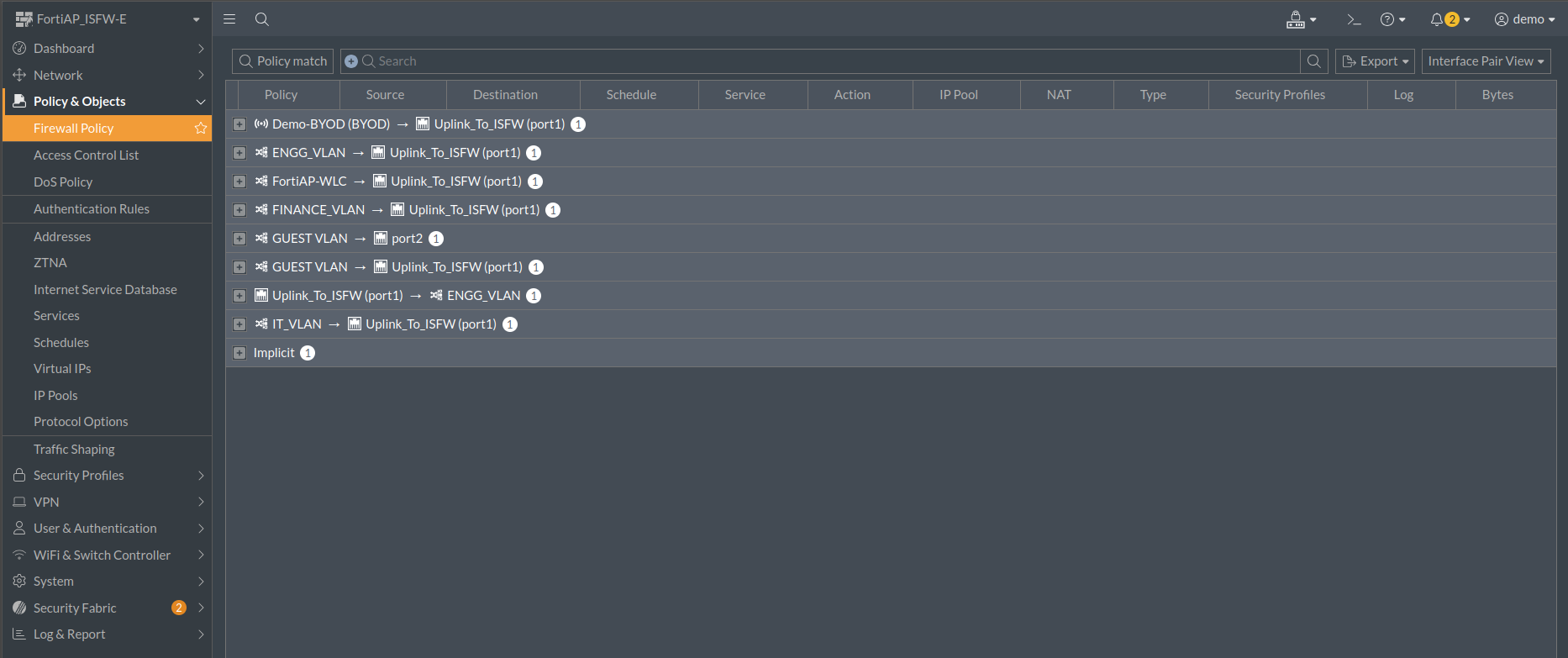
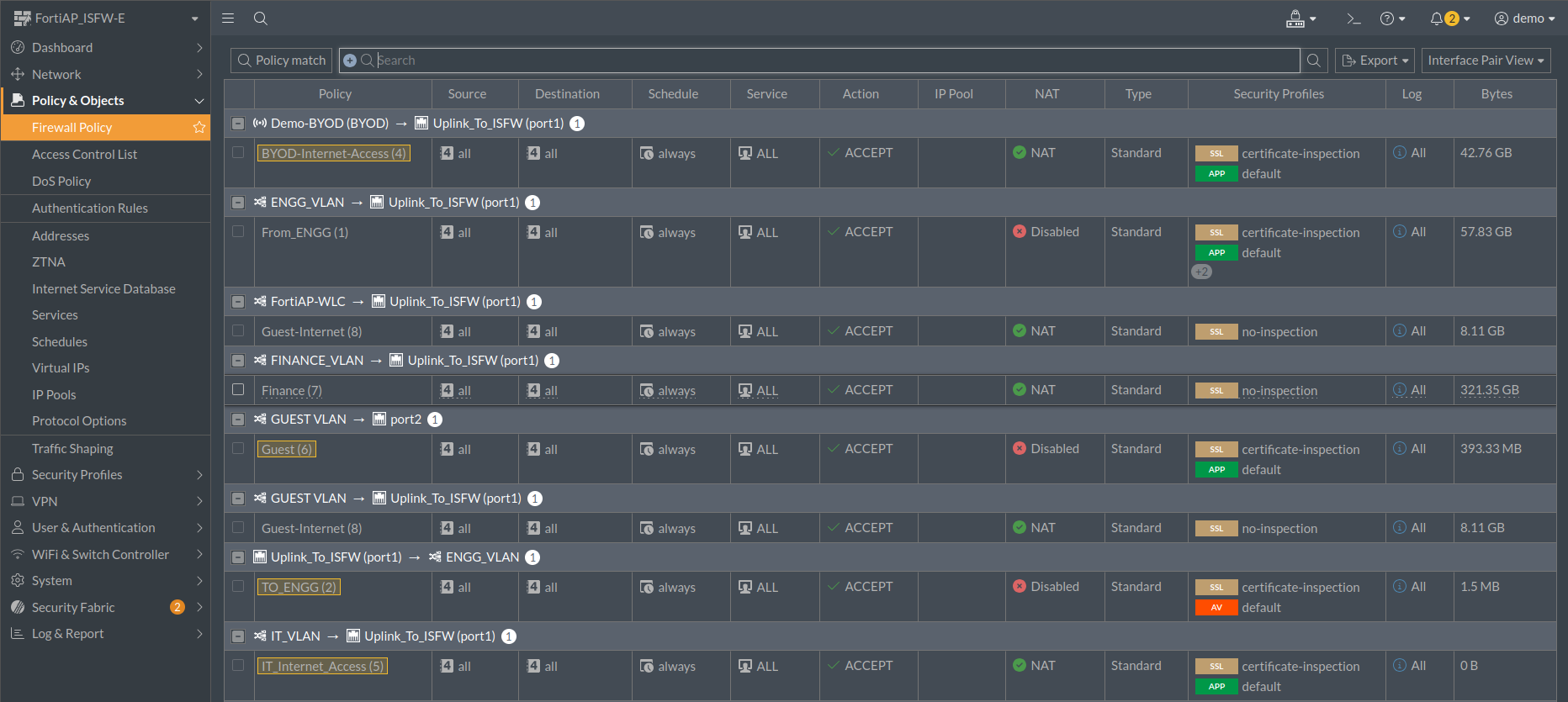
**FortiGate üzerinden port nasıl açılır ve kapatılır?**

