epati
BİLİŞİM TEKNOLOJİLERİ

Kısa Anlatım

Ürün: Antikor v2 - Layer2 Tünelleme

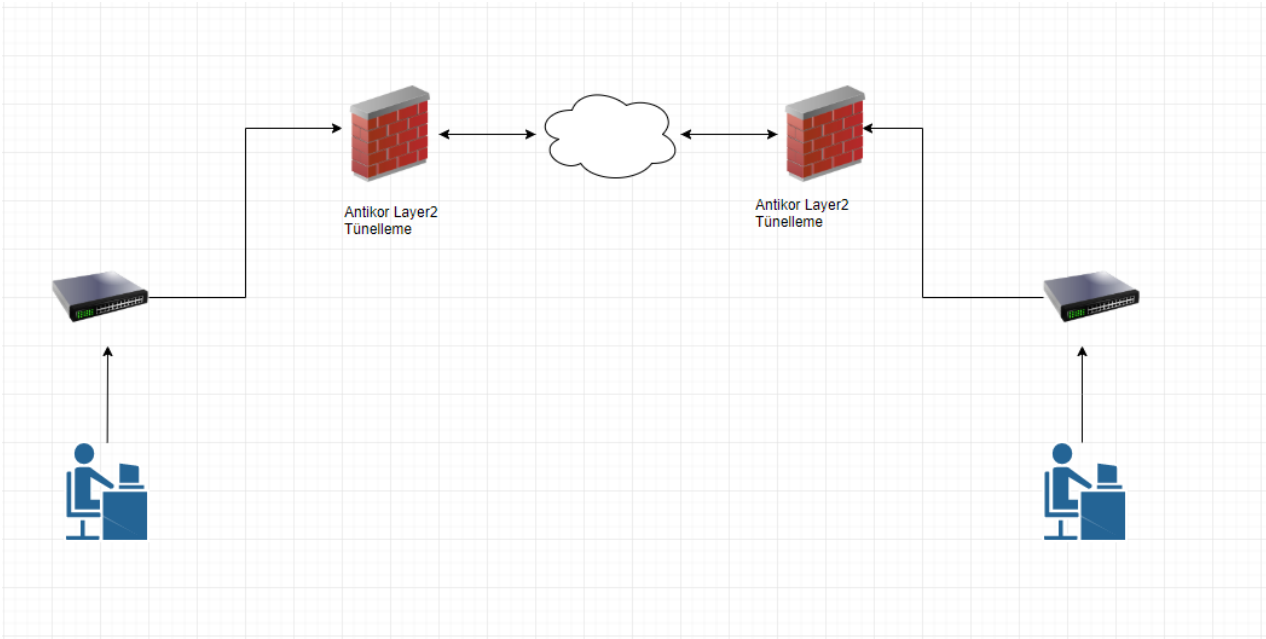
Yapılandırma Örnekleri

www.epati.com.tr

Kısa Anlatım

AntiKor Tünelleme, uzak ağlar arasında IP üzerinden Layer2 düzeyinde güvenli köprüleme yaparak kapalı bir ağ oluşturur. Ağlar arası iletişim şifreli olarak taşınır. Bir ağ, internet üzerinde başka ağ ile aynı switch'e bağlı gibi çalışır. Tünelleme kurulan karşılıklı IP adresleri arasında olan trafikte ayrıca IPsec şifreleme ile taşınabilir.

Network Şeması

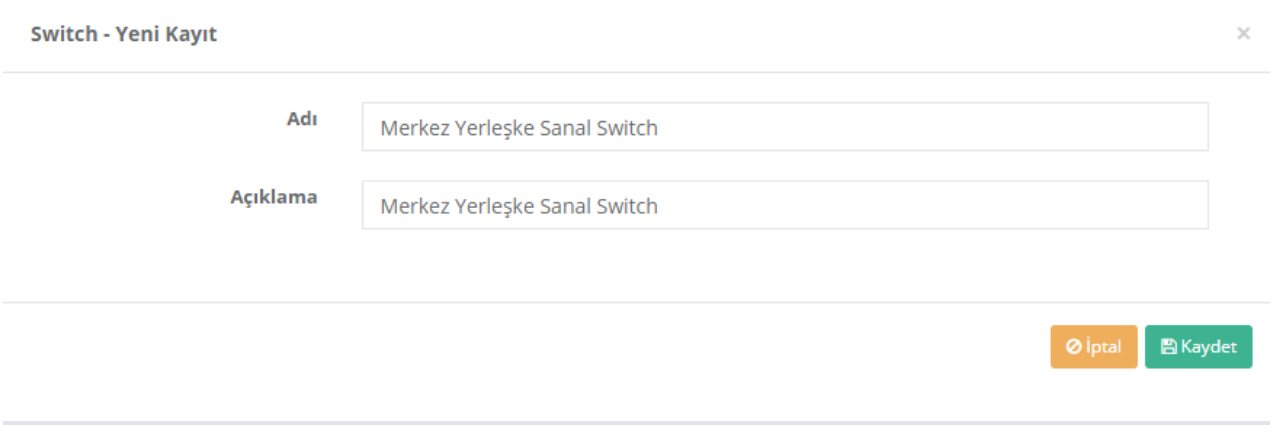


Konfigürasyon

Önemli : Tünel bağlantısı yapılmadan önce kurumlar birbirleriyle Layer3 haberleşmeleri gerekmektedir.

