epati

Güvenlik Duvarı Ayarları

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı

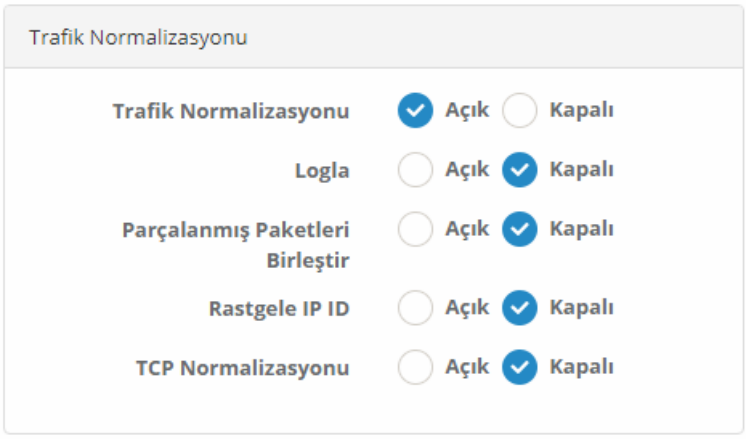
Kılavuzlar

www.epati.com.tr

Güvenlik Duvarı Ayarları

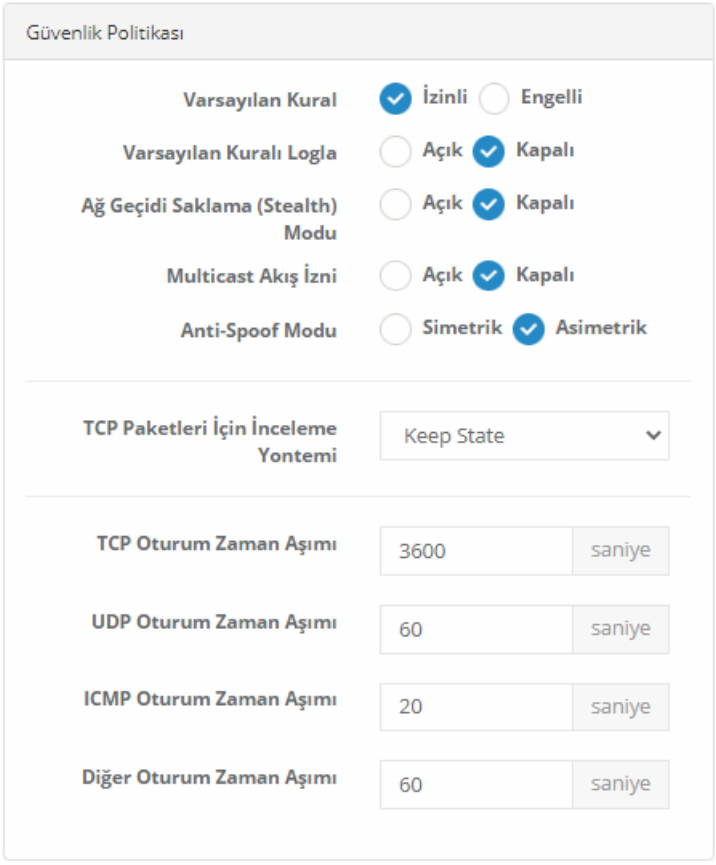
Güvenlik duvarı için trafik normalizasyonu, güvenlik politikası, form varsayılanları ve DoS Engelleme - Bağlantı Limitleri ayarları bu bölümden yapılmaktadır.

Trafik Normalizasyonu



İnternet üzerinde, gelen ve giden paketler, her zaman istenildiği gibi ideal olmayabilmektedir. Bunun birden fazla sebebi olabilir. Bunlardan birisi yanlış yapılandırılmış, yönlendirici (router) ayarlarından kaynaklanıyor olabilir. Dahası, kötü niyetli kişilerin, TCP/IP yapısını suistimal etme işlemlerinde, genellikle kirli (defragmented) paketleri kullanılmaktadır. Bu suistimallerin çözümlenmesi hususunda Trafik Normalizasyonu kullanılmaktadır.