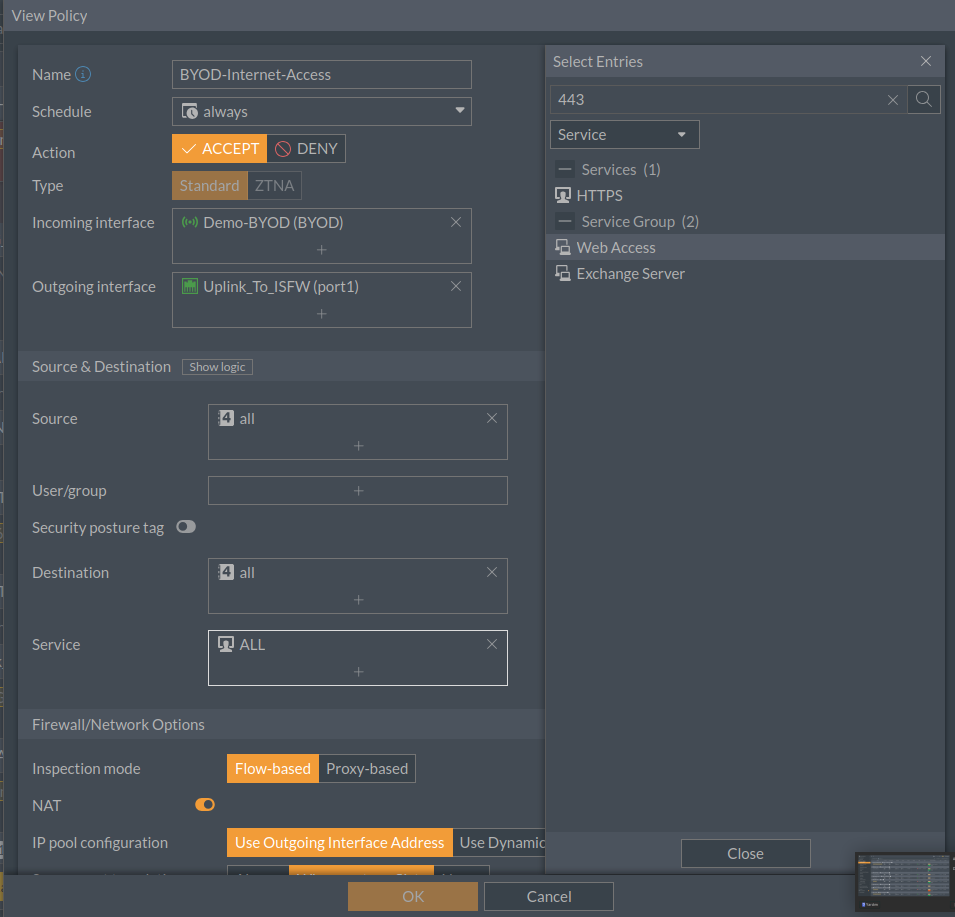
Daha önceden yazdığımız firaewall kuralları üzerinden açık ve kapalı portları görmek için firewall arayüzünde Policy & Objects bölümüne geliyoruz. Ardından Firewall Policy bölümünde değişiklik yapmak istediğimiz kuralı seçiyoruz.



