Sanal Kablo ile Filtreleme Yapılandırması

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı

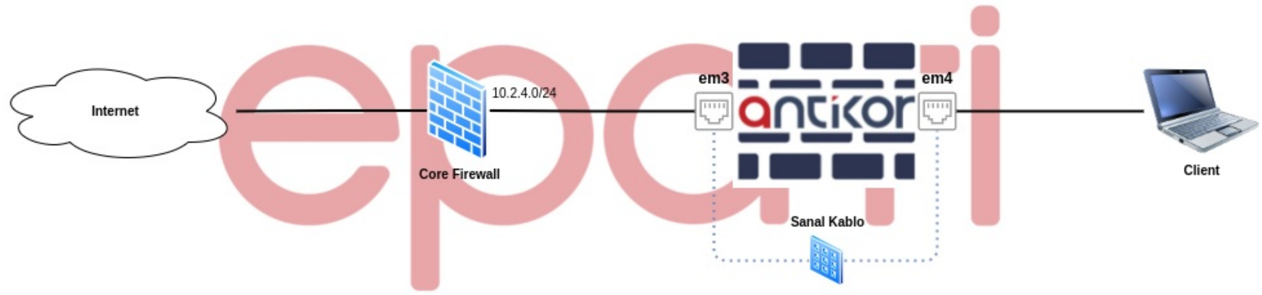
Yapılandırma Örnekleri

www.epati.com.tr

Sanal Kablo ile Filtreleme Yapılandırması

Sanal kablo, iki etherneti birbirine bağlayarak bir güvenlik duvarı kurulmaktadır. Birbirine bağlanan iki kablo arasında geçen trafik için güvenlik kural seti/kuralları yazılabilmektedir.

Topoloji

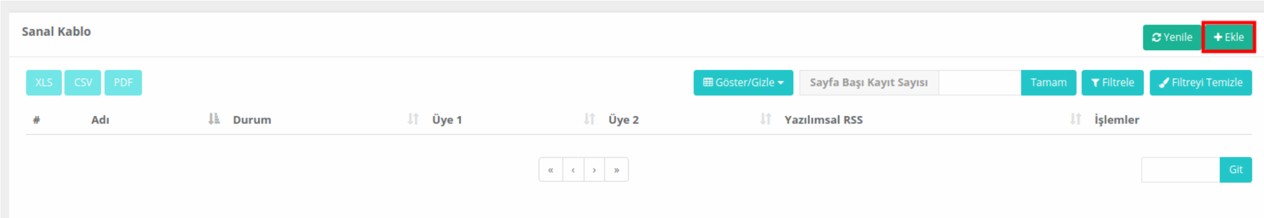


`Not:` Topolojide yer alan Core Firewall yerine NAT yapan herhangi bir cihaz(Router, Modem) geçebilmektedir.

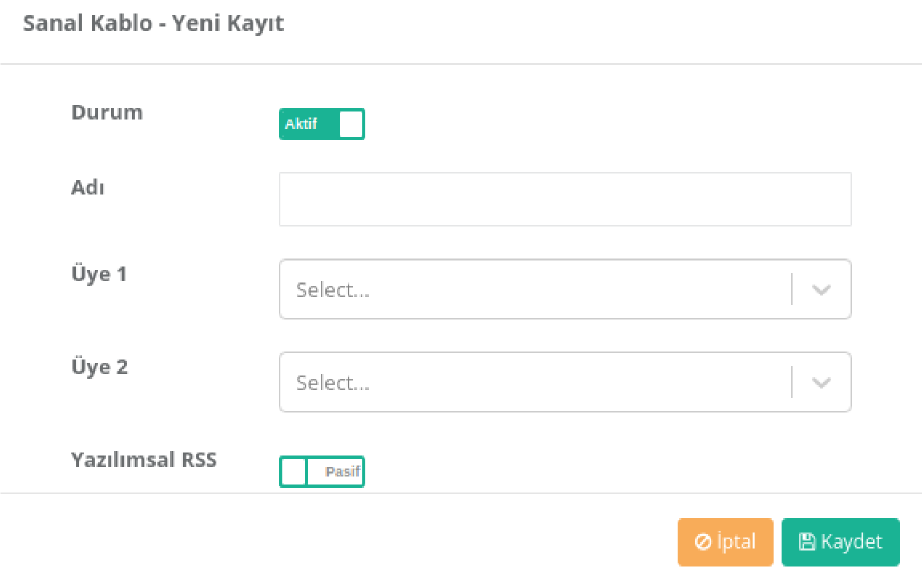
Yapılandırma örneğinde istemcinin 10.2.4.0/24 IP bloklu Core Firewall'dan IP alıp, internete çıkarken Antikor NGFW'de filtrelenmesi ve yapılan bu filtrelemenin loglarının görüntülenmesi planlanmıştır.

- Ağ Yapılandırması menüsü altında bulunan **Sanal Kablo** sayfasına gidilir.

