

epati

Güvenlik Kuralları Yapılandırması

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı
Yapılandırma Örnekleri

Güvenlik Kuralları Yapılandırması

Kısa Anlatım

Antikor NGFW istemcisinde istenmeyen herhangi bir IP ve/veya portun engellenmesinin nasıl yapılacağı anlatılmıştır.

Network Şeması

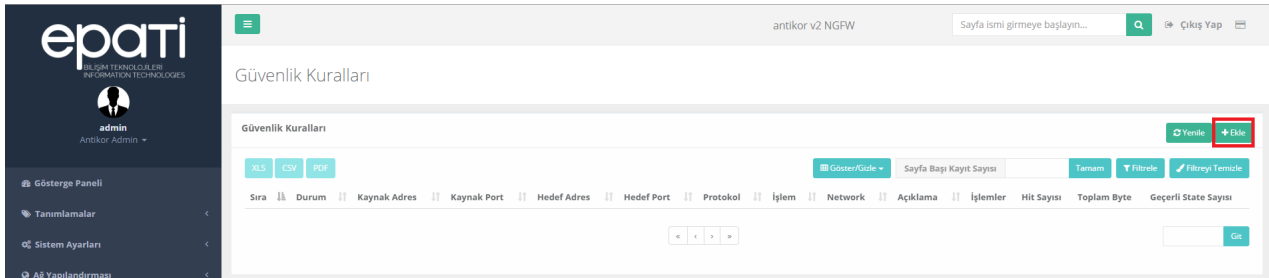


Konfigürasyon

İlk olarak **Güvenlik Ayarları** menüsünün içinde bulunan **Güvenlik Kuralları** açılmalıdır.



Güvenlik Kurallarında **Ekle** butonuna tıklanılmalıdır.



Örnek 1 (IP Adresini Engelleme/NATlı Geçirme)

- Genel Kurallar'da **İşlem;Engelle** seçildi ve **Açıklama** girildi.
- **IP Kurallarında Kaynak Adres** olarak istemcinin tabi olduğu LAN1 IP Bloğu (192.168.100.0/24) girildi.
- **Hedef Adres** olarak 212.101.122.34 IP adresi girildi.

- **Protokol** olarak **IP** seçildi.
- Network olarak **Tümü** seçildi.

Güvenlik Kuralları - Yeni Kayıt

Genel Kurallar

Sıra No:

Durum: Aktif

İşlem: Engelle

Trafiği Logla: Kapalı

Paket Yönü: Her İki Yön

Açıklama: IP Engel Kuralı

İnceleme Yöntemi: Statefull

Bayraklar: İzinli Engelli

IP Kuralları

Kaynak Adres: Listedekiler Hariç
192.168.100.0/24

Hedef Adres: Listedekiler Hariç
212.101.122.34/32

Protokol: IP

Kaynak Port: Listedekiler Hariç

Hedef Port: Listedekiler Hariç

Network: Tümü

Bağlantı Sayısı Limitleri

Bağlantı Sayısı Limitle:

Kişi Başı Maximum Bağlantı Sayısı:

5 Saniyede Maximum Bağlantı Sayısı:

Zamanlayıcı

Saat Dilimi:

- Ayarlar girildikten sonra **Kaydet** butonuna tıklanır.

epati
BİLGİ TEKNOLOJİLERİ
INFORMATION TECHNOLOGIES

admin
Antikör Admin

- Gösterge Paneli
- Tanımlamalar
- Sistem Ayarları
- Ağ Yapılandırması
- Duyuru ve Form Yönetimi

antikor v2 NGFW Staging - STAGING Sayfa ismi girmeye başlayın...

Güvenlik Kuralları Güncelleştirmeler Hazır

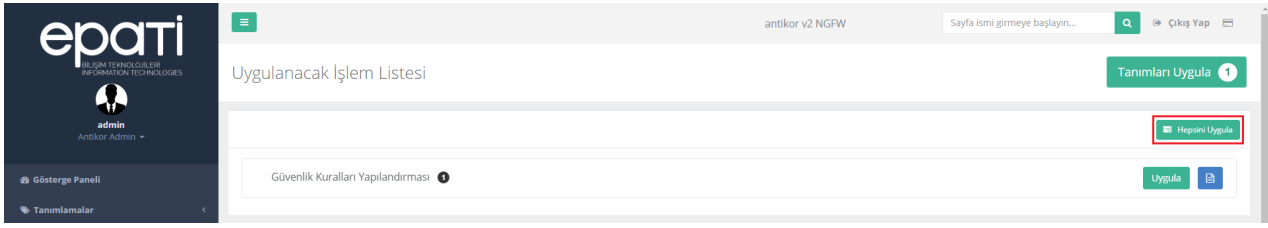
Güvenlik Kuralları Yenile Ekle

XLS CSV PDF Göster/Gökle Sayfa Başı Kayıt Sayısı Tamam Filtrele Filtreyi Temizle

Sıra	Durum	Kaynak Adres	Kaynak Port	Hedef Adres	Hedef Port	Protokol	İşlem	Network	Açıklama	İşlemler	Hit Sayısı	Toplam Byte	Geçerli State Sayısı
0	Aktif	192.168.100.0/24		212.101.122.34/32		IP	Engelle	Tümü	IP Engel Kuralı	<input type="button" value="Gör"/> <input type="button" value="Sil"/> <input type="button" value="Yenile"/> <input type="button" value="Ekle"/>	0	0	0

