

Kısa Anlatım Ürün: Antikor v2 - Layer2 Tünelleme Yapılandırma Örnekleri



www.epati.com.tr





Switch Ekle

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.

Tünel Ayarları

Switch - Yeni Kayıt		×	
Adı	Merkez Yerleşke Sanal Switch		
Açıklama	Merkez Yerleşke Sanal Switch		
	Ø İptal 🖺 Kayd	et	
Switch ekleme işlemi yapıldıktan sonra, oluşturduğumuz switche fiziksel port ve tünel eklemesi yapılır.			
Merkez Yerleşke Sanal Switch	Tünel Ekle 🛛 Fiziksel Port Ekle 👷 🥒		
Tünel Ekleme			

Genel Ayarlar		
Durum	Aktir	
Tünel Ayarları		
Port Türü	Tek Port	
Grup Adı		r
Tünel Adı		
Tünelleme Modu	Aktif Tünel	Ŧ
Aktif Tünel		
IPSec Şifreleme	Pasit	
Uyumluluk Modu	Paelt	
VLAN Ayarları		
VLAN Modu	Etiketsiz	Ŧ
VLAN ID		
VLANIar (Trunk)		
Native VLAN		

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

Fiziksel Port - Yeni Ka	yıt	×
Durum	Aktir	
Port Türü	Tek Port LACP	
Grup Adı		Ŧ
Ethernetler	×	•
MTU	1500	
VLAN Modu	Etiketsiz	Ŧ
VLAN ID		
VLANIar (Trunk)		
Native VLAN		

🖉 İptal 🛛 🖺 Kaydet

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 dotlq
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

Genel Ayarlar	
Durum	Attr
Tünel Ayarları	
Port Türü	Tek Port LACP
Grup Adı	intranet 👻
Tünel Adı	intranet
Tünelleme Modu	Aktif Tünel 🔻
Aktif Tünel	WAN3 - 10.10.30.1 <=> 10.10.10.1 ×
IPSec Şifreleme	Akir
Ön Paylaşımlı Anahtar	
Uyumluluk Modu	Pacif
VLAN Ayarları	
VLAN Modu	Etiketli ve Etiketsiz
VLAN ID	
VLANIar (Trunk)	1 × 701 × 702 ×
Native VLAN	

🧿 İptal 🔡 Kaydet

Fiziksel Port Ayarları

Fiziksel Port - Kayıt Düzeltme

Durum	Aktif
Port Türü	● Tek Port ◯ LACP
Grup Adı	intranet 👻
Ethernetler	enp0s20f2 × 👻
МТО	1500
VLAN Modu	Etiketli ve Etiketsiz
VLAN ID	
VLANIar (Trunk)	1 × 701 × 702 ×
Native VLAN	
	Ø İptal

Uç Yerleşke Tünelleme Ayarları

Tünel ayarları

Deserver	
Durum	Aktar
ünel Ayarları	
Port Türü	Tek Port LACP
Grup Adı	intranet -
Tünel Adı	intranet
Tünelleme Modu	Aktif Tünel
Aktif Tünel	
	WAN3 - 10.10.10.1 <=> 10.10.30.1 ×
IPSec Şifreleme	Axtir
Ön Paylaşımlı Anahtar	
Uyumluluk Modu	Pacif
/LAN Avarları	
-	
VLAN Modu	Etiketli ve Etiketsiz
VLAN ID	
VLANIar (Trunk)	1 × 701 × 702 ×
Native VLAN	

Øİptal 🖪 Kaydet

Fiziksel Port Ayarları

Durum	Aktir	
Port Türü	Tek Port LACP	
Grup Adı	intranet	Ŧ
Ethernetler	enp0s20f2	× •
МТО	1500	
VLAN Modu	Etiketli ve Etiketsiz	•
VLAN ID		
VLANIar (Trunk)	1 × 701 × 702 ×	
Native VLAN		
		Øİptal 🖺 Kaydet

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

Servis Durumları		× 🖂	L ^
Layer2 Tünelleme Motoru	Çalışıyor	P 🔲 C	
Layer3 Yönlendirme	Kapalı	C	
VPN - IPsec Servisi	Kapalı	C	
SNMP Servisi	Kapalı	C	