Güvenlik Politikası



Kurala uyan paketlerin durum bilgilerinin tutulmasında kullanılan yönergedir. Durum Denetimi (Stateful Inspection) 'ni göz önünde bulundurmaktadır. İstemcilerin, Güvenlik Duvarı üzerinden yaptıkları erişim bilgileri bir tablo içerisinde tutulur. Bu erişime geri dönen cevaplar, Güvenlik Duvarı içerisinde yer alan Durum(state) tablosundan kontrol edilir. Eğer istek durum tablosu içerisinde varsa, yani içeriden gelen bir isteğin devamı ise, paketin içeriye girmesine izin verilir. Aksi taktirde, paket düşürülür.

Varsayılan Kural

ALAN	AÇIKLAMA
Varsayılan Kural	Engelli ise güvenlik kuralları izin verilen portlar (TCP, UDP) harici tüm portlar engellenecektir.
Varsayılan Kuralı Logla	Logla seçildiğinde, varsayılan kuralla eşleşen trafik loglanır.
Ağ Geçidi Saklama (Stealth) Modu	Daha fazla ağ güvenliği için Gizli Mod açılabilir. Temel olarak, görünmezlik özelliği sunar.
Multicast Akış İzni	Özellik açıldığında Multicast trafiğine ait option parametresine izin verilir. Güvenlik duvarı ayarları “Varsayılan Engelle” olarak kullanılıyor ise, Multicast ip adreslerine izin verecek güvenlik kuralı yazılmalıdır. Güvenlik duvarı ayarları “Varsayılan İzinli” olarak kullanılıyor ise, Multicast trafiği için bu özelliğin açılması yeterli olacaktır.
Anti-Spoof Modu	Simetrik modda iken paketler dönerken atladığı yönlendirme noktalarını takip ederken, asimetrik modda farklı rota kullanmaktadır.

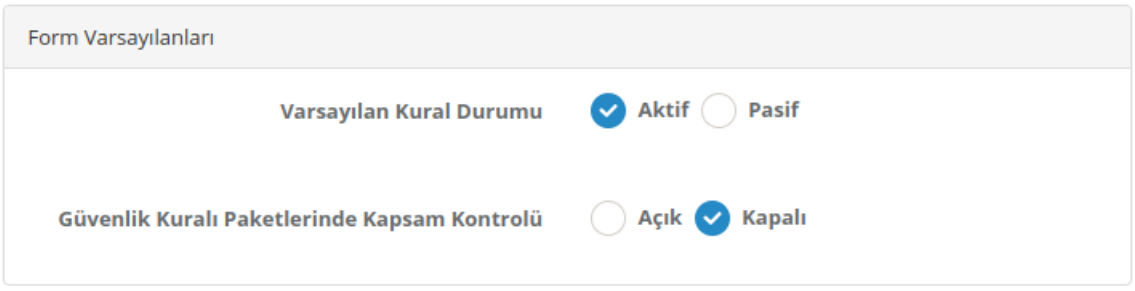
Not: Varsayılan Kural *Engelli* durumda ve Web Filtreleme Servisi açık ise TCP 80 (HTTP portu) ve 443 (HTTPS Portu) portuna Güvenlik Kurallarında izin verilmelidir. Aksi halde bu portlarda da engel uygulanacaktır.

TCP Paketleri İçin İnceleme Yontemi

ALAN	AÇIKLAMA
Keep State	Sadece durum kontrolü yapılır. Bu durum kontrolü TCP, UDP ve ICMP protokolleri için geçerlidir.
Modulate State	TCP protokolü içerisinde akmaya başlayan bir veride, ISN(Initial Sequence Number) bölümünün güçlendirilmesi için kullanılmaktadır. Genellikle TCP/IP katmanındaki boşlukların suistimaline karşı alınmış bir önlemdir. Bu durum sadece TCP protokolü için geçerlidir.
Syn Proxy	Özellikle SYN saldırılarında kullanılan bir durumdur. (Spoofed TCP SYN Flooding Attacks) Yalancı ağlardan gelerek, TCP SYN baskın saldırısını kullanan, kötü niyetli kişilerin saldırılarından korunmak için oluşturulmuş bir tampon alan, Güvenlik Duvarı tarafından oluşturulur. TCP bağlantıları bu tampon alandan geçerken, bütün SYN paketleri direk olarak alıcısına teslim edilmeden, 3 aşamalı el sıkışma prosedürüne tam olarak uyup uymadığı kontrol edilir. Bu prosedüre uymadan gelen, SYN paket baskınları (art arda gönderilen tüm SYN paketleri), Güvenlik Duvarı tarafından alıcısına teslim edilmez ve düşürülür. Bu sayede SYN baskın saldırılarının önüne geçilmiş olur. Syn Proxy state yönergesi aynı zamanda hem Keep State yönergesini hem de Modulate State yönergelerinide kendi içerisinde barındırmaktadır.