Sanal Kablo

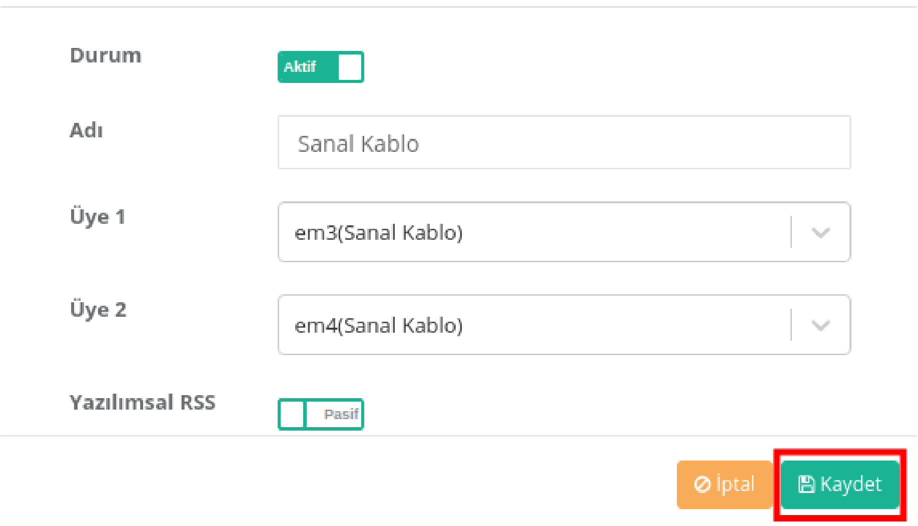


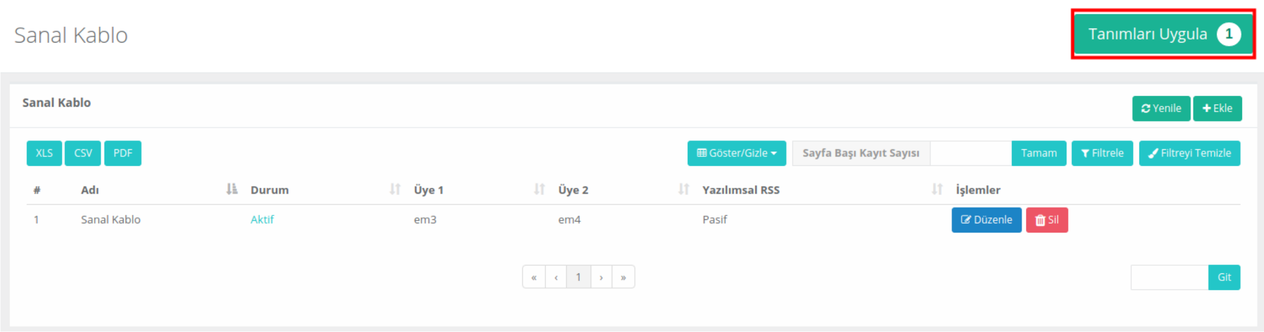
- Yeni Sanal Kablo eklenir. Sanal kablo eklerken üyeler herhangi bir yerde kullanılmayan ethernetler arasından seçilmektedir.

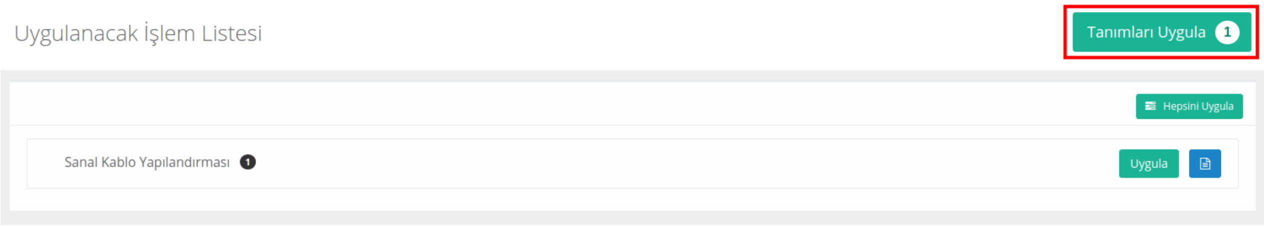


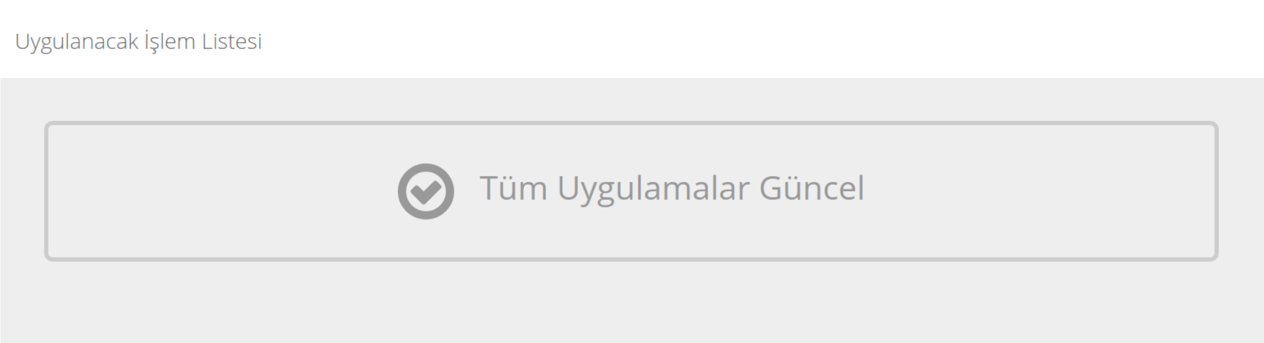
`Not:` Seçilecek olan üyelere ait ethernetler aynı marka veya model değil ise**Yazılımsal RSS** aktifleştirilir. Yazılımsal RSS'in aktifleştirilmesi performans düşüşüne sebebiyet vermektedir. Bu nedenle aynı marka ve model ethernetler arasında sanal kablo çalışmasının yapılması önerilmektedir.

- Ayarlar kaydedilir ve tanımlar uygulanır.

