

epati

Antikor NGFW Güvenlik Duvarı Raporları Yapılandırması

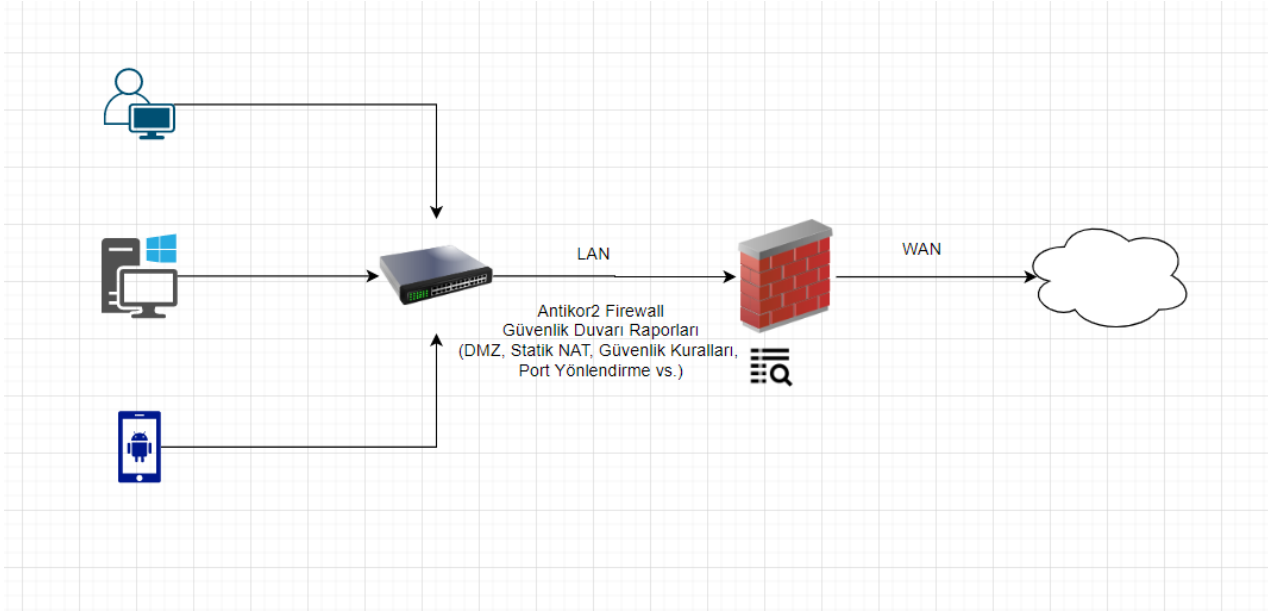
Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı
Yapılandırma Örnekleri

Antikor NGFW Güvenlik Duvarı Raporları Yapılandırması

Kısa Anlatım

Güvenlik duvarında yazılan kurallarına göre yapılan trafiğin logu bu sayfadan gözlemlenmektedir.

Network Şeması



Konfigürasyon

Güvenlik Kuralları Yapılandırması

Güvenlik kurallarında tanımlanmış olduğumuz kurala göre (Natlı Geç, Natsız Geç, Engelle ve Reddet) trafiğin logunu tutacağımız bölümdür.

Örnek;

Güvenlik Ayarları menüsünde **Güvenlik Kuralları** sayfası açılır ve bir kural tanımlanır veya var olan kural düzenlenir

Genel Kurallar

Sıra No

Durum Aktif

İşlem Engelle

Trafiği Logla Açık

Paket Yönü Her İki Yön

Açıklama Antikor2 NGFW

İnceleme Yöntemi Statefull

Bayraklar

IP Kuralları

Listedekiler Hariç

Kaynak Adres

Listedekiler Hariç

Hedef Adres

Protokol ICMP

Listedekiler Hariç

Kaynak Port

Listedekiler Hariç

Hedef Port

Network tumu

Bağlantı Sayısı Limitleri

Bağlantı Sayısı Limite

Kişi Başı Maximum Bağlantı Sayısı

5 Saniyede Maximum Bağlantı Sayısı

Zamanlayıcı

Saat Dilimi

Kural yazıldıktan sonra resimde görüldüğü gibi **Trafiği Logla** seçeneği aktif edilmelidir, aksi takdirde trafik loglanmayacaktır. Kural kaydedildikten sonra istemciden hedef adrese doğru engellenen trafik **Güvenlik Duvarı Logları** sayfasında görüntülenebilecektir.

