epati

Sanal Kablo ile Filtreleme Yapılandırması

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı Yapılandırma Örnekleri

www.epati.com.tr

EPOTI 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

Sanal Ka	blo					C Yenile + Ekle
XLS	CSV PDF				📾 Göster/Gizle 👻 Sayfa Başı Kayıt Sayısı	Tamam Tiltrele Filtreyi Temizle
#	Adı	👫 Durum	↓î Üye 1	↓î Üye 2	1 Yazılımsal RSS	1 işlemler

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

Sanal Kablo - Yeni Kayıt							
Durum	Aktif						
Adı							
Üye 1	Select						
Üye 2	Select	· ·					
Yazılımsal RSS	Pasif						
		📀 İptal 🛛 🖺 Kaydet					

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.

Durum	Aktif	
Adı	Sanal Kablo	
Üye 1	em3(Sanal Kablo)	· ·
Üye 2	em4(Sanal Kablo)	· ·
Yazılımsal RSS	Pasif	
		🖉 İptal 🛛 🖹 Kaydet

Sanal Kablo							Tanımları Uygula 1
Sanal Kablo							C Yenile + Ekle
XLS CSV PDF				⊞ Göster/Gizle ▼	Sayfa Başı Kayıt Sayısı	Taman	n 🔻 Filtrele 🖌 Filtreyi Temizle
# Adı	↓ L Durum	Ĵî Üye 1	Ĵ↑ Üye 2	1 Yazılımsal RSS		lî İşlemler	
1 Sanal Kablo	Aktif	em3	em4	Pasif		🕼 Düzenle 👔 S	il
			« < 1 > »				Git
Uygulanacak İşlem	Listesi						Tanımları Uygula 1
							🗃 Hepsini Uygula
Sanal Kablo Vapilandu	rması 🗿						

Uygulanacak İşlem Listesi



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

E		antikor v2 NGFW Staging - STAGING	Sayfa ismi girmeye başlayın	Q 🕪 Çıkış Yap	
Gösterge Paneli					
Sistem Kullanımı	^ ×	Servis Durumları		20 6	山 ^
CPU Bellek	Disk	Balkūpū Servisi	Kapalı	> = C	
17% 79%	6%	Karadelik Servisi	Kapalı	> = c	
0 100 0 10	0 0 100	Anti-Spoof Servisi	Kapalı	C	
		Güvenlik Duvarı	Çalışıyor	🕨 🗖 😋	
Arayüz Durumları	~ ×	Sanal Kablo Motoru	Kapalı		
Gruplanmamış	Sanal Kablo - Sanal Kablo	Web Sunucu Güvenliği	Kapalı	P = C	
		Uygulama Güvenliği / IPS Motoru	Çalışıyor	> 🗖 C	
		🖌 Uygulama Güvenliği Kuralları	Kapalı	> = C	
em0 em1 em2 em5 WAN1 LAN1 LAN2 MGMT	em3 em4	😐 IPS Kuralları	Kapalı	> = c	
005056:a1:23:8 005056:a1:7e:fb 005056:a1:88:68 005056:a1:88:5e Devrede Devrede Devrede Devrede 1000hear	00:50:56:a1:ab:5d 00:50:56:a1:90:ac Devrede Devrede	Antivirüs Motoru	Kapalı	> = C	
TUUUDase1 TUUUDase1 TUUUDase1 TUUUDase1	1000base1	Web Filtreleme Motoru	Kapalı	> = C	
		↦ Forwarded For Bilgisini Gizle	🖨 ByPass 📕		
Ethernet Bant Genişliği Kullanımı	Tümü × 👻	↦ HTTP Denetim Servisi	ByPass	> . C	
	~ X	↦ HTTPS Denetim Servisi	ByPass	► ■ C	
2 Mbit/s		🖌 Sayfa Yasaklama Servisi	ByPass	> • •	

• Gösterge panelinde servis durumlarından Sanal Kablo Motoru açılır.