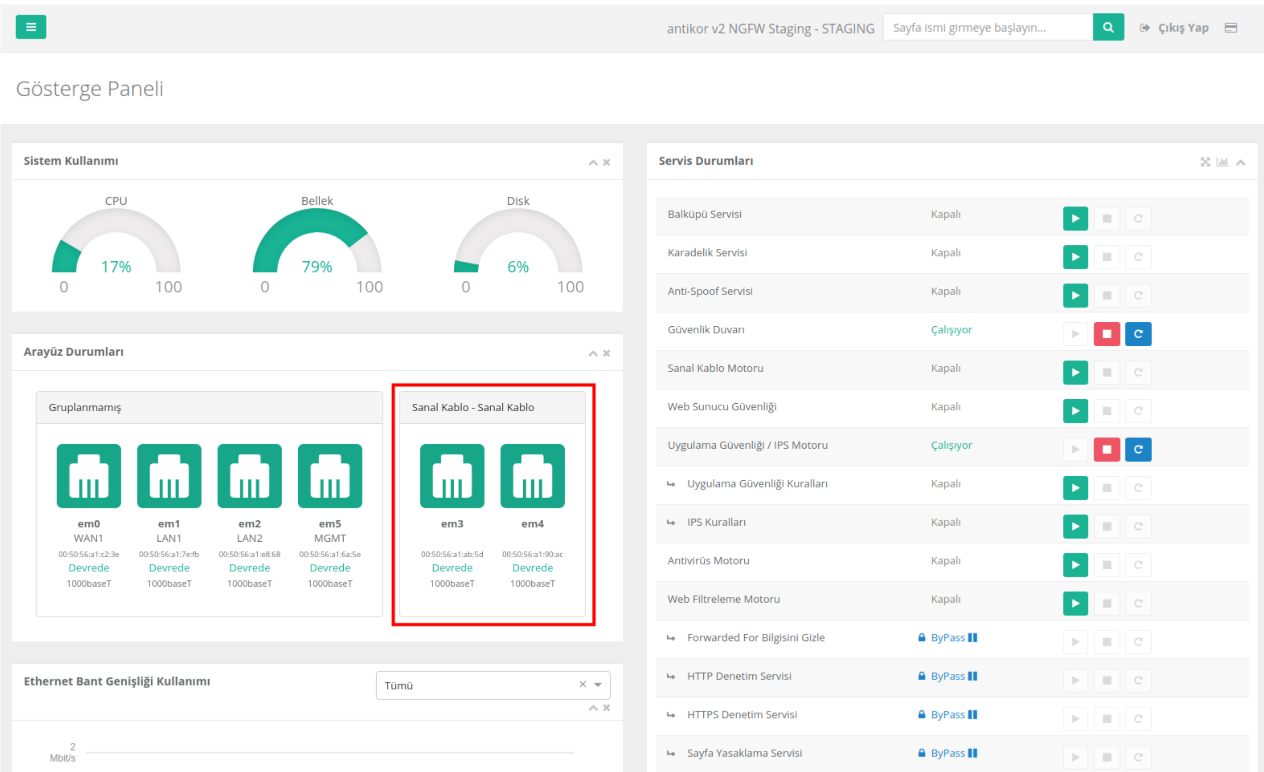




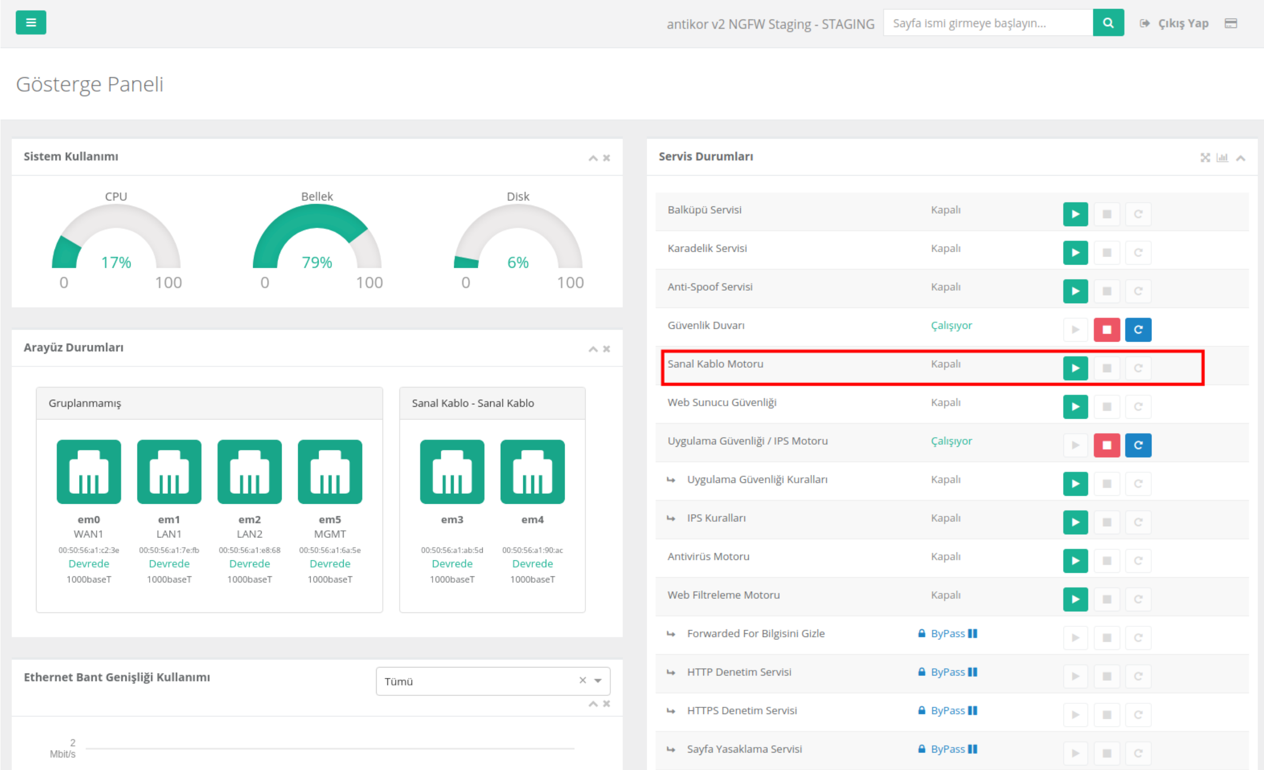


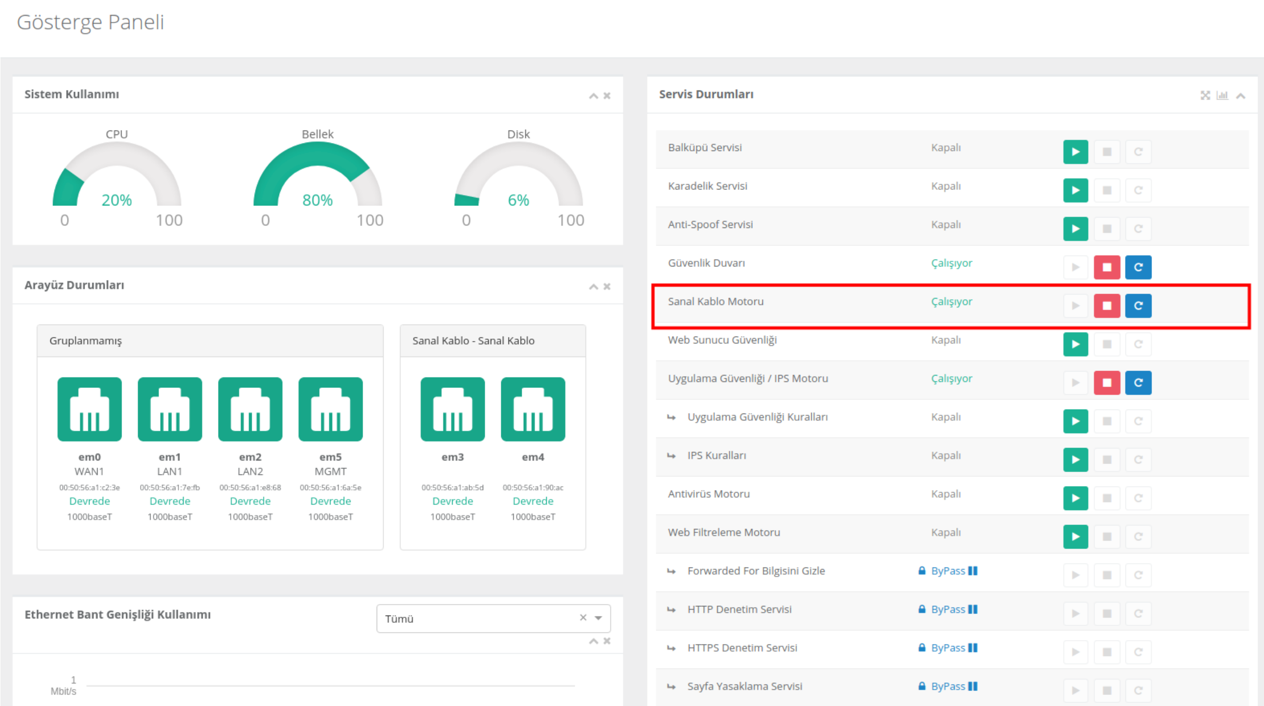


- Gösterge Panelinde arayüz durumlarından sanal kabloların bağlı olduğu kontrol edilir.

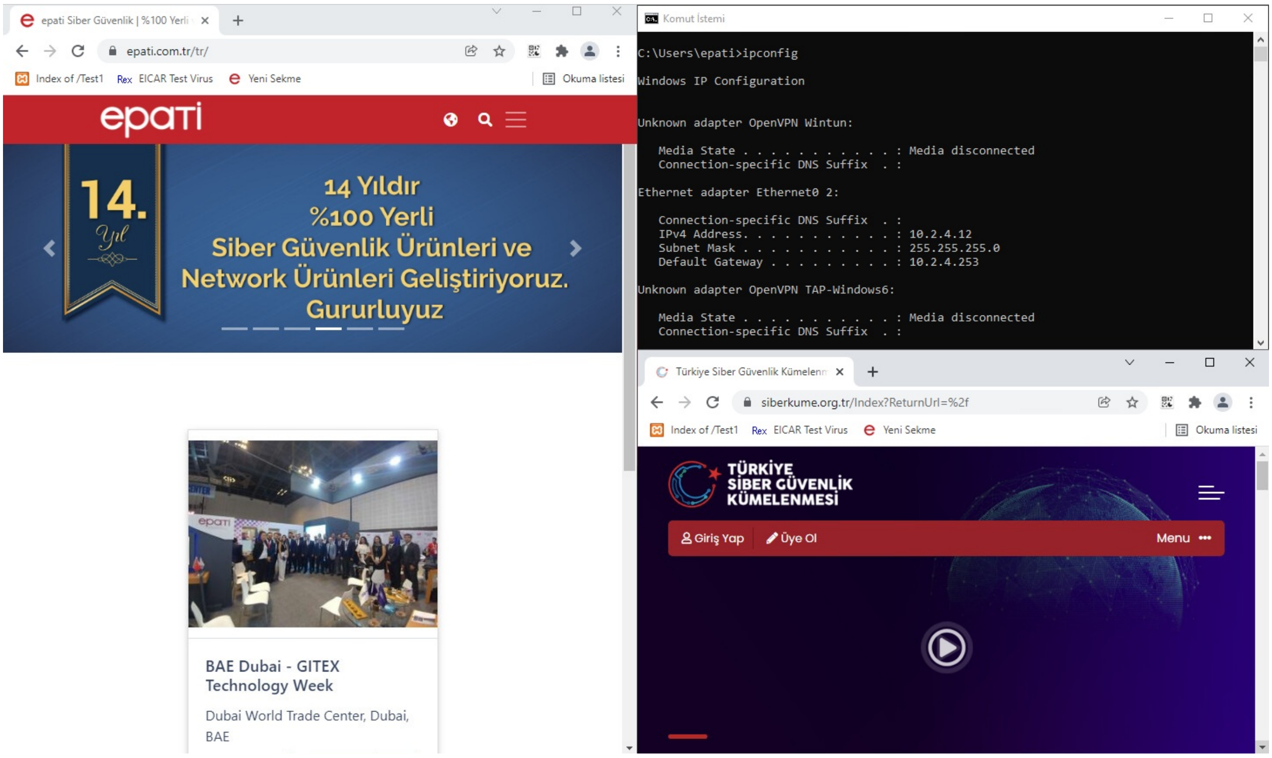