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	ΙP	192.168.58.15 >	192.168.58.10:	ICMP	echo	request, id 1, seq 613, length 40
09:32:35.926727	ΙP	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	ΙP	192.168.58.15 >	192.168.58.10:	ICMP	echo	request, id 1, seq 614, length 40
09:32:36.942412	ΙP	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	ΙP	192.168.58.15 >	192.168.58.10:	ICMP	echo	reply, id 10010, seq 598, length 64
09:32:37.957775	ΙP	192.168.58.15 >	192.168.58.10:	ICMP	echo	request, id 1, seq 615, length 40
09:32:37.958051	ΙP	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	ΙP	192.168.58.15 >	192.168.58.10:	ICMP	echo	reply, id 10010, seq 599, length 64
09:32:38.973374	ΙP	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	ΙP	192.168.58.10 >	192.168.58.15:	ICMP	echo	request, id 10010, seq 600, length 64
09:32:39.092924	ΙP	192.168.58.15 >	192.168.58.10:	ICMP	echo	reply, id 10010, seq 600, length 64
09:32:39.988961	ΙP	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	ΙP	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 ful	ll protocol decode		
listening on enp0s20f2, link-type EN10MB (Ethernet), cap	ture size 262144 bytes		
09:56:02.816414 00:1e:68:9c:5a:58 > 1c:75:08:33:47:b4, et	thertype 802.1Q (0x8100), le	ength 102: vlan 701, p 0, ethertype	IPv4, 192.168.58.10 > 192.168.58.15:
, length 64			
09:56:02.817213 lc:75:08:33:47:b4 > 00:le:68:9c:5a:58, e	thertype 802.1Q (0x8100), le	ength 102: vlan 701, p 0, ethertype	IPv4, 192.168.58.15 > 192.168.58.10:
length 64			
09:56:03.574239 lc:75:08:33:47:b4 > 00:le:68:9c:5a:58, e	thertype 802.10 (0x8100), le	ength 78: vlan 701, p 0, ethertype I	Pv4, 192.168.58.15 > 192.168.58.10:
gth 40			
09:56:03.574464 00:le:68:9c:5a:58 > lc:75:08:33:47:b4, e	thertype 802.10 (0x8100), le	ength 78: vlan 701, p 0, ethertype I	Pv4, 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, e	thertype 802.1Q (0x8100), le	ength 102: vlan 701, p 0, ethertype	IPv4, 192.168.58.10 > 192.168.58.15:
, length 64			
09:56:03.818390 lc:75:08:33:47:b4 > 00:1e:68:9c:5a:58, e	thertype 802.10 (0x8100), le	ength 102: vlan 701, p 0, ethertype	IPv4, 192.168.58.15 > 192.168.58.10:
length 64			
09:56:04.589879 lc:75:08:33:47:b4 > 00:le:68:9c:5a:58, e	thertype 802.10 (0x8100), le	ength 78: vlan 701, p 0, ethertype I	Pv4, 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, e	thertype 802.1Q (0x8100), le	ength 78: vlan 701, p 0, ethertype I	Pv4, 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, e	thertype 802.10 (0x8100), le	ength 102: vlan 701, p 0, ethertype	IPv4, 192.168.58.10 > 192.168.58.15:
, length 64			
09:56:04.819557 lc:75:08:33:47:b4 > 00:le:68:9c:5a:58, e	thertype 802.10 (0x8100), le	ength 102: vlan 701, p 0, ethertype	IPv4, 192.168.58.15 > 192.168.58.10:

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

epati:~\$ topdump) -eni enp0s20f																
tcpdump: verbose	output suppre	ssed, use	-v or -vv for :	full protoc	col deco	de											
listening on enp	0s20f2, link-t	ype EN10M	(Ethernet), ca	apture size	262144	bytes											
10:03:20.480574	lc:75:08:33:47	:b4 > 00:	le:68:9c:5a:58,	ethertype	802.1Q	(0x8100),	length	78: v	7lan 7	02, p	0, 6	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: v	7lan 7	02, p	0, 6	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, 1	р O,	ethertype	e IPv4,	192.168.5	8.10 :	> 192.16	8.58.15:
, length 64																	
10:03:20.567485	lc:75:08:33:47	:b4 > 00:	le:68:9c:5a:58,	ethertype	802.1Q	(0x8100),	length	102:	vlan	702, 1	р0,	ethertype	e IPv4,	192.168.5	8.15 :	> 192.16	8.58.10:
length 64																	
10:03:21.496153	lc:75:08:33:47	:b4 > 00:	le:68:9c:5a:58,	ethertype	802.1Q	(0x8100),	length	78: v	7lan 7	02, p	0, 6	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: v	7lan 7	02, p	0, 6	ethertype	IPv4,	192.168.58	.10 >	192.168	.58.15:
h 40																	

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

Bağlant: intranet Adi intranet Durum ast Kaynak IPvd IPvd 10.10.30.1 Hedef IP IPvd IPvd 10.10.10.1 Faz 1 Takas Modu Main Kriptolama Algoritmasi Sha1 Metedu On Paylaşımli Anaht Metedu Modp768 V Algoritmasi Ön Paylaşımli Anahtar Sikıştırma Algoritmasi Sikıştırma Algoritmasi On Paylaşımli Impart Sikıştırma Algoritmasi Sikıştırma Algoritmasi Sikıştırma Impart Sikıştırma Impart Sikıştırma Impart Impart Impart Impart Impart Impart Impart Impart Impart Impart Impart Impart Impart Impart Impart Impart Impart Impart <tr< th=""><th>Uç Bilgileri</th><th></th><th></th><th></th><th>ID Yapılandırması</th><th></th><th></th><th></th></tr<>	Uç Bilgileri				ID Yapılandırması			
Durum Att Kaynak IP IP 10.10.30.1 Hedef IP IP IP 10.10.10.1 Faz 1	Bağlantı Adı	intran	et		Kaynak ID Türü		P Adresi)omain(FQDN)	
Kaynak IP Hedef IP IP ID ID Faz 1 Faz 1 Faz 1 Kriptolama Algoritmasi Algoritmasi Sha1 V Metodu On Paylaşımlı Anahtar On Paylaşımlı Image: Imag	Durum	Aktir	l		Kaynak ID			
Hedef IP IPv4 10.10.10.1 Faz 1 Faz 1 Takas Modu main Xriptolama Algoritmasi Sha1 V Kimlik Doğrulama Metodu Ön Paylaşımlı Anahtar Sikiştirma Algoritmasi Sikiştirma Algoritmasi Metodu Medp768 Sikiştirma Algoritmasi Algoritmasi Anahtar Netodu </th <th>Kaynak IP</th> <th>IPv4</th> <th>10.10.30.1</th> <th></th> <th>Hedef ID Türü</th> <th></th> <th>D Adresi</th> <th></th>	Kaynak IP	IPv4	10.10.30.1		Hedef ID Türü		D Adresi	
Faz 1 Takas Modu main Takas Modu main Takas Modu main Takas Modu main Takas Modu main Takas Modu main Takas Modu main Takas Modu main Takas Modu Main Mash Algoritmasi Sha1 Takas Modu Ön Paylaşımlı Anahtar Hash Algoritmasi Sikiştirma Algoritmasi Metodu Modp768 Takas Modu Metodu Modp768 Metodu Modp768 Metodu Modp768 Takas Modu Metodu Modp768 Metodu Modp768 Metodu Modp768 Takas Metodu Modp768 Takas Metodu Modp768 Metodu Modp768 Mahtar Mahtar Metodu Metodu Metodu Metodu Metodu Metodu	Hedef IP	IPv4	10.10.10.1			0	Domain(FQDN)	
Faz 1 Takas Modu main Takas Modu main Kiptolama Algoritmasi aes Hash Algoritmasi Sha1 Kimlik Doğrulama Metodu Ön Paylaşimli Anahtar Faz 2 PFS Grubu Modp768 Kimlik Doğrulama Metodu Modp768 Sikiştırma Algoritmasi Metodu Modp768 Sikiştırma Algoritmasi Metodu Modp768 Metodu Modp768 Metodu Modp768 Anahtar Metodu Modp768 Metodu Modp768 Metodu Modp768 Metodu Modp768 Metodu Modp768 Metodu Metodu Metodu Metodu Metodu Metodu Metodu Metodu Metodu Metodu Metodu Metodu Metodu Metodu					Hedef ID			
Faz 1 Faz 2 Takas Modu main Kriptolama aes Algoritmasi aes Hash Algoritmasi sha1 Kimlik Doğrulama Ön Paylaşımlı Anaht Metodu modp768 Ön Paylaşımlı modp768								
Takas Modu main Kriptolama Algoritmasi Algoritmasi Sha1 Nash Algoritmasi Sha1 Sha1 Metodu Ön Paylaşımlı Anahtar PFS Grubu modp768 Metodu modp768 Metodu	Faz 1				Faz 2			
Kriptolama aes Algoritması sha1 Hash Algoritması sha1 Sha1 Kimlik Doğrulama Metodu Ön Paylaşımlı Anaht DH Grubu modp768 Ön Paylaşımlı Anahtar	Takas	Modu	main	•	PFS Grub	u	modp768	Ŧ
Hash Algoritması sha1 ▼ Kimlik Doğrulama Metodu Ön Paylaşımlı Anaht ▼ DH Grubu modp768 ▼ Ön Paylaşımlı Anahtar	Kript Algor	olama itması	aes	•	Kriptolam Algoritmas	a 51	aes	•
Kimlik Doğrulama Metodu Ön Paylaşımlı Anaht Sıkıştırma Algoritması deflate DH Grubu modp768 Ön Paylaşımlı Anahtar	Hash Algor	itması	sha1	•	Kimlik Doğrulam Algoritmas	a 51	hmac_sha1	*
DH Grubu modp768 v Ön Paylaşımlı Anahtar	Kimlik Doğr M	ulama letodu	Ön Paylaşımlı Anaht	•	Sıkıştırm Algoritmas	a 51	deflate	*
Ön Paylaşımlı Anahtar	DH	Grubu	modp768	•				
	Ön Payl Ar	aşımlı nahtar	•••••					
	0							