NAT'ı Geç İşlemi İçin;

- Genel Kurallar'da **İşlem**; NAT'ı Geç seçildi ve **Açıklama** girildi.
- **IP Kurallarında** **Kaynak Adres** olarak istemcinin tabi olduğu LAN1 IP Bloğu (192.168.100.0/24) girildi.
- **Hedef Adres** olarak 185.195.231.35 IP adresi girildi.
- **Protokol** olarak **IP** seçildi.
- Network olarak **Tümü** seçildi.
- Sonuç olarak 192.168.100.0/24 bloğunda olan bir istemci 185.195.231.35 IP adresine giderken Güvenlik Duvarı üzerinden NAT'ı geçerek hedefine ulaşacak.



Örnek 2 (Port Engelleme)

- Genel Kurallar'da **İşlem;Engelle** seçildi ve **Açıklama** girildi.
- **IP Kurallarında Kaynak Adres** olarak istemcinin tabi olduğu LAN1 IP Bloğu (192.168.100.0/24) girildi.
- **Hedef Adres** olarak **tümü seçildi**.

Hedef Adres

Protokol **Tümünü Seç**

Kaynak Port IPv4 IPv6

Hedef Port

- **Protokol** olarak **TCP** seçildi.
- **Kaynak Port** olarak **tümü seçildi**.

Kaynak Port

Hedef Port **Tümünü Seç**

Network

Network

- **Hedef Port** olarak TCP 80, TCP 443 ve TCP 7001-7002 harici (Listedekiler Hariç İşaretlendi) tüm portlar seçilmiş oldu.
- Network olarak **Tümü** seçildi.
- **Zamanlayıcı** ile kuralın hafta içi mesai saatleri içinde etkin olması sağlandı. (Hafta İçi 08:00 - 17:00)

Genel Kurallar

Sıra No

Durum Aktif

İşlem Engelle

Trafiği Logla Kapatı

Paket Yönü Her İki Yön

Açıklama TCP Port Engeli

İnceleme Yöntemi Statefull

Bayraklar İzinli Engelli

Seçiniz... Seçiniz...

IP Kuralları

Listedekiler Hariç

Kaynak Adres 192.168.100.0/24

Listedekiler Hariç

Hedef Adres 0.0.0.0/0 ::/0

Protokol TCP

Listedekiler Hariç

Kaynak Port TCP 1-65535

Listedekiler Hariç

Hedef Port TCP 80 TCP 443 TCP 7001 - 7002

Network Tümü

Bağlantı Sayısı Limitleri

Bağlantı Sayısı Limite

Kişi Başı Maximum Bağlantı Sayısı

5 Saniyede Maximum Bağlantı Sayısı

Zamanlayıcı

Saat Dilimi Hafta İçi 08:00 - 17:00

- Ayarlar girildikten sonra **Kaydet** butonuna tıklanır.

epati BİLGİ TEKNOLOJİLERİ INFORMATION TECHNOLOGIES

admin Antikor Admin

Gösterge Paneli Tanımlamalar Sistem Ayarları Ağ Yapılandırması Duyuru ve Form Yönetimi

antikor v2 NGFW Sayfa ismi girmeye başlayın...

Güvenlik Kuralları Tanımları Uygula

Güvenlik Kuralları

XLS CSV PDF Göster/Göle Sayfa Başı Kayıt Sayısı Tamam Filtrele Filtreyi Temizle

Sıra	Durum	Kaynak Adres	Kaynak Port	Hedef Adres	Hedef Port	Protokol	İşlem	Network	Açıklama	İşlemler	Hit Sayısı	Toplam Byte	Geçerli State Sayısı
0	Aktif	192.168.100.0/24	TCP 1-65535	0.0.0.0	TCP 80 TCP 443 TCP 7001-7002	TCP	Engelle	Tümü	TCP Port Engeli		0	0	0

- Tanımlar uygulanarak yapılandırma tamamlanır.

epati BİLGİ TEKNOLOJİLERİ INFORMATION TECHNOLOGIES

admin Antikor Admin

Gösterge Paneli Tanımlamalar Sistem Ayarları Ağ Yapılandırması Duyuru ve Form Yönetimi

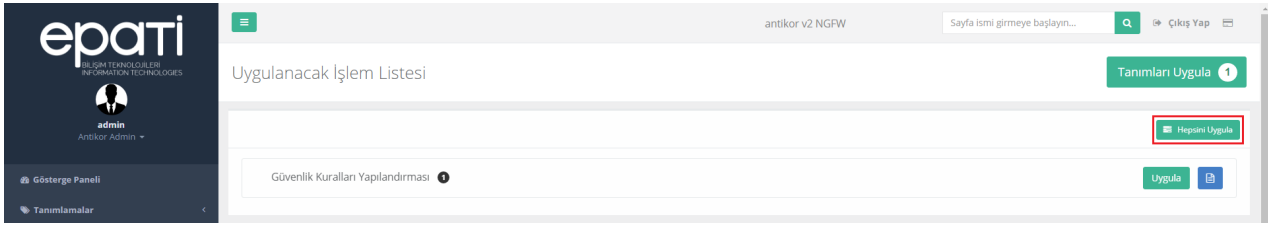
antikor v2 NGFW Sayfa ismi girmeye başlayın...