- Gösterge panelinde servis durumlarından **Sanal Kablo Motoru** açılır.



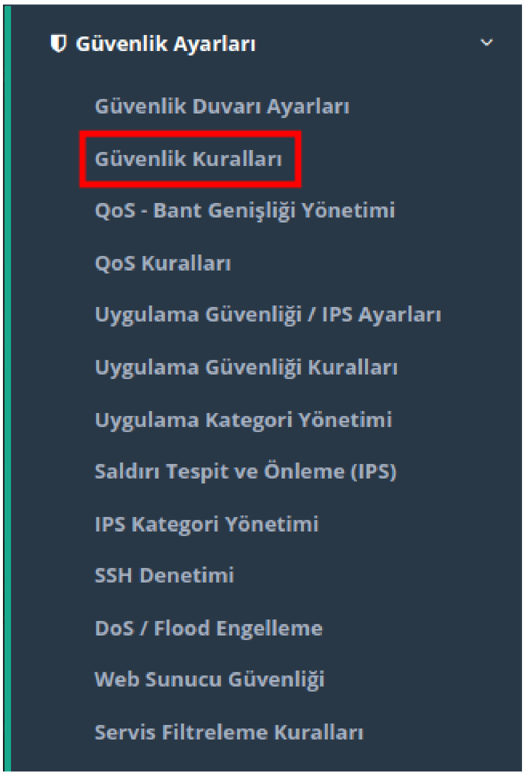


- Sanal kabloya bağlı istemcinin 10.2.4.0/24'lü bloktan IP aldığı ve internete çıktığı kontrol edilir.

