epati

Kullanma Kılavuzu Ürün: Antikor v2 - Layer2 Tünelleme

Kılavuzlar



www.epati.com.tr

epati Gösterge Paneli

Bu bölüm anlık olarak;

- Sistem kullanımını,
- Servis durumları,
- Arayüz durumlarını,
- Ethernet bant genişliğini,
- Bildirim geçmişi
- Network önbellek ve network paket durumunu gösterir.

Sistem Kullanımı



Arayüz Durumları

Arayüz Durumları

Devrede

1000 Mbps



Atanimamiş Atanımamiş Oc:c4:7a:c7:67:6b Oc:c4:7a:c7:62:ba Devredişi Devredişi -1 Mbps -1 Mbps eno2 WAN1 0c:c4:7a:c7:62:bb Devrede

1000 Mbps

 $\sim x$

Oſ

Ethernet Bant Genişliği Kullanımı



Bildirim Geçmişi Tümünü Görüntüle 🔺 🗙 Bildirim Tarih Ethernet Link durumu değişti. Çıkarılan(lar): eno2,eno3 06.12.2019 14:57 1 Ethernet Link durumu değişti. Çıkarılan(lar): eno4 06.12.2019 10:50 1 Ethernet Link durumu değişti. Takılan(lar): eno4 05.12.2019 12:43 Ethernet Link durumu değişti. Çıkarılan(lar): eno4 05.12.2019 12:42 1 Ethernet Link durumu değişti. Takılan(lar): eno4 04.12.2019 14:38 Ethernet Link durumu değişti. Çıkarılan(lar): eno4 04.12.2019 14:31 Ethernet Link durumu değişti. Çıkarılan(lar): eno1 04.12.2019 14:31 Bthernet Link durumu değişti. Çıkarılan(lar): eno4 04.12.2019 05:53 Ethernet Link durumu değişti. Takılan(lar): eno2,eno4 04.12.2019 05:53 Bthernet Link durumu değişti. Çıkarılan(lar): eno4 04.12.2019 05:53

Network Önbellek Durumu

Network Önbellek Durumu



Network Paket Durumu

Network Paket Durumu

#	Ethernet Adı	Gelen Paket	Giden Paket	Gelen Hatalı Paket	Giden Hatalı Paket	Paket Kaybı
1	eno1	0	0	0	0	0
2	eno2 (WAN1)	101743	127683	0	0	3
3	eno3 (LAN1)	0	95062	0	0	0
4	eno4	0	0	0	0	0
5	lo1 (WAN2)	0	95027	0	0	0
6	lo2 (WAN3)	0	95026	0	0	0
7	switch1	5279	41	0	0	0
8	switch3	0	41	0	0	0

ePati Siber Güvenlik Teknolojileri A.Ş. Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN $\wedge x$

 $\wedge x$

ераті



Antikor v2 Layer2 Tünel İstemci - Kılavuzları

Antikor v2 Layer2 Tünelleme v2.0 Kurulum Kılavuzu

Antikor v2 Layer2 Tünelleme v2.0 Kullanma Kılavuzu

ePati Siber Güvenlik Teknolojileri A.Ş. Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN



ераті



Antikor v2 Layer2 Tünel Omurga Kullanma Kılavuzu

- Doküman Sürümü: v2.1
- Güncelleme Tarihi: 22.03.2021

Bu doküman, Antikor v2 Layer2 Tünelleme v2.0'ın kullanımına ait bilgileri içermektedir.

İçindekiler

- 1. Gösterge Paneli
 - 1.1 Gösterge Paneli
- 2. Tanımlamalar
 - 2.1. Kimlik Tanımlamaları
 - 2.2. Ağ Tanımlamaları
 - 2.3. Port Tanımlamaları
- 3. Tünel Yapılandırması
 - 3.1. Tünel Ayarları
- 4. Sistem Ayarları
 - 4.1. DNS Ayarları
 - 4.2. Oturum Ayarları
 - 4.3. SNMP Ayarları
 - 4.4. Cluster Ayarları
 - 4.5. Dil Ayarları
 - 4.6. Syslog Ayarları
 - 4.7. Log Ayarları
 - 4.8. SSL Sertifikası Yönetimi
- 5. Ağ Yapılandırması
 - 5.1. IP Havuzları
 - 5.2. Ethernet Atama
 - 5.3. Sanal Ethernet VLAN Etiketi Tabanlı
 - 5.4. Sanal Ethernet Birleştirme
 - 5.5. Sanal Ethernet Loopback
 - 5.6. Ethernet Durumları
- 6. Raporlar
 - 6.1. Sistem Yönetim Raporları
 - 6.2. Dinamik Raporlar
- 7. Anlık Gözlem
 - 7.1. Network Monitörü
- 8. VPN Yönetimi
 - 8.1. IPsec VPN Ayarları
 - 8.2. IPsec VPN Profilleri
- 9. Yönlendirme Yönetimi
 - 9.1. Statik Yönlendirme
 - 9.2. Yönlendirme Tablosu
- 10. Performans
 - 10.1. Cpu Durumu

- 10.2. Bellek Durumu
- 10.3. Disk Durumu
- 10.4. Ethernet Bant Genişlikleri
- 11. Araçlar
 - 11.1. Yardımcı Araçlar
 - 11.2. Yedekle Geri Yükle
 - 11.3. Tarih/Saat Ayarları
 - 11.4. IP & Network Hesaplama
 - 11.5. Güç Yönetimi
- 12. Kullanıcı Yönetimi
 - 12.1. Kullanıcı Grupları
 - 12.2. Kullanıcı Rolleri
 - 12.3. Yönetim Paneli Kullanıcıları
 - 12.4. Yönetim Paneli Erişim Ayarları
 - 12.5. Yasaklanan Kullanıcılar

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



EPOTİ SSH Kullanım Kılavuzu

CONCICCOL V2 Tümleşik Siber Güvenlik Sistemi

Kullanıcı adı ile Antikor'a SSH bağlantısı yapmak için SshClient, Putty vb. programlar kullanılabilmektedir. Kurum içinden bağlanılıyorsa Antikor'un iç IP adresi, kurum dışından bağlanılıyorsa dış IP adresi kullanılır. Port numarası 22022'dir. Kullanıcılar kendi kullanıcı adları ile giriş yapabilirler.

Önemli Not: Yanlışlıkla 22 portuna yapılacak SSH isteklerinde, Balküpü servisi açıksa; balküpü ayarları varsayılanda 22 portundan gelen bir istek olduğunda bunu saldırı olarak görmekte ve kullanıcının belirlediği süre boyunca (varsayılan 30 dakika) o IP adresini engellemektedir.

SSH Komutları

C:\Users\test≻ssh epatisiber@10.2.1.146 -p 22022 Enter passphrase for key 'C:\Users\test/.ssh/id_rsa':					
== A	Antikor L2 Tunelleme ==				
Komut l %epatis	listesi icin '?' komutunu kullanabilirsiniz. siber@10.2.1.146 - ePati Siber Guvenlik A.S.:~\$				

• adminKonsolu komutu,

Monitör ve klavye aracılığıyla erişilebilen konsol arayüzü, SSH bağlantısı aracılığıyla da erişilebilir.

Antikor2 - Admin Konsol	u	
	Ana Menu Network Yapilandirmasi Servis Yonetimi Yonetim Paneli Ayarlari Lisans Bilgileri	
	5 Terminal	

• arp komutu,

IP adresi bilinen cihazların fiziksel adreslerini öğrenmemizi sağlayan protokoldür. Parametreleri listeleyerek kullanım genişletilebilir.



• cd komutu,

Dizinler arası geçişi sağlar. Bir adım geriye dönmek için "cd .." komutu kullanılır.

• clear komutu,

SSH bağlantısında ekranda bulunan bilgileri temizler.

• cluster-durumu komutu,

Tünel üzerinde (Cluster oluşturulmuş ise) Cluster durumu (state) hakkında bilgi vermektedir.

• disk-bilgisi komutu,

Disk tercihi yapılarak, disk performans bilgisini verir. ada0 adlı diskin performans sonuçları;

yonetici:~\$ disk-bilgisi ada0						
ada0						
512	# sectorsize					
500107862016	# mediasize in bytes (466G)					
976773168	# mediasize in sectors					
4096	# stripesize					
Θ	# stripeoffset					
969021	# Cylinders according to firmware.					
16	# Heads according to firmware.					
63	# Sectors according to firmware.					
846ASZ7HS	# Disk ident.					
Seek times:						
Full stroke:	250 iter in 7.947133 sec = 31.789 msec					
Half stroke:	250 iter in 6.113373 sec = 24.453 msec					
Quarter stroke:	500 iter in 9.766473 sec = 19.533 msec					
Short forward:	400 iter in 2.955254 sec = 7.388 msec					
Short backward:	400 iter in 3.999140 sec = 9.998 msec					
Sea outer:	2048 iter in 0.182564 sec = 0.089 msec					
Seg inner:	2048 iter in 0.232245 sec = 0.113 msec					
Transfer rates:						
outside:	102400 kbytes in 1.285826 sec = 79638 kbytes/sec					
middle:	102400 kbytes in 1.527101 sec = 67055 kbytes/sec					
inside	102400 kbytes in 2.459787 sec = 41630 kbytes/sec					
inside.	102-100 kbytes in 2:455767 See - 41050 kbytes75ee					

• disk-listesi komutu,

Donanımdaki mevcut disklerin bilgisini gösterir. ada0 adlı diskin, açıklaması, boyutu vb. bilgileri içeren çıktı;



• donanim-bilgisi komutu,

Sunucunun (ram, cpu vb.) donanım özelliklerini gösterir. Enter tuşuna basılarak çıktının devamı görülebilir.