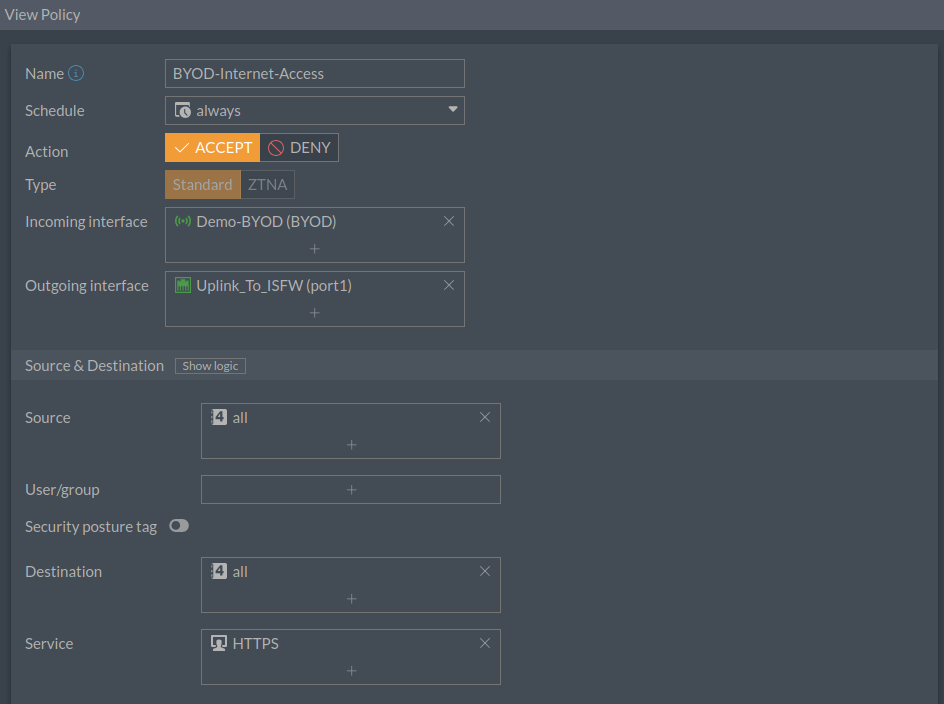
Bu ekran, iç ağdaki VLAN veya portlardan internete doğru tanımlanmış tüm güvenlik kurallarını göstermektedir. Her kuralda "Service: ALL" ifadesi yer aldığı için HTTP, HTTPS, SSH, FTP, DNS gibi tüm servislerin çıkışına izin verilmektedir. Kurallar "ACCEPT" olarak ayarlandığı ve "Schedule" kısmı "always" olduğu için bu izinler sürekli ve herhangi bir kısıtlama olmadan geçerlidir.



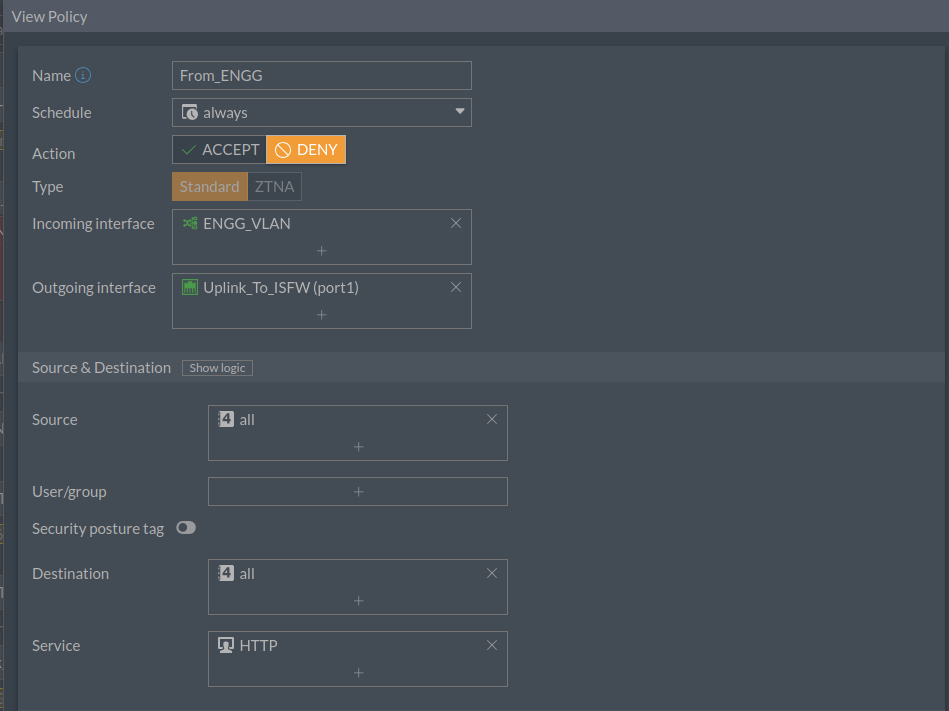
Şimdi Bir kural üzerinde değişiklik yapalım. BYOD-Internet-Access isimli firewall kuralını, sadece HTTPS trafiğine (TCP 443) izin verecek şekilde sınırlandıralım.