Güvenlik Kuralları Tanımları Uygula

Güvenlik Kuralları

XLS CSV PDF Göster/Göle Sayfa Başı Kayıt Sayısı Tamam Filtrele Filtreyi Temizle

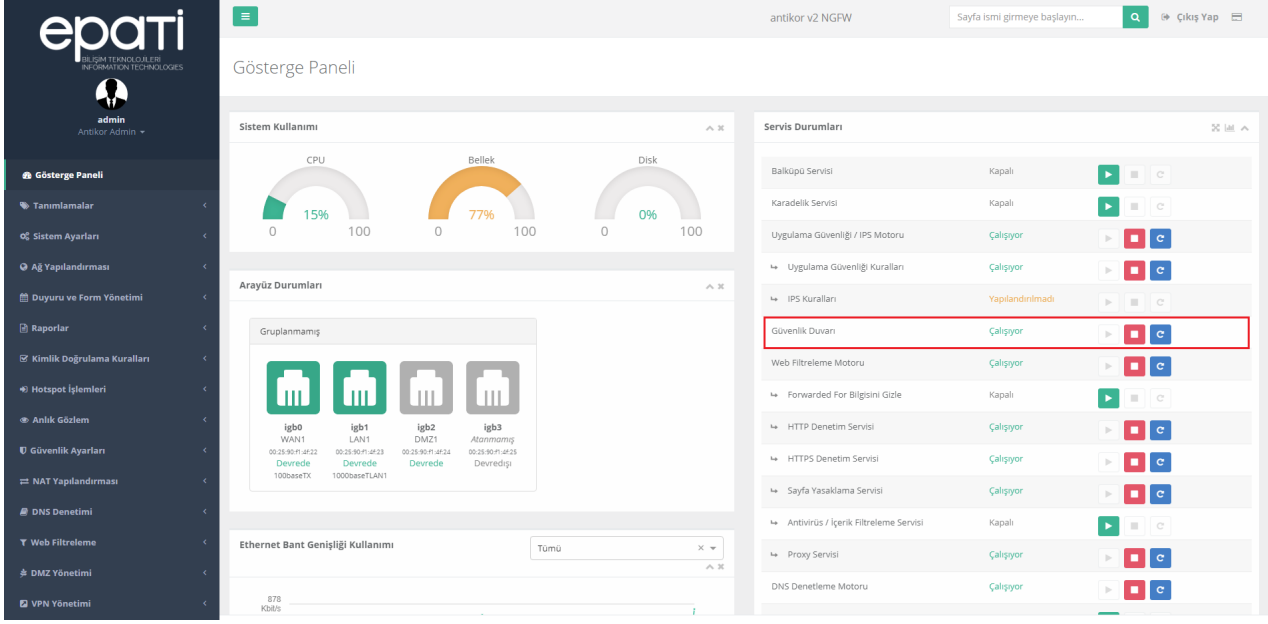
Sıra	Durum	Kaynak Adres	Kaynak Port	Hedef Adres	Hedef Port	Protokol	İşlem	Network	Açıklama	İşlemler	Hit Sayısı	Toplam Byte	Geçerli State Sayısı
0	Aktif	192.168.100.0/24	TCP 1-65535	0.0.0.0	TCP 80 TCP 443 TCP 7001-7002	TCP	Engelle	Tümü	TCP Port Engeli		0	0	0



Dip Not: Yapılandırma örneği (Port Engelleme) aynı şekilde **Protokol** olarak **UDP** seçilerek de yapılabilmektedir.

Hatırlatma

- **Gösterge Panelinde** bulunan **Servis Durumlarından Güvenlik Duvarı Servisini** açmayı unutmayınız.



Not: Yapılandırma örneklerinde verilen IP adresleri, Portlar vb. veriler örnek teşkil etmesi amacı ile oluşturulmuştur. Lütfen güvenlik duvarınıza kendi topoloji ve konfigürasyonunuza uygun ayarlar giriniz.

ePati Siber Güvenlik Teknolojileri A.Ş.
Mersin Üniversitesi Çiftlikköy Kampüsü
Teknopark İdari Binası Kat: 4 No: 411
Posta Kodu: 33343 Yenişehir / MERSİN

www.epati.com.tr
bilgi@epati.com.tr
+90 324 361 02 33
+90 324 361 02 39

