epati

Antikor NGFW Güvenlik Duvarı Raporları Yapılandırması

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı

Yapılandırma Örnekleri

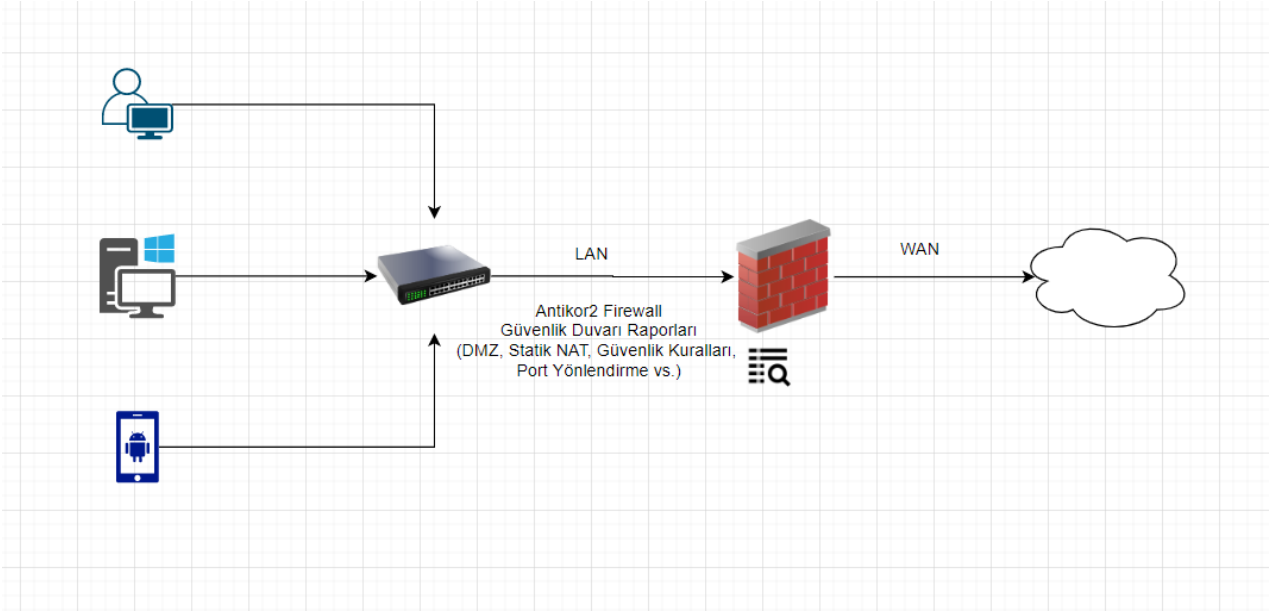
www.epati.com.tr

Antikor NGFW Güvenlik Duvarı Raporları Yapılandırması

Kısa Anlatım