• eth-logs

Ethernet durumlarına ait logları görüntüler.

• ethernet komutu,

Ethernet yazıp entere basıldığında bütün Ethernetlerin ve VLAN Ethernetlerinin anlık gönderme/alma trafiği görülür. Burada Rx Download, Tx Uploaddır. h harfine basarak yardımdan kullanılabilecek değerler ve zaman alınır.

- d değerleri Byte/KB/MB/GB otomatik çevirir.
- u değerleri bytes, bits, packets, errors cinsinden gösterir. Her u bastığımızda bir sonrakine geçer. Buradaki packets saniyedeki paket sayısı, errors ise saniyedeki hata sayısı
- t ortalama 30 saniye için başlangıçtan itibaren mevcut ve max oranları görüntülenir.
- a Kullanılmayan ethernetleri de gösterir.
- "+" Normalde 0.500 s dir. Her + bastığımızda 100 ms süreyi artırır.
- "-" Normalde 0.500 s dir. Her bastığımızda 100 ms süreyi azaltır.
- n input değerini değiştirir.
- q Programdan çıkışı sağlar.

Ethernet komutunun çıktısı aşağıdaki ekran görüntüsünde verilmiştir.

bwm-ng v0.6.3 (probing every 0.500s), press 'h' for help						
- iface	- 7 F	Rx	Tx	Total		
=======================================						
lo:	0.00	b/s	0.00 b/s	0.00 b/s		
ens32:	958.08	b/s	2.59 kb/s	3.54 kb/s		
ens33:	0.00	b/s	0.00 b/s	0.00 b/s		
total:	958.08	b/s	2.59 kb/s	3.54 kb/s		

• exit komutu,

Bağlandığınız kullanıcının SSH oturumunu düşürür.

• grep komutu,

Girdi olarak verilen dosyalarda belirlenen kelimeyi satır satır arama işlemi yapar.

• help komutu,

Yardım menüsünü açar, "?" ile aynı işlevi görmektedir.

%epatisiber@10.2.1.146 - ePati Siber Guvenlik A.S.:~\$ help					
adminKonsolu	ip	poweroff	sw-stats		
arp	iperf	route	tcpdump		
cd	ipsec	servis	telnet		
clear	<pre>ipsec-debug</pre>	soket-yeniden-baslat	traceroute		
cluster-durumu	kullanici	ssh	tunel-ayarlari		
cluster-shell	less	sudo	tunnel-flows		
disk-bilgisi	lisans	sw-list	tunnel-tcpdump		
disk-listesi	lpath	sw-mac-table	uname		
donanim-bilgisi	lsudo	sw-mac-table-clear	uptime		
eth-logs	mgmt-shell	sw-mac-table-stats	uygula		
ethernet	more	sw-port-stats	webTarayici		
exit	ndp	sw-show-interfaces	yedek-olustur		
grep	netstat	sw-show-lacp	yenidenBaslat		
help	nslookup	sw-show-lacp-stats			
history	paket	sw-show-rstp			
ifconfig	ping	sw-show-stp			

• history komutu,

SSH'ta en son kullanılmış komutların çıktısını gösterir.

• ifconfig komutu,

Temel amacı gerçek ethernetler ile oluşturduğumuz VLAN ethernetlerine IP vermektir. IP bilgilerini görmek için de "ifconfig" komutu aracılığıyla bilgilere ulaşılabilir. IP vermek için, sudo ifconfig bge0 10.2.2.1/24 up yazılmalıdır.

• ip komutu,

IP ile ilgili işlemler yapılır. Link, address ve route gibi.

• iperf komutu,

İki istemci arasındaki network hız testi için kullanılır. iperf -s paremetresi, bir istemcinin server olmasını sağlar. iperf -c host parametresi, bir istemcinin client olmasını sağlar.

• ipsec komutu,

IPSec ayarlarına müdahele edilmektedir. Ayrıca start, restart, update ve versiyon gibi paremetreler de barındırmaktadır.

ipsec command [arguments]
Commands:
start restart [arguments]
update/reload/stop
up down route unroute <connectionname></connectionname>
down-srcip <start> [<end>]</end></start>
status statusall [<connectionname>]</connectionname>
listalgs listpubkeys listcerts [utc]
listcacerts listaacerts listocspcerts [utc]
listacerts listgroups listcainfos [utc]
listcrls listocsp listplugins listall [utc]
listcounters resetcounters [name]
<pre>leases [<poolname> [<address>]]</address></poolname></pre>
rereadsecrets rereadcacerts rereadaacerts
rereadocspcerts rereadacerts rereadcrls rereadall
purgecerts purgecrls purgeike purgeocsp
scepclient pki
stroke
version
Refer to the ipsec(8) man page for details.
Some commands have their own man pages, e.g. pki(l) or scepclient(8).

• kullanici komutu,

Etherneti kullanan kullanıcı bilgileri görülür.

- kullanici –i bge0, Yerel Ağımızdaki IP'ler ile internetteki IP adreslerini gösterir.
- kullanici -- i bge1, Dış taraftaki gerçek IP'ler ile internetteki IP adreslerini gösterir.
- kullanici –i bge2, Sunucu bölgesindeki IP'ler ile internetteki IP adreslerini gösterir.

Antikor'un Web arayüzündeki Anlık Web Erişimi sadece Web isteklerini gösterirken burada 65536 portun tamamı görülebilmektedir. Dolayısıyla torrent kullanıcılarına ait trafik belirlenebilir. Ekran görüntüsü aşağıdaki gibidir.

	12.5Kb			25.0кb	37.5Kb		50.0Kb		62.5K
.2.1.141	-			=> 192.168.10.11			0.98Kb	944b	998b
							1606	160b	213b
.40.222.57				=> 192.168.10.11			00	114b	114b
03 38 335 103				~= 102 168 10 11			00	1890	19.90
93.20.223.293				<=			06	33b	sb
0.2.1.4				=> 192.168.10.11			06	326	756b
							06	326	208b
elay-35df5207.net.anyd	esk.com			=> 192.168.10.11			06	32b	42b
							06	326	40b
72.217.17.174				=> 192.168.10.11			06	00	250
40 222 08				102 168 10 11			00	00	250
				-> 192.108.10.11			00	05	276
92.168.10.255				=> 192,168,10,11			06	ob	Ob
				<=			06	06	47b
04.79.197.200				=> 192.168.10.11			06	06	16b
							06	0b	16b
3.184.220.29				=> 192.168.10.11			06	06	16b
							06	06	16b
12.101.122.34				=> 192.168.10.11			06	00	80
12 101 122 140				<=			00	00	80
12.101.122.140				=> 192.108.10.11			00	00	eb.
.40.222.110				=> 192,168,10,11			06	0b	Sh
				<=			0b	06	th
	0.0750	eesk.	as ash				a oarth	1.13%	1.07%
Cum:	9.07KB	peak:	4.22Kb			rates:	160b	4.13KD	01.4b
OTAL -	11.8KB		19.4Kb				1.146b	1.56Kh	2.77%
VINL I	19:000		1.0 - 40.0				A + A HIGH	A - 3000	6. F / PAD

Sadece bir VLAN'daki kullanıcılara bakılması halinde kullanici -- i bge0.166

• less komutu,

Ekrana sığmayacak olan uzun çıktılar less komutu ile ekrana sığdırılarak gösterilir.

• lisans komutu,

Antikor'un lisans bilgilerini gösterir.

%epatisiber@10.2.1.146 - ePati Siber Guvenlik A.S.:~\$ lisans				
Lisans Sahibi	ePati Siber Güvenlik A.Ş Demo			
Lisanslı Ürün	antikor Layer2 TN Staging - STAGING			
Sözleşme Başlangıç Tarihi	30.04.2019 12:00:00			
Sözleşme Bitiş Tarihi	31.12.2021 12:00:00			

• Ipath komutu,

Yetkili olunan klasörleri listeler.

• Isudo komutu,

Sudo yetkili olan komutları listeler.

• mgmt-shell komutu,

Kullanıcı bağımsız yönetim için oluşturulmuş olan ethernet arayüzünde yapılacak işlemler için management shell'e düşer.

