### ****FortiWeb nedir?****

**FortiWeb**, Fortinet firmasının geliştirdiği bir **Web Application Firewall (WAF)** ürünüdür. Web uygulamalarını; SQL injection, XSS, CSRF, RFI, LFI gibi saldırılara karşı korumak için tasarlanmıştır. Gelen HTTP/HTTPS trafiğini analiz eder, zararlı içerikleri filtreler ve sadece güvenli trafiğin arka uç sunuculara ulaşmasına izin verir.

Ayrıca, yük dengeleme, bot koruması, API güvenliği, SSL/TLS offloading ve log yönetimi gibi gelişmiş özellikleri de barındırır.

### ****FortiWeb Dashboard****

Arayüzdeki dashboard (gösterge paneli), sistemin durumunu hızlıca görmek için kullanılır. İşte en sık görülen widget’lar ve görevleri:

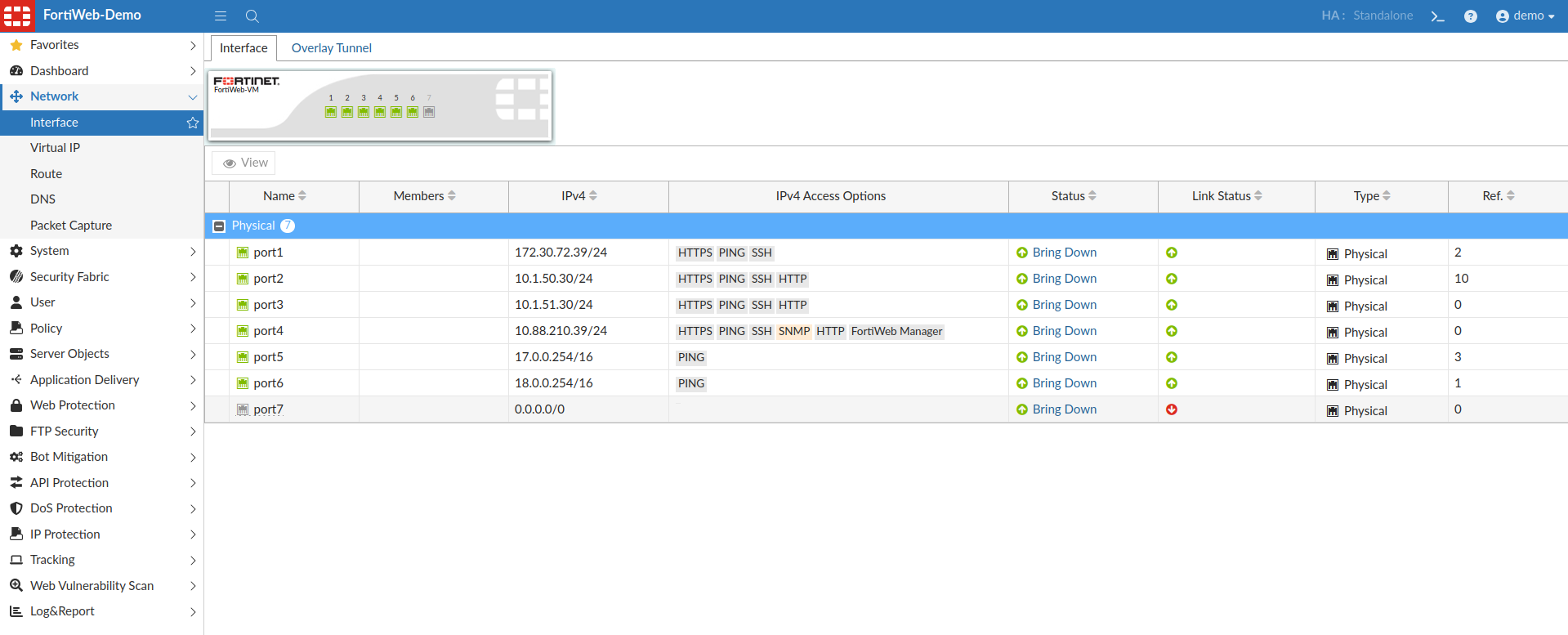
* **System Information:** Cihazın modeli, seri numarası, yazılım versiyonu, çalışma süresi gibi sistemsel bilgiler burada gösterilir.
* **License Information:** FortiWeb’in lisans durumu (örneğin saldırı imza güncellemeleri aktif mi) bu bölümde yer alır.
* **Interface Status:** Cihaz üzerindeki fiziksel ve sanal ağ arayüzlerinin durumu (bağlı mı, IP adresi ne) buradan izlenir.
* **Resource Usage / System Performance:** CPU, RAM ve disk kullanımı gibi donanım kaynaklarının anlık durumu gösterilir.
* **System Event Logs:** Cihaz üzerinde gerçekleşen olayların kısa özetleri burada yer alır (örneğin yapılandırma değişiklikleri, reboot vs).
* **Attack Log / Alert Summary:** Web uygulamalarına yapılan saldırılar ve sistemin verdiği tepkiler (bloklama, uyarı) burada özetlenir.
* **Policy Hit Count:** Hangi WAF policy’lerinin ne kadar trafik aldığı ve ne kadar saldırı tespit ettiği bilgisi burada görüntülenir.
* **Top Attacks / Top Attackers:** En çok tespit edilen saldırı türleri ve saldırı yapan IP’ler bu panellerde yer alır.

### FortiWeb Network?

**Network** sekmesi, FortiWeb cihazının ağ ayarlarının yapıldığı, yani dış dünya ve arka uç sunucularla **nasıl haberleşeceğini belirlediğin** bölümdür. Cihazın IP yapılandırmasından tut, yönlendirme, DNS ve proxy ayarlarına kadar tüm temel ağ iletişimi buradan yönetilir.