Örnek Log;

Güvenlik Duvarı Raporları

2020-03-02 16:40:29 2020-03-23 23:59:59

Otomatik Yenileme PA3F

Sayfa Başı Kayıt Sayısı

#	Tarih	Saat	İşlem	Tür	Tetikleyen Kayıt ID	Giriş/Çıkış	Ethernet	Protokol	Kaynak IP	Kaynak Port	Hedef IP	Hedef Port
1	2020-03-17	09:39:38.961738	Engelleme	Güvenlik Kuralları	-1	Çıkış	WAN1 (igb0)	ICMP	192.168.100.11	0	8.8.8.8	0
2	2020-03-17	09:39:33.963018	Engelleme	Güvenlik Kuralları	-1	Çıkış	WAN1 (igb0)	ICMP	192.168.100.11	0	8.8.8.8	0
3	2020-03-17	09:39:28.962334	Engelleme	Güvenlik Kuralları	-1	Çıkış	WAN1 (igb0)	ICMP	192.168.100.11	0	8.8.8.8	0
4	2020-03-17	09:39:23.962633	Engelleme	Güvenlik Kuralları	-1	Çıkış	WAN1 (igb0)	ICMP	192.168.100.11	0	8.8.8.8	0
5	2020-03-17	09:39:18.959842	Engelleme	Güvenlik Kuralları	-1	Çıkış	WAN1 (igb0)	ICMP	192.168.100.11	0	8.8.8.8	0
6	2020-03-17	09:39:13.963252	Engelleme	Güvenlik Kuralları	-1	Çıkış	WAN1 (igb0)	ICMP	192.168.100.11	0	8.8.8.8	0
7	2020-03-17	09:39:08.96351	Engelleme	Güvenlik Kuralları	-1	Çıkış	WAN1 (igb0)	ICMP	192.168.100.11	0	8.8.8.8	0
8	2020-03-17	09:38:58.963065	Engelleme	Güvenlik Kuralları	-1	Çıkış	WAN1 (igb0)	ICMP	192.168.100.11	0	8.8.8.8	0
9	2020-03-17	09:38:53.963397	Engelleme	Güvenlik Kuralları	-1	Çıkış	WAN1 (igb0)	ICMP	192.168.100.11	0	8.8.8.8	0
10	2020-03-17	09:38:48.962677	Engelleme	Güvenlik Kuralları	-1	Çıkış	WAN1 (igb0)	ICMP	192.168.100.11	0	8.8.8.8	0
11	2020-03-17	09:38:43.96099	Engelleme	Güvenlik Kuralları	-1	Çıkış	WAN1 (igb0)	ICMP	192.168.100.11	0	8.8.8.8	0
12	2020-03-17	09:38:38.964273	Engelleme	Güvenlik Kuralları	-1	Çıkış	WAN1 (igb0)	ICMP	192.168.100.11	0	8.8.8.8	0
13	2020-03-17	09:38:33.964561	Engelleme	Güvenlik Kuralları	-1	Çıkış	WAN1 (igb0)	ICMP	192.168.100.11	0	8.8.8.8	0
14	2020-03-17	09:38:28.964871	Engelleme	Güvenlik Kuralları	-1	Çıkış	WAN1 (igb0)	ICMP	192.168.100.11	0	8.8.8.8	0
15	2020-03-17	09:38:23.96415	Engelleme	Güvenlik Kuralları	-1	Çıkış	WAN1 (igb0)	ICMP	192.168.100.11	0	8.8.8.8	0
16	2020-03-17	09:38:18.963398	Engelleme	Güvenlik Kuralları	-1	Çıkış	WAN1 (igb0)	ICMP	192.168.100.11	0	8.8.8.8	0

Anti-Spoof Yapılandırması

Anti-Spoof loglarının görünmesi isteniyorsa **Gösterge Panelinden Anti-Spoof** servisinin açılmış olması yeterli olacaktır. Güvenlik duvarı raporları sayfasından filtre yaparak ilgili logları görebilirsiniz.

