epati

Güvenlik Kuralları Yapılandırması

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı Yapılandırma Örnekleri

www.epati.com.tr



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.

	8	antikor v2 NGFW	Sayfa ismi girmeye başlayın	Q 🕞 Çıkış Yap 🚍
	Güvenlik Kuralları			
admin Antikor Admin 👻	Güvenlik Kuralları			3 Yenile + Ekde
R Gösterge Paneli	XLS CSV PDF	⊞ Göster/Gizle ▼ Sayfa Baş	ji Kayit Sayisi Tamam	▼ Filtrele 🖌 Filtreyi Temizle
🗣 Tanımlamalar 🗸 🤇	Sıra 🎚 Durum Kaynak Adres Kaynak Port Hedef Adres Hedef Port Protokol	រាំ İşlem រាំ Network រាំ Açıklama	🗄 İşlemler Hit Sayısı Toplam By	yte Geçerli State Sayısı
۵\$ Sistem Ayarları				Git
C Až Vandandum as				

Örnek 1 (IP Adresini Engelleme/NATIı 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		IP Kuralları	
Sıra No			Listedekiler Hariç
Durum	Aktif	Kaynak Adres	192.168.100.0/24 ×
İşlem	Engelle		Listedekiler Hariç
Trafiği Logla	Lingelle .	Hedef Adres	212.101.122.34/32 ×
Paket Yönü	Har İki Vön	Protokol	IP •
Açıklama			Listedekiler Hariç
3	IP Engel Kurali	Kaynak Port	
İnceleme Yöntemi	Statefull		Listedekiler Hariç
Bayraklar	İzinli Engelli	Hedef Port	
	36ýmz	Network	Tümü x 🔻
Bağlantı Sayısı Limitle	eri	Zamanlayıcı	
I	Bağlantı Sayısı Limitle	Saat Dilimi	
Kişi Başı Max	kimum Bağlantı Sayısı		
5 Saniyede Max	kimum Bağlantı Sayısı		
Ayarlar girild	ikten sonra Kaydet butonuna tıklar	ıır.	
opati		antikor vž	2 NGFW Staging - STAGING Sayfa ismi girmeye başlayın Q 🐵 Çıkış Yap 🗄

enati		antikor vz NGEW Staging - STAGING Sayia bini girmeye başlayın 💘 🤤 çikiş tap 🖂
BILISM TEKNOLOJILERI INFORMATION TECHNOLOGIES	Güvenlik Kuralları	Süncelleştirmeler Hazır
admin Antikor Admin -	Güvenlik Kuralları	DYonile +Bke
	XLS CSV PDF	I Göster/Gizle → Sayfa Başı Kayıt Sayısı Tamam T Filtrele I filtreyi Temizle
Gösterge Paneli Gösterge Paneli	Sira Durum Kavnak Kavnak Hedef Adres Hedef	Protokol İslem Network Acıklama İslemler Hit Toplam Gecerli State
🗞 Tanımlamalar 🤇	Jh Jî Adres Jî Port Jî Jî Port	L1 L1 L1 L1 Sayısı Byte Sayısı
📽 Sistem Ayarları 🗸	0 Aktif 192,168,100,0/24 212,101,122,34/32	IP Engelo Túmú IPEngel (2 (2) (2) + ↓ (5) 0 0 0 Kurali
😡 Ağ Yapılandırması 🧹		c 1 > >
🚔 Duyuru ve Form Yönetimi 🛛 🔍		

NATII Geç İşlemi İçin;

- Genel Kurallar'da İşlem;NATlı 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 NATlı geçerek hedefine ulaşacak.

×

Genel Kurallar	IP Kuralları
Sira No	Listedekiler Hariç
Durum Aktif	Kaynak Adres 192.168.100.0/24 ×
işlem NATlı Gec 🔻	Listedekiler Hariç
Trafiği Logla	Hedef Adres 185.195.231.35/32 ×
Paket Yönü Her İki Yön 🔻	Protokol IP v
Açıklama NATlı Geçiş Kuralı	Listedekiler Hariç
inceleme Statefull	Reyliek FUL
Yöntemi Bayraklar İzinli Engelli	Listedekiler Hariç Hedef Port
Seçiniz Seçiniz	Notwork
	iumu x *
Bağlantı Sayısı Limitleri	Zamanlayıcı
Bağlantı Sayısı Limitle	Saat Dilimi
Kişi Başı Maximum Bağlantı Sayısı	
5 Saniyede Maximum Bağlantı Sayısı	
	Ø lptal 🛛 🖺 Kayde
• Ayarlar gırıldıkten sonra Kaydet butonuna tıklanır.	