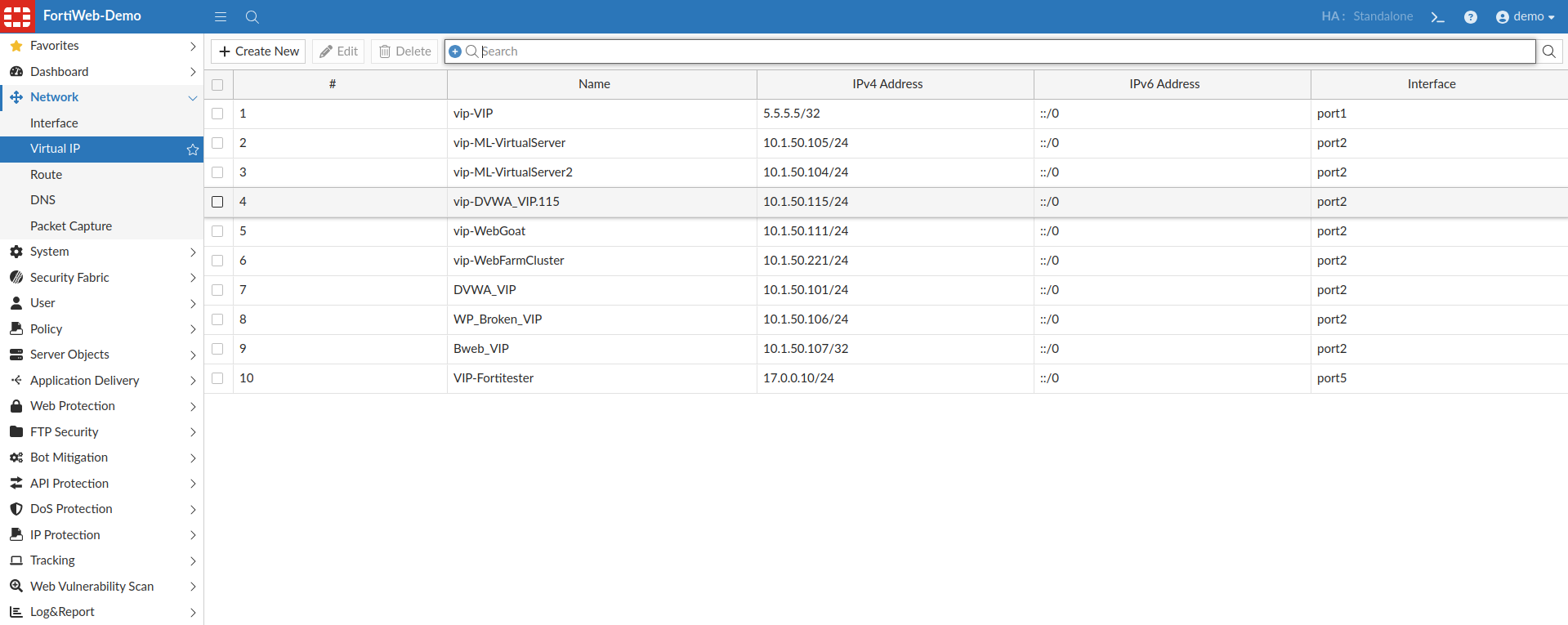
### ****Interface:****

Bu bölümde FortiWeb cihazının hangi fiziksel portlarının aktif olduğu, hangi IP adreslerini kullandığı ve bu portların hangi network segmentlerine ait olduğu tanımlanır. Örneğin, port1 genelde iç ağa bakan arayüz olurken, port2 dış ağ (WAN) trafiğini alabilir. Her arayüze sabit IP verilebilir, DHCP ayarlanabilir veya VLAN tanımlanabilir. Ayrıca arayüzlerin yönetim erişim izinleri (HTTP, HTTPS, SSH gibi) de buradan kontrol edilir.



### ****Virtual IP (VIP):****

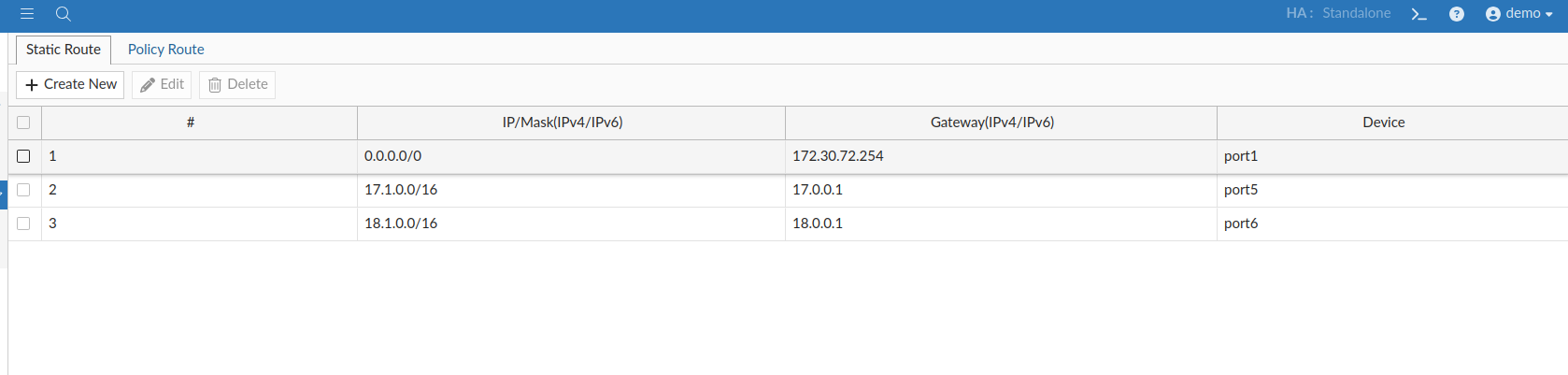
FortiWeb’in dış dünyadan gelen HTTP/S isteklerini karşılamak için kullandığı mantıksal IP adresidir. Yani gerçek sunucu IP’si gizlenir, client’lar sadece VIP’yi görür. FortiWeb, bu VIP’ye gelen trafiği filtreler, kontrol eder ve belirlenen kurallar çerçevesinde arka uç sunuculara yönlendirir. VIP genelde Virtual Server ile eşleştirilerek kullanılır; bu ikili birlikte çalışır.



### ****Route (Statik Yönlendirme):****

Route bölümü, FortiWeb’in giden trafiği hangi ağ geçidine (gateway) ve hangi arayüzden göndereceğini belirler. Yani, FortiWeb’den çıkan verilerin “hangi yoldan” çıkacağını tanımlar. Böylece, farklı IP aralıklarına doğru trafiği doğru ağ kapılarından yönlendirmiş olur.

**Statik rotalar FortiWeb’in “giden” trafiğinin yönlendirilmesi içindir**.



### ****1.**** Bu, **varsayılan rota (default route)**. Yani FortiWeb eğer hedef IP adresini başka bir kuralla eşleştiremiyorsa, trafiği **port1 üzerinden 172.30.72.254** adresine gönderir. Bu genellikle **internet çıkışı veya genel ağ erişimi** için kullanılır.