Örnek Log ;

Güvenlik Duvarı Raporları

2020-01-27 07:56:40 2020-03-24 23:59:59 Yenile

Otomatik Yenileme PAŞİF

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

#	Tarih	Saat	İşlem	Tür	Tetikleyen Kayıt ID	Giriş/Çıkış	Ethernet	Protokol	Kaynak IP	Kaynak Port	Hedef IP	Hedef Port
1	2020-03-18	17:15:59.631534	Engelleme	Antispoof	-1	Giriş	WAN1 (igb0)	UDP	192.168.100.11	137	192.168.100.255	137
2	2020-03-18	17:15:59.631465	Engelleme	Antispoof	-1	Giriş	WAN1 (igb0)	UDP	192.168.100.11	137	192.168.100.255	137
3	2020-03-18	17:15:58.880901	Engelleme	Antispoof	-1	Giriş	WAN1 (igb0)	UDP	192.168.100.11	137	192.168.100.255	137
4	2020-03-18	17:15:58.880778	Engelleme	Antispoof	-1	Giriş	WAN1 (igb0)	UDP	192.168.100.11	137	192.168.100.255	137
5	2020-03-18	17:15:58.880712	Engelleme	Antispoof	-1	Giriş	WAN1 (igb0)	UDP	192.168.100.11	137	192.168.100.255	137
6	2020-03-18	17:15:58.639091	Engelleme	Antispoof	-1	Giriş	WAN1 (igb0)	UDP	192.168.100.11	58360	239.255.255.250	1900
7	2020-03-18	17:15:58.613853	Engelleme	Antispoof	-1	Giriş	WAN1 (igb0)	UDP	192.168.100.11	58360	239.255.255.250	1900
8	2020-03-18	17:15:58.588095	Engelleme	Antispoof	-1	Giriş	WAN1 (igb0)	UDP	192.168.100.11	58360	239.255.255.250	1900
9	2020-03-18	17:15:58.562063	Engelleme	Antispoof	-1	Giriş	WAN1 (igb0)	UDP	192.168.100.11	58360	239.255.255.250	1900
10	2020-03-18	17:15:58.536106	Engelleme	Antispoof	-1	Giriş	WAN1 (igb0)	UDP	192.168.100.11	58360	239.255.255.250	1900
11	2020-03-18	17:15:58.510113	Engelleme	Antispoof	-1	Giriş	WAN1 (igb0)	UDP	192.168.100.11	58360	239.255.255.250	1900
12	2020-03-18	17:15:58.484074	Engelleme	Antispoof	-1	Giriş	WAN1 (igb0)	UDP	192.168.100.11	58360	239.255.255.250	1900
13	2020-03-18	17:15:58.478207	Engelleme	Antispoof	-1	Giriş	WAN1 (igb0)	UDP	192.168.100.11	58356	224.0.0.252	5355
14	2020-03-18	17:15:58.458086	Engelleme	Antispoof	-1	Giriş	WAN1 (igb0)	UDP	192.168.100.11	58360	239.255.255.250	1900
15	2020-03-18	17:15:58.431918	Engelleme	Antispoof	-1	Giriş	WAN1 (igb0)	UDP	192.168.100.11	58360	239.255.255.250	1900
16	2020-03-18	17:15:58.405553	Engelleme	Antispoof	-1	Giriş	WAN1 (igb0)	UDP	192.168.100.11	58360	239.255.255.250	1900
17	2020-03-18	17:15:58.12985	Engelleme	Antispoof	-1	Giriş	WAN1 (igb0)	UDP	192.168.100.11	137	192.168.100.255	137

Statik NAT Yapılandırması

Statik NAT trafiği logla için **Statik NAT** sayfası açılır bir kural tanımlanır, kuralın erişimleri yazılırken **Trafiği Logla** seçeneği mutlaka **aktif** edilmelidir. Güvenlik duvarı raporları sayfasından filtre yaparak ilgili logları görebilirsiniz.

Statik Nat Erişimleri - Kayıt Düzeltme



Durum

Aktif

Port Bilgisi

TCP 80 x

TCP 443 x

Trafiği Logla

Açık

Erişecek Ağ

0.0.0.0/0 x

:::0 x

Açıklama

Antikor2 NGFW

Azami Bağlantı Sayısı

1000

5 saniyedeki Bağlantı Sayısı

100

İptal

Kaydet

Örnek Log;

#	Tarih	Saat	İşlem	Tür	Tetikleyen Kayıt ID	Giriş/Çıkış	Ethernet	Protokol	Kaynak IP	Kaynak Port	Hedef IP	Hedef Port
1	2020-03-24	08:09:49.510672	Pas Geçme	Statik NAT	17	Giriş	WAN1 (ix1)	TCP	176.40.80.218	54462	10.35.0.32	80
2	2020-03-24	08:09:49.506047	Pas Geçme	Statik NAT	17	Çıkış	(LAN1.35) Server (ix0.35)	TCP	176.40.80.218	54461	10.35.0.32	80
3	2020-03-24	08:09:49.506016	Pas Geçme	Statik NAT	17	Giriş	WAN1 (ix1)	TCP	176.40.80.218	54461	10.35.0.32	80
4	2020-03-24	08:09:49.479674	Pas Geçme	Statik NAT	17	Çıkış	(LAN1.35) Server (ix0.35)	TCP	176.40.80.218	54460	10.35.0.32	80
5	2020-03-24	08:09:49.479529	Pas Geçme	Statik NAT	17	Giriş	WAN1 (ix1)	TCP	176.40.80.218	54460	10.35.0.32	80
6	2020-03-24	08:09:49.479415	Pas Geçme	Statik NAT	17	Çıkış	(LAN1.35) Server (ix0.35)	TCP	176.40.80.218	54459	10.35.0.32	80
7	2020-03-24	08:09:49.479385	Pas Geçme	Statik NAT	17	Giriş	WAN1 (ix1)	TCP	176.40.80.218	54459	10.35.0.32	80
8	2020-03-24	08:09:49.478707	Pas Geçme	Statik NAT	17	Çıkış	(LAN1.35) Server (ix0.35)	TCP	176.40.80.218	54458	10.35.0.32	80
9	2020-03-24	08:09:49.478672	Pas Geçme	Statik NAT	17	Giriş	WAN1 (ix1)	TCP	176.40.80.218	54458	10.35.0.32	80
10	2020-03-24	08:09:49.119599	Pas Geçme	Statik NAT	17	Çıkış	(LAN1.35) Server (ix0.35)	TCP	176.40.80.218	54457	10.35.0.32	80
11	2020-03-24	08:09:49.119563	Pas Geçme	Statik NAT	17	Giriş	WAN1 (ix1)	TCP	176.40.80.218	54457	10.35.0.32	80
12	2020-03-24	08:09:26.303428	Pas Geçme	Statik NAT	17	Çıkış	(LAN1.35) Server (ix0.35)	TCP	176.40.80.218	54384	10.35.0.32	80
13	2020-03-24	08:09:26.303391	Pas Geçme	Statik NAT	17	Giriş	WAN1 (ix1)	TCP	176.40.80.218	54384	10.35.0.32	80
14	2020-03-24	08:09:26.303099	Pas Geçme	Statik NAT	17	Çıkış	(LAN1.35) Server (ix0.35)	TCP	176.40.80.218	54383	10.35.0.32	80
15	2020-03-24	08:09:26.303059	Pas Geçme	Statik NAT	17	Giriş	WAN1 (ix1)	TCP	176.40.80.218	54383	10.35.0.32	80

DMZ Sunucu Yönetimi Yapılandırması

DMZ Yönetimi menüsünden **Dmz Sunucu Yönetimi** sayfası açılır ve yeni bir kayıt veya var olan kayıta düzenleme yapılır. **Erişimler** sayfası açılır ve ekle/düzenle butonuna tıklanır. Bilgiler yazıldıktan sonra **Trafiği Logla** butonu aktif edilir. Güvenlik duvarı raporları sayfasından filtre yaparak ilgili logları görebilirsiniz.

Durum Aktif

Port Bilgileri

TCP 80 x

Trafiki Logla

 Açık

Eriřecek Ađ

0.0.0.0/0 x ::/0 x

Açıklama

Antikor NGFW DMZ Eriřimleri

Kiři Baři
Maximum
Bađlantı Sayısı

1000

5 Saniyede
Maximum
Bađlantı Sayısı

100

İptal

Kaydet

Port Yönlendirme Yapılandırması

Port Yönlendirme trafiki logla için **Port Yönlendirme** sayfası açılır bir kural tanımlanır, kural oluşturulurken **trafiki logla** seçeneđi aktif edilir. Güvenlik duvarı raporları sayfasından filtre yaparak ilgili logları görebilirsiniz.