Bu kural sayesinde BYOD ağına bağlı kullanıcılar yalnızca **HTTPS (443)** portunu kullanarak internete erişebilir. Diğer tüm servisler (HTTP, FTP, SSH, DNS vb.) **engellenmiştir**. Erişim sürekli olarak aktiftir.



Şimdi yeni kuralımız üzerinden iç ağdan dış ağa yapılan trafiği kontrol eder. **Tüm portlara izin verilir**, ancak **HTTP (TCP/80) trafiği özel olarak engellenmiştir**. Böylece kullanıcılar FTP, HTTPS, SSH gibi diğer servisleri kullanabilirken, port 80 üzerinden gerçekleşen şifresiz web erişimleri (HTTP) güvenlik gerekçesiyle engellenmiş olur.



**IDS & IPS**

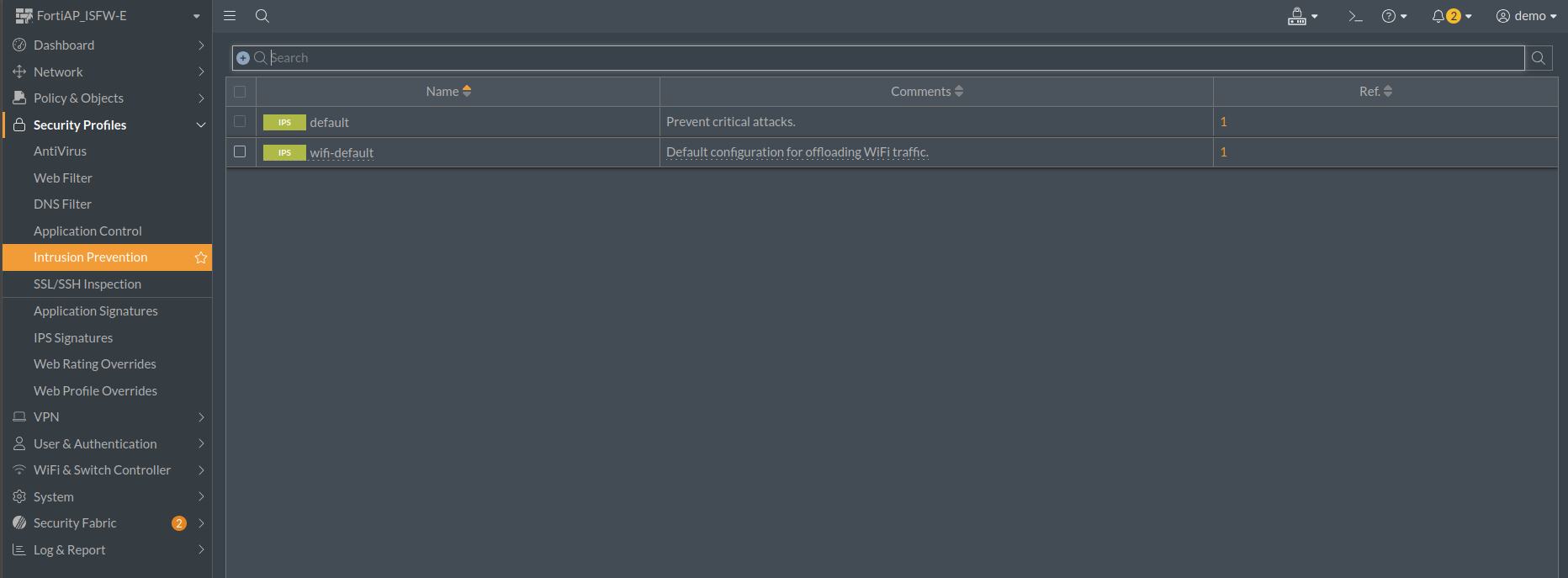
IPS (Intrusion Prevention System) ve IDS (Intrusion Detection System), ağ trafiğini analiz ederek tehditleri tespit etmek için kullanılır. IDS yalnızca şüpheli etkinlikleri algılar ve uyarı üretir, IPS ise bu tehditleri algıladıktan sonra engelleme işlemi de yapar.

**FortiGate cihazlarında bağımsız bir IDS (Intrusion Detection System) modülü yoktur**; yalnızca **IPS (Intrusion Prevention System)** bulunmaktadır.