### ****2.**** Bu kural, FortiWeb’in **17.1.0.0/16 ağına** gidecek trafiği **port5** üzerinden, **17.0.0.1** ağ geçidine yönlendirmesini sağlar. Bu da muhtemelen iç ağda bulunan bir sunucu grubu ya da başka bir segmenttir.

**3.** Benzer şekilde, bu kural da **18.1.0.0/16 ağına** gidecek olan trafiği **port6** üzerinden, **18.0.0.1** ağ geçidine gönderecek şekilde ayarlanmıştır. Yani farklı bir ağ segmentine yönlendirme yapılmakta.

### ****DNS:****

FortiWeb’in domain isimlerini IP’ye çevirebilmesi için kullanacağı DNS sunucuları burada tanımlanır. Örneğin loglarda ya da policy’lerde IP yerine alan adlarının görünmesi isteniyorsa bu çözümleme DNS sunucuları sayesinde yapılır. Ayrıca, FortiWeb kendi güncellemeleri için de DNS çözümlemesine ihtiyaç duyar.

### ****Packet Capture:****

Bu araç, FortiWeb üzerinden geçen ağ trafiğini analiz etmek için kullanılır. Belirli bir arayüzde, belirli filtrelerle paket yakalanabilir. Örneğin bir sunucuya ulaşamama problemi varsa, gelen-giden paketler bu araçla yakalanıp incelenebilir. TCPDump mantığıyla çalışır, çıktı dosyaları indirilebilir ve Wireshark gibi araçlarda analiz edilebilir.

**FortiWeb System:**

### Global Resources:

FortiWeb cihazının kullanacağı genel kaynaklar ve limitler burada tanımlanır. Örneğin, CPU ve bellek kullanımı sınırları, maksimum bağlantı sayısı gibi sistem performansını ve kaynak yönetimini etkileyen ayarlar bu bölümde yapılır.

### Config:

FortiWeb’in genel yapılandırma ayarlarının yapıldığı yerdir. Cihazın genel çalışma şeklini belirleyen parametreler (saat ayarları, log ayarları, varsayılan değerler vb.) burada bulunur.

### Tags:

Web uygulamaları, IP adresleri veya diğer nesneler için özel etiketler (tags) oluşturulabilir. Bu etiketler, politika ve raporlama işlemlerinde kolaylık sağlar, nesneleri gruplandırmaya yarar.

### HA (High Availability):

FortiWeb cihazlarının yedeklilik (redundancy) ve kesintisiz hizmet için bir arada çalışmasını sağlayan ayarların yapıldığı bölümdür. Bu sayede bir cihazda problem olsa bile diğer cihaz devreye girer.

### Admin:

FortiWeb cihazına erişim ve yönetimle ilgili kullanıcı hesapları, yetkiler, oturum ayarları ve güvenlik politikalarının yönetildiği bölümdür.

### Maintenance:

Cihazın bakımıyla ilgili işlemler burada yapılır. Yazılım güncellemeleri, yedekleme, geri yükleme, yeniden başlatma gibi günlük yönetim işlemleri bu bölümden yürütülür.

**FortiWeb Security Fabric:**

### Fabric Connector:

FortiWeb’in, Fortinet Security Fabric içerisindeki diğer cihazlarla (FortiGate, FortiAnalyzer vb.) **doğrudan bağlantı kurmasını** sağlar. Bu bağlantılar sayesinde FortiWeb, diğer cihazlarla **tehdit bilgisi paylaşabilir**, **kural senkronizasyonu yapabilir** ve **merkezi log yönetimi** gibi işlemleri gerçekleştirebilir. Bu sayede güvenlik altyapısı daha bütünleşik çalışır.

### External Connectors:

FortiWeb’in Fortinet dışındaki güvenlik çözümleriyle (örneğin SIEM, LDAP, AWS, Azure, REST API servisleri vb.) **entegrasyon kurmasını** sağlar. Bu entegrasyonlar sayesinde FortiWeb, dış kaynaklı tehdit verilerini alabilir ya da olay bilgilerini harici sistemlere iletebilir. Ayrıca kimlik doğrulama sistemleriyle de buradan bağlantı sağlanabilir.

### Automation:

Olaylara otomatik yanıt verme yeteneğini tanımlar. Örneğin, belirli bir saldırı tespit edildiğinde otomatik olarak bir e-posta gönderme, IP’yi kara listeye alma ya da bir webhook tetikleme gibi **otomasyon kuralları** buradan ayarlanır. Böylece sistem yöneticisinin müdahalesine gerek kalmadan bazı tehditlere anında yanıt verilebilir**.**

**FortiWeb User**

### ****User Group:****

FortiWeb üzerinde tanımlı olan kullanıcıları gruplandırmak için kullanılır. Bu gruplar, erişim kontrol politikalarında ya da kimlik doğrulama işlemlerinde kullanılır. Örneğin sadece belirli bir kullanıcı grubunun bir web uygulamasına erişmesini istiyorsan, burada bir grup tanımlanıp o politika ile eşleştirilir.

### Remote Server:

LDAP, RADIUS veya Active Directory gibi **harici kimlik doğrulama sunucularının** FortiWeb’e bağlanmasını sağlar. Böylece kullanıcı doğrulama işlemleri FortiWeb üzerinden değil, organizasyonun merkezi kullanıcı yönetim sistemleri üzerinden yapılabilir. Bu hem güvenlik hem de yönetim kolaylığı sağlar.

### PKI User:

**Dijital sertifika (X.509)** ile kimlik doğrulama yapmak isteyen kullanıcılar burada tanımlanır. FortiWeb, kullanıcıların kimliğini dijital sertifikaları üzerinden doğrulayabilir. Genellikle kurumsal ortamlarda, daha yüksek güvenlik gerektiren uygulamalarda tercih edilir.

### OAuth Server:

FortiWeb’in **OAuth 2.0 protokolü** ile çalışan kimlik doğrulama sunucularına (örneğin Google, Azure AD, Okta vb.) bağlanmasını sağlar. Bu sayede kullanıcılar, OAuth destekli kimlik sağlayıcıları ile oturum açabilir. Modern web uygulamalarıyla entegre çalışmak için kullanılır.

