **Security Profile** uygulamayarak **no-inspection** seçin. Log kayıtlarının tamamını almak için **All-Sessions** seçeneğini seçip policy seçeneğinin aktif olduğunu kontrol ederek devam edelim. Aşağıda Security Profiles ve SSL Inspection ne olduğuna dair açıklamalar mevcuttur.

Security Profiles, FortiGate cihazlarında ağ trafiğini zararlı içeriklere ve tehditlere karşı incelemek için kullanılan güvenlik denetimleri kümesidir. Bu profiller, bir Firewall Policy ile ilişkilendirilerek trafiğin detaylı analiz edilmesini ve güvenliğin artırılmasını sağlar.

Başlıca Security Profile Türleri:

1. **Antivirus**: Virüs ve zararlı yazılımları tespit eder ve engeller.
2. **Web Filter**: Web sitelerine erişimi filtreler (örneğin, kategori veya URL bazlı).
3. **Application Control**: Uygulama tabanlı trafik kontrolü sağlar.
4. **IPS (Intrusion Prevention System)**: Saldırıları tespit eder ve engeller.
5. **SSL/SSH Inspection**: Şifreli trafiği analiz eder.
6. **Data Leak Prevention (DLP)**: Hassas veri sızıntısını önler.
7. **Email Filter**: E-posta trafiğini zararlı içeriklere karşı korur.

SSL Inspection, şifreli trafiği inceleyerek tehditleri tespit ve engelleme sürecidir.

Security Profiles

AntiVirus ☐

Web Filter ☐

DNS Filter ☐

Application Control ☐

IPS ☐

File Filter ☐

SSL Inspection no-inspection

Logging Options

Log Allowed Traffic ☒ Security Events ☒ All Sessions ☒

Generate Logs when Session Starts ☒

Capture Packets ☐

Comments 0/1023

Enable this policy ☒

OK Cancel

5- İnternet erişimimizde mevcutta kullanılan **Policy ID** görüntülemek için **Log&Report** kısmında **Forward traffic** kısmında görüntüleyelim. Görseldeki gibi internet erişimimiz az önce oluşturmuş olduğumuz Full_Acces kuralı ile sağlanmaktadır.