Ancak, **FortiGate IPS**, istenirse **"detect only" (yalnızca algıla)** modunda çalıştırılarak **IDS gibi davranabilir**. Yani saldırıları sadece tespit eder, engelleme yapmaz. Bu ayar, IPS profilinde yapılır:

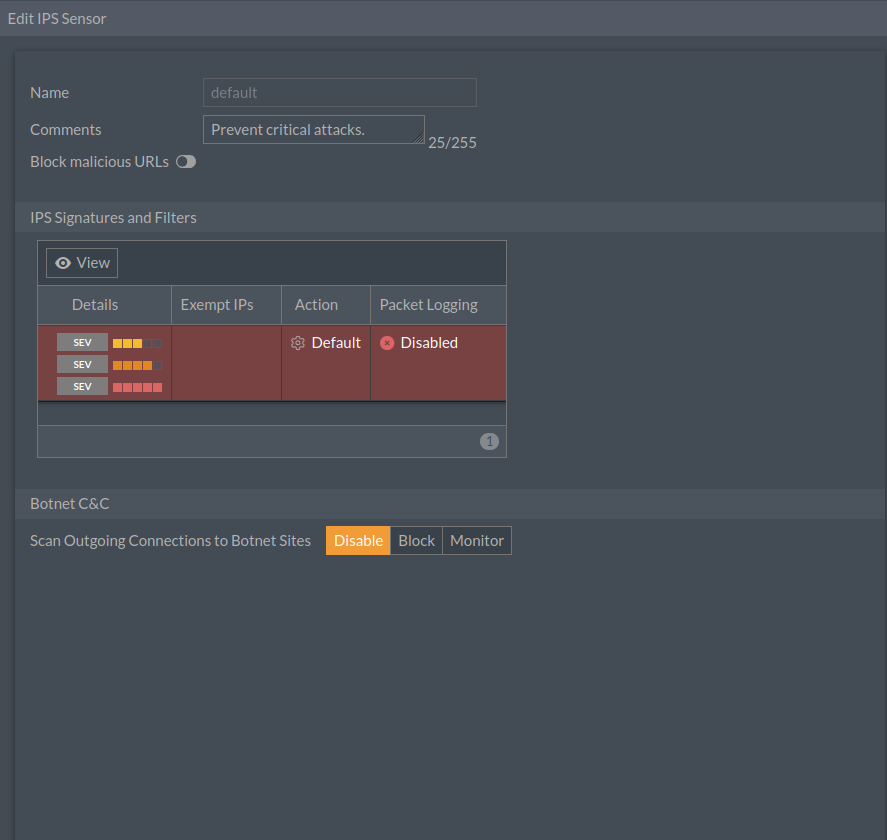
**Security Profiles > Intrusion Prevention** bölümünde ilgili IPS profiline girilir.

Aşağıda görüldüğü gibi varsayılan olarak iki tane IPS profili var. Birini seçip biraz inceleyelim.



FortiGate IPS ekranında, kritik seviyesi 3 ve üzeri olan saldırılar için IPS sistemi etkin durumdadır, yani bu tür saldırılar tespit edildiğinde varsayılan eylem olan engelleme uygulanır. Ancak, bu saldırılarla ilgili herhangi bir paket loglama (kayıt alma) işlemi yapılmamaktadır.

## "Botnet C&C" bölümü ise, ağdaki cihazların botnet komut ve kontrol sunucularına yaptığı çıkış bağlantılarını izlemek için kullanılır. Bu özellik şu anda devre dışı bırakılmış durumdadır. Yani ağdaki bir cihaz zararlı bir botnet ağına bulaşmış ve dışarıya bağlantı kuruyorsa, FortiGate bu bağlantıyı kontrol etmez, engellemez ya da kaydetmez.