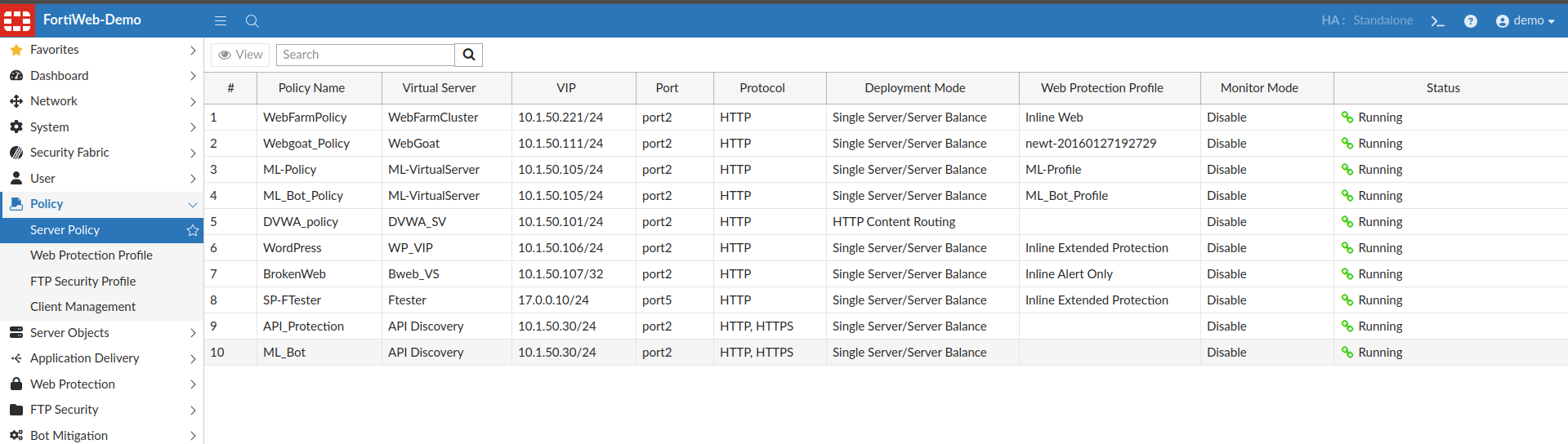
**FortiWeb Policy:**

### ****Policy:****

FortiWeb’de gelen isteklerin **nasıl işleneceğini ve hangi güvenlik kurallarının uygulanacağını** belirleyen ana bölümdür. Web trafiğine yönelik kurallar burada tanımlanır; hangi sunucuya yönlendirileceği, hangi filtrelerin uygulanacağı, hangi kullanıcıların erişeceği gibi işlemler bu bölümde kontrol edilir.

### ****Server Policy:****

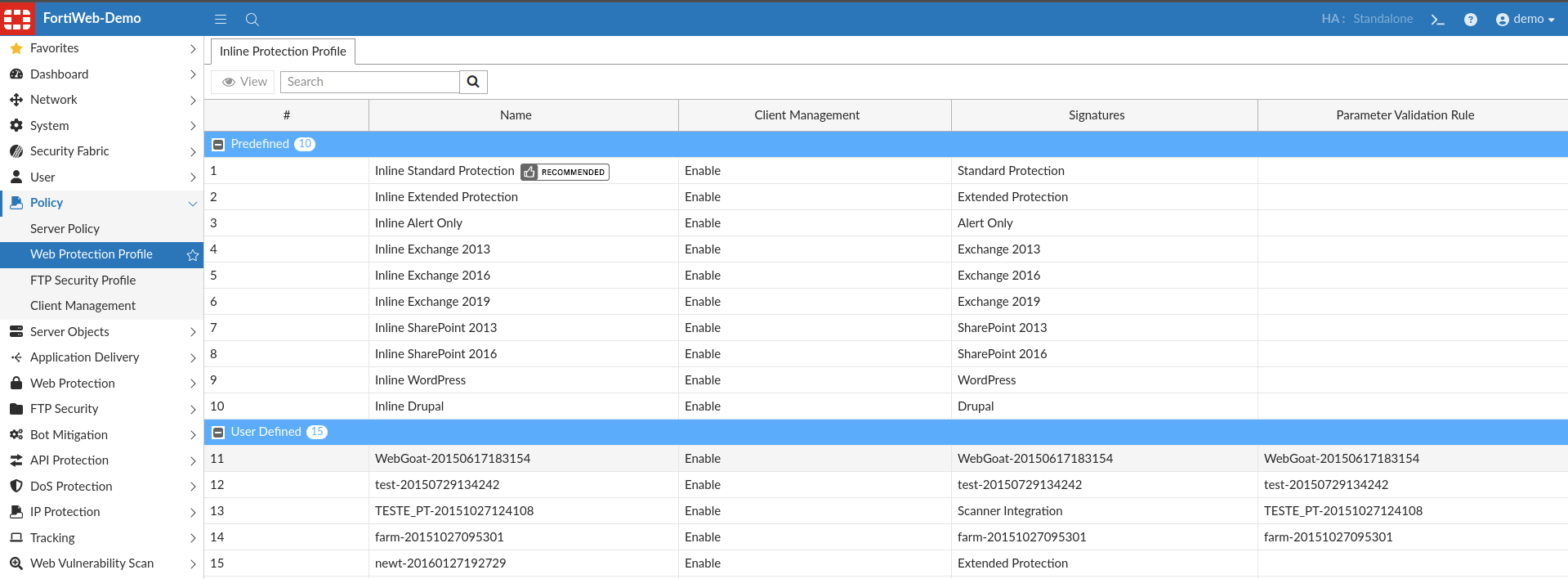
FortiWeb’e gelen HTTP/S trafiğinin hangi **arka uç sunucuya (backend)** yönlendirileceğini ve bu trafik üzerinde hangi güvenlik profillerinin uygulanacağını belirler. Bir nevi “trafik yönetim ve koruma kuralıdır.” Her web uygulaması için ayrı bir Server Policy tanımlanabilir.