• more komutu,

Bir komutun daha fazla bilgi vermesi için kullanılan komuttur.

• ndp komutu,

IPv4 protokolünde kullanılan ARP, ICMP vb. özelliklerin yerini almıştır.

- ndp a, Geçerli tüm ndp girişlerini gösterir.
- ndp –d, Bir süper-user kullanıcısı –d paremetresi ile hostname olarak adlandırılan ana makine için bir girişin silinmesine olanak tanır.
- ndp –i, Bir ndp girişi -s parametresi ile eklendiğinde kullanılacak arabirimin dizinini belirtir.
- ndp –I, ndp için varsayılan Ethernet keşif arayüzünü siler.
- ndp -s, Donanım adresi ile ana makine adı için bir ndp girişi oluşturur. Temp komutta belirtilmedikçe giriş

yonetici:~\$ ndp -a Neighbor fe80::1%bge1 fe80::1%bge0	Linklayer Address 00:e0:66:c4:58:d9 00:e0:66:c1:0c:2f	Netif Expire S Flags bgel permanent R bge0 permanent R
resort ingeo_	00100100101100121	bgeo permanente n

• netstat komutu,

Ağ bağlantıları bilgilerini gösterir. (TCP, UDP, Port Numarası, Durum bilgisi.) Birçok parametresi vardır.

- netstat -m, Network durumu hakkında bilgi verir.
- netstat –n, Sunucu üzerinde kurulmuş bağlantıların listesini verir.

yonetici:~\$ netstat Active Internet connections								
Proto	Recv-Q Se	nd-Q Local Address	Foreign Address	(state)				
tcp4	Θ	0 localhost.6379	localȟost.22559	LAST ACK				
tcp4	Θ	0 localhost.6379	localhost.14552	LAST_ACK				
tcp4	Θ	0 10.2.1.141.22022	10.2.1.141.14535	ESTABLISHED				
tcp4	Θ	0 10.2.1.141.14535	10.2.1.141.22022	ESTABLISHED				
tcp4	Θ	0 10.2.1.141.22022	10.2.1.141.37400	ESTABLISHED				
tcp4	Θ	0 10.2.1.141.37400	10.2.1.141.22022	ESTABLISHED				
tcp4	Θ	0 10.2.1.141.22022	10.2.1.12.1423	ESTABLISHED				
tcp4	Θ	0 10.2.1.141.22022	10.2.1.12.1422	ESTABLISHED				
tcp4	Θ	0 10.2.1.141.22022	10.2.1.12.1415	ESTABLISHED				
tcp4	Θ	0 localhost.postgresql	localhost.59082	ESTABLISHED				

• nslookup komutu,

DNS Serverin düzgün çalışıp çalışmadığı kontrol etmek için kullanılır.

• paket komutu,

Antikor paketlerinin sürüm ve durum bilgilerini gösterir.

Paket Sürüm Listesi					
Paket	Sürüm	Durum			
Yapılandırma Yöneticisi - Staging	2.0.59	Güncel			
Arayüz Modülü - Staging	2.0.157	Güncel			
Araç Kutusu - Staging	2.0.5	Güncel			
Yönetimsel Araçlar	2.0.16	Güncel			
Haberleşme Modülü - Staging	2.0.160->2.0.161	Kurulmaya Hazır			
Haberleşme Aracısı	2.0.15	Güncel			
Modül Yöneticisi	2.0.15	Güncel			
Yönetici Konsolu - Staging	2.0.17	Güncel			
Haberleşme Yöneticisi (Router)	2.0.5	Güncel			
Eklenti - Ortam Sağlayıcı	2.0.11	Güncel			
Eklenti - Bildirim İletici	2.0.40	Güncel			
Eklenti - İzleyici	2.0.31	Güncel			
Eklenti - Bildirim Gönderici Modülü	2.0.17	Güncel			
Eklenti - Syslog	2.0.22	Güncel			
Modul Yoneticisi Yönetici Konsolu - Staging Haberleşme Yöneticisi (Router) Eklenti - Ortam Sağlayıcı Eklenti - Bildirim İletici Eklenti - İzleyici Eklenti - Bildirim Gönderici Modülü Eklenti - Syslog	2.0.15 2.0.17 2.0.5 2.0.11 2.0.40 2.0.31 2.0.17 2.0.22	Güncel Güncel Güncel Güncel Güncel Güncel Güncel			

• ping komutu,

Hedef bilgisayar, sunucu gibi cihazların çalışmasını, uzaklığını vb. işlevleri tespit için kullanılır.

Icmp_seq, Paketin başlık bilgisi, her ping paketinde başlık sırası artacaktır. TTL (time to live), Paketin yaşam süresi. Time, Ping iletişiminin ne kadar zamanda gerçekleştiği bilgisi.

```
%epatisiber@10.2.1.146 - ePati Siber Guvenlik A.S.:~$ ping 10.2.1.253
PING 10.2.1.253 (10.2.1.253) 56(84) bytes of data.
64 bytes from 10.2.1.253: icmp_seq=1 ttl=255 time=0.762 ms
64 bytes from 10.2.1.253: icmp_seq=2 ttl=255 time=0.891 ms
64 bytes from 10.2.1.253: icmp_seq=3 ttl=255 time=0.854 ms
64 bytes from 10.2.1.253: icmp_seq=4 ttl=255 time=0.989 ms
```

poweroff komutu,

Tünel sunucunun kapatılmasını sağlar.

• route komutu,

İşletim sistemine yeni route eklemek veya silmek için kullanılır.

- sudo route delete default, o anki route siler.
- sudo route add default 10.2.1.253

Aşağıdaki görüntüde ilk önce route silinip sonra yeniden eklenmiştir.



• servis komutu,

Antikor servislerinin durumları hakkında bilgi verir. Servisler "Çalışıyor, Kapalı, Bypass ya da Yapılandırılmadı" olarak aşağıda görülmektedir.

Servis Listes:	i	
Servis	Açıklama	Durum
tunel routing vpn-ipsec snmp-servisi	Layer2 Tünelleme Motoru Layer3 Yönlendirme VPN - IPSec Servisi SNMP Servisi	Çalışıyor Kapalı Yapılandırılmadı Kapalı

• soket-yeniden-baslat komutu,

Soketin yeniden başlatılması için kullanılır.

• ssh komutu,

Uzak bağlantı için kullanılan bir protokoldür.

P 10.2.1.141 - PuTTY
login as: yonetici Using keyboard-interactive authentication. Password for yonetici@antiKor2.epati.com.tr: Last login: Tue Feb 27 08:51:43 2018 from 10.2.1.141
== ePati Bilisim Teknolojileri == == Antikor v2 UTM Firewall ==
Komut listesi icin '?' komutunu kullanabilirsiniz. yonetici:~\$

sudo komutu,

Sudo, çalıştırma yetkisi olan komutları root yetkili olarak çalıştırılmasını sağlar. Route ekleme ve silme işlemlerinin yapılabilmesi için, sudo yetkilendirmesi gerekmektedir.



• sw-list komutu,

Switchleri listeler.

switch_id	adi	aciklama
switchl (1 row)	Merkez	Merkez

• sw-mac-table komutu,

Komut sonuna girilen switch için port,VLAN ve MAC adresi bilgilerini listeler. (Örnek kullanım:sw-mac-table switch1)

port	VLAN	MAC	Age
tunel3	250	lc:75:08:33:48:8e	Θ
ens34	250	00:50:56:a1:d6:54	Θ

sw-mac-table-clear komutu,

Komut sonuna girilen switch'in MAC adresi tablosunu temizler. (Örnek kullanım:sw-mac-table-clear switch1)

table successfully flushed epati:~\$ [

sw-mac-table-stats komutu,

Komut sonuna girilen switch'in MAC tablosuna ait durumları listeler. (Örnek kullanım:sw-mac-table-stats switch1)

```
Statistics for bridge "switch1":
Current/maximum MAC entries in the table: 2/131072
Current static MAC entries in the table : 0
Total number of learned MAC entries : 9
Total number of expired MAC entries : 3
Total number of evicted MAC entries : 0
Total number of port moved MAC entries : 0
```

• sw-port-stats komutu,

Portlara ait durumlar listelenir.