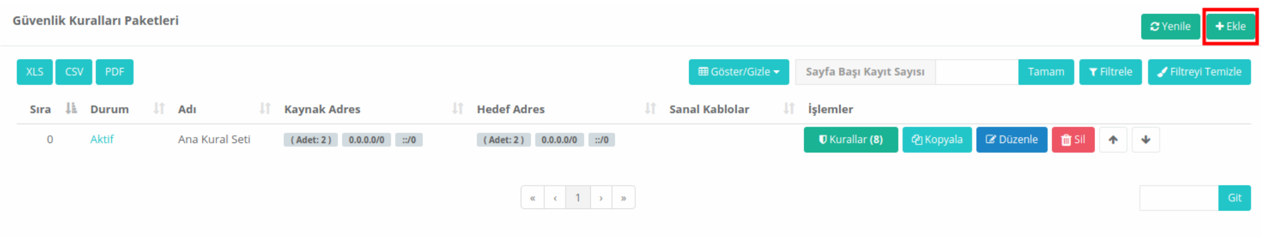



```
C:\Users\epati>ipconfig

Windows IP Configuration


Unknown adapter OpenVPN Wintun:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.2.4.12
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.2.4.253

Unknown adapter OpenVPN TAP-Windows6:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\epati>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=60ms TTL=113
Reply from 8.8.8.8: bytes=32 time=60ms TTL=113
Reply from 8.8.8.8: bytes=32 time=63ms TTL=113
Reply from 8.8.8.8: bytes=32 time=61ms TTL=113

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 60ms, Maximum = 63ms, Average = 61ms

C:\Users\epati>ping epati.com.tr

Pinging epati.com.tr [46.101.122.133] with 32 bytes of data:
Reply from 46.101.122.133: bytes=32 time=58ms TTL=53
Reply from 46.101.122.133: bytes=32 time=59ms TTL=53
Reply from 46.101.122.133: bytes=32 time=57ms TTL=53
Reply from 46.101.122.133: bytes=32 time=57ms TTL=53

Ping statistics for 46.101.122.133:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 57ms, Maximum = 59ms, Average = 57ms

C:\Users\epati>
```

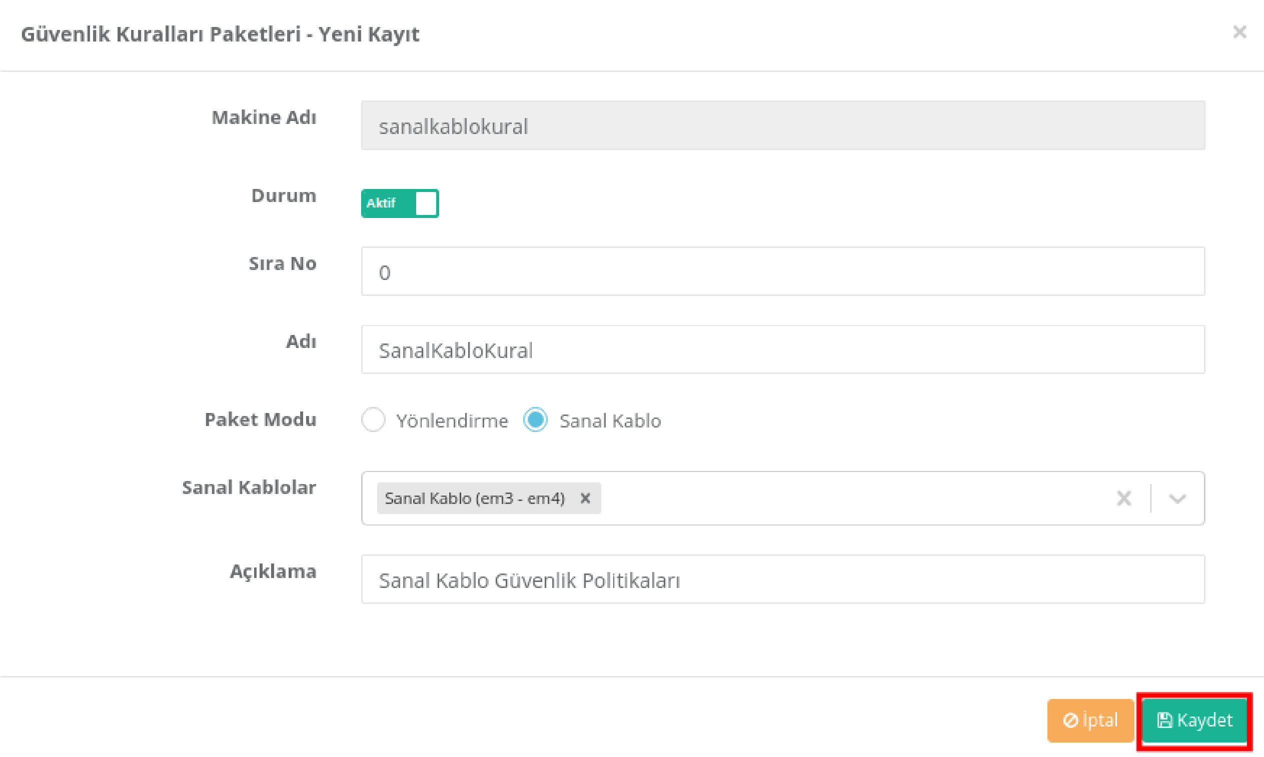
- Güvenlik Ayarları menüsü altında bulunan **Güvenlik Kurallarına** gidilir.