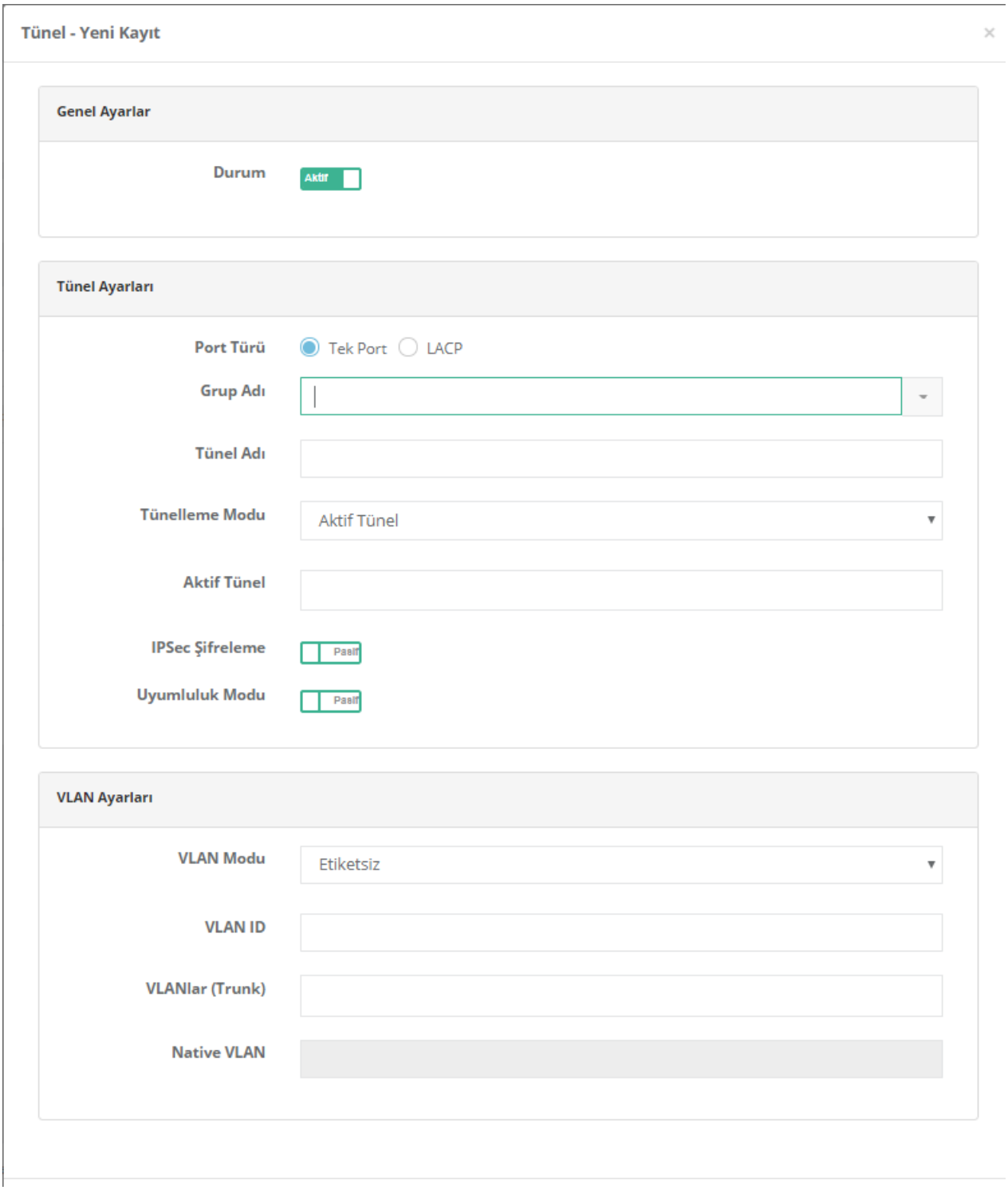
İlk olarak arayüzde **Tünel Yapılandırması** - **tünel ayarları** sayfası açılır.

Açılan sayfada **Switch ekle** butonuna basılarak sanal bir switch oluşturulur, switche ad ve açıklama yazılır.



Switch ekleme işlemi yapıldıktan sonra, oluşturduğumuz switche**fiziksel port ve tünel eklemesi** yapılır.

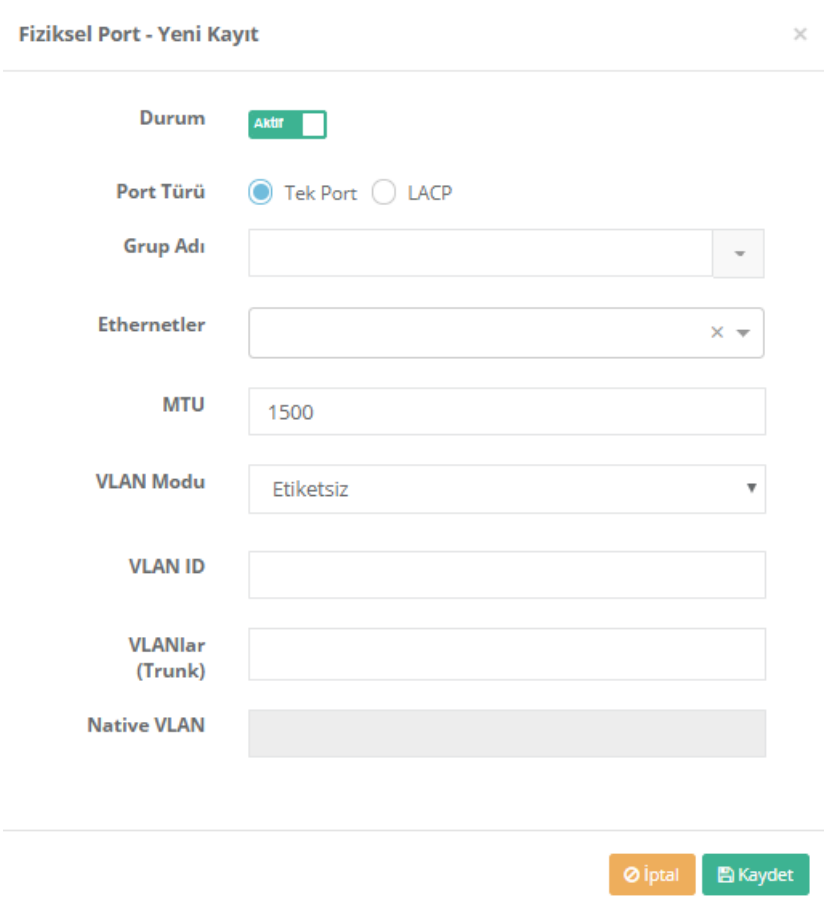
Tünel Ekleme



Genel Ayarlar	Açıklama
Durum	Aktif veya pasif seçilir.

Tünel Ayarları	Açıklama
Port Türü	Tek port veya LACP seçilir.
Grup adı	Grup adı girilir.
Tünel Adı	Tünel Adı girilir.
Tünelleme Modu	Aktif Tünel seçilir.
IPSec Şifreleme	Aktif, Pasif durumu seçilir.
Uyumluluk Modu	Tünel v2 ile uyumlu çalışan moddur.
Aktif Tünel	Karşı tünel IP adresi yazılır.
Vlan Modu	Etiketsiz veya Etiketli ve Etiketsiz seçilir.
Vlan ID	VLAN ID yazılır.
Vlanlar Trunk	Taşınacak vlanlar yazılır.
Native VLAN	native vlan yazılır.

Fiziksel Port Ekleme



Adı	Açıklama
`Durum`	Aktif Pasiflik durumu seçilir.
`Port Türü`	Tek port veya LACP seçilir.
`Ethernetler`	Taşınacak vlanlar için IPsiz bacağın olacağı ethernet arayüzü seçilir.
`MTU`	MTU değeri belirlenir.
`VLAN Modu`	Etiketsiz veya Etiketli ve Etiketsiz seçilir.
`VLAN ID`	VLAN ID yazılır.
`VLANlar Trunk`	Taşınacak vlanlar yazılır.
`Native VLAN`	native vlan yazılır.

Switch Tarafında Yapılacak Ayarlar

Merkez Switch

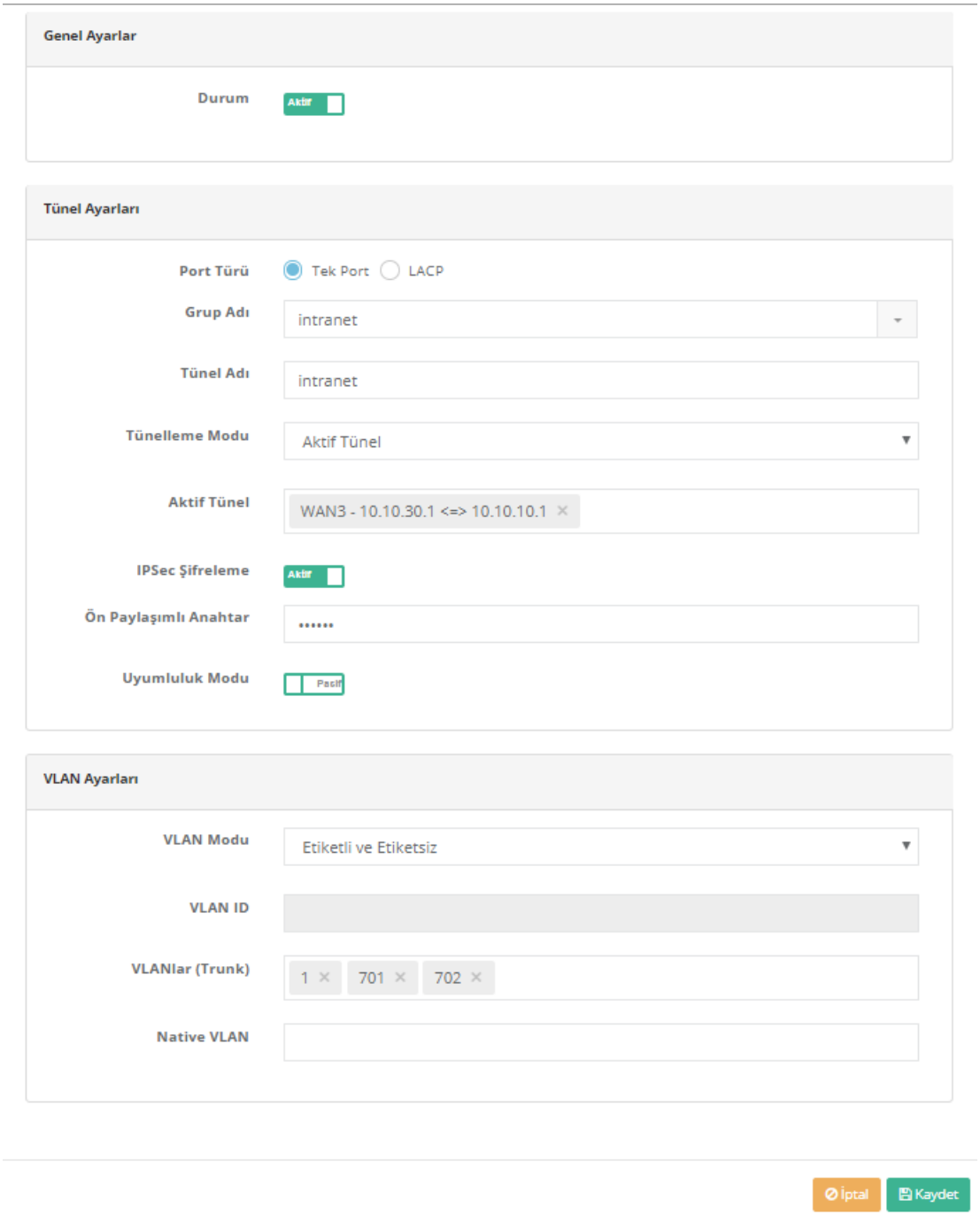
```
Switch#show running-config
Building configuration...
vlan 1
   name "DEFAULT_VLAN"
   untagged 1-4,8-24
   no ip address
   tagged 5
   no untagged 6-7
   exit
vlan 702
   name "Intranet_2"
   untagged 7
   tagged 5
   exit
vlan 701
   name "Intranet_1"
   untagged 6
   tagged 5
   exit
```