| | | | | | | | | | | | | |
|-----------------------|---|-----------|-------------------|---|------------------|----------------------|-----------------|--|--|--|--|--|
| Dashboard | Result: Accept (all) Date/Time: >= 2024/11/10 23:35:40 Add Filter | | | | | | | | | | | |
| Network | Date/Time | Source | Device | Destination | Application Name | Result | Policy ID | | | | | |
| Policy & Objects | Second ago | 10.0.1.10 | 02:09:06:00:01:01 | 151.101.0.81 | | 2.19 kB / 6.21 kB | Full_Access (2) | | | | | |
| Security Profiles | Second ago | 10.0.1.10 | 02:09:06:00:01:01 | 95.100.133.146 (a95-100-133-146.deploystatic.akamai.net) | | 1.31 kB / 1.68 kB | Full_Access (2) | | | | | |
| VPN | Second ago | 10.0.1.10 | 02:09:06:00:01:01 | 95.100.133.139 (a95-100-133-139.deploystatic.akamai.net) | | 1.31 kB / 1.68 kB | Full_Access (2) | | | | | |
| User & Authentication | Second ago | 10.0.1.10 | 02:09:06:00:01:01 | 216.58.214.174 | | 4.25 kB / 8.83 kB | Full_Access (2) | | | | | |
| WiFi Controller | Second ago | 10.0.1.10 | 02:09:06:00:01:01 | 216.58.214.68 (fra15s10-in-f4.1e100.net) | | 15.59 kB / 241.10 kB | Full_Access (2) | | | | | |
| System | Second ago | 10.0.1.10 | 02:09:06:00:01:01 | 52.222.169.66 (server-52-222-169-66.cdg52.r.cloudfront.net) | | 59.38 kB / 18.57 kB | Full_Access (2) | | | | | |
| Security Fabric | Second ago | 10.0.1.10 | 02:09:06:00:01:01 | 52.222.169.66 (server-52-222-169-66.cdg52.r.cloudfront.net) | | | Full_Access (2) | | | | | |
| Log & Report | Second ago | 10.0.1.10 | 02:09:06:00:01:01 | 216.58.213.78 | | 3.24 kB / 47.51 kB | Full_Access (2) | | | | | |
| Forward Traffic | Second ago | 10.0.1.10 | 02:09:06:00:01:01 | 142.250.74.234 (par10s40-in-f10.1e100.net) | | 3.14 kB / 6.80 kB | Full_Access (2) | | | | | |
| Local Traffic | Second ago | 10.0.1.10 | 02:09:06:00:01:01 | 216.58.214.174 | | 3.98 kB / 8.73 kB | Full_Access (2) | | | | | |
| Sniffer Traffic | Second ago | 10.0.1.10 | 02:09:06:00:01:01 | 216.58.214.68 (fra15s10-in-f4.1e100.net) | | 15.32 kB / 241.00 kB | Full_Access (2) | | | | | |
| System Events | 2 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 172.217.20.177 (waw02s07-in-f17.1e100.net) | | 2.90 kB / 7.37 kB | Full_Access (2) | | | | | |
| Security Events | 2 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 216.58.214.163 (mad01s26-in-f163.1e100.net) | | 1.87 kB / 5.04 kB | Full_Access (2) | | | | | |
| Log Settings | 2 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 216.239.32.36 | | 5.90 kB / 8.01 kB | Full_Access (2) | | | | | |
| Threat Weight | 2 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 216.58.213.78 | | 2.91 kB / 47.40 kB | Full_Access (2) | | | | | |
| | 2 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 142.250.74.234 (par10s40-in-f10.1e100.net) | | 2.87 kB / 6.64 kB | Full_Access (2) | | | | | |
| | 3 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 142.250.75.238 (par10s41-in-f14.1e100.net) | | 2.81 kB / 8.71 kB | Full_Access (2) | | | | | |

6- Peki iki farklı kuralımız olursa varsayılan olarak hangi kuralımız geçerli olur?

Haydi deneyelim;

Aşağıda yer alan kuralımızda Local_Subnet' imizden Destination da yeralan Linux makinemize ping erişimini engelleyeceğiz. Bunun için kuralda Service kısmında PING servisi ve Action olarakda DENY (Reddetmek) seçeneğini seçili olması gerekiyor. PING kavramının açıklaması aşağıda yer almaktadır.

Ping: Bir cihazın ağ bağlantısını test etmek için kullanılan basit bir komut veya araçtır.

New Policy

NameBlock_Ping

Incoming Interfaceport3

Outgoing Interfaceport1

SourceLOCAL_SUBNET

DestinationLinux_ETH1

Schedulealways

ServicePING

ActionACCEPTDENY

☒ Log Violation Traffic

CommentsWrite a comment...0/1023

Enable this policy☒

7- Local networkümüzde yeralan bir cihazımızdan **LINUX_ETH1** hedef ip adresine ping gönderelim.

```
Administrator@ubuntu-2204-desktop:~$ ping 10.200.1.254
PING 10.200.1.254 (10.200.1.254) 56(84) bytes of data.
64 bytes from 10.200.1.254: icmp_seq=1 ttl=63 time=2.31 ms
64 bytes from 10.200.1.254: icmp_seq=2 ttl=63 time=1.75 ms
64 bytes from 10.200.1.254: icmp_seq=3 ttl=63 time=1.50 ms
64 bytes from 10.200.1.254: icmp_seq=4 ttl=63 time=1.04 ms
64 bytes from 10.200.1.254: icmp_seq=5 ttl=63 time=1.06 ms
64 bytes from 10.200.1.254: icmp_seq=6 ttl=63 time=1.10 ms
64 bytes from 10.200.1.254: icmp_seq=7 ttl=63 time=1.06 ms
^C
--- 10.200.1.254 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6009ms
rtt min/avg/max/mdev = 1.041/1.403/2.310/0.449 ms
Administrator@ubuntu-2204-desktop:~$
```

Yazmış olduğumuz Block_Ping kuralı neden gerçekleşmedi ?