* **#:** Politika listesindeki sıra numarasını gösterir.
* **Policy Name**: Politikanın adını belirtir. Bu ad, yönetici tarafından politikayı tanımlamak ve ayırt etmek için verilir. Örnek olarak, "WebFarmPolicy", "WebGoat\_Policy", "ML\_Bot" gibi isimler görüyorsunuz.
* **Virtual Server**: Politikanın uygulandığı Sanal Sunucuyu (Virtual Server) gösterir. Sanal Sunucu, FortiWeb'in trafiği dinlediği ve gelen istekleri gerçek sunuculara yönlendirdiği mantıksal bir arayüzdür. "WebFarmCluster", "WebGoat", "ML-VirtualServer" gibi isimler görüyorsunuz.
* **VIP**: Sanal Sunucunun IP adresini gösterir. Bu IP adresi, dışarıdan gelen trafiğin FortiWeb cihazına ulaşmak için kullandığı adrestir. Örnek olarak, "10.1.50.221/24" veya "10.1.50.111/24" gibi adresler görüyorsunuz.
* **Port**: FortiWeb'in trafiği dinlediği port numarasını gösterir. Tabloda çoğunlukla "port2" kullanıldığını görüyorsunuz.
* **Protocol**: Politikanın hangi ağ protokolü üzerinde çalıştığını belirtir. Tabloda "HTTP" ve "HTTP, HTTPS" protokolleri kullanıldığını görüyorsunuz.
* **Deployment Mode**: FortiWeb'in trafiği nasıl işlediğini gösterir.
* "Single Server/Server Balance": Bu mod, FortiWeb'in gelen trafiği tek bir sunucuya yönlendirebileceği veya birden fazla arka uç sunucusu arasında dengeleyebileceği anlamına gelir.
* "HTTP Content Routing": Bu mod, gelen isteğin içeriğine (örneğin URL'ye veya başlıklarına) göre farklı sunuculara yönlendirileceğini belirtir.
* **Web Protection Profile**: Bu, FortiWeb'in web trafiğini korumak için kullandığı güvenlik ayarlarını içeren profildir. Bu profil, XSS (Cross-Site Scripting), SQL Injection gibi saldırılara karşı koruma, bot koruması, imza tabanlı saldırı tespiti gibi özellikleri içerir.
* "Inline Web": Gelen trafiği aktif olarak tarayan ve zararlı olarak algılananları engelleyen bir profil.
* "Inline Extended Protection": Daha kapsamlı ve detaylı koruma sağlayan bir profil.
* "Inline Alert Only": Sadece uyarı veren, trafiği engellemeyen bir profil.
* **Monitor Mode**: Politikanın izleme modunu belirtir. Tabloda tüm politikalar "Disable" (Devre Dışı) olarak görünüyor. "Enable" (Etkin) olması durumunda, trafik pasif olarak izlenir ve anormallikler raporlanır ancak engellenmez.
* **Status**: Politikanın mevcut durumunu gösterir. Tabloda tüm politikaların "Running" (Çalışıyor) durumunda olduğunu görüyorsunuz, bu da politikaların etkin ve trafik üzerinde işlem yaptıkları anlamına gelir.

### ****Web Protection Profile:****

Burada, Server Policy’lerde kullanılmak üzere tanımlanan **güvenlik profilleri** yer alır. İçerisinde XSS, SQL Injection, URL filtreleme, cookie güvenliği gibi **web uygulaması güvenliğiyle ilgili koruma ayarları** bulunur. Web trafiğini analiz edip zararlı içeriği engelleyen asıl kurallar buradadır.

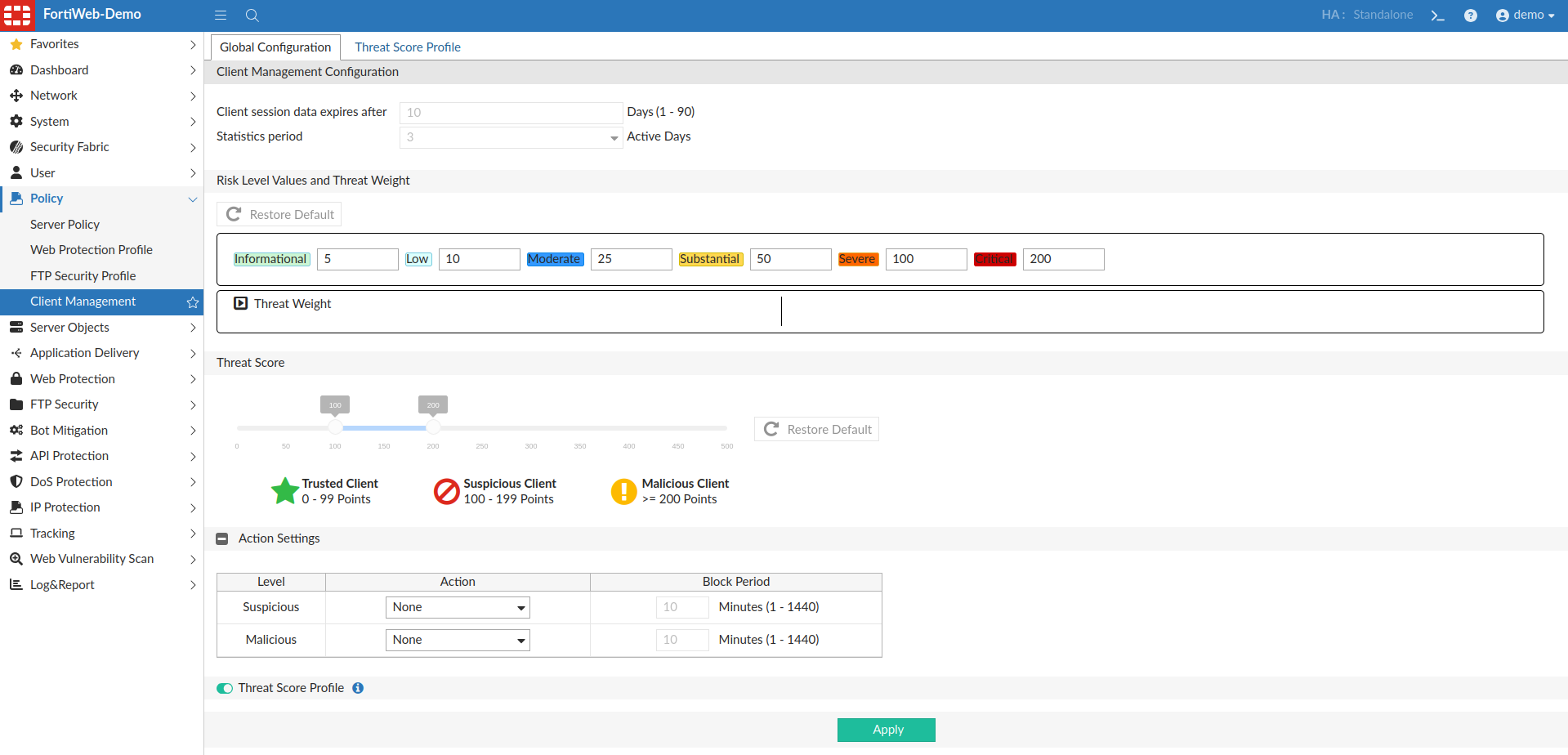
****

### ****FTP Security Profile:****

FTP trafiği kullanılıyorsa, bu trafiğe uygulanacak güvenlik önlemleri bu profilde tanımlanır. Komut kontrolü, dosya filtreleme gibi FTP’ye özel saldırılara karşı koruma sağlar. Web tabanlı sistemlerin yanında FTP servisleri kullanan yapılar için gereklidir.