epati 🗉		antikor v2 NGFW	Sayfa ismi girmeye başlayın Q 🕞 Çıkış Yap 🗄
	Güvenlik Kuralları		Tanımları Uygula 1
admin Antikor Admin 👻	Güvenlik Kuralları		𝔅 Yenile
	XLS CSV PDF	🖩 Göster/Gizle 👻 Sayfa Başı	Kayıt Sayısı Tamam 🛛 Tiltrele 🖌 Filtreyi Temizle
es Gosterge Paneli	Sira Durum Kaynak Kaynak Hedef Adres Hedef Protokol Ik II Adres II Port II II Port II Port II	işlem Network Açıklama İşlemler	Hit Toplam Geçerli State Sayısı Byte Sayısı
Ø\$ Sistem Ayarları 🗸	0 Aktif 192,168.100.0/24 212.101.122.34/32 IP	Engelle Tümü Engel Kuralı 🕼 🧟	
\varTheta Ağ Yapılandırması 🤇	1 Aktif 192.164.100.0/24 185.195.231.35/32 IP	NATÎI Tûmû NATli Geçiş 🕼 🛛	8 1 4 5
🋗 Duyuru ve Form Yönetimi 🛛 🔍	« c 1	<u>د</u> د	Git
🖻 Raporlar 🛛 <			

• Tanımlar uygulanarak yapılandırma tamamlanır.

epati		antikor v2 NGFW	Sayfa ismi girmeye başlayın Q 🕞 Çıkış Yap 🗟
BILISIM TEKNOLOJILERI INFORMATION TECHNOLOGIES	Güvenlik Kuralları		Tanımları Uygula 1
admin Antikor Admin -	Güvenlik Kuralları		C Yenile + Ekle
🐵 Gösterge Paneli	XLS CSV PDF	⊞ Göster/Gizle → Sayfa Başı	Kayıt Sayısı Tamam T Filtrele 🖌 Filtreyi Temizle
🗞 Tanımlamalar 🛛 <	Sıra Durum Kaynak Kaynak Hedef Adres Hedef	Protokol İşlem Network Açıklama İşlemler	Hit Toplam Geçerli State Sayısı Byte Sayısı
og Sistem Ayarları 🤇	0 Aktif 192.168.100.0/24 212.101.122.34/32	IP Engello Tümü IP Engel 🕼 🖓	
🖗 Ağ Yapılandırması 🔇 🤇		« c 1 > »	Git
🛗 Duyuru ve Form Yönetimi 🛛 🔍			

enati		antikor v2 NGFW	Sayfa ismi girmeye başlayın	Q 🕞 Çıkış Yap 🖽
	Uygulanacak İşlem Listesi			Tanımları Uygula 1
admin Antikor Admin 👻				🗃 Hepsini Uygula
🏟 Gösterge Paneli	Güvenlik Kuralları Yapılandırması 🕐			Uygula
🗞 Tanımlamalar 🤇				

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	0.0.0.0/0 × ::/0 ×	
Protokol	✓ Tümünü Seç	×
	IP Adresi	-
Kaynak Port	● IPv4 ○ IPv6	
	IPv4	
Hodof Port	L	

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

Kaynak Port	TCP 1-65535 ×			
	✓ Tümünü Seç		×	
Hedef Port	Port Aralığı Girişi		v	
	Başlangıç Portı	Bitiş Portu	~	
Network	L 📄 🖿 #			

- 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	IP Kuralları	
Sira No	Kaynak Adres	Listedekiler Hariç 192.168.100.0/24 ×
Durum Akti		
işlem Engelle	▼ Hedef Adres	Listedekiler Hariç
Trafiği Logla Kapalı		0.0.0.0/0 ×/0 ×
Paket Yönü Her İki Yön	• Protokol	TCP 🔻
Açıklama TCP Port Engeli	Kaynak Dert	Listedekiler Hariç
inceleme Statefull	Каулак Рогс	TCP 1-65535 ×
Yöntemi		✓ Listedekiler Hariç
Seçiniz Seçiniz	Hedef Port	TCP 80 × TCP 443 ×
		TCP 7001 - 7002 ×
	Network	Tümü 🗙 🔻
Bağlantı Sayısı Limitleri	Zamanlayıcı	
Bağlantı Sayısı Limitle	Saat Dilimi	Hafta İçi 08:00 - 17:00 ×
Kişi Başı Maximum Bağlantı Sayısı		
5 Saniyede Maximum Bağlantı Sayısı		
		🖉 İptal 🖺 Kaydet
Ayarlar girildikten sonra Kaydet butonuna til	klanır.	