Uç Nokta Switch

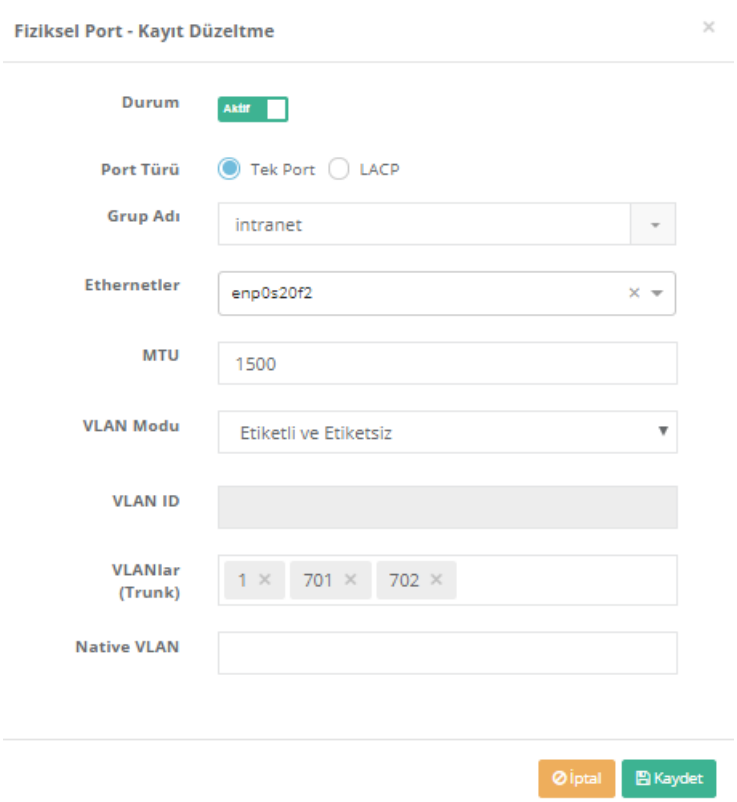
```
Switch#show running-config
Building configuration...
interface FastEthernet4/0/5
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,701,702
 switchport mode trunk
!
interface FastEthernet4/0/6
 switchport access vlan 701
 switchport mode access
!
interface FastEthernet4/0/7
 switchport access vlan 702
 switchport mode access
```