Uç Nokta Tünel

ıç Bilgileri				ID Yapılandırması			
Bağlantı Adı	intrane	et		Kaynak ID Türü		Adresi main(FQDN)	
Durum	Aktir			Kaynak ID			
Kaynak IP	IPv4	10.10.10.1		Hedef ID Türü		A data ai	
Hedef IP	IPv4	10.10.30.1				main(FQDN)	
				Hedef ID			
az 1				Faz 2			
Takas	Modu	main	Ŧ	PFS Grub	u	modp768	•
Kripto Algori	olama itması	aes	•	Kriptolam Algoritma:	a 51	aes	•
Hash Algori	tması	sha1	•	Kimlik Doğrulam Algoritma:	a 51	hmac_sha1	•
Kimlik Doğru M	ulama etodu	Ön Paylaşımlı Anaht	•	Sıkıştırm Algoritma:	a 51	deflate	Ψ.
DH	Grubu	modp768	•				

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

Servis Durumları			21日入
Layer2 Tünelleme Motoru	Çalışıyor	> 🗖 C	
Layer3 Yönlendirme	Kapalı	> = c	
VPN - IPsec Servisi	Çalışıyor		
SNMP Servisi	Kapalı	C	

SSH ile IPsec Şifreleme trafiğini Gözlemlemek

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

ccpdump -ni enp0s20f0
copdump: 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=0xclcef8cl,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=0xclcef8cl,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=0xclcef8cl,seq=0x104), length 140
10:53:21.760520 IP 10.10.10.1 > 10.10.30.1: ESP(spi=0xclcef8cl,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=0xclcef8cl,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=0xclcef8cl,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=0xclcef8cl,seq=0x108), length 140
10:53:23.791743 IP 10.10.10.1 > 10.10.30.1: ESP(spi=0xclcef8cl,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=0xclcef8cl,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=0xclcef8cl,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.

epati Bilişim Teknolojileri San. ve Tic. Ltd. Şti. Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN