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

Network Şeması



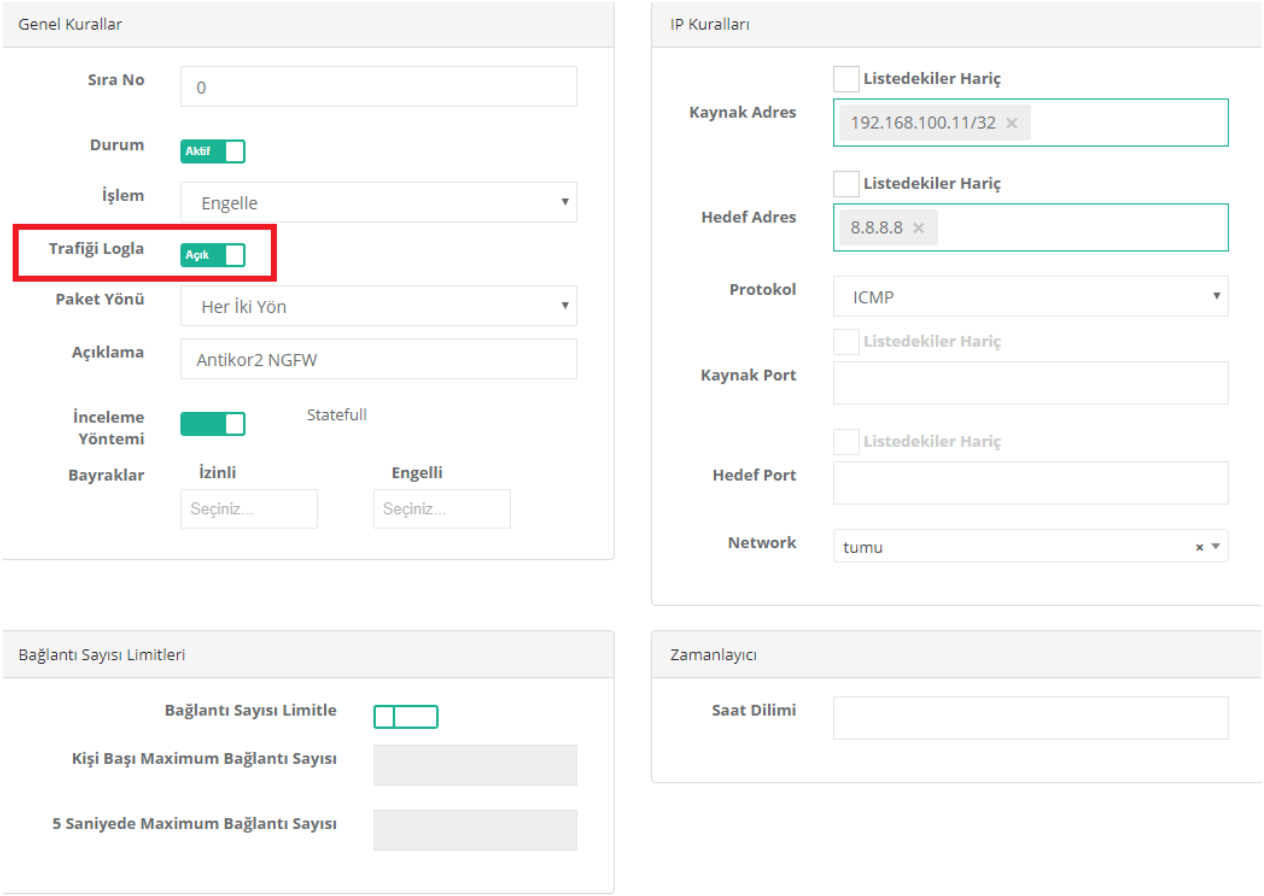
Konfigürasyon

Güvenlik Kuralları Yapılandırması

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

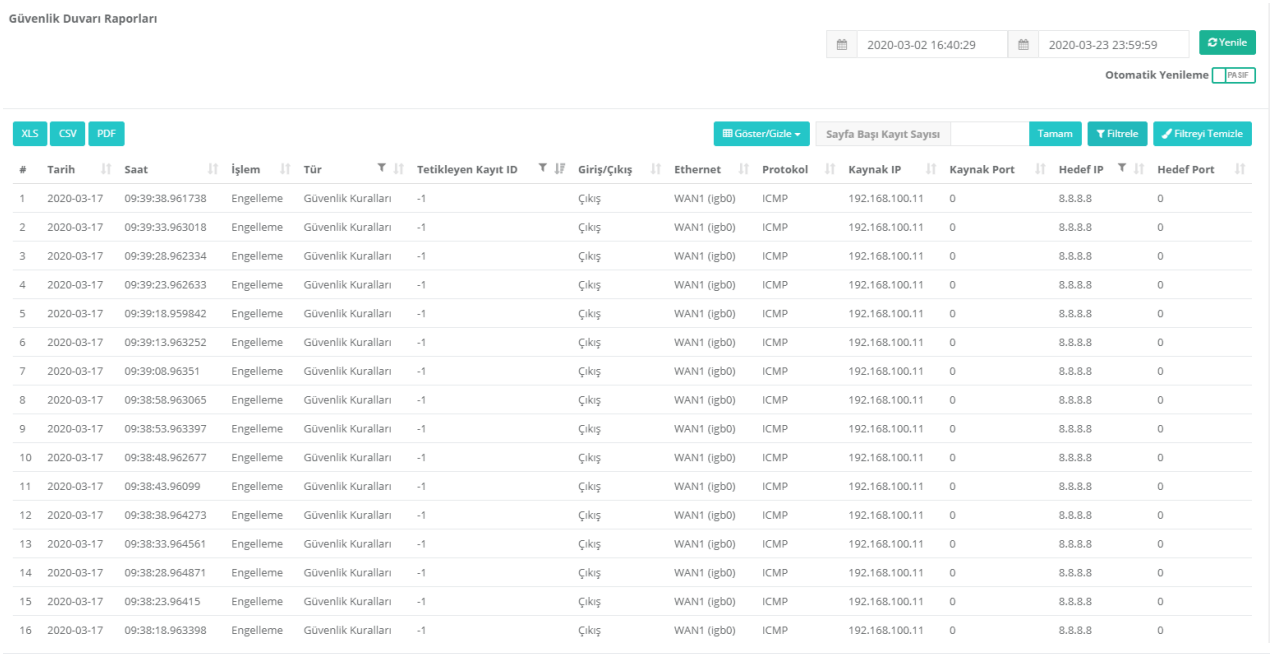
Örnek;