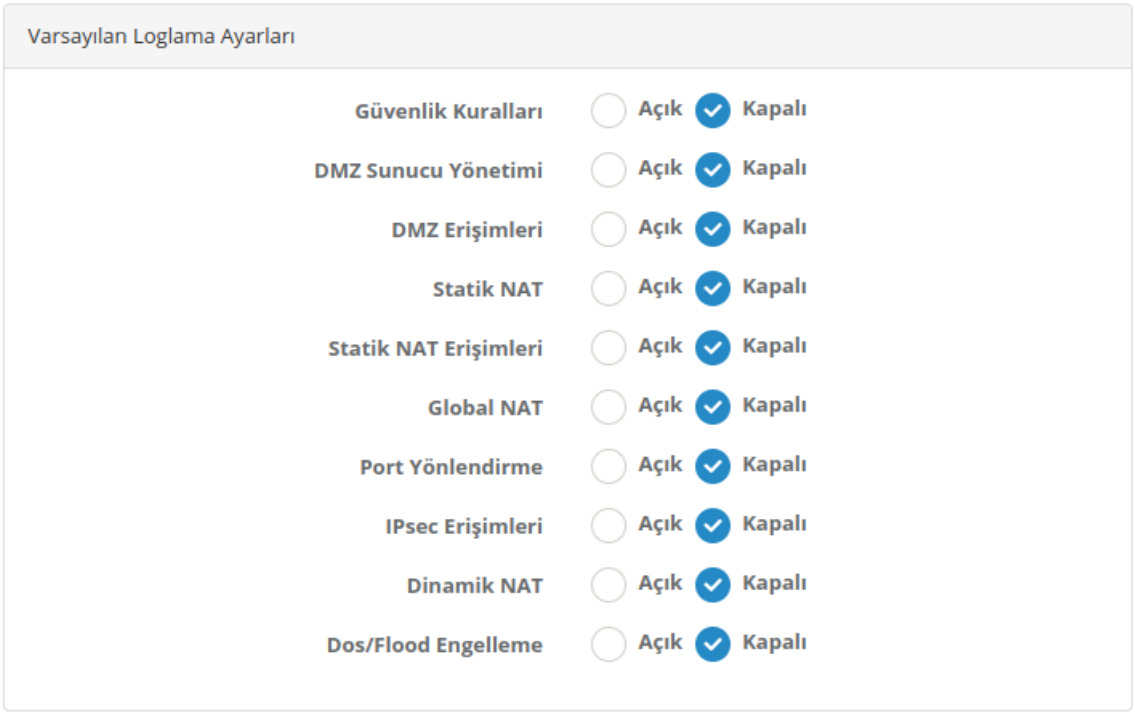
Protokol bazlı varsayılan zaman aşımı yapılandırması bulunmaktadır. Varsayılan TCP zaman aşımı 3600 ms dir.

Form Varsayılanları



Güvenlik kurallarına eklenecek yeni kurallar için varsayılanda *Aktif* veya *Pasif* gelişi ayarlanmaktadır.

Varsayılan Loglama Ayarları



İlgili özelliklerin varsayılan olarak loglanmasının açık veya kapalı olacağı seçilir

DoS Engelleme - Bağlantı Limitleri

Dos (Denial Of Service- Servis Hizmet Reddi) saldırısı bir hedefe yönelik gerçekleştirilen, sistemin hizmet vermesini, kullanıcıların sisteme erişmesini engelleyen bir saldırı türüdür. Sisteme erişimin engellenmemesi açısından kişi başı maximum bağlantı sayısı ve 5 saniyede maximum bağlantı sayısı limitlendirilebilmektedir. Bu limitler aşıldığı takdirde saldırı yapanın engellenme süresi kullanıcı tarafından belirlenebilmektedir.

Posta Kodu: 33345 Tehişehir / MERSİN
+90 324 361 02 39