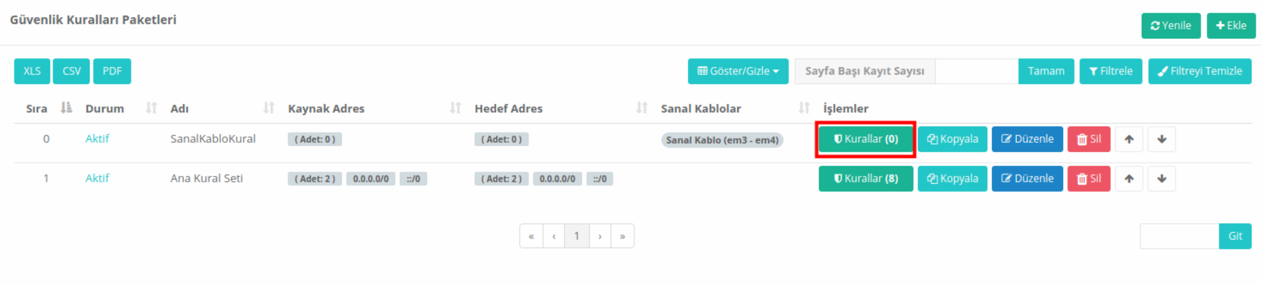
- Yeni bir **Güvenlik Kuralı Paketi** eklenir.



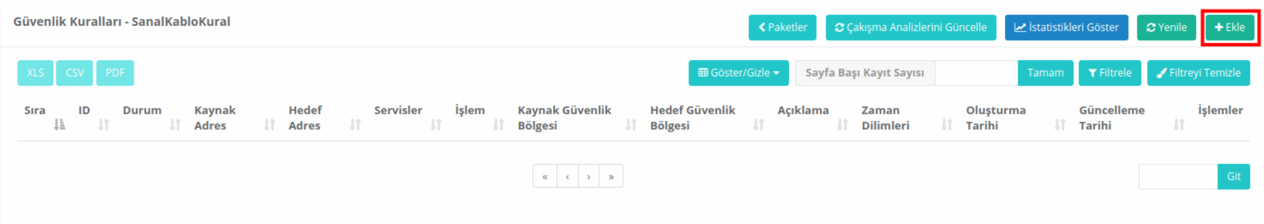
- **Paket Modu Sanal Kablo** seçilir, filtrelenecek sanal kablo ile birlikte adı ve açıklaması girilir ve kaydedilir. (Adı alanı maksimum 15 karakter olarak kabul edilmektedir.)



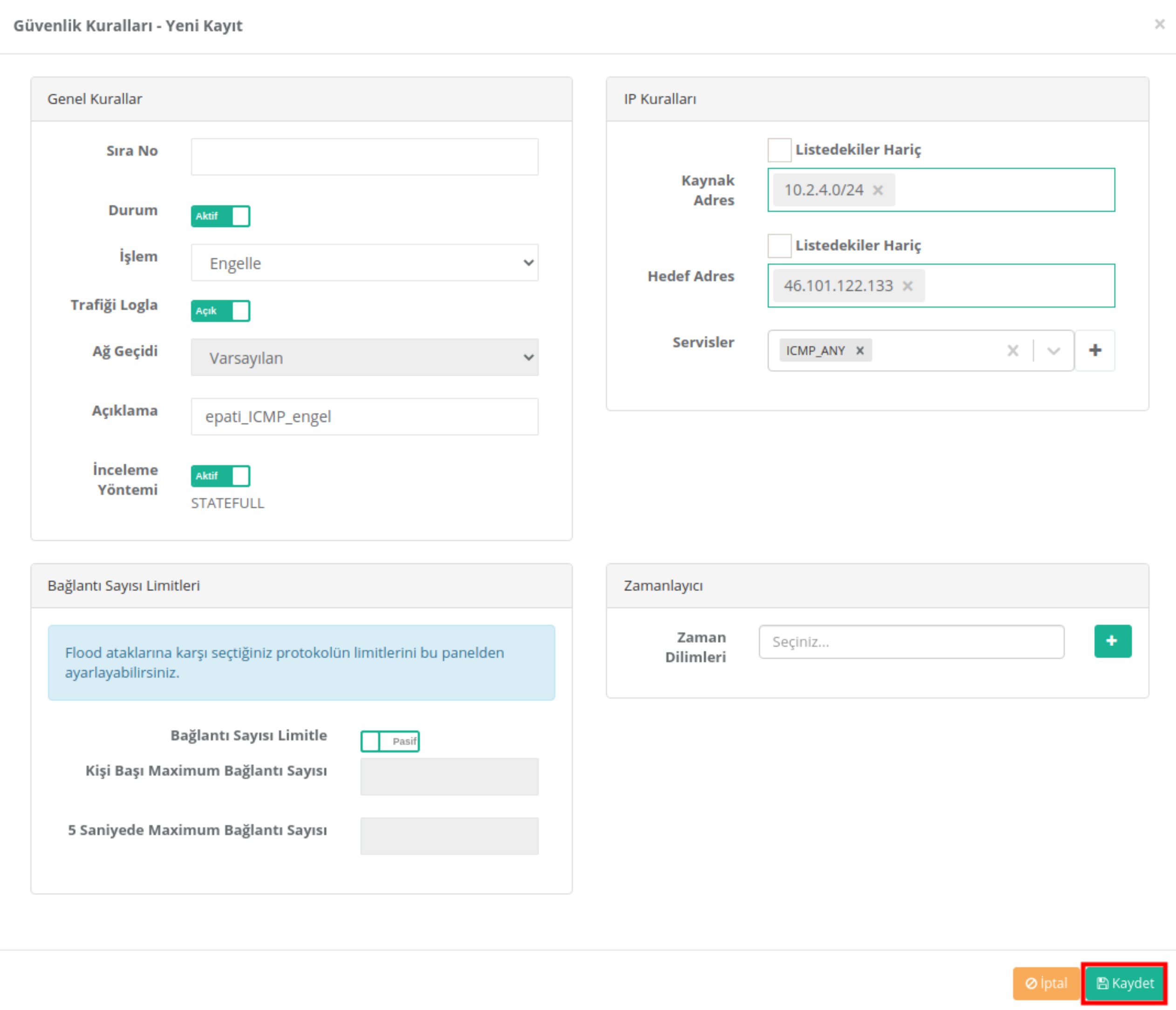
- Oluşturulan güvenlik kuralı paketine kural yazmak için ilgili paketin **Kurallar** butonuna tıklanır.