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



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;

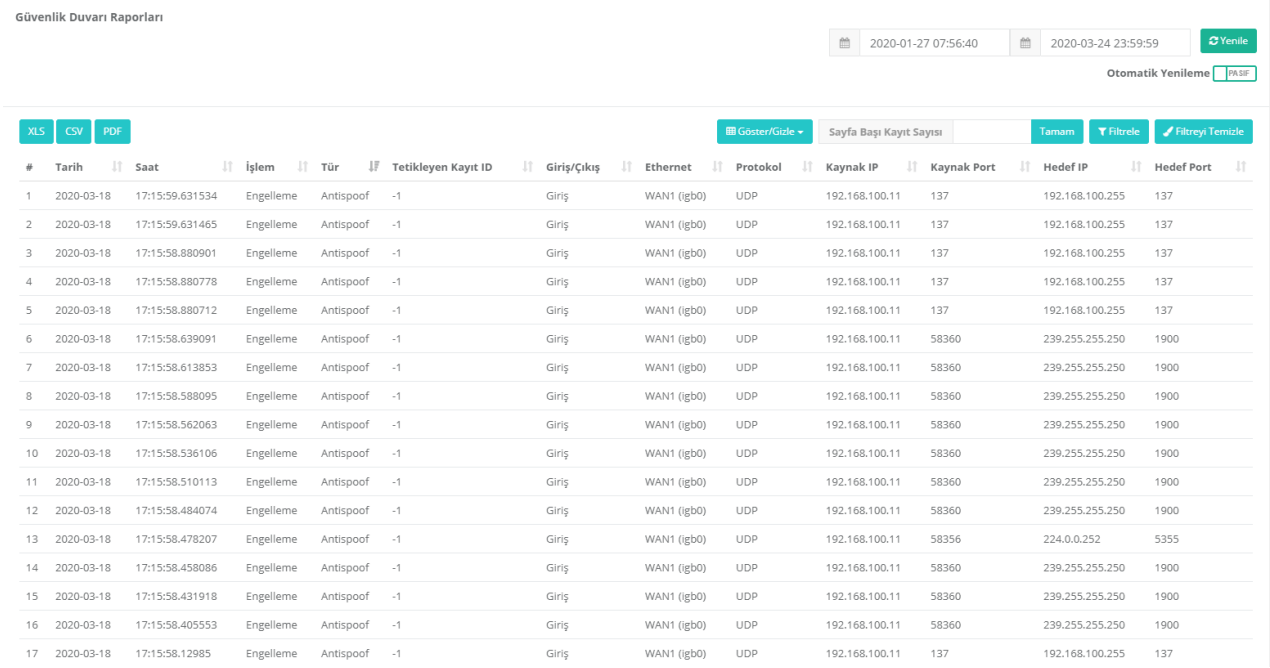


#	Tarih	Saat	İşlem	Tür	Tetikleyen Kayıt ID	Giriş/Çıkış	Ethernet	Protokol	Kaynak IP	Kaynak Port	Hedef IP	Hedef Port
1	2020-03-17	09:39:38.961738	Engelleme	Güvenlik Kuralları	-1	Çıkış	WAN1 (igb0)	ICMP	192.168.100.11	0	8.8.8.8	0
2	2020-03-17	09:39:33.963018	Engelleme	Güvenlik Kuralları	-1	Çıkış	WAN1 (igb0)	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.