*****Çünkü kurallar, en spesifikten genele doğru yazılmalı ve FortiGate cihazında daha üst sıradaki kurallar öncelikli olarak çalışır. Bu nedenle, doğru bir sıralama ve kapsamlı bir planlama yapılması kritik öneme sahiptir.

Yani Block_Ping kuralımıza gelmeden Internet_Access tarafındaki kuralımız çalışıyor. Bu yüzden makineye gönderdiğimiz ping komutu çalışmaktadır.

| NAME | STATUS | ENABLED | SOURCE | DEST | ACTION | LOG | PROTECT | INSPECT | LOG |
|-----------------|--------------|------------|--------|---|--------|---------|-------------------|---------|-----|
| Internet_Access | LOCAL_SUBNET | all | always | ALL_ICMP DNS HTTP HTTPS SSH | ACCEPT | Enabled | ssl no-inspection | All | 0 B |
| Block_Ping | LOCAL_SUBNET | LINUX_ETH1 | always | PING | DENY | | | All | 0 B |
| Implicit | | | | | | | | | |

???Hadi şimdi Block_Ping kuralımızı Internet_Access kuralının üstüne taşıyalım ve ne olduğunu birlikte kontrol edelim.

| | | | | | | | | | |
|---|-----------------|--------------|------------|--------|---|--------|---------|-------------------|----------------|
| 4 | Block_Ping | LOCAL_SUBNET | LINUX_ETH1 | always | PING | DENY | | All | 0 B |
| 3 | Internet_Access | LOCAL_SUBNET | all | always | ALL_ICMP DNS HTTP HTTPS SSH | ACCEPT | Enabled | ssl no-inspection | All 6.39 MB |

- | | | | | | | | | |
|-------------------------|--|---|-----------|-------------------|--------------|------------------|------------------------|----------------|
| Dashboard | Result: Deny (all) Date/Time: >= 2024/11/10 23:35:40 Add Filter | | | | | | | |
| Network | Date/Time | % | Source | Device | Destination | Application Name | Result | Policy ID |
| Policy & Objects | 5 seconds ago | | 10.0.1.10 | 02-09:0f:00:01:01 | 10.200.1.254 | | Deny: policy violation | Block_Ping (4) |
| Security Profiles | 6 seconds ago | | 10.0.1.10 | 02-09:0f:00:01:01 | 10.200.1.254 | | Deny: policy violation | Block_Ping (4) |
| VPN | 7 seconds ago | | 10.0.1.10 | 02-09:0f:00:01:01 | 10.200.1.254 | | Deny: policy violation | Block_Ping (4) |
| User & Authentication | 8 seconds ago | | 10.0.1.10 | 02-09:0f:00:01:01 | 10.200.1.254 | | Deny: policy violation | Block_Ping (4) |
| WiFi Controller | 9 seconds ago | | 10.0.1.10 | 02-09:0f:00:01:01 | 10.200.1.254 | | Deny: policy violation | Block_Ping (4) |
| System | 10 seconds ago | | 10.0.1.10 | 02-09:0f:00:01:01 | 10.200.1.254 | | Deny: policy violation | Block_Ping (4) |
| Security Fabric | 0 seconds ago | | 10.0.1.10 | 02-09:0f:00:01:01 | 10.200.1.254 | | Deny: policy violation | Block_Ping (4) |
| Log & Report | 1 seconds ago | | 10.0.1.10 | 02-09:0f:00:01:01 | 10.200.1.254 | | Deny: policy violation | Block_Ping (4) |
| Forward Traffic | 2 seconds ago | | 10.0.1.10 | 02-09:0f:00:01:01 | 10.200.1.254 | | Deny: policy violation | Block_Ping (4) |
| Local Traffic | 3 seconds ago | | 10.0.1.10 | 02-09:0f:00:01:01 | 10.200.1.254 | | Deny: policy violation | Block_Ping (4) |
| Sniffer Traffic | 4 seconds ago | | 10.0.1.10 | 02-09:0f:00:01:01 | 10.200.1.254 | | Deny: policy violation | Block_Ping (4) |
| System Events | 5 seconds ago | | 10.0.1.10 | 02-09:0f:00:01:01 | 10.200.1.254 | | Deny: policy violation | Block_Ping (4) |
| Security Events | 6 seconds ago | | 10.0.1.10 | 02-09:0f:00:01:01 | 10.200.1.254 | | Deny: policy violation | Block_Ping (4) |
| Log Settings | 7 seconds ago | | 10.0.1.10 | 02-09:0f:00:01:01 | 10.200.1.254 | | Deny: policy violation | Block_Ping (4) |
| Threat Weight | 18 seconds ago | | 10.0.1.10 | 02-09:0f:00:01:01 | 10.200.1.254 | | Deny: policy violation | Block_Ping (4) |
| | 19 seconds ago | | 10.0.1.10 | 02-09:0f:00:01:01 | 10.200.1.254 | | Deny: policy violation | Block_Ping (4) |
| | 20 seconds ago | | 10.0.1.10 | 02-09:0f:00:01:01 | 10.200.1.254 | | Deny: policy violation | Block_Ping (4) |

ISDB (Intrusion Signature Database), FortiGate cihazlarında kullanılan bir veritabanıdır ve IDS/IPS (Intrusion Detection and Prevention System) sistemlerinin çalışmasını sağlayan imza tabanlarını içerir. Bu veritabanı, ağ trafiğindeki şüpheli aktiviteleri tespit etmek için kullanılan imza (signature) tabanlı tehdit algılama yöntemlerine dayanır.

- **Tehdit Tespiti:** ISDB, ağ trafiğini analiz ederek, bilinen saldırıların ve güvenlik açıklarının imzalarını içerir. Bu imzalar, belirli bir saldırıyı tanımlamak için kullanılan benzersiz şablonlardır.
- **Güvenlik Profilinin Bir Parçası:** ISDB, FortiGate cihazlarının IPS (Intrusion Prevention System) özelliği ile entegre çalışarak, zararlı trafiği tespit eder ve engeller.
- **Sürekli Güncelleme:** Fortinet, sürekli olarak yeni tehditleri ve saldırı imzalarını veritabanına ekler, böylece ISDB her zaman güncel ve etkili olur.

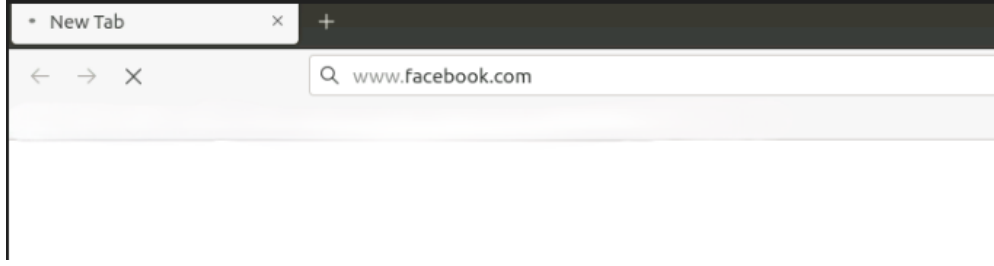
- 1- Bir kural oluşturup ISDB nesnesini hedef olarak kullanalım. Policy diğer seçenekler hakkında bilgi sahibi olmuştuk. Burada Destination kısmına tıklayarak **Internet Service** kısmında yeralan engellemek istediğimiz **Facebook-Web** servisini seçiyoruz. Action kısmında **DENY** (engelle) ile birlikte policy'mizi oluşturalım.

The screenshot shows the 'Edit Policy' window. The policy name is 'Block_Facebook'. The incoming interface is 'port3' and the outgoing interface is 'port1'. The source is 'LOCAL_SUBNET'. The destination is 'Facebook-Web' (highlighted with a red box). The schedule is 'always'. The action is 'DENY'. The 'Log Violation Traffic' checkbox is checked. The 'Enable this policy' checkbox is also checked. On the right, the 'Select Entries' window shows the 'Internet Service' category with a list of services. 'Facebook-Web' is highlighted with a red box.

- 2- Oluşturmuş olduğumuz kuralın Internet_Acces kuralından dolayı pasif kalacağı için **Block_Facebook** kuralımızı bir üste taşıyarak çalışmasını sağlayalım.

| | | | | | | |
|---|-----------------|--------------|--------------|--------|---|--------|
| 4 | Block_Facebook | LOCAL_SUBNET | Facebook-Web | always | Internet Service | DENY |
| 3 | Internet_Access | LOCAL_SUBNET | all | always | ALL_ICMP DNS HTTP HTTPS SSH | ACCEPT |

3-Hadi şimdi Local makinelerimizden birinden **Facebook**'a erişmeye çalışalım.



4- Facebook' a erişemiyoruz. Hemen log kayıtlarını kontrol edelim. Oluşturduğumuz **Block_Facebook** kuralının aktif bir şekilde çalıştığını gözlemliyoruz.

| | | | | | |
|---------------|-----------|-------------------|---------------|------------------------|--------------------|
| 0 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 185.60.219.35 | Deny: policy violation | Block_Facebook (4) |
| 0 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 185.60.219.35 | Deny: policy violation | Block_Facebook (4) |
| 0 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 185.60.219.35 | Deny: policy violation | Block_Facebook (4) |
| 6 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 185.60.219.35 | Deny: policy violation | Block_Facebook (4) |
| 6 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 185.60.219.35 | Deny: policy violation | Block_Facebook (4) |
| 6 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 185.60.219.35 | Deny: policy violation | Block_Facebook (4) |
| 4 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 185.60.219.35 | Deny: policy violation | Block_Facebook (4) |
| 4 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 185.60.219.35 | Deny: policy violation | Block_Facebook (4) |
| 8 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 185.60.219.35 | Deny: policy violation | Block_Facebook (4) |
| 8 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 185.60.219.35 | Deny: policy violation | Block_Facebook (4) |
| 8 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 185.60.219.35 | Deny: policy violation | Block_Facebook (4) |
| 8 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 185.60.219.35 | Deny: policy violation | Block_Facebook (4) |
| 0 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 185.60.219.35 | Deny: policy violation | Block_Facebook (4) |
| 0 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 185.60.219.35 | Deny: policy violation | Block_Facebook (4) |
| 0 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 185.60.219.35 | Deny: policy violation | Block_Facebook (4) |
| 0 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 185.60.219.35 | Deny: policy violation | Block_Facebook (4) |
| 1 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 185.60.219.35 | Deny: policy violation | Block_Facebook (4) |
| 1 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 185.60.219.35 | Deny: policy violation | Block_Facebook (4) |
| 1 seconds ago | 10.0.1.10 | 02:09:06:00:01:01 | 185.60.219.35 | Deny: policy violation | Block_Facebook (4) |
| Minute ago | 10.0.1.10 | 02:09:06:00:01:01 | 10.200.1.254 | Deny: policy violation | Block_Facebook (4) |
| Minute ago | 10.0.1.10 | 02:09:06:00:01:01 | 10.200.1.254 | Deny: policy violation | Block_Facebook (4) |
| Minute ago | 10.0.1.10 | 02:09:06:00:01:01 | 10.200.1.254 | Deny: policy violation | Block_Facebook (4) |
| Minute ago | 10.0.1.10 | 02:09:06:00:01:01 | 10.200.1.254 | Deny: policy violation | Block_Facebook (4) |