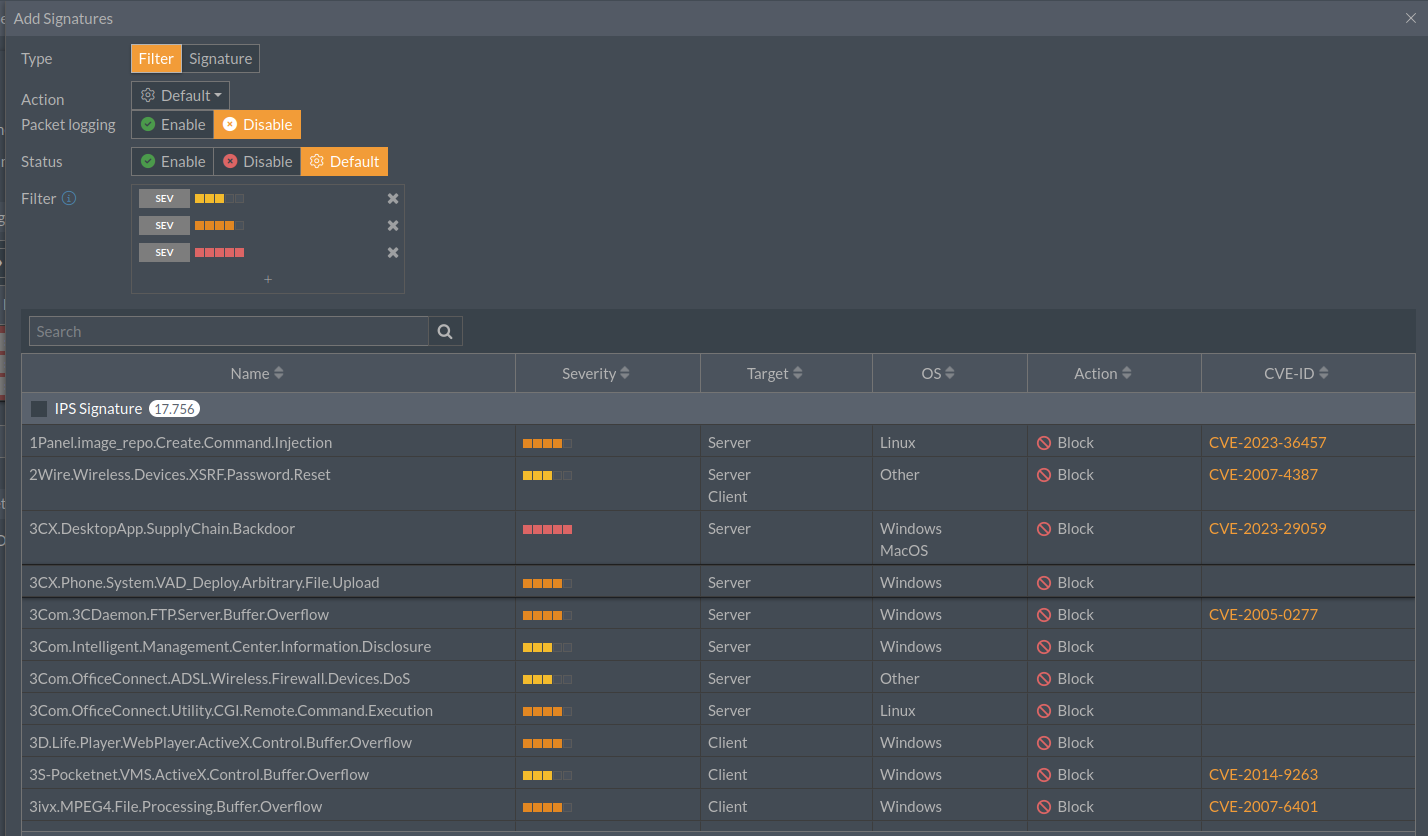
Şimdi varsayılan eylemi incelemek için “view” seçeneğini seçiyoruz.

Bu ekran FortiGate IPS (Intrusion Prevention System) sensöründe etkin olan imzaları (signatures) gösterir. Her imza, belirli bir güvenlik açığını veya saldırı türünü temsil eder.

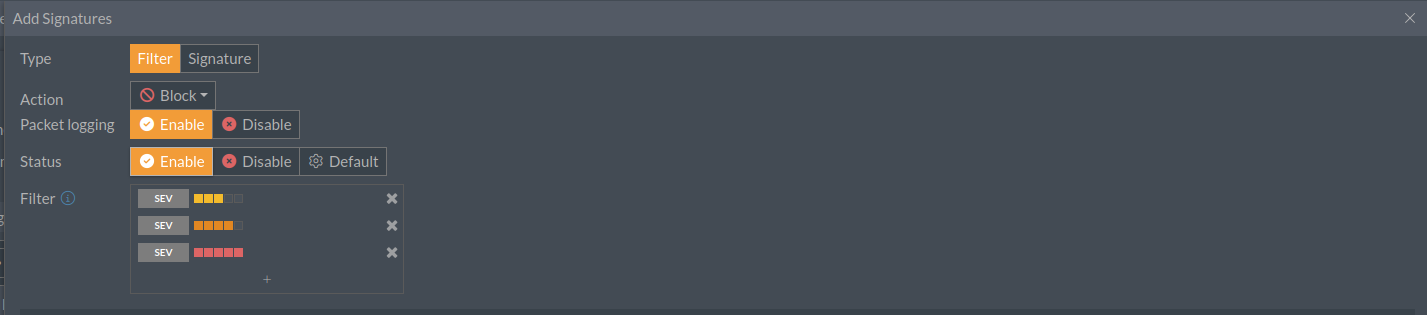
* **Type: Filter: Belirli özelliklere göre (kritiklik seviyesi gibi) imza seçimi yapılır.**
* **Action: Default:** Seçilen imzalar için ön tanımlı aksiyon uygulanacak (örneğin Block).
* **Packet Logging: Disable yani** Paket kayıtları tutulmayacak.
* **Status: Enable:** Bu imzalar aktif (engelleme yapılabilir).
* **Filter (SEV):** Seviye 3 ve üzeri (orta, yüksek, çok yüksek) kritik tehdit imzaları seçilmiş.