Gösterge Paneli



Servis Durumları			8 Iai 🔺
Balkūnū Servisi	Kapalı		
Kandalli Gandal	Kapali		
Karadelik Servisi	каран		
Anti-Spoof Servisi	Kapalı	C	
Güvenlik Duvarı	Çalışıyor	> C	
Sanal Kablo Motoru	Kapalı		
Web Sunucu Güvenliği	Kapalı	► = C	
Uygulama Güvenliği / IPS Motoru	Çalışıyor	> 🗖 C	
↦ Uygulama Güvenliği Kuralları	Kapalı		
↦ IPS Kuralları	Kapalı	> • •	
Antivirüs Motoru	Kapalı	> (
Web Filtreleme Motoru	Kapalı	P = C	
➡ Forwarded For Bilgisini Gizle	🔒 ByPass 📕		
↦ HTTP Denetim Servisi	🔒 ByPass 📕		
HTTPS Denetim Servisi	🔒 ByPass 📕		
↦ Sayfa Yasaklama Servisi	🔒 ByPass 📕		

Gösterge Paneli

Sistem Kullanımı	^ ×	Servis Durumları		X Lill 🔺
CPU Bellek	Disk	Balküpü Servisi	Kapalı	
20% 80%	6%	Karadelik Servisi	Kapalı	
0 100 0 100	0 100	Anti-Spoof Servisi	Kapalı	
Annua Dunumlan		Güvenlik Duvarı	Çalışıyor	> C
Arayuz Duruman	^ ×	Sanal Kablo Motoru	Çalışıyor	> [c
Gruplanmamış	Sanal Kablo - Sanal Kablo	Web Sunucu Güvenliği	Kapalı	C
		Uygulama Güvenliği / IPS Motoru	Çalışıyor	> C
		↦ Uygulama Güvenliği Kuralları	Kapalı	C
em0 em1 em2 em5 WAN1 LAN1 LAN2 MGMT	em3 em4	↦ IPS Kuralları	Kapalı	D C
00:50:56:a1:22:3e 00:50:56:a1:7e:rb 00:50:56:a1:e8:68 00:50:56:a1:6a:5e Devrede Devrede 0:50:56:a1:ab:5d 00:50:56:a1:90:ac Devrede Devrede	Antivirüs Motoru	Kapalı	C	
1000base i 1000base i 1000base i 1000base i	1000base1 1000base1	Web Filtreleme Motoru	Kapalı	C
		↦ Forwarded For Bilgisini Gizle	🔒 ByPass 📕	▶ ■ C
Ethernet Bant Genişliği Kullanımı	ūmū × 👻	↦ HTTP Denetim Servisi	🖨 ByPass 🚺	
	^ ×	↦ HTTPS Denetim Servisi	🔒 ByPass 📕	► ■ C
1 Mbit/s		↦ Sayfa Yasaklama Servisi	🔒 ByPass 📕	

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



• Güvenlik Ayarları menüsü altında bulunan Güvenlik Kurallarına gidilir.



• Yeni bir Güvenlik Kuralı Paketi eklenir.

Güvenlik Kı	ıralları Pak	ketleri						2 Yenile + Ekle
XLS CSV	/ PDF				⊞ Göster/Gizle ▼	Sayfa Başı Kayıt Sayısı	Tamam T iltrele	🖌 Filtreyi Temizle
Sıra 🄱	Durum	.↓† Adı	👫 Kaynak Adres	1 Hedef Adres	ំ† Sanal Kablolar ំំំំំំំំំំំំំំំំំំំំំំំំំំំំំំំំំំំំ	İşlemler		
0	Aktif	Ana Kural Se	ti (Adet: 2) 0.0.0.0/0 ::/0	(Adet: 2) 0.0.0.0/0 ::/0		🛡 Kurallar (8) 🖉 Kopyala	🕼 Düzenle 👔 Sil 🔹	¥
				« < 1 > »				Git

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

Güvenlik Kuralları Paketleri - Yer	ii Kayıt	×
Makine Adı	sanalkablokural	
Durum	Aktif	
Sira No	0	
Adı	SanalKabloKural	
Paket Modu	🔵 Yönlendirme 🔘 Sanal Kablo	
Sanal Kablolar	Sanal Kablo (em3 - em4) X 🗸 🗸	
Açıklama	Sanal Kablo Güvenlik Politikaları	