Durum AktifTrafik Logla Açık

Protokol TCP

Açıklama test

Yerel IP Adresi IPv4 10.49.7.40

Yerel Port 22022 22022

WAN Adresi IPv4 193.193.193.193

WAN Portu 33333 33333

 Listekiler Hariç
Erişecek Ağ 0.0.0.0/0 x ::/0 xKişi Başı
Maximum
Bağlantı Sayısı 10005 Saniyede
Maximum
Bağlantı Sayısı 100

İptal

Kaydet

Global NAT Yapılandırması

Global NAT trafiği logla seçeneğini için **Ethernet Atamada** veya **VLAN Yapılandırmasında** oluşturulan kayıtlarda **Global NAT Trafik Logla** seçeneği aktif edilir. Güvenlik duvarı raporları sayfasından filtre yaparak ilgili logları görebilirsiniz.

LAN Ethernet Örneği ;

Ethernet Durumları

Durum Aktif

Arayüz LAN1

Ethernet Adı igb1

Hız autoselect

MTU 1500

Web Arayüzü Erişimi Aktif

Açıklama LAN1

IPv6 Ayarları

Otomatik IPv6 Al

EUI64 Pasif

IPv6 Adresi IPv6 ffff::1/8

DHCPv6 Başlangıç IPv6

DHCPv6 Bitiş IPv6

DHCPv6 Relay Adresi IPv6

IPv4 Ayarları

Otomatik IPv4 Al

IPv4 Adresi IPv4 192.168.100.1/24

DHCPv4 Havuzu Modu Tüm İstemcilere IP Dağıt

DHCPv4 Başlangıç IPv4 192.168.100.10

DHCPv4 Bitiş IPv4 192.168.100.250

DHCPv4 Ağ Geçidi IPv4 192.168.100.1

DHCPv4 Relay Adresi IPv4

Global NAT IPv4 10.2.1.180

Global NAT Trafik Logla Kapalı

Seçenekler

MAC Eşleme NAT

Kayıt Al Anons Yap

DHCPv6 Sunucusu DHCPv4 Sunucusu

DHCPv6 Relay DHCPv4 Relay

Managed Bayrağı Other Bayrağı

İptal

Kaydet

Vlan Ethernet Örneği ;

Genel Durumlar

Durum Aktif

Adı

VLAN ID

Bağlantı Türü

Ethernet Arayüzü

Açıklama

IPv6 Ayarları

Otomatik IPv6 Al

EUI64 Pasif

IPv6 Adresi

DHCPv6 Başlangıç

DHCPv6 Bitiş

DHCPv6 Relay Adresi

IPv4 Ayarları

Otomatik IPv4 Al

IPv4 Adresi

DHCPv4 Havuzu Modu

DHCPv4 Başlangıç

DHCPv4 Bitiş

DHCPv4 Ağ Geçidi

DHCPv4 Relay Adresi

Global NAT

Global NAT Trafik Logla Açık

Seçenekler

MAC Eşleme NAT

Kayıt Al Anons Yap

DHCPv6 Sunucusu DHCPv4 Sunucusu

DHCPv6 Relay DHCPv4 Relay

Managed Bayrağı Other Bayrağı

Hedefe Göre NAT Yapılandırması

Hedefe Göre NAT trafiği logla seçeneği için **NAT Yapılandırması** menüsünde **Hedefe Göre NAT** sayfasına gidilir. Kural ekle/düzenle yaparken ilgili kayıtlar tamamlandıktan sonra **Trafiği Logla** seçeneği aktif edilir. Güvenlik duvarı raporları sayfasından filtre yaparak ilgili logları görebilirsiniz.

Hedefe Göre NAT - Yeni Kayıt

x

Durum Aktif

Trafiği Logla Açık

Ethernet Arayüzü

Kaynak Adres

Hedef Adres

Hedef Port

Nat Adresi

Açıklama

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