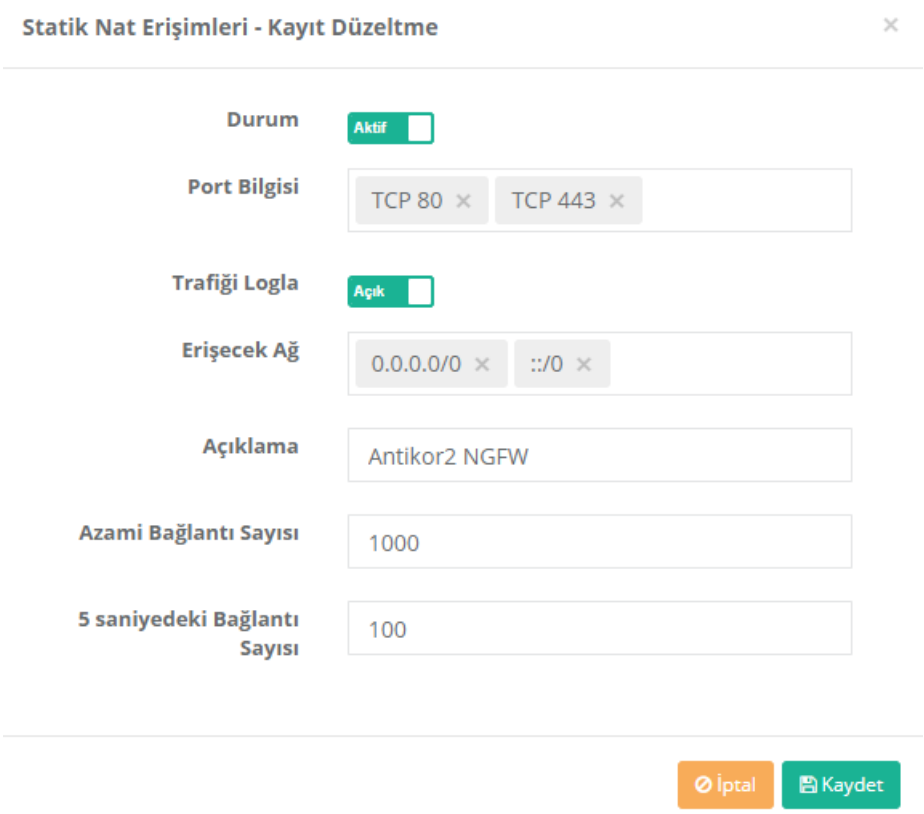
Örnek Log ;



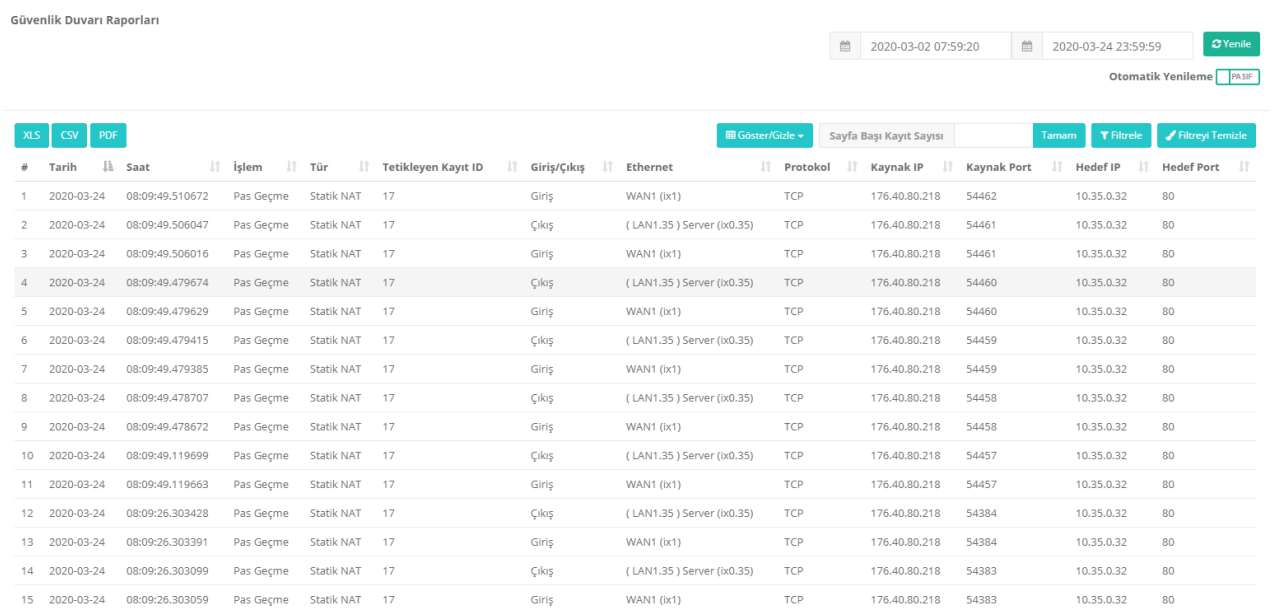
#	Tarih	Saat	İşlem	Tür	Tetikleyen Kayıt ID	Giriş/Çıkış	Ethernet	Protokol	Kaynak IP	Kaynak Port	Hedef IP	Hedef Port
1	2020-03-18	17:15:59.631534	Engelleme	Antispoof	-1	Giriş	WAN1 (igb0)	UDP	192.168.100.11	137	192.168.100.255	137
2	2020-03-18	17:15:59.631465	Engelleme	Antispoof	-1	Giriş	WAN1 (igb0)	UDP	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.