Merkez Yerleşke Tünelleme Ayarları

Tünel ayarları

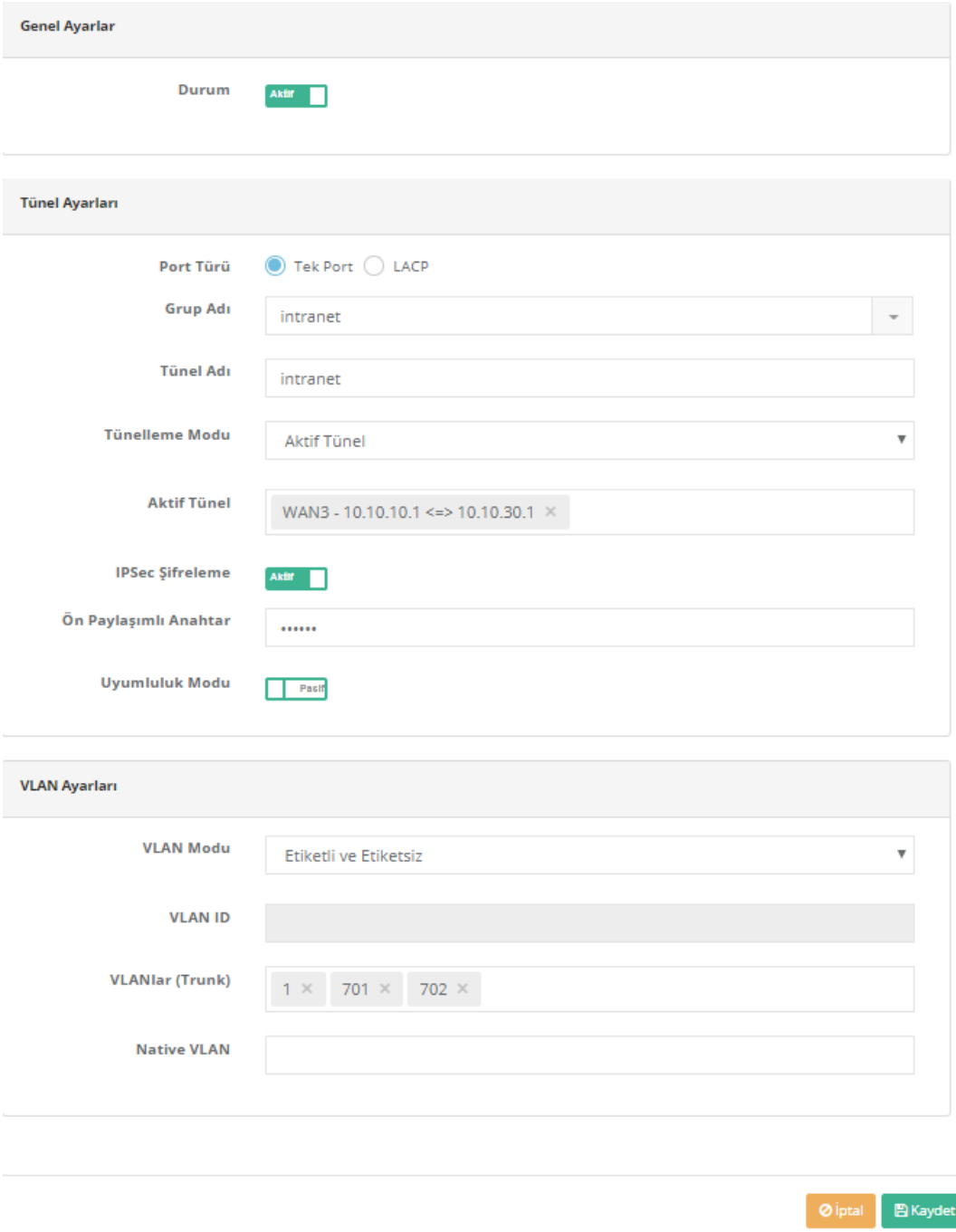


Fiziksel Port Ayarları

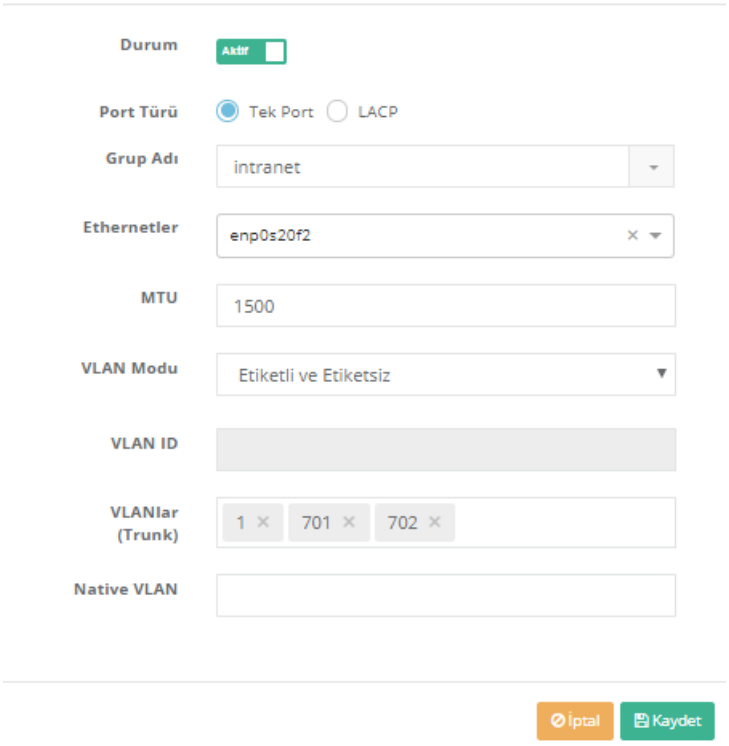


Uç Yerleşke Tünelleme Ayarları

Tünel ayarları



Fiziksel Port Ayarları



Tüm ayarlar tamamlandıktan sonra Gösterge panelinde **Layer2 Tünelleme Motoru** servisinin açılması gerekmektedir.

SSH ile Trafik Gözlemleme

Merkez Antikor Tünelin arkasında 192.168.58.10, Uç yerleşke Antikor tünelin arkasında bulunan 192.168.58.15 IP adresleri tünel sayesinde aynı networkteymiş gibi birbirine ping atabilmektedir. Merkezden uç noktaya taşımış olduğumuz vlan trafiğini SSH'tan takip edebiliriz. **tcpdump -ni enp0s20f2** (tünel ayarlarında taşımış olduğumuz IP'siz bacak). Trafiktende görüldüğü üzere tünel ile uç noktada bulunan herhangi bir cihazın MAC adresini taşıyabilirsiniz.

```
09:32:35.926525 IP 192.168.58.15 > 192.168.58.10: ICMP echo request, id 1, seq 613, length 40
09:32:35.926727 IP 192.168.58.10 > 192.168.58.15: ICMP echo reply, id 1, seq 613, length 40
09:32:36.020367 IP 192.168.58.10 > 192.168.58.15: ICMP echo request, id 10010, seq 597, length 64
09:32:36.021046 IP 192.168.58.15 > 192.168.58.10: ICMP echo reply, id 10010, seq 597, length 64
09:32:36.942183 IP 192.168.58.15 > 192.168.58.10: ICMP echo request, id 1, seq 614, length 40
09:32:36.942412 IP 192.168.58.10 > 192.168.58.15: ICMP echo reply, id 1, seq 614, length 40
09:32:37.044227 IP 192.168.58.10 > 192.168.58.15: ICMP echo request, id 10010, seq 598, length 64
09:32:37.044868 IP 192.168.58.15 > 192.168.58.10: ICMP echo reply, id 10010, seq 598, length 64
09:32:37.957775 IP 192.168.58.15 > 192.168.58.10: ICMP echo request, id 1, seq 615, length 40
09:32:37.958051 IP 192.168.58.10 > 192.168.58.15: ICMP echo reply, id 1, seq 615, length 40
09:32:38.068241 IP 192.168.58.10 > 192.168.58.15: ICMP echo request, id 10010, seq 599, length 64
09:32:38.068955 IP 192.168.58.15 > 192.168.58.10: ICMP echo reply, id 10010, seq 599, length 64
09:32:38.973374 IP 192.168.58.15 > 192.168.58.10: ICMP echo request, id 1, seq 616, length 40
09:32:38.973602 IP 192.168.58.10 > 192.168.58.15: ICMP echo reply, id 1, seq 616, length 40
09:32:39.092250 IP 192.168.58.10 > 192.168.58.15: ICMP echo request, id 10010, seq 600, length 64
09:32:39.092924 IP 192.168.58.15 > 192.168.58.10: ICMP echo reply, id 10010, seq 600, length 64
09:32:39.988961 IP 192.168.58.15 > 192.168.58.10: ICMP echo request, id 1, seq 617, length 40
09:32:39.989192 IP 192.168.58.10 > 192.168.58.15: ICMP echo reply, id 1, seq 617, length 40
09:32:40.116226 IP 192.168.58.10 > 192.168.58.15: ICMP echo request, id 10010, seq 601, length 64
```

tcpdump -eni enp0s20f2 komutu ile vlan trafiğini görebilirsiniz.