PORT	RX-PKT	RX-BYTE	TX-PKS	TX-BYTE	
ens34:	916072	786960358	35732	3222069	
tunel3:	16183	1339194	14852	30851284	
tunel4:	Θ	Θ	914	77053	

sw-show-interfaces komutu,

Komut sonuna girilen switch'e üye arayüzleri listeler. (Örnek kullanım: sw-show-interfaces switch1)



• sw-show-lacp komutu,

Komut sonuna girilen switch için lacp arayüzleri listeler. (Örnek kullanım:sw-show-lacp switch1)

--- lacp2 ---status: active
sys_id: 00:50:56:a1:16:09 sys_priority: 65534 aggregation key: 1 lacp time: slow member: ens34: current detached port_id: 1 port_priority: 65535 may_enable: false actor sys_id: 00:50:56:a1:16:09 actor sys priority: 65534 actor port_id: 1 actor port_priority: 65535
actor key: 1 actor state: activity aggregation collecting distributing partner sys_id: 00:50:56:a1:16:09 partner sys_priority: 65534 partner port_id: 2 partner port_priority: 65535 partner key: 1 partner state: activity aggregation collecting distributing member: ens35: current detached port_id: 2 port_priority: 65535 may enable: false actor sys_id: 00:50:56:a1:16:09 actor sys priority: 65534 actor port id: 2 actor port_priority: 65535 actor key: 1 actor state: activity aggregation collecting distributing

• sw-show-lacp-stats komutu,

Komut sonuna girilen switch için lacp arayüzlerine ait durumları listeler. (Örnek kullanım:sw-show-lacp-stats switch1)

```
---- lacp2 statistics ----
member: ens34:
  TX PDUs: 32
  RX PDUs: 32
  RX Bad PDUs: 0
  RX Marker Request PDUs: 0
  Link Expired: 0
  Link Defaulted: 0
  Carrier Status Changed: 0
member: ens35:
  TX PDUs: 32
RX PDUs: 32
  RX Bad PDUs: 0
  RX Marker Request PDUs: 0
  Link Expired: 0
  Link Defaulted: 0
  Carrier_Status Changed: 0
```

• sw-show-rstp komutu,

Switch'te rstp devredeyse; komut sonuna girilen switch'e ait rstp bilgilerini listeler. (Örnek kullanım:sw-

```
show-rstp switch1)
```

```
No such RSTP object
ovs-appctl: ovs-vswitchd: server returned an error
epati:~$ sw-show-rstp switch1
---- switch1 ----
Root ID:
  stp-priority
                   32768
  stp-system-id
                  00:50:56:a1:1e:f0
  stp-hello-time
                  2s
                   20s
  stp-max-age
  stp-fwd-delay
                   15s
  This bridge is the root
Bridge ID:
                   32768
  stp-priority
  stp-system-id
                  00:50:56:a1:1e:f0
                   2s
  stp-hello-time
                   20s
  stp-max-age
  stp-fwd-delay
                   15s
  Interface Role
                         State
                                    Cost
                                              Pri.Nbr
             Designated Forwarding 200000
  tunel4
                                              128.1
                                              128.2
  lagg1
             Designated Forwarding 20000
```

• sw-show-stp komutu,

Switch'te stp devredeyse; komut sonuna girilen switch'e ait stp bilgilerini listeler. (Örnek kullanım:sw-show-stp switch1)

```
--- switch1 ----
Root ID:
  stp-priority
                32768
                  4a:a6:e4:b3:6a:4d
  stp-system-id
  stp-hello-time 2s
                  20s
  stp-max-age
                  15s
  stp-fwd-delay
  This bridge is the root
Bridge ID:
  stp-priority
                32768
                  4a:a6:e4:b3:6a:4d
  stp-system-id
  stp-hello-time
                  2s
  stp-max-age
                  20s
  stp-fwd-delay
                  15s
  Interface Role
                        State
                                    Cost
                                          Pri.Nbr
             designated listening
                                    19
                                          128.1
  tunel4
```

• sw-stats komutu,

Komut sonuna girilen switch'e ait istatistiksel verileri listeler.

Event coverage, avg rate	over last:	5 seconds, last	minute, last hour	r, hash=d7d9e943:
<pre>rev_mac_learning</pre>	0.0/sec	0.033/sec	0.0056/sec	total: 45
<pre>mac_learning_learned</pre>	0.0/sec	0.033/sec	0.0053/sec	total: 23
<pre>mac_learning_expired</pre>	0.0/sec	0.000/sec	0.0008/sec	total: 7
mac_learning_moved epati:~\$	0.0/sec	0.000/sec	0.0000/sec	total: 38

S

• tcpdump komutu,

Ağ dinlemek için kullanılan tcpdump komutunun, birçok parametresi vardır.

- tcpdump D, Ağ üzerinde dinlenebilecek bütün arayüzleri listeler.
- tcpdump -i bge0, bge0 arayüzünün dinlenmesini sağlar.
- tcpdump -n src net 10.2.1.141 Belirtilen ağ adresinden gelen paketleri listeler.
- tcpdump -ni bge, Yerel ağın trafiğini izler. bge ethernet arayüzüne bağlı VLAN'ları da gösterir.
- tcpdump -ni bge0.166 host 10.2.2.2, 166 vlanındaki sadece bu IP'nin trafiğini gösterir.
- tcpdump ether host 11:22:33:44:55:66, bu mac adresli bilgisayarın trafiğini gösterir.
- tcpdump -i bge0.166 host 10.2.2.2 or 10.2.2.10, Bu 2 IP'nin trafiğini gösterir.
- tcpdump udp and (src port 161 or 162 or 514), UDP ile kaynak portu 161,162 ve 514 olanları göster.
 Örnekleri çoğaltmak mümkün.

yonetici:~\$ tcpdump -ni bgel
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on bgel, link-type EN10MB (Ethernet), capture size 65535 bytes
09:14:45.424123 IP 10.2.1.141.22022 > 10.2.1.12.1415: Flags [P.], seq 1477914982:1477915018, ack 155735475
5, win 128, length 36
09:14:45.424447 IP 10.2.1.12.1415 > 10.2.1.141.22022: Flags [.], ack 36, win 2048, length 0
09:14:46.086969 ARP, Request who-has 10.2.1.190 tell 10.2.1.254, length 46
09:14:46.439086 IP 10.2.1.141.22022 > 10.2.1.12.1415: Flags [P.], seq 36:240, ack 1, win 128, length 204
09:14:46.479312 IP 10.2.1.12.1415 > 10.2.1.141.22022: Flags [.], ack 240, win 2053, length 0

• telnet komutu,

Uzaktan bir bilgisayara ya da servera bağlanmak için kullanılan komuttur. SSH'a göre daha az güvenlidir. Aşağıdaki görüntü gibi bağlantı sağlayabilirsiniz, telnet için ayarlarınız yapılı ise bağlantı oturumu kurulacaktır.



• traceroute komutu,

IP paketinin hedefe giderken, hangi routerlar üzerinden geçtiğinin bilgisini vermektedir.

• tunel-ayarlari komutu,

Tünel network ayarlarını görüntüler.

• tunnel-flows komutu,

Bir porttan geçen anlık sessionları görüntüler.

• tunnel-tcpdump komutu,

Tünele ait trafiğin dinlenmesi için kullanılır.

• uname komutu,

İşletim sistemini çıktı olarak verir. (-a parametresi ile birlikte kullanıldığında işletim sistemine ait tüm detayları çıktı olarak verir.)

```
%epatisiber@10.2.1.146 - ePati Siber Guvenlik A.S.:~$ uname -a
Linux Antikor-v2.epati.com.tr 5.10.79-1-lts #1 SMP Fri, 12 Nov 2021 19:04:00 +0000
x86_64 GNU/Linux
%epatisiber@10.2.1.146 - ePati Siber Guvenlik A.S.:~$ uname
Linux
%epatisiber@10.2.1.146 - ePati Siber Guvenlik A.S.:~$
```

• uptime komutu,

Cihazın ne kadar süredir açık olduğu bilgisini verir.



• uygula komutu,

Arayüzde "Tanımları Uygula" butonu ile aynı işlevi görmektedir.

- uygula –a Uygulanması beklenen tanımları uygular.
- uygula --cf istenilen kuralın uygulanmasını sağlar.

Mesela aşağıdaki görüntüde DNS ayarları tekrardan uygulanmıştır.

yonetici:~\$ uygula -cf dns-ayarlari

- uygula –fa, Antikordaki bütün kuralları tekrardan uygular.
- uygula -la, Servislerin durumlarına dair bilgiler verir.

Uygulama Listesi		
Uygulama	Açıklama	Durum
ag-tanim-yenile	Ağ Tanımları Yenileme	Güncel
ag-yapilandirmasi	Ağ Yapılandırması	Güncel
giris-banner	Giriş Banner Yapılandırıcı	Güncel
ssh-kullanici	Ssh Kullanıcıları	Güncel
ssh-yetki	Ssh Yetkileri	Güncel
cluster-senkronizasyonu-full	Cluster Senkronizasyonu (Full)	Güncel
dns-ayarlari	DNS Yapılandırması	Güncel
ethernet-atama	Ethernet Atama	Güncel
panel-erisim	Web Paneli Erişim Yapılandırması	Güncel
sanal-ethernet-lagg	Sanal Ethernet - Birleştirme	Güncel
sanal-ethernet-loopback	Sanal Ethernet - Loopback	Güncel
sanal-ethernet-vlan	Sanal Ethernet - VLAN Etiketi Tabanlı	Güncel
snmp	Snmp	Güncel
statik-yonlendirme	Statik Yönlendirme	Güncel
syslog	Syslog Ayarları	Güncel
tunnel	Tünel Yapılandırması	Güncel
vpn-ipsec	IPsec VPN Yapılandırması	Güncel
yonetim-paneli	Yönetim Paneli Ayarları	Güncel
cluster	Cluster Ayarları	Güncel
ethernet-web-arayuzu-erisimi	Ethernet Web Arayüzü Erişimi	Güncel
cluster-guncelleme-senkronizasyonu	Cluster Güncelleme Senkronizasyonu	Güncel
cluster-senkronizasyonu	Cluster Senkronizasyonu	Güncel
yeniden-uygulama-buffer	[Gizli] Yeniden Uygulama Buffer (Cluster Pasif Cihaz)	Güncel
cluster-servis-senkronizasyonu	Cluster Servis Senkronizasyonu	Güncel

• yedek-olustur komutu,

Cihazın yedek dosyası oluşturulur.