### ****Client Management:****

FortiWeb üzerinden erişim yapan istemcilerin (client’ların) **takibi, kontrolü ve sınırlandırılması** için kullanılır. IP bazlı veya oturum bazlı sınırlamalar uygulanabilir. Aynı zamanda belirli kullanıcı gruplarına özel kısıtlamalar da buradan yönetilir.

****

**Fortiweb Application Delivery:**

* **URL Rewriting (URL Yeniden Yazma):**

**Gelen bir isteğin URL'sini, gerçek sunucuya iletilmeden önce otomatik olarak değiştirmenizi sağlar. Bu, arka uç sunucularının karmaşık URL yapılarını gizlemek veya yönlendirmeler yapmak için kullanılır.**

* **Site Publish (Site Yayımlama):**

Bu seçenek, FortiWeb'in bir "reverse proxy" (ters vekil) gibi davranarak arka uçtaki gerçek web sunucularını internete açmasını sağlar. Dışarıdan gelen tüm trafik önce FortiWeb'e gelir, o da gerekli kontrolleri yapıp trafiği iç ağdaki sunucuya yönlendirir.

* **Compression (Sıkıştırma):**

Web içeriğini (HTML, CSS, JavaScript vb.) sunucudan istemciye gönderilmeden önce sıkıştırarak veri boyutunu azaltır. Bu, sayfa yükleme sürelerini hızlandırır ve bant genişliği kullanımını düşürür.

* **Scripting (Betik Oluşturma):**

Gelen trafiğe özel, karmaşık kurallar veya işlem mantığı eklemenizi sağlar. Genellikle LUA betikleri kullanılarak, standart FortiWeb özelliklerinin ötesinde esnek ve özel çözümler üretmek için kullanılır.

* **Waiting Room (Bekleme Odası):**

Yoğun trafik durumlarında veya web sitesi kapasitesinin aşıldığı durumlarda, kullanıcıları sanal bir bekleme odasına alır. Bu sayede sunucuların aşırı yüklenmesi engellenir ve hizmetin tamamen kesilmesi yerine, kullanıcılar sırayla siteye alınır. Bu, özellikle bilet satışları veya kampanya dönemleri gibi yüksek trafik beklentisi olan zamanlarda kullanılır.

**FortiWeb Web Protection:**

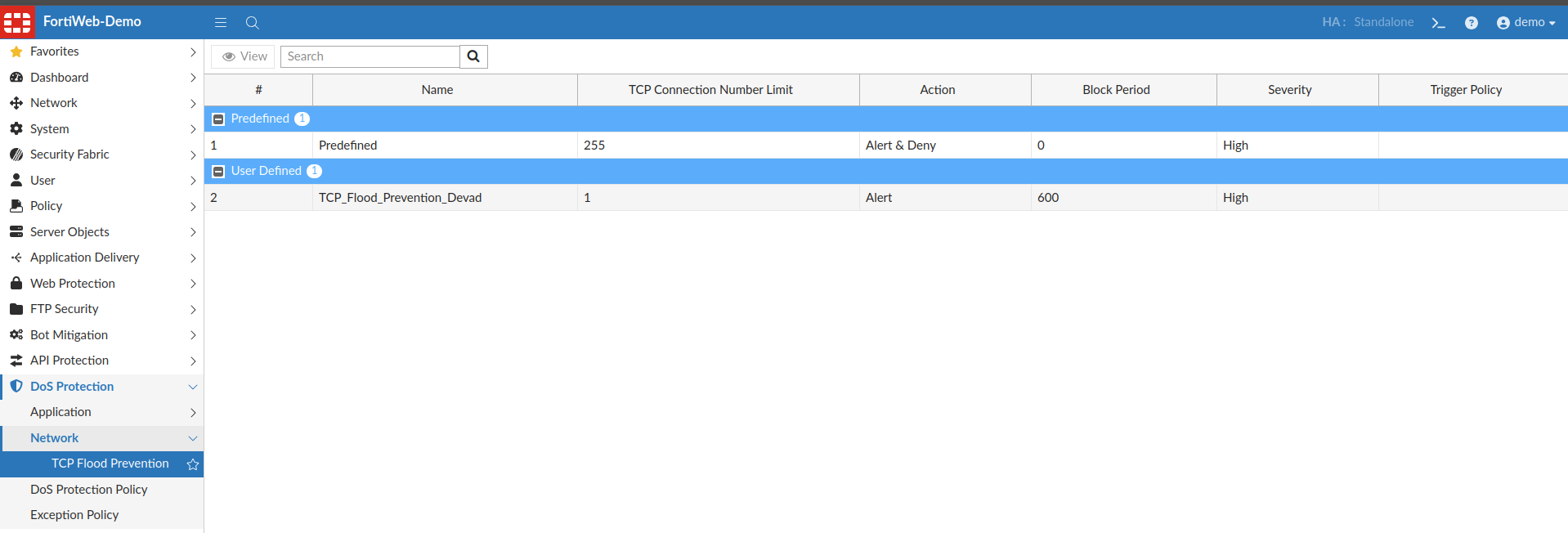
* **Known Attacks: Bu bölüm, en yaygın ve bilinen web saldırılarına karşı koruma sağlar. FortiWeb, bu saldırıları imzalar (signature) aracılığıyla tanır ve engeller. Örnek olarak SQL Enjeksiyonu (SQL Injection), Siteler Arası Betik Çalıştırma (Cross-Site Scripting - XSS) gibi saldırılar bu kategoriye girer.**
* **Advanced Protection:** Bu bölüm, daha karmaşık ve gelişmiş saldırılara karşı koruma sağlar. İçeriğinde genellikle oturum güvenliği (session security), otomatik istek doğrulama (auto-learning), anormal davranış tespiti gibi özellikler bulunur.
* **Cookie Security:** Web sitelerinin kullandığı çerezlerin (cookies) güvenliğini sağlamaya yönelik ayarları içerir. Çerezlerin şifrelenmesi, bütünlüğünün kontrol edilmesi ve saldırganlar tarafından manipüle edilmesinin önlenmesi gibi işlevleri vardır.
* **Data Loss Prevention:** Web sunucunuzdan dışarıya hassas verilerin (örneğin kredi kartı numaraları, kimlik numaraları) sızmasını engeller. FortiWeb, giden trafiği tarayarak tanımlanmış kalıplara uyan verilerin dışarı çıkmasını engeller veya loglar.
* **Input Validation:** Web formlarına veya URL'lere girilen verilerin geçerliliğini ve güvenliğini kontrol eder. FortiWeb, önceden tanımlanmış kurallara uymayan (örneğin beklenmedik karakterler içeren) girdileri engelleyerek saldırıları önler.
* **Protocol:** HTTP/HTTPS protokollerinin kurallarına aykırı olan istekleri tespit edip engeller. Örneğin, protokol standartlarına uymayan bozuk veya manipüle edilmiş istek başlıklarını (header) reddeder.
* **Access:** Kimin hangi kaynaklara erişebileceğini kontrol etmek için kullanılır. IP adresi bazlı erişim kontrolü, kullanıcı kimlik doğrulaması veya URL bazlı yetkilendirme gibi ayarlar bu bölümde yapılır.
* **ML Based Anomaly Detection:** Makine öğrenimi (Machine Learning) kullanarak web sitesinin normal davranışını öğrenir ve bu normal davranıştan sapmaları (anomalileri) tespit eder. Bu, imzası henüz bilinmeyen (zero-day) yeni saldırı türlerine karşı koruma sağlar.
* **Web Anti-Defacement:** Web sitenizin içeriğinin izinsiz bir şekilde değiştirilmesini (tahrif edilmesini) engeller. FortiWeb, web sayfalarının içeriğini periyodik olarak kontrol eder ve herhangi bir değişiklik tespit ettiğinde siteyi orijinal haline geri yükler veya uyarı verir.