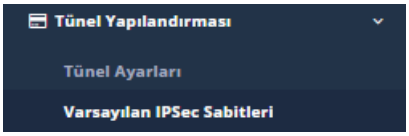
```
tcpdump -eni enp0s20f2
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s20f2, link-type EN10MB (Ethernet), capture size 262144 bytes
09:56:02.816414 00:1e:68:9c:5a:58 > 1c:75:08:33:47:b4, ethertype 802.1Q (0x8100), length 102: vlan 701, p 0, ethertype IPv4, 192.168.58.10 > 192.168.58.15:
, length 64
09:56:02.817213 1c:75:08:33:47:b4 > 00:1e:68:9c:5a:58, ethertype 802.1Q (0x8100), length 102: vlan 701, p 0, ethertype IPv4, 192.168.58.15 > 192.168.58.10:
length 64
09:56:03.574239 1c:75:08:33:47:b4 > 00:1e:68:9c:5a:58, ethertype 802.1Q (0x8100), length 78: vlan 701, p 0, ethertype IPv4, 192.168.58.15 > 192.168.58.10:
gth 40
09:56:03.574464 00:1e:68:9c:5a:58 > 1c:75:08:33:47:b4, ethertype 802.1Q (0x8100), length 78: vlan 701, p 0, ethertype IPv4, 192.168.58.10 > 192.168.58.15:
h 40
09:56:03.817603 00:1e:68:9c:5a:58 > 1c:75:08:33:47:b4, ethertype 802.1Q (0x8100), length 102: vlan 701, p 0, ethertype IPv4, 192.168.58.10 > 192.168.58.15:
, length 64
09:56:03.818390 1c:75:08:33:47:b4 > 00:1e:68:9c:5a:58, ethertype 802.1Q (0x8100), length 102: vlan 701, p 0, ethertype IPv4, 192.168.58.15 > 192.168.58.10:
length 64
09:56:04.589879 1c:75:08:33:47:b4 > 00:1e:68:9c:5a:58, ethertype 802.1Q (0x8100), length 78: vlan 701, p 0, ethertype IPv4, 192.168.58.15 > 192.168.58.10:
gth 40
09:56:04.590125 00:1e:68:9c:5a:58 > 1c:75:08:33:47:b4, ethertype 802.1Q (0x8100), length 78: vlan 701, p 0, ethertype IPv4, 192.168.58.10 > 192.168.58.15:
h 40
09:56:04.818786 00:1e:68:9c:5a:58 > 1c:75:08:33:47:b4, ethertype 802.1Q (0x8100), length 102: vlan 701, p 0, ethertype IPv4, 192.168.58.10 > 192.168.58.15:
, length 64
09:56:04.819557 1c:75:08:33:47:b4 > 00:1e:68:9c:5a:58, ethertype 802.1Q (0x8100), length 102: vlan 701, p 0, ethertype IPv4, 192.168.58.15 > 192.168.58.10:
length 64
```

tcpdump -eni enp0s20f2 vlan 701 komutu ile vlan 701 trafiğini görebilirsiniz.

```
epati:~$ tcpdump -eni enp0s20f2
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s20f2, link-type EN10MB (Ethernet), capture size 262144 bytes
10:03:20.480574 1c:75:08:33:47:b4 > 00:1e:68:9c:5a:58, ethertype 802.1Q (0x8100), length 78: vlan 702, p 0, ethertype IPv4, 192.168.58.15 > 192.168.58.10:
gth 40
10:03:20.480807 00:1e:68:9c:5a:58 > 1c:75:08:33:47:b4, ethertype 802.1Q (0x8100), length 78: vlan 702, p 0, ethertype IPv4, 192.168.58.10 > 192.168.58.15:
h 40
10:03:20.566717 00:1e:68:9c:5a:58 > 1c:75:08:33:47:b4, ethertype 802.1Q (0x8100), length 102: vlan 702, p 0, ethertype IPv4, 192.168.58.10 > 192.168.58.15:
, length 64
10:03:20.567485 1c:75:08:33:47:b4 > 00:1e:68:9c:5a:58, ethertype 802.1Q (0x8100), length 102: vlan 702, p 0, ethertype IPv4, 192.168.58.15 > 192.168.58.10:
length 64
10:03:21.496153 1c:75:08:33:47:b4 > 00:1e:68:9c:5a:58, ethertype 802.1Q (0x8100), length 78: vlan 702, p 0, ethertype IPv4, 192.168.58.15 > 192.168.58.10:
gth 40
10:03:21.496383 00:1e:68:9c:5a:58 > 1c:75:08:33:47:b4, ethertype 802.1Q (0x8100), length 78: vlan 702, p 0, ethertype IPv4, 192.168.58.10 > 192.168.58.15:
h 40
^C
```

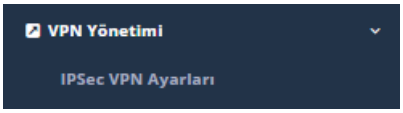
İki Tünel Arası trafiği IPsec ile Şifreleme

İlk olarak sırasıyla **Tünel ayarları** ardından **Varsayılan IPsec sabitleri** sayfası açılır.