Aşağı bölümde yer alan tablo ise:

* **Name**: Tespit edilen saldırının adı.
* **Severity (Kritiklik)**: Saldırının tehlike derecesi (renkli çubuklarla gösterilir – kırmızı en yüksek).
* **Target**: Bu saldırının hedeflediği sistem tipi (Server/Client).
* **OS**: Hedef işletim sistemi (Linux, Windows, vb.).
* **Action**: “Block” ise saldırı engellenir.
* **CVE-ID**: Bu güvenlik açığına ait resmi CVE numarasıdır. CVE hakkında daha fazla bilgi almak için üstüne tıklamak yeterli.

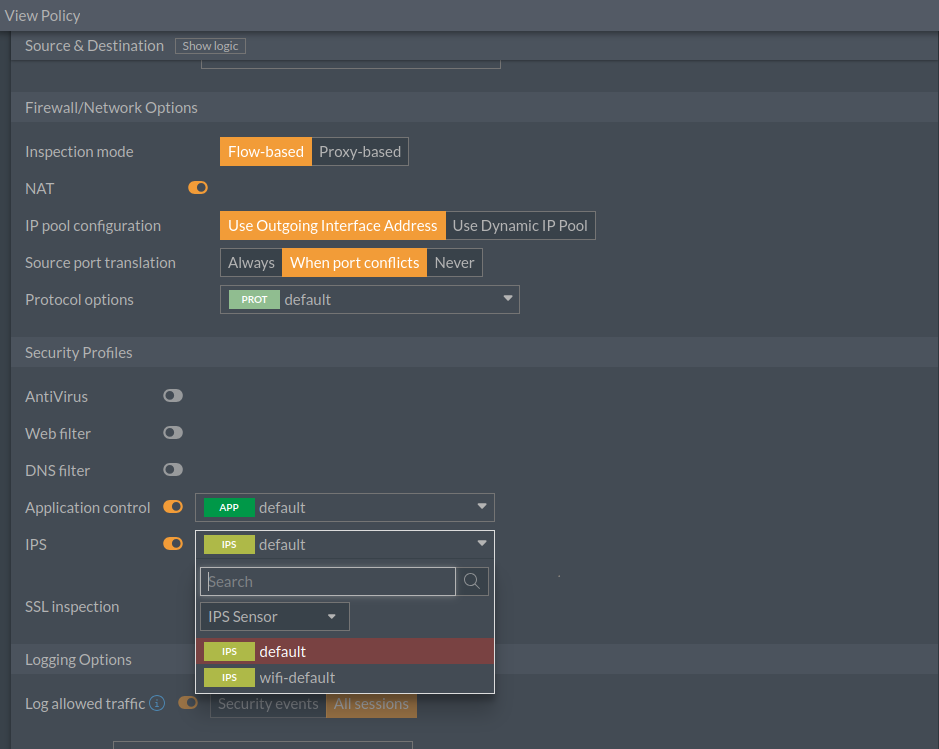


Eğer değiştirmek isterseniz örneğin yeni bir IPS oluşturup kritiklik seviyesi 3 ve üstü olanları engellemek istersek aşağıdaki gibi ayarlamanız gerekecektir. Aşağıdaki gibi ayarlarsanız kritiklik seviyesi 3 ve üstü olanları engelleyecek ve Packet logging yapacak. Ayrıca bunlara ek olarak bazı kritiklik seviyesi 3 olup herhangi bir zaafiyet yoksa aşağıdaki tablo üzerinde action’u “pass” yapabiliriz.



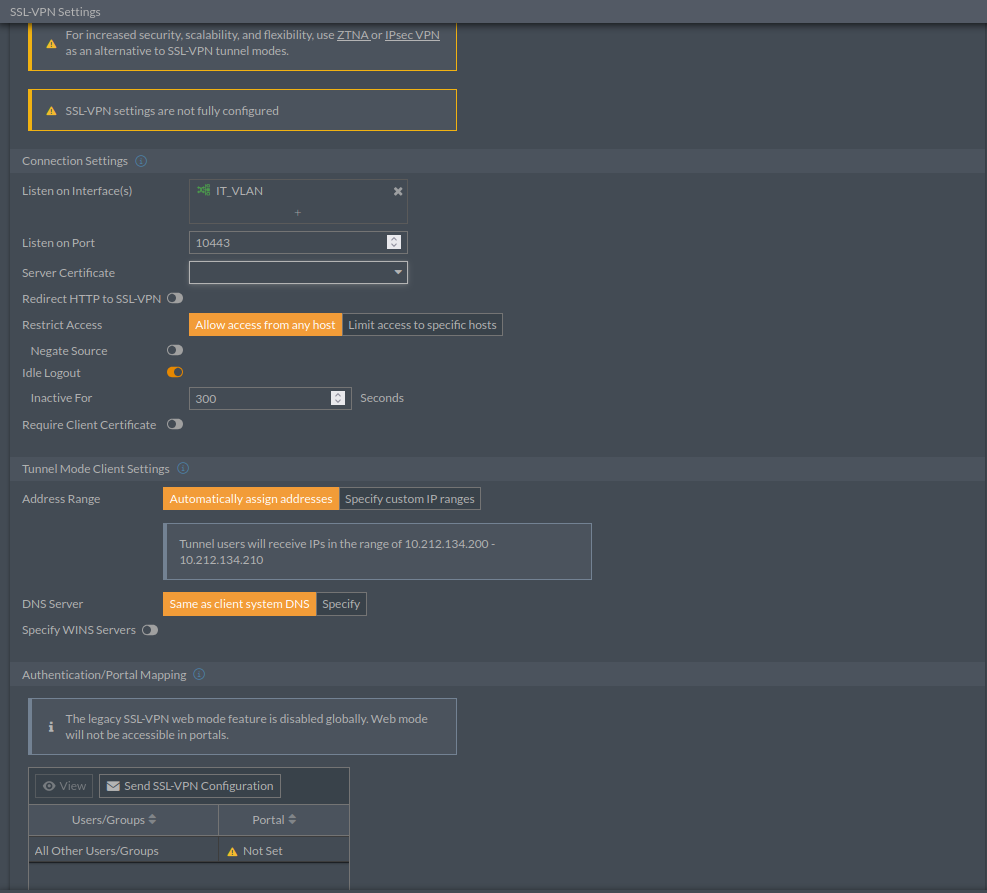
Burda oluşturduğumuz kuralı Policy & Objects → Firewall Policy bölümünden kuralımıza ekleyebiliriz.