enati		antikor v2 NGFW	Sayfa ismi girmeye başlayın Q 🕫 Çıkış Yap 🚍
	Güvenlik Kuralları		Tanımları Uygula 🚺
admin Antikor Admin 👻	Güvenlik Kuralları		3 Yenile + Elde
🅸 Gösterge Paneli	XLS CSV PDF	🖽 Göster/Gizle 👻 Sayfa Başı	Kayıt Sayısı Tamam 🕇 Filtrele 🖌 Filtreyi Temizle
• • Tanımlamalar <	Sıra Durum Kaynak Kaynak Hedef Hedef Port Il İl Adres II Port II Adres II	Protokol İşlem Network Açıklama 기 기 기 기	İşlemler Hit Toplam Geçerli State Sayısı Byte Sayısı
Øå Sistem Ayarları 🧹	0 Aktif 192.168.100.0/24 TCP 1 - 65335 0.0.0.0/0 ! TCP 80 TCP 443 =/0 TCP 7001 - 7002	TCP Engelle Tümü TCP Port Engeli	
\varTheta Ağ Yapılandırması 🛛 <			Git
🛗 Duyuru ve Form Yönetimi 🛛 🔇			

• Tanımlar uygulanarak yapılandırma tamamlanır.

epati		antikor v2 NGFW	Sayfa ismi girmeye başlayın 🔍 🕒 Çıkış Yap 🖻
BILISIM TEXNOLOJILERI INFORMATION TECHNOLOGIES	Güvenlik Kuralları		Tanımları Uygula 1
admin Antikor Admin 👻	Güvenlik Kuralları		& Yenile + Elde
🍘 Gösterge Paneli	XLS CSV PDF	III Göster/Gitle → Sayfa Baş	i Kayıt Sayısı Tamam Tiltrele Filtreyi Temizle
🐨 Tanımlamalar 🛛 <	Sira Durum Kaynak Kaynak Hedef Hedef Port	Protokol İşlem Network Açıklama It İt İt İt	İşlemler Hit Toplam Geçerli State Sayısı Byte Sayısı
🕫 Sistem Ayarları 🗧 <	0 Aktif 192.168.100.0/24 TCP 1-65535 0.0.0.0/0 TCP 80 TCP 443	TCP Engelle Tümü TCP Port Engeli	
🖗 Ağ Yapılandırması 🔍		e < 1 > »	Git
🏥 Duyuru ve Form Yōnetimi 🔹 🤇			

		antikor v2 NGFW	Sayfa ismi girmeye başlayın	Q 🕞 Çıkış Yap 🗄
	Uygulanacak İşlem Listesi			Tanımları Uygula 1
admin Antikor Admin 👻				📰 Hepsini Uygula
🏟 Gösterge Paneli	Güvenlik Kuralları Yapılandırması 🕚			Uygula
🗞 Tanımlamalar 🤇				

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.

enati			antikor v2 NGFW	Sayfa ismi girmeye başlayın	Q 🛛 🗇 Çıkış Yap 🖽
	Gösterge Paneli				
admin Antikor Admin 👻	Sistem Kullanımı	~ ×	Servis Durumları		2년 스
📾 Gösterge Paneli	CPU Bellek	Disk	Balküpü Servisi	Kapalı	P = C
🗞 Tanımlamalar	< 15% 77%	0%	Karadelik Servisi	Kapalı	
0° Sistem Ayarları	 0 100 0 100 	0 0 100	Uygulama Güvenliği / IPS Motoru	Çalışıyor	> 🗖 C
😡 Ağ Yapılandırması	C		↦ Uygulama Güvenliği Kuralları	Çalışıyor	> [] C
🗎 Duyuru ve Form Yönetimi	Arayûz Durumları	~ *	↦ IPS Kuralları	Yapılandırılmadı	> . C
🖻 Raporlar	Gruplanmamış		Güvenlik Duvarı	Çalışıyor	> 🗖 C
😨 Kimlik Doğrulama Kuralları			Web Filtreleme Motoru	Çalışıyor	
*) Hotspot İşlemleri			🐱 Forwarded For Bilgisini Gizle	Kapalı	
👁 Anlık Gözlem	igb0 igb1 igb2 igb3 MANS LANS DATA diseases		🖌 HTTP Denetim Servisi	Çalışıyor	> - c
🛡 Güvenlik Ayarları	Constantiation of the second secon		HTTPS Denetim Servisi	Çalışıyor	> C
≓ NAT Yapılandırması	C 100baseTX 1000baseTLAN1		🖌 Sayfa Yasaklama Servisi	Çalışıyor	
🖉 DNS Denetimi	C		→ Antivirüs / İçerik Filtreleme Servisi	Kapalı	
Y Web Filtreleme	Ethernet Bant Genişliği Kullanımı	Tũmũ × 👻	↦ Proxy Servisi	Çalışıyor	
≠ DMZ Yönetimi	· · · ·	~ *	DNS Denetleme Motoru	Çalışıyor	
VPN Yönetimi	Kbit/s	1			

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