Örnek Log;


Güvenlik Duvarı Raporları

2020-03-02 07:59:20 2020-03-24 23:59:59 Yenile

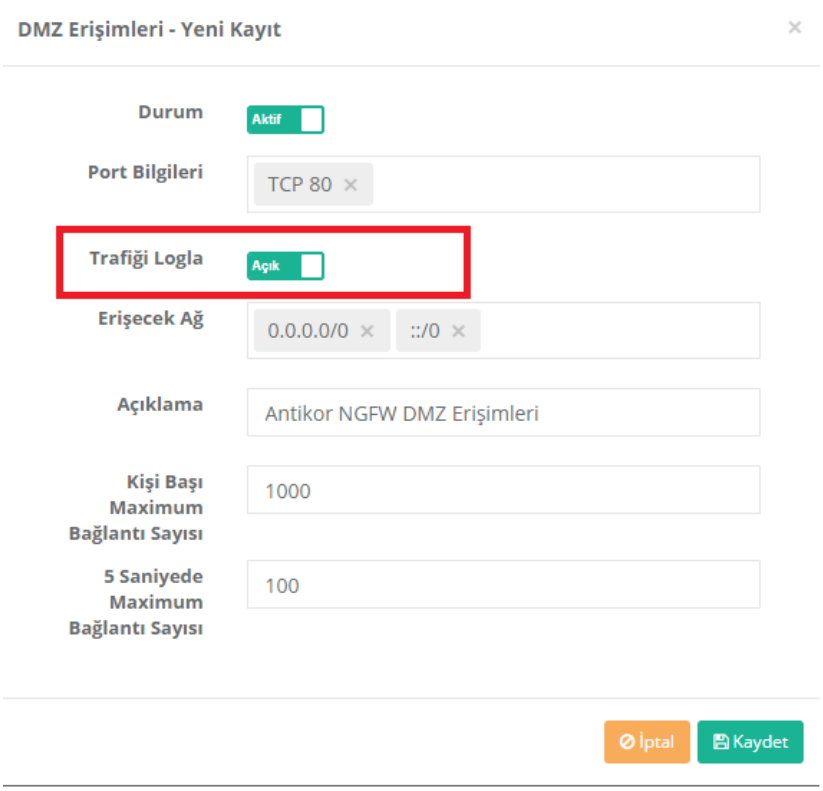
Otomatik Yenileme PASİF

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	2020-03-24	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	08:09:49.479629	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	08:09:49.119699	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	08:09:49.119663	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