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

Güven	ik Ku	ıralları Pa	aketle	ri														🛛 Yenile	+ Ekle
XLS	CSV	PDF									🖽 Göster/Gizle 👻	Sa	ayfa Başı Kayıt Sayı	ISI	Tamam	T Filt	rele	🖌 Filtreyi	Temizle
Sira	1£	Durum	11	Adı		Kaynak Adres		lt i	Hedef Adres	J1	Sanal Kablolar	11	İşlemler						
C		Aktif		SanalKabloKura		(Adet: 0)		1	(Adet: 0)		Sanal Kablo (em3 - em4)		🛡 Kurallar (0)	🔄 Kopyala	🕼 Düzenle	💼 Sil	1	*	
1		Aktif		Ana Kural Seti		(Adet: 2) 0.0.0.0	0/0 ::/0	[(Adet: 2) 0.0.0.0/0 ::/0				🛡 Kurallar (8)	🕲 Kopyala	🕼 Düzenle	💼 Sil	1	*	
									« c 1 >	Ð									Git
٠	Ek	i le bu	utor	nuna tik	lan	nır.													
Güver	lik Kı	uralları -	Sanali	KabloKural							< Pa	ketler	🛛 Çakışma Analiz	zlerini Güncelle	🛃 İstatisti	kleri Göste	r 🧯	🕽 Yenile	+ Ekle
XLS	CS	V PDF									⊞ Göster/Gizle ▼	Sa	ıyfa Başı Kayıt Sayı	SI	Tamam	T Filt	rele	🖌 Filtreyi	Temizle
Sıra	11	ID D ↓†	urum	Kaynak Iî Adres		Hedef S Adres J†	Servisler	İşler Î	m Kaynak Güvenlik ‡1 Bölgesi	ļţ	Hedef Güvenlik A Bölgesi Iî	Açıklar	na Zaman ↓† Dilimleri	Oluş ↓† Tari	sturma hi 🎝	Günce Tarihi	lleme	lt I	şlemler
									« < > »										Git

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

×

enel Kurallar			IP Kuralları	
Sıra No			Kaynak	Listedekiler Hariç
Durum	Aktif		Adres	10.2.4.0/24 ×
İşlem	Engelle	~	Hedef Adres	Listedekiler Hariç
Trafiği Logla	Açık			40.101.122.135 A
Ağ Geçidi	Varsayılan	~	Servisler	ICMP_ANY X V +
Açıklama	epati_ICMP_engel			
İnceleme Yöntemi	Akii STATEFULL			
ağlantı Sayısı Lim	itleri		Zamanlayıcı	
Flood ataklarına ayarlayabilirsini	ı karşı seçtiğiniz protokolün limitlerini bu panelden z.		Zaman Dilimleri	Seçiniz
Kişi Başı Ma	Bağlantı Sayısı Limitle Pasif ximum Bağlantı Sayısı			
5 Sanivede Ma	ximum Bağlantı Sayısı			

Güvenlik Kuralları - Yeni Kayıt

Güvenlik Kuralları - SanalKabloKural	≮ Paketler Ø Çakışma Analizlerini Güncelle 🗠 İstatistikleri Göster Ø Yenile + Ekle
XLS CSV PDF	I Göster/Gizle → Sayfa Başı Kayıt Sayısı Tamam T Filtrele V Filtreyi Temizle
Sıra ID Durum Kaynak Hedef Servisler İşlem Kaynak Hedef Adres Adres Güvenlik Güvenlik ఓ 네 네 네 데 데 데 데 Bölgesi 네 Bölgesi 네	Açıklama Zaman Oluşturma Güncelleme İşlemler Dilimleri Tarihi Tarihi 1 lî lî
8 6 Aktif 2 (Adet: 1) (Adet: 1) Servis: ICMP_ANY Engelle Tümü Tümü 102.4.0/24 46.101.122.133	epati_ICMP_engel 19.01.2022 19.01.2022 2 2 2 2 10.01.2022 10:06:03
	GR
• Tanımlar uygulanır.	
Güvenlik Kuralları	Tanımları Uygula 🔳
Güvenlik Kuralları - SanalKabloKural	CPaketter ②Çakışma Analizlerini Güncelle Ld İstatistikleri Göster ②Yenile + Eke
XLS CSV PDF	■ Göster/Gizle - Sayfa Başı Kayıt Sayısı Tamam Teiltrele Filtrele Filtrele
Sıra ID Durum Kaynak Hedef Adres Servisler İşlem Kaynak Hedef Güvenli Ik II II Adres II II II Güvenlik Bölgesi I Bölgesi	lik Açıklama Zaman Oluşturma Güncelleme İşlemler İT Dilimleri İT Tarihi İT Tarihi İT
8 6 Aktif (2 (Adec 1) (Adec 1) Servici (CMP, ANY Engelie Tumu Tumu 192.4.6/24 44.191.122.133	epati_ICMP_engel 19.01.2022 19.01.2022 27 20 0 + +
	00
Uygulanacak İşlem Listesi	Tanımları Uygula 1
	E Hepsini Uygula
Sanal Kablo - Güvenlik Kuralları 🕑	Uygula
Uygulanacak İşlem Listesi	
Tüm Uygulama	alar Güncel