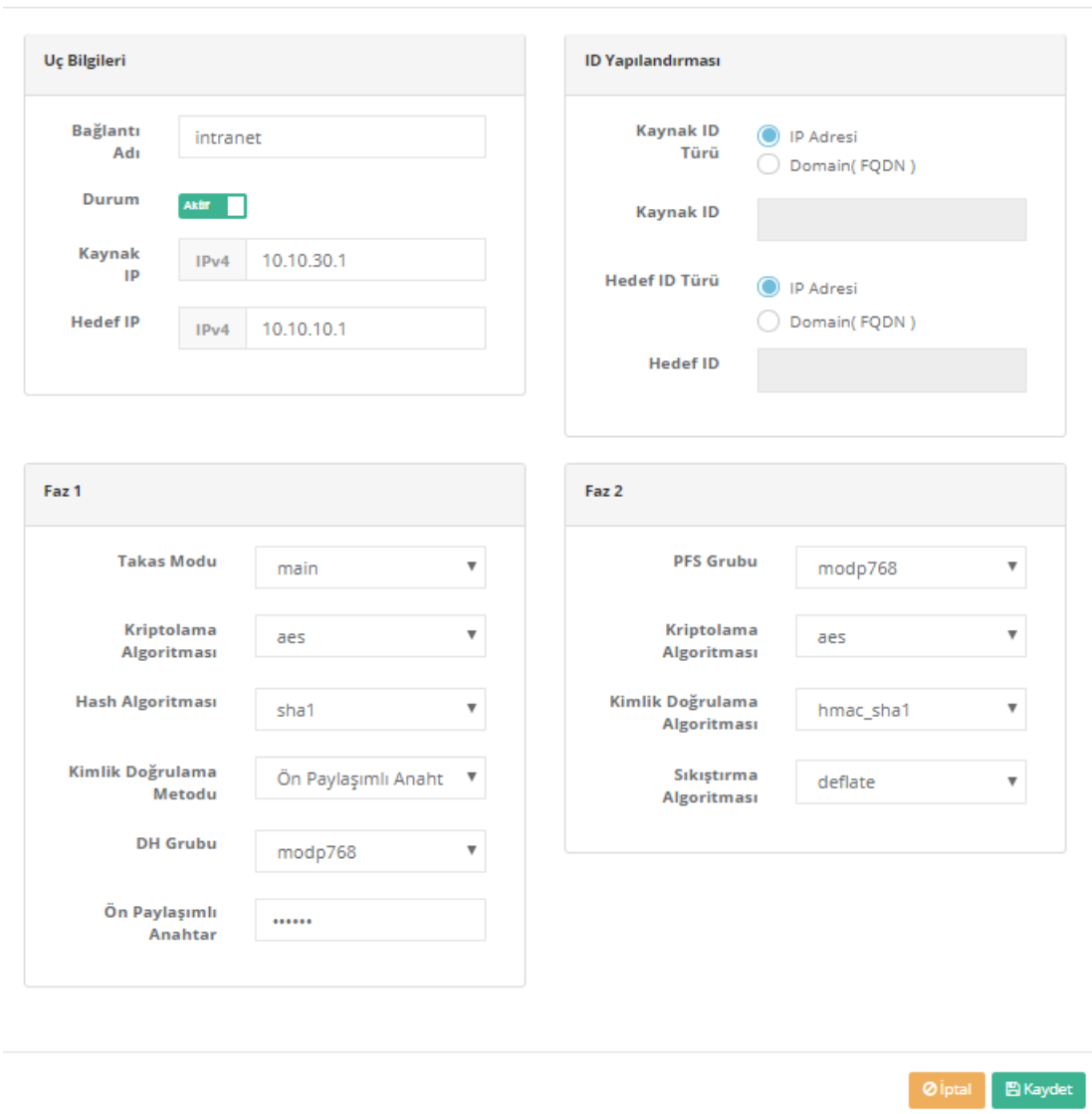
Açılan sayfada default ayarlar kaydedilir. Ipsec sabitlerinde değişiklik yapılacaksa her iki tünelinde sabitleri aynı olmalıdır.

Daha sonra arayüzde **VPN Yönetimi** ardından **IPsec VPN** sayfası açılır.

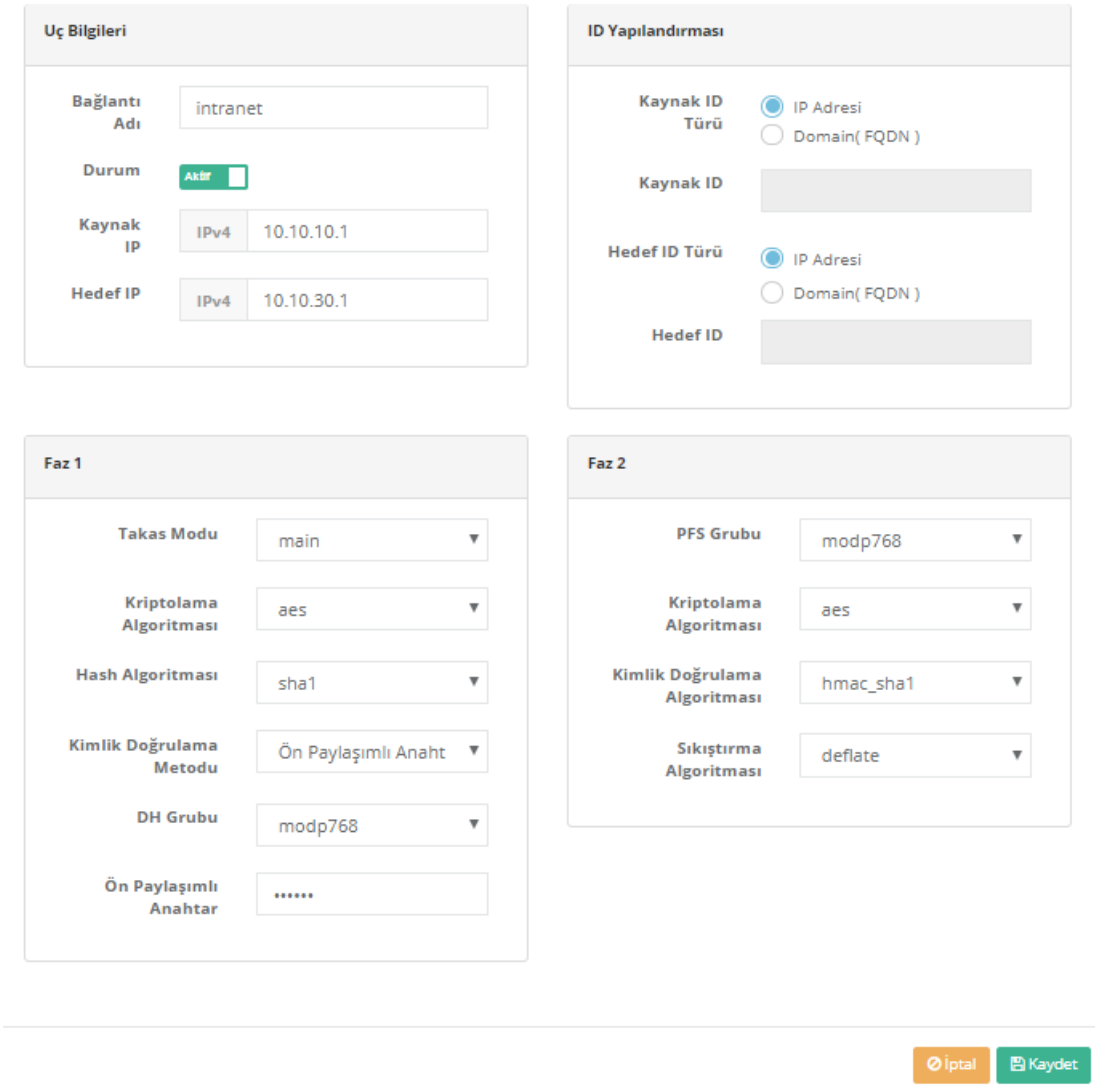


Açılan sayfada İki tünel ile ilgili gerekli ayarlar yapılır. Resimlerde Merkez ve Uç tünelin ayarları görünmektedir.