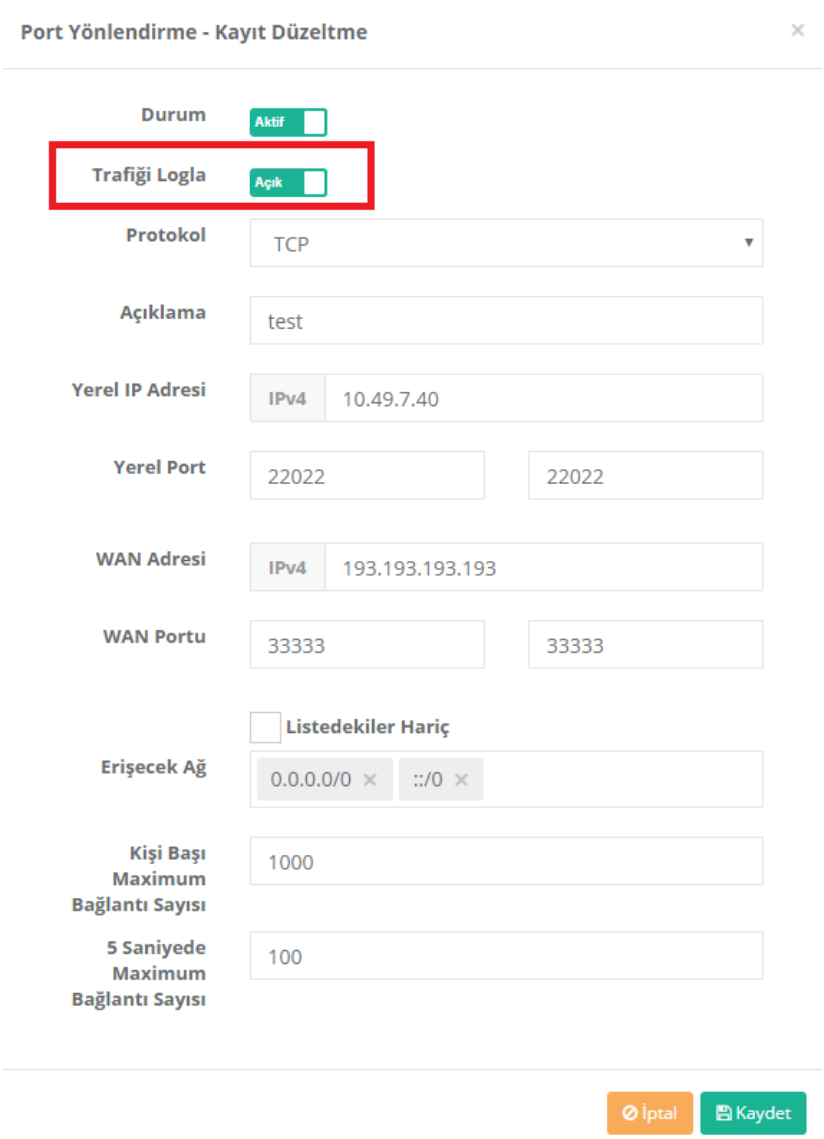
DMZ Sunucu Yönetimi Yapılandırması

DMZ Yönetimi menüsünden **Dmz Sunucu Yönetimi** sayfası açılır ve yeni bir kayıt veya var olan kayıtta 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.



Port Yönlendirme Yapılandırması

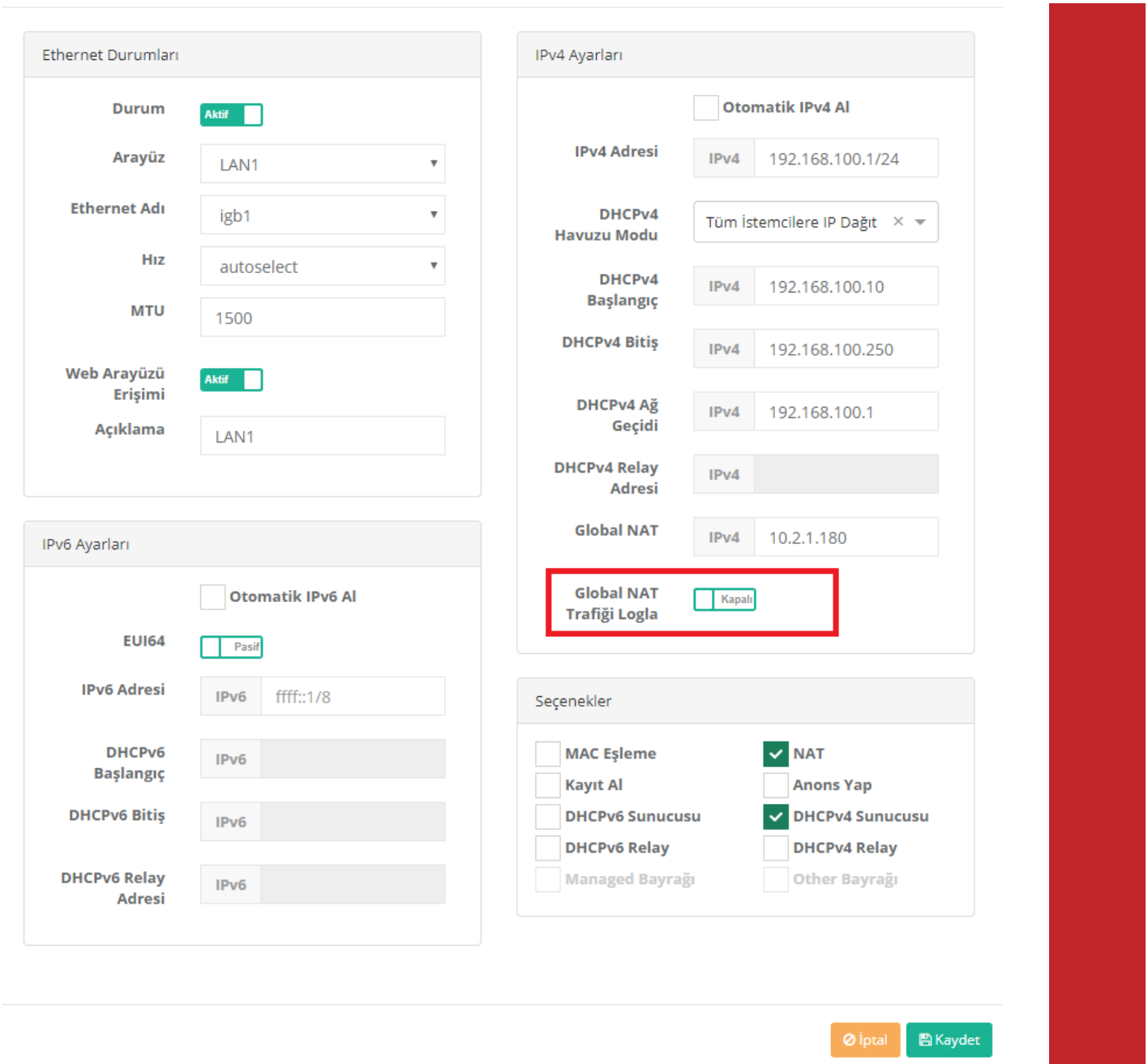
Port Yönlendirme trafiği logla için **Port Yönlendirme** sayfası açılır bir kural tanımlanır, kural oluşturulurken **trafiği logla** seçeneği aktif edilir. Güvenlik duvarı raporları sayfasından filtre yaparak ilgili logları görebilirsiniz.