• 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:
   Connection-specific DNS Suffix . :
Ethernet adapter Ethernet0 2:
   Connection-specific DNS Suffix . :
   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.

🖹 Raporlar

HTTP Erişim Raporları HTTPS Erişim Raporları Proxy Erişim Raporları DHCPv4 Raporları DHCPv6 Raporları Sistem Raporları Sistem Yönetim Raporları Rapor Ayarları Rapor Yönetimi Rapor Arşivi Veritabanı Raporları Oturum Geçmişi SSL VPN Raporları En Çok Ziyaret Edilen Adresler Güvenlik Duvarı Raporları Dinamik Raporlar

Dinamik Raporlar

Anti Spam Raporları	Cluster Raporlari	DNS Filtreleme Raporları
DoS / Flood Engelleme	R IPsec Servis Raporları	Paket Filtreleme Raporları
🖋 PPP Debug Logiari	💅 PPP Raporları	Saldırı Tespit ve Önleme (IPS) Raporları
SSH Denetimi Raporları	SSH Koruma Raporları	Trafik Oturum Raporları
Uygulama Güvenliği Raporları	Sanal Kablo Raporları	Web Erişim Raporları
Web Sunucu Güvenliği Raporları	WF İçerik ve Antivirüs Tarama Raporları	WF Sayfa Yasaklama Raporları
Asaklanan Kullanıcılar Raporları		

• Logları görüntülemek için Sanal Kablo Raporlarına tıklanır.

Dinamik Raporlar

Mnti Spam Raporlari	Cluster Raporlari	DNS Filtreleme Raporları
DoS / Flood Engelleme	R IPsec Servis Raporları	Paket Filtreleme Raporlari
💋 PPP Debug Logları	y PPP Raporları	Saldırı Tespit ve Önleme (IPS) Raporları
SSH Denetimi Raporları	SSH Koruma Raporlari	Trafik Oturum Raporları
🔶 Uygulama Güvenliği Raporları	Sanai Kabio Raporiari	Web Erişim Raporları
Web Sunucu Güvenliği Raporları	WF İçerik ve Antivirüs Tarama Raporları	WF Sayfa Yasaklama Raporları
Yasaklanan Kullanıcılar Raporları		

• İlgili istemciden belirlediğimiz IP adresinin engel logu görüntülenmektedir.

Sanal Kablo Raporlari												- Raporlara Dön	
BCSV @ PDF @ XLS @ HTML Sayla Başi 50 Kayıt Göster / Gister/Gide + \$ Siralama + Y Filtreleme \$ O								me 🥒 😋					
# Zaman Damgası	Karar €≎⊕⇒	Protokol	Kaynak K. Adı ♦ ‡ Ø ⇒	Kaynak Adres ♦ ‡ � →	Kaynak Port	Hedef K. Adı ♦ \$ Ø ⇒	Hedef Adres ← ‡	Hedef Port ←	Ağ Arayüzü € \$ \$> →	VLAN ≪ ≎ ⊕ ⇒	Açıklama ≪ ≑ ≪ ⇒	Sistem ♦ \$ Ø €	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