• webTarayici komutu,

Konsol üzerinde web siteleri açmak için kullanılan komuttur.

# #ePatig 🛿 beslemesi ePatig 🗑 yorum beslemesi alternate alternate alternate alternate alternate	ileri
<pre>(epati-TR.svg) * UTM FIREMALL * L2 TIMPL * LOGLAMA * REFERANSLARIMIZ + MISTERI PANELI + HISTERI PANELI + EIXTL INLERIMIZ + BIZE ULAISIN + GIZEULAISIN + GIZEULAISIN</pre>	
(BUTTON) URINALERINIZ	
TENNIK DESTEK	
[USEMAP:ortas.png]	
* Turkish (tr) Turkish * English (en) English * arleer-tby+tm (ar) arleer+b+y+tm	
× Yasal Bilgiler İletisim İK * D∭K∭manlar	
Logo Header Menu	
* ANASAYFA * UTN FERMALL * TINELLEME * LOGLAN PANELT * REFERANCE * REFERANCE LIME * BIZE ULASIN * ETKINLIKLERIMIZ * REFERANSLARIMIZ	

• yenidenBaslat komutu,

Sunucuyu yeniden başlatmak için kullanılır.

• ? komutu,

Yardım menüsünü açar, "help" ile aynı işlevi görmekte.

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



ераті



Antikor v2 Layer2 Tünelleme Kurulum Kılavuzu

- Doküman Sürüm: v1.2
- Güncelleme Tarihi: 10.02.2023

Online İnceleme

Antikor v2 Layer2 Tünelleme'yi online incelemek için tıklayınız.

Kullanıcı adı: demo

Parola: demo

Kurulum Öncesi

- ÖNEMLİ NOT: Kurulumdan önce sanal makineye ihtiyaç duyulabilecek tüm NIC leri atayınız. Kurulumdan sonra yapılacak NIC ekleme ve çıkarma işlemleri, lisansın düşmesine sebebiyet verecektir.
- Fiziksel Sunucu ortamı sağlandıktan sonra en az 8Gb USB Ventoy (https://www.ventoy.net/en/download.html) programı ile formatlanarak aşağıdaki linkleri verilen ISO bu USB ye atılır. Sonrasında Fiziksel/Sanal sunucular boot açılışı USB olacak şekilde başlatılır ve ürün kurulumu yapılır.
- Sanal sunucu için, ISO gereken klasöre yüklenmelidir.
- Kurulum esnasında internet erişimi gerekmektedir. Lisans doğrulaması için DNS sorgularına cevap alınabilmesi ve 95.173.165.10 ip adresinin 7001, 7002 ve 22022 portlarına erişim izni gerekmektedir.
- Kurulumdan sonra internet erişimi zorunlu değildir.

ISO dosyasını edinmek için tıklayınız.

Kuruluma başlamadan önce, kurulum CD'sinin veya ISO dosyasının Epati Siber Güvenlik tarafından sağlandığından emin olunuz. CD zarfının üzerindeki güvenlik mührünün zarar görmemiş olmadığından emin olunuz.

Not: Bu kontroller sırasında herhangi bir şüphe olması durumunda kuruluma devam etmeyiniz.

Tünelleme yazılımı fiziksel olarak korumalı bir ortamda kullanılmak üzere hazırlanmıştır. Kurulumdan önce donanıma sadece yetkili kişilerin eriştiğinden emin olun.

Kurulacak makinenin minimum 64 GB SSD diske ve 2 GB belleğe sahip olduğuna emin olun.

Kurulum sırasında herhangi bir adımda <a>[ctrl] tuşuna basıldığı vakit kurulum başa dönecektir.

Kurulum



mtikor ∨2 Installe

Boot Antikor v2 Installer (x86_64) Boot existing OS Run Memtest86+ (RAM test) Hardware Information (HDT) Reboot Power Off

> Press [Tab] to edit options www.epati.com.tr



Yukarıdaki ekranda;

- Boot Antikor v2 Installer (x86 64) Yeni Antikor L2 Tünelleme kurulumu içindir.
- Boot existing OS Antikor L2 Tünelleme kurulum ekranından çıkar.
- Run Memtest86+ (Ram test) Ram testi yapılmak istenirse bu seçenek seçilmelidir.
- Hardware Information (HDT) Donanım bilgilerinin görüntülenmesi istenilirse bu seçenek seçilmelidir.
- Reboot Yeniden başlatmak istenilirse bu seçenek seçilmelidir.
- Power Off Antikor L2 Tünelleme cihazı kapatılmak istenirse bu seçenek seçilmelidir.

Dil Seçimi

Tünelleme yazılımı için kullanılacak olan dil seçimi belirtilir.



Ağ Yapılandırması

Bu ekranda 2 adet Ethernet görülmektedir. Kurulum hangi Ethernet üzerinden yapılacaksa o Ethernet seçilip kuruluma devam edilir.

Not: Ethernet kartları gösterilmemesi durumunda, bağlantıları kontrol edin ve "Yenile - Durumu Yeniden Kontrol Et" seçeneğini seçin.

tikor v2 - Tümleşik Siber Güvenlik Sistemi
Ağ Yapılandırması
enp0s8[Kablo Takılı] 82540EM Gigabit Ethernet Controller [Kablo Takılı] 82540EM Gigabit Ethernet Controller YenileYenileDurumu Yeniden Kontrol Et
<tamam> <iptal></iptal></tamam>

DHCP - Manuel Seçimi

Seçilen ethernetten internete el ile IP vererek veya DHCP seçilerek otomatik IP alınması gerekir. DHCP için hâlihazırda IP dağıtan bir sisteminizin olduğu varsayılır.

Antikor v2 - Tümleşik Siber Güve	enlik Sistemi	
enp0s8	Ağ Yapılandırması - Yapılandırma Türünü Seçiniz MCP Otomatik Yapılandırma Manual El ile Yapılandırma 	

Arayüz: enp0s8 broadcast_address=1 dhcp_lease_time=864 dhcp_message_type=5 dhcp_server_identif domain_name_servers filename=test.pxe ip_address=10.0.3.1 network_number=10.0 couters=10.0.3.2 subnet_cidr=24 subnet_mask=255.255 Yukarıdaki Yapıland	0.0.3.255 00 ier=10.0.3.2 ='193.255.128.2 1.1.1 5 1.3.0 i.255.0 lirmayi Onayliyor musur	.1 8.8.8.8' nuz?	
	<evet></evet>	⟨H ayir ⟩	_

Eğer IP dağıtan sisteminiz yoksa el ile IP verilerek devam edilir. Bu verdiğiniz IP'nin dışarıya erişirken WEB(80 portu), Ping (ICMP) ve SSL (443 portu) bağlantısının açık olduğunu kontrol ediniz. Bunlar kapalı ise kurulumunuz tamamlanmayacaktır.

Aşağıda manuel IP verilerek kuruluma devam edilmiştir.

Antikor v2 - Tümleşik Si	ber Güvenlik Sistemi		
	Ağ Yapılandırması IP Adresi Alt Ağ Maskesi Ag Geçidi DMS Sunucusu ⟨ <u>T</u> amam⟩	10.0.3.15 255.255.255.0 10.0.3.2 8.8.8.8	

IP Adresi, Alt Ağ Maskesi, Ağ Geçidi Veya DNS Sunucusu alanları zorunlu olup herhangi birinin girilmemesi durumunda hata mesajı gösterilip kuruluma devam edilemeyecektir. Benzer şekilde bu alanlara IP adresi formatı dışında farklı bir formatta girdi yapılırsa "Geçersiz IP adresi" hatası alınacaktır.

tikor v2 - Tümleşik Siber Güvenlik Sistemi
Ag Yapilandirmasi 3: enn0s8: <broadcast.multicast.up.lower up=""> mtu 1500 gdisc fg codel state UP group</broadcast.multicast.up.lower>
default glen 1000
link/ether 08:00:27:ba:30:bb brd ff:ff:ff:ff:ff
inet 10.0.3.15/24 scope global enp0s8 ualid lft forever preferred lft forever
default via 10.0.3.2 dev enp0s8
10.0.3.0/24 dev enposo proto kernel scope link src 10.0.3.15
Yukarıdaki Yapılandırmayı Onaylıyor musunuz?
<mark>⟨Evet⟩</mark> ⟨Hayir>

IP adresi, manuel olarak yapılandırıldıktan sonra IP ve ağ geçidi yukarıdaki gibi gösterilmektedir. Eğer onaylıyorsanız Evet seçilerek kuruluma devam edebilir veya Hayır seçilerek kurulumun başına dönebilirsiniz.

10.0.3.2 - Ağ Geçidine Ping Atılıyor... Ağ Geçidine Ulaşılabiliyor Sunucuya Erişim Kontrol Ediliyor... İnternete Ulaşılabiliyor Zaman Damgası Alınıyor...

Lisans

Epati Siber Güvenlik tarafından verilmiş olan lisans bilgileri girilir.

Antikor v2 -	Tümleşik Siber Güvenlik Sistemi
	Lisans-Kontrolii
	Lisans Anahtarını Giriniz
	<pre><tamam> <iptal></iptal></tamam></pre>

Disk Bölümleme

Sunucu üzerinde 2-3 farklı disk var ise, Antikor Tünelleme yazılımı ve logları 2 farklı diske kurulabilir. Tek disk var ise seçilen diske kurulum yapılacaktır.

Antikor V2 -	Tümleşik Siber (Güvenlik Sistemi
		Antikor OS Diskini Seçiniz
		<pre>/dev/sda 16 GiB /Tamam> <iptal></iptal></pre>
Antikor 12	- Timlesik Sihen (Giuenlik Sistemi
		Log Diskini Seçiniz /dev/sda 16 GiB (Tamam) <iptal></iptal>



 $Kurulum \ için \ diskin \ biçimlendirilmesi \ gerekmektedir. \ {\tt Evet} \ seçerek \ devam \ edilir.$

Antikor v2 - Tümleşik Siber Güvenlik Sistemi Disk Yapılandırması Antikor OS Disk Bölümlendirmesi Yapılıyor... Log Disk Bölümlendirmesi Yapılıyor... Bölümleme Tablosu Yeniden Okunuyor... #1 Bölüm Biçimlendiriliyor... #2 Bölüm Biçimlendiriliyor...

Ant	; il	(or	ν2		Tüml	leşi	\mathbf{k}_{-}	Si	ber	Güven.	lik	S	ist	temi	l
-----	------	-----	----	--	------	------	------------------	----	-----	--------	-----	---	-----	------	---

Antikor v2 - Tümleşik Siber Güvenlik Sistemi Yükleniyor-Lütfen Bekleyiniz...

80%

ant i Kor 2

PAKETLER	KURULUYOR

Yapilandirma Yoneticisi - Staging Arayuz Modulu - Staging	2.0.72 2.0.218	Kurulmaya Hazir <mark>Indir</mark> iliyor
Arac Kutusu - Staging	2.0.7	Kurulmaya Hazir
Yonetimsel Araclar	2.0.20	Kurulmaya Hazir
Haberlesme Modulu - Staging	2.0.205	Guncel
Haberlesme Aracisi	2.0.17	Sirada (Indirme)
Yonetici Konsolu - Staging	2.0.23	Sirada (Indirme)
Haberlesme Yoneticisi (Router) -	2.0.5	Sirada (Indirme)
Eklenti - Ortam Saglayici - Staging	2.0.8	Kurulmaya Hazir
Eklenti - Bildirim Iletici - Staging	2.0.5	Kurulmaya Hazir
Eklenti - Izleyici - Staging	2.0.11	Kurulmaya Hazir
Eklenti - Bildirim Gonderici Modulu -	2.0.7	Kurulmaya Hazir
Eklenti - Syslog - Staging	2.0.9	Kurulmaya Hazir
Eklenti - Cluster Yonetimi - Staging	2.0.27	Kurulmaya Hazir
Modul Yoneticisi - Staging	2.0.3	Guncel
Web SSH Modulu - Staging	2.0.4	Kurulmaya Hazir

Toplam Ilerleme %44



Bu aşamadan sonra kurulum tamamlanmıştır. Sunucu yeniden başlatılır. İlk başlatmadan sonra, ayarlar tamamlanır ve "login" ekranı gelir.

/	
Welcome to AntiKor 2 AntiKor 2 AntiKor 2'ye Hosgeldiniz	
l ePati Information Technologies ePati Bilisim Teknolojileri 	
http://www.epati.com.tr/ http://www.antikor.com.tr/ Tel. : +90 324 361 02 33 Fax : +90 324 361 02 39	
** Arayuz URL: https://10.0.3.15:8800 Antikor-v2 login: _	

Antikor L2 Tünelleme Sunucusunun WEB ara yüzüne nasıl girilir?

Bilgisayarda bulunan herhangi bir web tarayıcısı ile cihaza erişip gerekli ayarlar yapılabilmektedir. (Internet Explorer, Chrome, Firefox, vs.) Yazılım ayarlarını yapmadan önce yukarıdaki gibi Tünelleme kurulum IP adresinin doğruluğunu ve kabloların takılı olduğundan emin olunuz.

• Tarayıcının adres kısmına sunucuya verilmiş olan IP adresi https://10.0.3.15:8800 girilir. Port 8800 olduğu için "https://" nin yazılması unutulmamalıdır.

C		
	antikor v2 Tünelleme	
	Giriş yapmak için bilgileri giriniz.	
kul	llanıcı Adı	
Par	rola	
	Giriş	
	ePati Bilişim Teknolojileri © 2016	
	Dil Seçiniz : tr en ar	

• Açılan sayfada, kullanıcı adı "admin" ve parolayı "antikor" yazarakGiriş butonuna tıklanır.

epati		antikor Layer2 TN - EPA-TN-K4-TR Sayfa ismi girmeye başlayın	🔾 🕞 Çıkış Yap 🚍
	Gösterge Paneli		
admin Antikor Admin 👻	Sistem Kullanımı	Servis Durumları	X 🖻 🔺
🏂 Gösterge Paneli	CPU Bellek Disk	Layer2 Tünelleme Motoru Çalışıyor	C
🗞 Tanımlamalar 🗸 <	2% 11% 6%	Layer3 Yönlendirme Kapalı	
🚍 Tünel Yapılandırması 🛛 🔇	0 100 0 100 0 100	IPsec VPN Servisi Çalışıyor	> 🚺 😋
0 ° Sistem Ayarları 🤇	Ethernet Bant Genielläi Kullanum	SNMP Servisi Çalışıyor	▶ □ ○
🖗 Ağ Yapılandırması 🛛 🔇	Tümü X •		
🖩 Raporlar 🗸 🤇	4	Network Önbellek Durumu	~ ×
👁 Anlık Gözlem <	CUUM	Network Belleği - MTU 1500 Network Belleği - M	MTU 4000
VPN Yönetimi <	MDDS .		
🛠 Yönlendirme Yönetimi 🧹 🤇	2	0% 0%	100
📥 Performans 🧹	Mbi/s	Network Belleği - MTU 9000 Network Belleği - N	NTU 16000
۶ Araçlar <	1 MDI/S		
🌲 Bildirim Yönetimi 🤇		0% 0% 0%	100
🖀 Yönetim Paneli Ayarları 🛛 🔇	bil/s 12:49:45 12:49:55 12:50:00 12:50:05		
		Arayūz Durumları	^ ×
	Network Paket Durumu	Gruplanmamis	

Arayüze giriş yapıldıktan sonra ilk adım olarak güvenlik amacı ile Parolanın değiştirilmesi gerekmektedir. Kullanıcı Yönetimi menüsü altında bulunan **Yönetim Paneli Kullanıcıları** sekmesine tıklanır.



Ardından "Detaylar" butonuna tıklanır.

Yöne	tim Paneli Kul	llanıcıları											2 Yenile + Ekle
XLS	CSV PDF							🎟 Göster/Gizle 🗸	Sayfa Başı Kay	ıt Sayısı	Tamam	T Filtrele	🖌 Filtreyi Temizle
#	Durum	🖺 Adı	↓î Soyadı	👫 Kullanıcı Adı	İşlemler								
1	Aktif	Antikor	Admin	admin	🕼 Düzenle	💼 Sil 🛛 😁 Gi	rup Üyelikleri	→ Yetkiler ve Roller	* Detaylar	🗢 Sertifika Yönetimi 🔫			
					α	< 1 > x							Git

Açılan sayfada "Düzenle" butonuna tıklanır.

Yönetim Paneli Kullanıcıları

	a Kul	ullanıcı De
kor Admin		
anıcı Adı : admin		
cı Bilgileri		
r Soyadi : Antikor Admin		
anici Adi : admin		
osta : bilgi@epati.com.tr		
uşturma Tarihi :		
iş Yapılan iP Adresi : 10.2.1.157		
riş Yapılan Tarih : 2021-03-22 12:49:46+03		
riş Yapılan Son IP Adresi : 10.2.1.157		
riş Yapılan Son Tarih : 2021-03-19 17:28:03+03		
riş Sayısı : 6		
n Tarafından Olucturuldu		

Kullanıcı bilgileri bölümünde yeni Parola belirlenerek "Kaydet" butonuna tıklanır.

Profil Fotoğrafı Yükle
Profil Fotoğrafi : 🕹 Yükle

Kimlik Bilgileri	
Adı	Antikor
Soyadı	Admin
ePosta	bilgi@epati.com.tr

Kullanıcı Bilgileri	
Kullanıcı Adı	admin
	Kullanıcı Parolasını Değiştir.



	Parolanızı Güncelleyin	
Eski Parola	I.	
Yeni Parola	₹)	
Yeni Tekrar	₹)	
	🖺 Kaydet	

Kurumsal Güvenlik Politikası

Yönetim Paneli Ayarları menüsünün altında bulunan Yönetim Paneli Erişim Ayarları sayfasına gidilir.



WEB yönetim arayüzüne hangi IP adres(ler)inden giriş yapılacağını gösterir. Kısıtlı erişim seçilirse erişilmesi istenen IP adres(ler)inin veya Network adres(ler)inin belirtilmesi gerekir.

Yönetim Paneli Erişim Ayarları							🗘 Yenile 🕇 Ekle
			Yönetim Pan	eli Erişim Ayarları			
		Çalışma Modu Trafiği Logla Sertifika Bazlı Ki Harici Kaynaklar Web Arayüzü Eri	mlik Doğrulama dan Kimlik Doğrulama şim Protokolü 😫	Her Yerden Erişim Kapatî Kapatî O http 💿 https	~		
	XLS	CSV PDF					
	#	IP Adresi	👫 Açıklama	1 işlemler			
	1	0.0.0/0		🕼 Düzenle	🛍 Sil		
	2	10.0.0/8		🕼 Düzenle	🛍 Sil		
	з	172.16.0.0/12		🕼 Düzenle	🛍 sil		
	4	192.168.0.0/16		🕼 Düzenle	🛍 Sil		
			α c 1 → 3	9	Git		

ALAN	AÇIKLAMA
Her Yerden Erişim	IP adres kısıtlaması olmadan herhangi IP adresinden AntiKor2 arayüzüne erişilebilir durumdadır.
Kısıtlı Erişim	Sadece belirlenen IP adres(ler)i veya network adres(ler)inden erişilebilir durumdadır.
Trafiği Logla	Buton aktif edilerek yönetim paneli erişim logları Syslog sunucuya gönderilmesi sağlanabilir.
Sertifika Bazlı Kimlik Doğrulama	Yönetim Paneli Kullanıcılarında oluşturulan sertifika ile giriş yapılacak ise Açık olmalıdır. Açık olduğu takdirde sertifika bulunan yönetim paneli kullanıcıları haricinde kimse arayüze giriş yapamaz.
Harici Kaynaklardan Kimlik Doğrulama	Harici kaynaklardan doğrulamayı aktif eder.
Web Arayüzü Erişim Protokolü	Arayüze yapılacak olan bağlantı türü seçilir.

ePati Siber Güvenlik Teknolojileri A.Ş. Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN 
Ethernet Atama



Antikor L2 Tünel üzerinde bulunan ethernetlerin ayarlarının yapıldığı bölümdür. Yerel Ağ (LAN), İnternete Çıkış (WAN), Sunucu Bölgesi (DMZ) ve PPPoE ayarları bu bölümden yapılır. Lisans içeriğine göre birden çok LAN, WAN ve DMZ arayüzü eklenebilir.

Ethern	t Atan	าล										C Yenile	WAN Ekie LA	N Ekie DMZ Ekie PPPoE Ekie
XLS CSV FDF Sayfa Başı Kayıt Sayısı							Tamam	▼ Filtrele 🖌 Filtreyi Temizle						
# D	urum	lt cl	uster Üyeliği	🕴 Web Arayüzü Erişimi	🎼 Güvenlik Bölgesi	👫 Arayüz 👫	Ethernet Adı 🛛 🕸	Seçili Hız	LT MTU LI	IPv4 Adresi	IPv6 Adresi	1 Seçenekler	🕴 Açıklama	11 İşlemler
1 A	ctif	Ak	tif	Aktif	wan-zone	WAN1	enp3s0 - Fiziksel	autoselect	1500	10.2.1.178/24				🕼 Düzenle 🛛 🛅 Sil
							« < 1 > »							Git

WAN Ekle Yeni Kayıt

Durum	Aktif
Güvenlik Bölgesi	wan-zone
Arayüz	WAN2
Ethernet Adı	enp4s0
Hız	autoselect
MTU	1500
Web Arayüzü Erişimi	Aktif
Cluster Üyeliği	Pasif
Açıklama Avarları	
Açıklama Ayarları	
Açıklama Ayarları Otomatik IPv4 Al IPv4 Adresi	IPv4 10.10.10/24
Açıklama Ayarları Otomatik IPv4 Al IPv4 Ağ Geçidi	IPv4 10.10.10/24 IPv4 10.10.10.1
Açıklama Ayarları Otomatik IPv4 Al IPv4 Ağ Geçidi IPv4 Ağ Geçidi	IPv4 10.10.10/24 IPv4 10.10.10.1
Açıklama Ayarları Otomatik IPv4 Al IPv4 Ağ Geçidi IPv4 Ağ Geçidi Otomatik IPv6 Al EUI64	IPv4 10.10.10.10/24 IPv4 10.10.10.1
Açıklama Ayarları Otomatik IPv4 AI IPv4 Ağ Geçidi IPv4 Ağ Geçidi Otomatik IPv6 AI EUI64	IPv4 10.10.10.10/24 IPv4 10.10.10.1 Pnoff IPv6 IPv6 ffff::10/8

Not: Ethernet atama bölümünden veya konsol ekranından WAN IP'si değiştirilirse; LAN yapılandırılmasında bulunan IPv4 ayarlarındaki Global NAT'ın bu IP'ye göre değiştirilmesi gerekmektedir.(LAN yapılandırılması seçenekler bölümünde NAT seçili ise değiştirilir.)

🖉 İptal 🛛 🖹 Kaydet

Ethernet Durumları

ALAN	AÇIKLAMA
Durum	Aktif ya da pasif olma durumu seçilir.
Güvenlik Bölgesi	Arayüzün bulunacağı güvenlik bölgesi seçilir.
Arayüz	Hangi arayüzün (WAN1, WAN2, …) kullanılacağı seçilir.
Ethernet Adı	Hangi fiziksel ethernet arayüzünün kullanılacağı seçilir.
Ніг	Hız belirlenir.
MTU	MTU değeri girilir

IP Ayarları

ALAN	AÇIKLAMA
Otoma tik IPv4 al	IPv4 adresinin otomatik olarak alınıp alınmayacağı seçilir.
IPv4 Adres i	Otomatik IPv4 Al seçilmez ise IPv4 adresi girilir.
Ağ Geçid i	Ağ geçidi yazılır.
Otoma tik IPv6 al	IPv6 adresinin otomatik olarak alınıp alınmayacağı seçilir.
EUI64	Aktive edildiği takdirde; Genişletilmiş Benzersiz Tanımlayıcı (Extended Unique Identifier), istemcinin 48 bitlik Ethernet MAC adresini kullanarak 64 bitlik Arayüz Kimliği oluşturmak için bu 48 bitlik adresin ortasına 16 bit yerleştirir.
IPv6 Adres i	Otomatik IPv6 Al seçilmez ise IPv6 adresi girilir.
IPv6 Ağ Geçid i	Otomatik IPv6 Al seçilmez ise IPv6 ağ geçidi girilir.

LAN Ekle Yeni Kayıt

lan-zone LAN1 enp4s0	IPv4 Adres DHCPv Havuzu Modu DHCPv	4 Tüm İstemcilere IP Dağıt ×
LAN1 enp4s0	DHCPv4 Havuzu Mode	4 Tüm İstemcilere IP Dağıt 🛛 🗙
enp4s0		
autoselect	Baslangi	4 IPv4
uutoserett	✓ DHCPv4 Biti	s IPv4
1500		
Akiif	DHCPv4 Ag Geçid	ĝ IPv4
Pasif	DHCPv4 Relay Adres	y IPv4
	Seçenekler MAC Eşleme	
Otomatik IPv6 Al	Carl Charles Control C	Anons Yap
Pasif	DHCPv6 Rel Managed Ba	ay DHCPv4 Relay
IPv6 ffff::1/8		
IPv6		
IPv6		
IPv6		
	Axttr Pasif Otomatik IPv6 AI Pasif IPv6 IPv6 IPv6 IPv6 IPv6	Attif Pasif Pasif Otomatik IPv6 AI Pasif IPv6 IPv6 IPv6

Not: Yeni kayıt(LAN Ekle ve DMZ Ekle için) oluştururken seçenekler bölümünde seçilmiş olan servis/servisler; gösterge panelindeki servis durumlarından ilgili servis/servisler başlatılmalıdır.