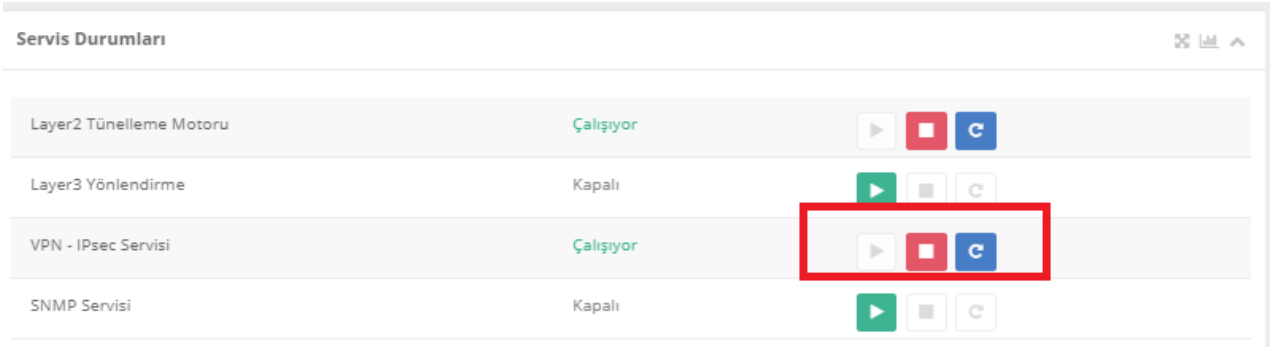
Merkez Tünel



Uç Nokta Tünel



Tüm ayarlar tamamlandıktan sonra gösterge panelinde **VPN - Ipsec** servisi başlatılmalıdır.



SSH ile IPsec Şifreleme trafiğini Gözlemlemek

SSH ile Ipsec trafiğinin sağlıklı aktığını görebilmek için **tcpdump -ni enp0s2f0 (Tünelin WAN bacağı)* trafiği gözlemlenir trafikte **ESP** paketi görünmesi IPsec şifrelemenin çalıştığını göstermektedir.

```
tcpdump -ni enp0s20f0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s20f0, link-type EN10MB (Ethernet), capture size 262144 bytes
10:53:20.247618 IP 10.10.30.1 > 10.10.10.1: ESP(spi=0xcc485d30,seq=0x106), length 140
10:53:20.248256 IP 10.10.10.1 > 10.10.30.1: ESP(spi=0xc1cef8c1,seq=0x102), length 140
10:53:20.510069 Loopback, skipCount 0, Reply, receipt number 0, data (40 octets)
10:53:20.744917 IP 10.10.10.1 > 10.10.30.1: ESP(spi=0xc1cef8c1,seq=0x103), length 116
10:53:20.745314 IP 10.10.30.1 > 10.10.10.1: ESP(spi=0xcc485d30,seq=0x107), length 116
10:53:21.248767 IP 10.10.30.1 > 10.10.10.1: ESP(spi=0xcc485d30,seq=0x108), length 140
10:53:21.249388 IP 10.10.10.1 > 10.10.30.1: ESP(spi=0xc1cef8c1,seq=0x104), length 140
10:53:21.760520 IP 10.10.10.1 > 10.10.30.1: ESP(spi=0xc1cef8c1,seq=0x105), length 116
10:53:21.760887 IP 10.10.30.1 > 10.10.10.1: ESP(spi=0xcc485d30,seq=0x109), length 116
10:53:22.249888 IP 10.10.30.1 > 10.10.10.1: ESP(spi=0xcc485d30,seq=0x10a), length 140
10:53:22.250561 IP 10.10.10.1 > 10.10.30.1: ESP(spi=0xc1cef8c1,seq=0x106), length 140
10:53:22.672871 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 0c:c4:7a:6d:d9:ef, length 548
10:53:22.776083 IP 10.10.10.1 > 10.10.30.1: ESP(spi=0xc1cef8c1,seq=0x107), length 116
10:53:22.776417 IP 10.10.30.1 > 10.10.10.1: ESP(spi=0xcc485d30,seq=0x10b), length 116
10:53:23.251082 IP 10.10.30.1 > 10.10.10.1: ESP(spi=0xcc485d30,seq=0x10c), length 140
10:53:23.251732 IP 10.10.10.1 > 10.10.30.1: ESP(spi=0xc1cef8c1,seq=0x108), length 140
10:53:23.791743 IP 10.10.10.1 > 10.10.30.1: ESP(spi=0xc1cef8c1,seq=0x109), length 116
10:53:23.792086 IP 10.10.30.1 > 10.10.10.1: ESP(spi=0xcc485d30,seq=0x10d), length 116
10:53:24.252240 IP 10.10.30.1 > 10.10.10.1: ESP(spi=0xcc485d30,seq=0x10e), length 140
10:53:24.252886 IP 10.10.10.1 > 10.10.30.1: ESP(spi=0xc1cef8c1,seq=0x10a), length 140
10:53:24.587968 IP 10.10.30.1 > 10.10.10.1: ESP(spi=0xcc485d30,seq=0x10f), length 140
10:53:24.807357 IP 10.10.10.1 > 10.10.30.1: ESP(spi=0xc1cef8c1,seq=0x10b), length 116
10:53:24.807715 IP 10.10.30.1 > 10.10.10.1: ESP(spi=0xcc485d30,seq=0x110), length 116
```

ESP (Encapsulating Security Payload – Kapsüllenen Güvenlik Yükü)

ESP nedir ?

ESP protokolu gizilik ve kimlik denetimini beraber sağlayabilir. Bu protokol öncelikli olarak AH tarafından sıra numarası verilmiş IP paketlerini belirlenmiş algoritmalardan faydalanarak şifrelemek ve hedefe ulaştığında aynı algoritmaları kullanarak çözümlemektir. Böylece AH tarafından oluşabilecek güvenlik açığı engellenmiş olur.