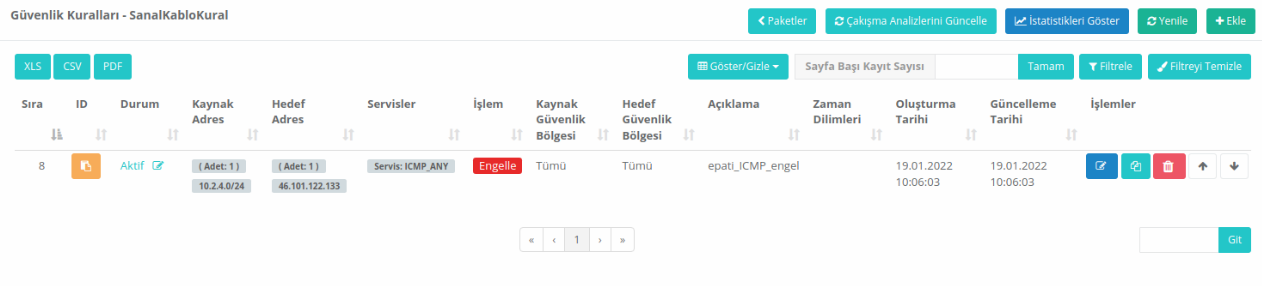


- **Ekle** butonuna tıklanır.

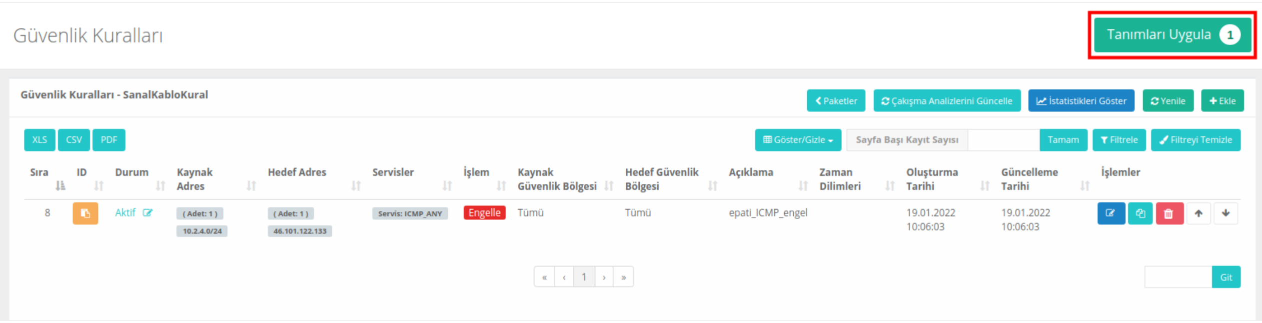


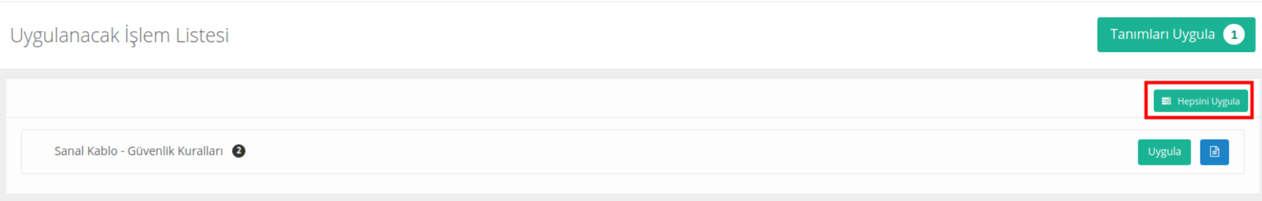
- Yazılan güvenlik kuralında daha önce ICMP erişimi sağladığımız 46.101.122.133 IP adresine engel kuralı yazıldı.

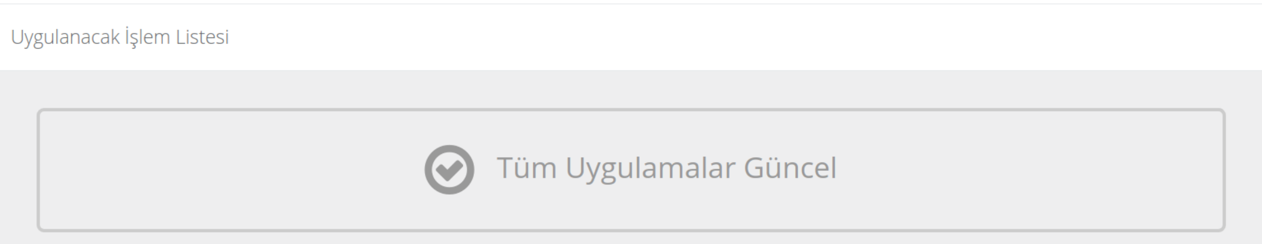




- Tanımlar uygulanır.