Kuralı “view” ettikten sonra IPS’i aktif hale getirip oluşturduğumuz IPS’i ekleyebiliyoruz.



**SSL-VPN**

FortiGate’de SSL-VPN, uzaktaki kullanıcıların şirket ağına güvenli şekilde bağlanmasını sağlar. Şirket içi kaynaklara erişmek amacıyla kullanılır. HTTPS (443) portu üzerinden çalışır ve genellikle güvenlik duvarı tarafından engellenmez. Kullanıcı, dışarıdan bağlandığında sanki şirket ağı içindeymiş gibi çalışabilir. Özellikle evden çalışanlar için kullanışlıdır.



**Listen on Interface(s):**  
VPN bağlantılarını karşılayacak olan fiziksel veya sanal ağ arayüzünü belirtir. Bu arayüz, VPN istemcilerinin bağlanmak istediği kurum ağına açılan noktadır.

**Listen on Port:**  
VPN istemcilerinin bağlantı kuracağı port numarasıdır. Burada 10443 seçilmiş. Kullanıcılar bu port üzerinden VPN bağlantısı kurar.

**Redirect HTTP to SSL-VPN:**  
Kullanıcılar 80 portundan (HTTP) gelirse otomatik olarak HTTPS (SSL-VPN) bağlantısına yönlendirilir.

**Restrict Access:**  
Hangi istemcilerin bağlantı kurabileceğini belirler. “Allow access from any host” seçiliyse, tüm kaynaklardan bağlantıya izin verilir.

**Idle Logout:**  
VPN bağlantısında belirli bir süre (örneğin 300 saniye) boyunca işlem yapılmazsa bağlantı otomatik olarak sonlandırılır.

**Require Client Certificate:**  
İstemciden bağlantı sırasında dijital sertifika istenip istenmeyeceğini belirler. Bu yapılandırmada devre dışı bırakılmış.

**Address Range:**  
VPN’e bağlanan kullanıcılara verilecek IP aralığıdır. Bu IP’lerle istemciler iç ağa erişim sağlar. Örnek aralık: 10.212.134.200 – 10.212.134.210

**DNS Server:**  
VPN istemcilerinin kullanacağı DNS ayarlarını belirtir. Burada istemcinin mevcut sistem DNS’i kullanılıyor.

**Authentication / Portal Mapping:**  
VPN’e kimlerin erişeceği ve hangi portalla eşleştirileceği tanımlanır. “All Other Users/Groups” için şu anda bir portal atanmadığı görülüyor.

**Örnek Senaryo:**

Uzaktan çalışan bir kullanıcı, şirketin iç ağına güvenli bir şekilde bağlanmak için **FortiGate SSL-VPN** kullanır. FortiGate üzerinde yapılan yapılandırmaya göre, VPN bağlantıları **10443** portu üzerinden kabul edilir ve bu bağlantılar, FortiGate cihazının **dış ağ (WAN) arayüzüne ait IP adresi** üzerinden gerçekleştirilir. Örneğin, FortiGate’in dış IP’si 77.68.45.50 ise, kullanıcı https://77.68.45.50:10443 adresine bağlanarak VPN oturumunu başlatır.

VPN bağlantısı başarıyla kurulduğunda, FortiGate tarafından kullanıcıya **10.212.134.200 – 10.212.134.210** aralığında bir **iç IP adresi** atanır (örneğin 10.212.134.204). Bu iç IP sayesinde, kullanıcı sanki şirket iç ağındaymış gibi sunuculara, dosya paylaşım sistemlerine veya diğer ağ kaynaklarına erişebilir.