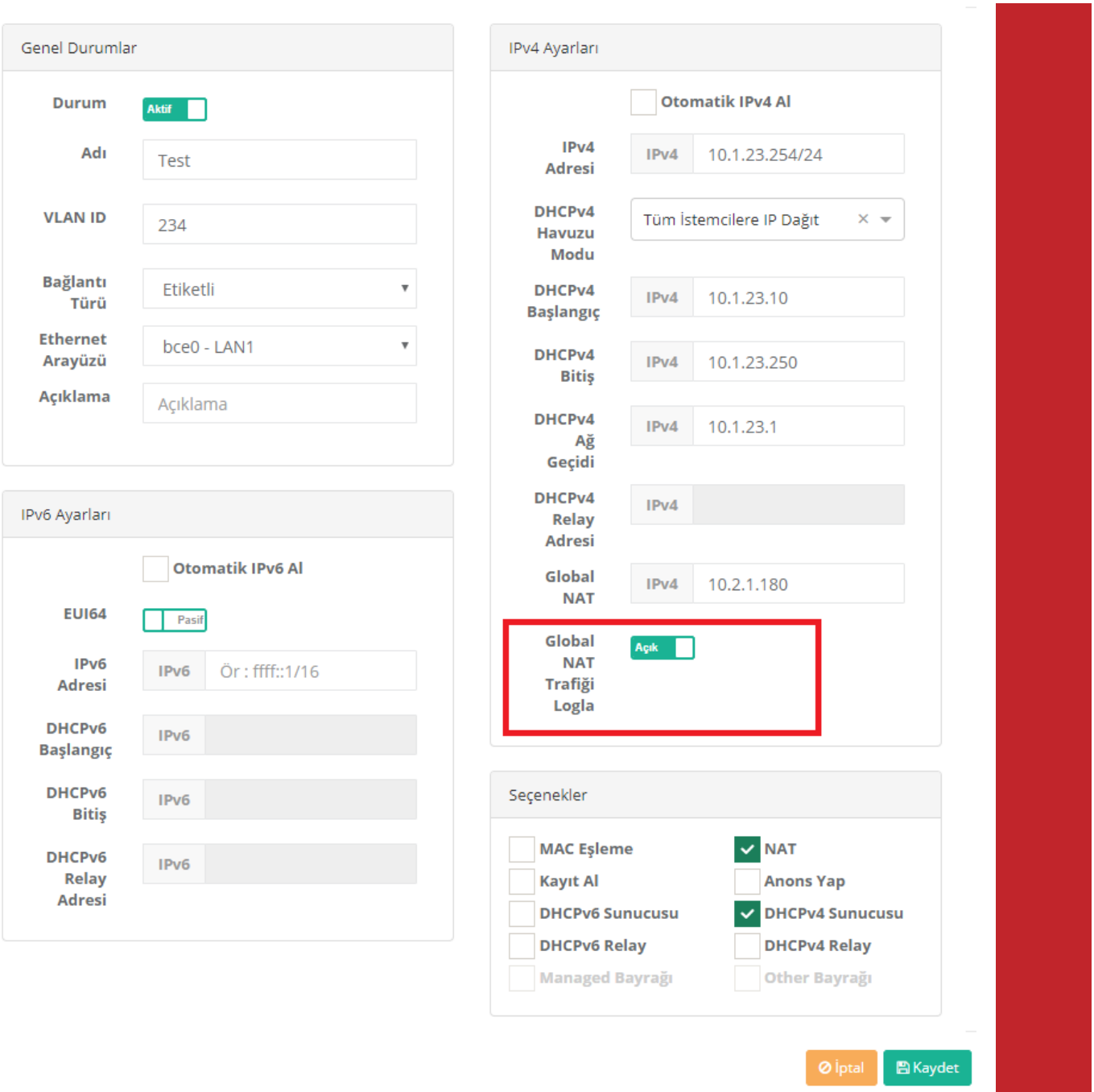
Global NAT Yapılandırması

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

LAN Ethernet Örneği ;

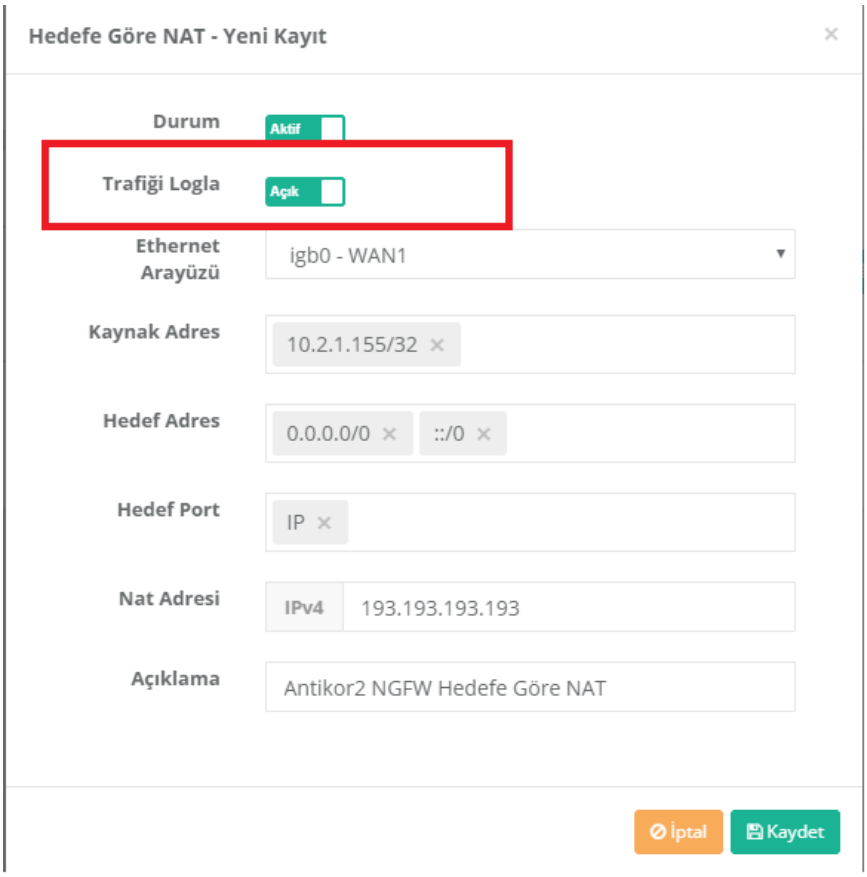


Vlan Ethernet Örneği ;



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.



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