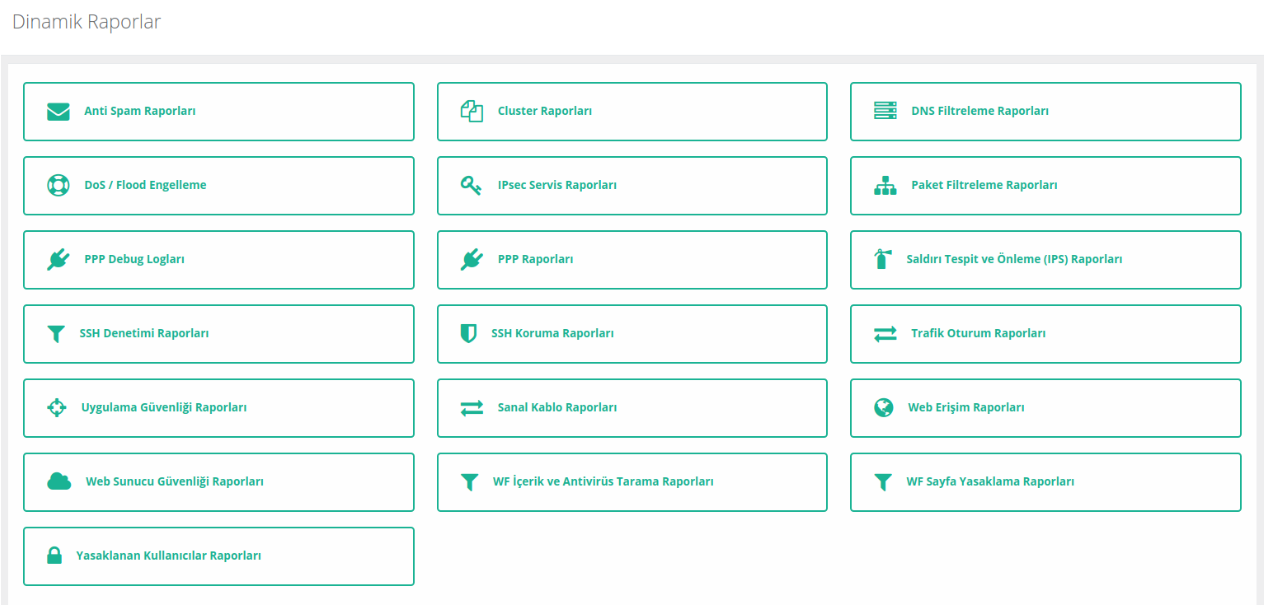




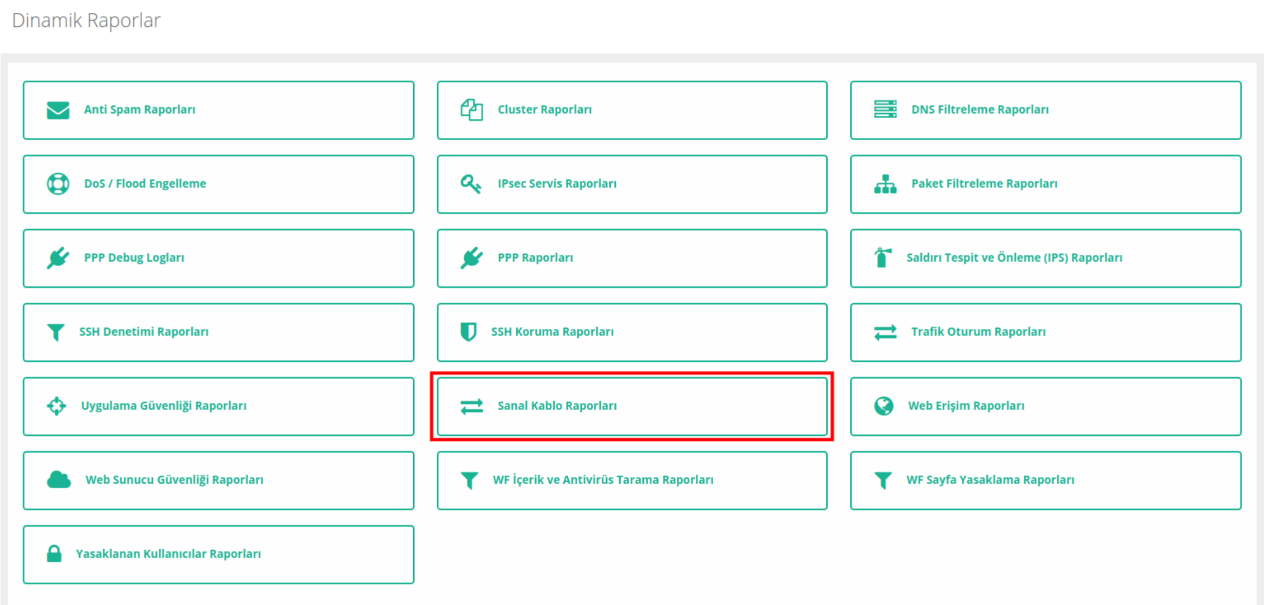
- İstemcide yapılan ICMP testlerinde ilgili IP adresini engellediği ve diğer IP adreslerinin izinli olarak erişim sağlandığı gözlemlenir.

```
C:\Users\epati>ipconfig

Windows IP Configuration


Unknown adapter OpenVPN Wintun:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.2.4.12
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.2.4.253

Unknown adapter OpenVPN TAP-Windows6:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\epati>ping 46.101.122.133

Pinging 46.101.122.133 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 46.101.122.133:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\epati>ping mynet.com

Pinging mynet.com [212.101.122.34] with 32 bytes of data:
Reply from 212.101.122.34: bytes=32 time=25ms TTL=246
Reply from 212.101.122.34: bytes=32 time=23ms TTL=246
Reply from 212.101.122.34: bytes=32 time=24ms TTL=246
Reply from 212.101.122.34: bytes=32 time=24ms TTL=246

Ping statistics for 212.101.122.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 23ms, Maximum = 25ms, Average = 24ms

C:\Users\epati>
```

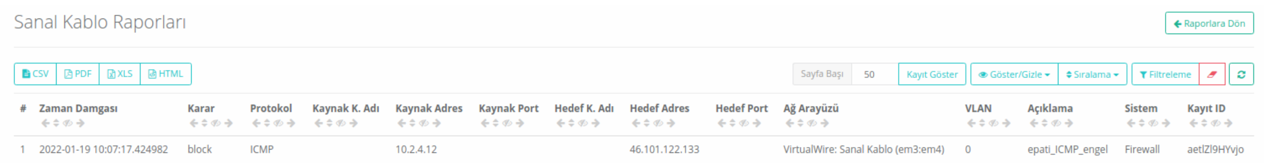
- **Raporlar** menüsü altında bulunan **Dinamik Raporlar** sayfasına gidilir.



- Logları görüntülemek için **Sanal Kablo Raporları**na tıklanır.



- İlgili istemciden belirlediğimiz IP adresinin engel logu görüntülenmektedir.



#	Zaman Damgası	Karar	Protokol	Kaynak K. Adı	Kaynak Adres	Kaynak Port	Hedef K. Adı	Hedef Adres	Hedef Port	Ağ Arayüzü	VLAN	Açıklama	Sistem	Kayıt ID
1	2022-01-19 10:07:17.424982	block	ICMP		10.2.4.12			46.101.122.133		VirtualWire: Sanal Kablo (em3:em4)	0	epati_ICMP_engel	Firewall	aetlZl9HYvjo

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