**FortiWeb Bot Mitigation:**

* **Biometrics Based Detection: Bu özellik, kullanıcının davranışlarını analiz ederek insan ile botu ayırt etmeye çalışır. Örneğin, fare hareketleri, klavye kullanım hızı gibi kullanıcı davranışlarının biyometrik verilerini değerlendirerek anormal davranış sergileyenleri bot olarak tanımlar.**
* **Threshold Based Detection:** Bu, belirli bir zaman diliminde gelen istek sayısını veya bir IP adresinden gelen trafiği izleyerek anormal trafiği tespit eder. Örneğin, bir IP adresinden saniyede 100'den fazla istek geliyorsa bunu bir bot saldırısı olarak algılayıp engelleme kuralı tanımlanabilir.
* **Bot Deception:** Bu özellik, kötü niyetli botları yanıltmak için tasarlanmıştır. Botları, insan kullanıcıların görmediği gizli bağlantılara veya sayfalara yönlendirerek onları tuzağa düşürür ve zararsız gibi görünen bu isteklerle meşgul ederek gerçek web içeriğine zarar vermelerini engeller.
* **Known Bots:** FortiWeb'in sürekli güncellenen bot imza veritabanını kullanarak bilinen iyi niyetli (örneğin, Google arama botları) ve kötü niyetli botları tanıyıp buna göre işlem yapmasını sağlar. İyi niyetli botlara izin verilirken, kötü niyetli botlar engellenir.
* **ML Based Bot Detection:** Makine öğrenimi (Machine Learning) algoritmalarını kullanarak web trafiğindeki kalıpları öğrenir ve normal trafikten sapmaları, yani bot davranışlarını, tespit eder. Bu yöntem, imza tabanlı algılamanın yetersiz kaldığı yeni ve bilinmeyen bot türlerine karşı etkilidir.
* **Advanced Bot Protection:** Bu bölüm, botlara karşı daha sofistike koruma mekanizmaları sunar. Bu, genellikle botların davranışlarını daha derinlemesine analiz eden ve daha detaylı kurallar belirlemenizi sağlayan gelişmiş özellikler içerir.
* **Exception Policy:** Bu politika, bot algılama kurallarının belirli koşullarda uygulanmamasını sağlamak için kullanılır. Örneğin, belirli bir IP adresinden veya kullanıcı aracısından gelen trafiği bot kontrolünden muaf tutmak istediğinizde bu bölümü kullanırsınız.

**FortiWeb Dos Protection:**

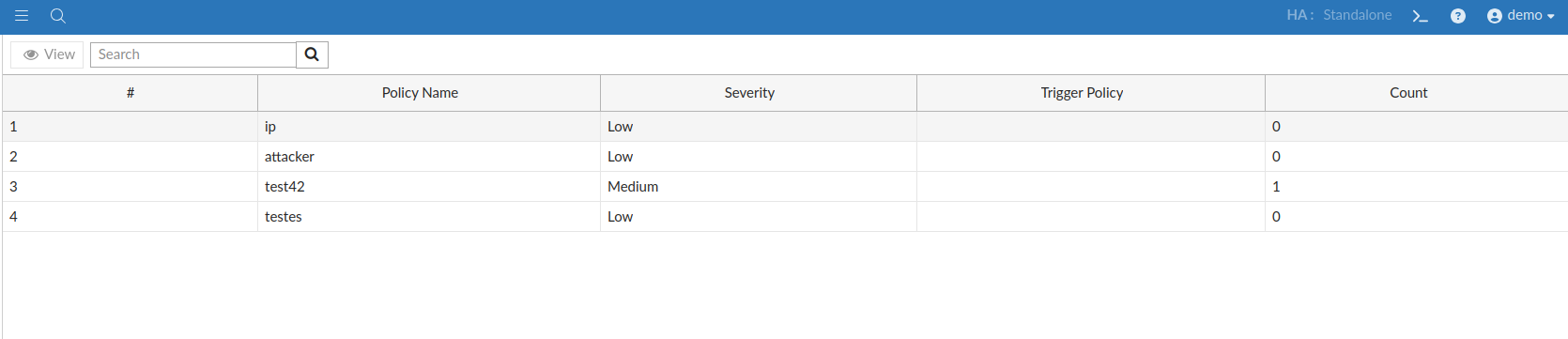
* **Application**: Bu bölüm, web uygulaması katmanındaki (HTTP/HTTPS) DoS saldırılarına karşı koruma sağlamak için kullanılır. Bu tür saldırılar genellikle sunucuyu aşırı miktarda geçerli gibi görünen web isteğiyle (örneğin, HTTP GET veya POST) boğarak kaynaklarını tüketmeyi hedefler. Burada, saniyedeki istek sayısı (RPS), eş zamanlı oturum sayısı gibi uygulama seviyesindeki limitler ve kurallar belirlenir.
* **Network:** Bu bölüm, daha alt seviyeli, ağ katmanındaki DoS saldırılarına (örneğin, TCP SYN flood) karşı koruma sağlamak için kullanılır. Bu saldırılar, sunucuya çok sayıda tamamlanmamış bağlantı isteği göndererek sunucunun bağlantı tablosunu doldurmayı hedefler. FortiWeb, bu bölümdeki ayarlar sayesinde anormal TCP veya UDP paketlerini tespit ederek bu tür saldırıları engeller.
* **DoS Protection Policy**: Bu bölüm, hem Uygulama hem de Ağ seviyesinde tanımladığınız koruma profillerini, hangi sanal sunuculara veya politikalara uygulayacağınızı belirlediğiniz yerdir. Bir nevi, DoS koruma ayarlarını toplayıp belirli bir web uygulamasına atadığınız ana yönetim noktasıdır.
* **Exception Policy**: DoS koruma kurallarının, belirli IP adresleri veya kullanıcı grupları için uygulanmamasını sağlamak amacıyla kullanılır. Örneğin, web sitenizin yöneticilerinin kullandığı IP adreslerini DoS koruma kurallarından muaf tutarak onların siteye erişiminin engellenmediğinden emin olmak için bu bölümden istisna tanımlayabilirsiniz.

****

* **#: Kuralın sıra numarasıdır.**
* **Name:** Kurala verilen addır. "Predefined" (Ön Tanımlı) ve "User Defined" (Kullanıcı Tanımlı) olmak üzere iki ana grup altında toplanır.
* **TCP Connection Number Limit:** Bu, bir IP adresinden belirli bir zaman aralığında gelebilecek maksimum eşzamanlı TCP bağlantı isteği (SYN paketi) sayısını belirler. Bu limit aşıldığında, FortiWeb belirlenen eylemi gerçekleştirir.
* Örnekteki "Predefined" kuralında bu limit 255 olarak belirlenmiş.
* "TCP\_Flood\_Prevention\_Devad" adlı kullanıcı tanımlı kuralda ise bu limit 1 olarak belirlenmiş, bu da çok daha sıkı bir kural olduğu anlamına gelir.
* **Action (Eylem):** Belirlenen limit aşıldığında FortiWeb'in ne yapacağını gösterir.
* "Predefined" kuralındaki eylem "Alert & Deny" (Uyar ve Engelle) olarak ayarlanmış. Bu, limit aşıldığında hem yöneticilere uyarı gönderileceği hem de o IP adresinden gelen bağlantı isteklerinin engelleneceği anlamına gelir.
* "TCP\_Flood\_Prevention\_Devad" kuralındaki eylem ise sadece "Alert" (Uyar) olarak ayarlanmış. Bu, limit aşıldığında yalnızca uyarı verileceği, ancak trafiğin engellenmeyeceği anlamına gelir.
* **Block Period (Engelleme Süresi):** Eğer eylem "Deny" veya "Alert & Deny" olarak ayarlandıysa, saldırgan IP adresinin ne kadar süreyle engelleneceğini belirler. Birimi saniyedir.
* "Predefined" kuralında süre 0 saniye olarak belirtilmiş, bu genellikle eşik değerinin aşılması durumunda anlık bir engelleme veya eylemin sürekli olarak geçerli olması anlamına gelebilir.
* "TCP\_Flood\_Prevention\_Devad" kuralında süre 600 saniye (10 dakika) olarak belirlenmiş. Bu, kuralı ihlal eden bir IP adresinin 10 dakika boyunca engelleneceği anlamına gelir.
* **Severity (Ciddiyet):** Bu kuralın log kayıtlarına veya raporlara yansıtılacak olan ciddiyet seviyesidir. Saldırının ne kadar önemli olduğunu belirtir. Her iki kuralda da ciddiyet seviyesi "High" (Yüksek) olarak ayarlanmış.
* **Trigger Policy (Tetikleyici Politika):** Bu sütun, bu kuralın hangi DoS koruma politikası ile ilişkilendirildiğini gösterir. Bu örnekte sütun boş, bu da bu kuralların doğrudan bir politikaya atanmadığını veya başka bir şekilde yönetildiğini gösterebilir.

**FortiWeb IP Protection:**

* **IP List:** Bu menüde, FortiWeb'in trafiğe karşı nasıl davranacağını belirlemek için özel olarak IP adres listeleri oluşturursunuz.
  + **Blacklist:** Belirlenen IP adreslerinden gelen tüm trafiği engellemek için kullanılır. Bu, bilinen saldırgan IP'lerini veya istenmeyen kaynakları dışlamak için idealdir.
  + **Whitelist:** Sadece belirlenen IP adreslerinden gelen trafiğe izin vermek için kullanılır. Genellikle iç ağdaki yöneticilerin veya güvenilir iş ortaklarının erişimini sağlamak amacıyla kullanılırken, diğer tüm IP'lerden gelen trafiği engeller.
  + Bu listeler, manuel olarak oluşturulabileceği gibi, FortiWeb'in diğer güvenlik özellikleri tarafından otomatik olarak da güncellenebilir (örneğin, bir saldırı tespit edildiğinde IP'nin kara listeye eklenmesi gibi).



* **GEO IP:** Bu özellik, trafiğin coğrafi konumuna (ülkesine) göre erişim kontrolü sağlar.
  + Örneğin, belirli bir ülkeden gelen trafiğin tamamını engellemek (örneğin, bir hizmeti sadece Türkiye'deki kullanıcılara sunuyorsanız) veya belirli bir ülkeden gelen trafiğe sadece uyarı vermek için kullanılır.
  + Bu, sıkça siber saldırıların kaynaklandığı bilinen bölgelerden gelen trafiği önlemeye yardımcı olabilir.
* **IP Reputation:** FortiGuard Labs'ın sürekli güncellediği global bir kötü niyetli IP adresi veritabanına dayanır.
  + Bu veritabanı, spam gönderen, kötü amaçlı yazılım dağıtan veya diğer siber suçlarla ilişkili olduğu bilinen IP adreslerini içerir.
  + FortiWeb, gelen trafiği bu veritabanındaki IP'lerle karşılaştırır. Gelen istek kötü niyetli bir IP adresinden geliyorsa, trafiği otomatik olarak engeller veya belirlediğiniz başka bir eylemi gerçekleştirir. Bu sayede, bilinen tehditlere karşı proaktif bir koruma sağlanır.