Ethernet Durumları

ALAN	AÇIKLAMA
Durum	Aktif ya da pasif olma durumu seçilir.
Güvenlik Bölgesi	Arayüzün bulunacağı güvenlik bölgesi seçilir.
Arayüz	Hangi Arayüzün (LAN1, LAN2,) kullanılacağı seçilir.
Ethernet Adı	Hangi fiziksel ethernet arayüzünün kullanılacağı seçilir.
Hız	Hız belirlenir.
MTU	MTU değeri girilir

×

ALAN	AÇIKLAMA
Otoma tik IPv4 al	IPv4 adresinin otomatik olarak alınıp alınmayacağı seçilir.
IPv4 Adres i	Otomatik IPv4 AI seçilmez ise IPv4 adresi girilir.
Ağ Geçid i	Ağ geçidi yazılır.
Otoma tik IPv6 al	IPv6 adresinin otomatik olarak alınıp alınmayacağı seçilir.
EUI64	Aktive edildiği takdirde; Genişletilmiş Benzersiz Tanımlayıcı (Extended Unique Identifier), istemcinin 48 bitlik Ethernet MAC adresini kullanarak 64 bitlik Arayüz Kimliği oluşturmak için bu 48 bitlik adresin ortasına 16 bit yerleştirir.
IPv6 Adres i	Otomatik IPv6 Al seçilmez ise IPv6 adresi girilir.

DHCP Ayarları

ALAN	AÇIKLAMA
DHCPv4 Başlangıç IP	LAN'da dağıtılacak olan IPv4 adreslerinin başlangıç IPv4 adresi girilir.
DHCPv4 Bitiş IP	LAN'da dağıtılacak olan IPv4 adreslerinin son IPv4 adresi girilir.
DHCPv4 Ağ Geçidi	Ağ geçidi girilir.
DHCPv6 Başlangıç IP	LAN'da dağıtılacak olan IPv6 adreslerinin başlangıç IPv6 adresi girilir.
DHCPv6 Bitiş IP	LAN'da dağıtılacak olan IPv6 adreslerinin son IPv6 adresi girilir.

Seçenekler

ALAN	AÇIKLAMA
DHCPv4	DHCPv4 kullanılıp kullanılmayacağı seçilir.
DHCPv6	DHCPv6 kullanılıp kullanılmayacağı seçilir.
Kayıt Al	Kayıt al sisteminin aktif olması istenir ise seçilir.
Anons Yap	Eklenen IP adresi için anons işlemi (BGP kullanılır) yapılacaksa seçilir.
MAC Eşleme	IP adreslerinin MAC adresleri ile eşleşip eşleşmeyeği seçilir.
DHCPv4 Relay	Gelen DHCP mesajlarını belirli bir DHCPv4 sunucusuna iletir.
DHCPv6 Relay	Gelen DHCP mesajlarını belirli bir DHCPv6 sunucusuna iletir.

Not: DHCP sunucuları (DHCPv4/v6) ile DHCP Relay (DHCPv4/v6) aynı anda çalışmamaktadır.

PPPoE Ekle Yeni Kayıt

İnternet bağlantısı servis sağlayıcı tarafından sağlanıyor ise servis sağlayıcıya ait ayarların tanımlandığı bölümdür.

 \times

Eth	Ethernet Atama - PPPoE - Yeni Kayıt 🛛 🗙 🗙				
	Ethorpot Durumlari				
	Ethernet Durumlari				
	Durum	AkBf			
	Güvenlik Bölgesi	wan-zone	~		
	Arayüz	WAN2	~		
	Ethernet Adı	enp4s0	~		
	Hız	autoselect	*		
	MTU	1500			
	Açıklama				
	Kullanıcı Bilgileri				
	Kullanıcı Adı	epati@ttnet			
	Parola	123456			
	Seçenekler				
	Yedek H	lat			

🥥 İptal 🛛 🖺 Kaydet

Ethernet Durumları

ALAN	AÇIKLAMA
Durum	Aktif ya da pasif olma durumu seçilir.
Güvenlik Bölgesi	Arayüzün bulunacağı güvenlik bölgesi seçilir.
Arayüz	Hangi arayüzün kullanılacağı seçilir.
Ethernet Adı	Hangi fiziksel ethernet arayüzünün kullanılacağı seçilir.
Ніг	Hız belirlenir.
MTU	MTU değeri girilir.

Kullanıcı Bilgileri

ALAN	AÇIKLAMA
Kullanıcı Adı	Abone olunan servis sağlayıcıya ait kullanıcı adı girilir.
Parola	Kullanıcı adına ait parola girilir.

Seçenekler

ALAN	AÇIKLAMA
Yedek Hat	Yedek hat olarak kullanılıp kullanılmayacağı seçilir.

ePati Siber Güvenlik Teknolojileri A.Ş. Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN





Ethernet Durumları

Fiziksel ethernet arayüzlerine ait durumları gösterir.

Ethernet Durumları

#	Yönetsel Durumu	Ağ Kablosu Durumu	Ethernet Adı	Adı	Medya Tipi	MAC Adresi	MTU	Bildirim Ledi
1	Devrede	Kablo Takılı	em0	WAN1	1000baseT	00:0c:29:27:73:a9	1500	Donanım desteklemiyor
2	Devrede	Kablo Takılı	em1	Atanmamış	1000baseT	00:0c:29:27:73:b3	1500	Donanım desteklemiyor

ALAN	AÇIKLAMA
Yönetsel Durumu	Ethernet arayüzünün durumunu gösterir.
Ağ Kablosu Durumu	Ethernet arayüzünün bağlantı durumunu gösterir.
Ethernet Adı	Sistem ethernet arayüz adını gösterir.
Adı	Antikor ethernet arayüz adını gösterir.
Medya Tipi	Bağlantı hızını gösterir.
MAC Adresi	Ethernet arayüzününün MAC adresini gösterir.
MTU	Paket boutunu gösterir.
Bildirim Ledi	Donanım destekliyor ise LED açılabilir.

ePati Siber Güvenlik Teknolojileri A.Ş. Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN





epati IP Havuzları



Yönetilecek olan ağ(lar)ın IP adres aralıkları bu menüde tanımlanır. Bu aralıklar, Antikor L2 Tünel'in denetleme mekanizmalarında kullanılacaktır.

IP adres havuzlarına kullanılmak istenen IP adresleri önceden eklenmelidir. Bazı işlemler (WAN Ekle) IP havuzlarına IP adreslerini eklemeden yapılamamaktadır.

IP Havuzları				🕻 Yenile 🕇 Ekle
XLS CSV PDF	🖽 Göster/Gizle 🗸	Sayfa Başı Kayıt Sayısı	Tamam Taltrele	🖌 Filtreyi Temizle
# Ethernet	↓ IP Bloğu	🕸 Açıklama	1 işlemler	
1 WAN1	192.168.168.0/24	WAN1	🕼 Düzenle 👔 Sil	
	« c 1	I > »		Git
IP Havuzları Ye	ni Kayıt			
IP Havuzları - Yeni	Kayıt		×	
Ethernet	Seçiniz		v	
Adres Ailesi	🔵 IPv4 🔵 IPv6			
IP Bloğu	IPv4			
Açıklama				
		Ø İptal	🖺 Kaydet	
ALAN	AÇIKLAMA			
Ethernet	Tanımlanacak olan IP adre seçilir.	eslerinin kullanacağı e	ethernet arayüzü	
Adres Ailesi	Tanımlanacak olan IP adre	es ailesi seçilir.		
IP Adres Bloğu	Tanımlanacak olan IP adre	es bloğu girilir.		
Açıklama	Açıklama girilir.			

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

epati IP Atama

Sistemde farklı veya aynı ethernet arayüzlerine birden fazla IP adres(ler)i verilmesi gerekirse bu bölümden istenilen IP adres(ler)i verilebilir.

P Atama						ØYenile +E
XLS CSV PDF # Durum	ţi I	Vetwork	IT IP Adresi	17 Açıklama	🖩 Göster/Gizle 🗸	Sayfa Baqi Kayit Sayisi Tanam Tribele Fridey Tende
1 Aktif	1	WAN1	20.0.0.5	test		CZ Düzenle CS
			4			
P Atama Yeni	Kayıt					
IP Atama - Yen	i Kayıt				×	
Du	rum	Aktif				
Netv	vork	Seçiniz.			•	
Adres A	ilesi	IPv4) IPv6			
IP Ac	lresi	IPv4	Ör : 10.10.10.10/24			
Açıkl	ama					
				Ø İptal 🖺	Kaydet	
ALAN	AÇ	IKLAMA				
Network	Eth seç	ernet Atan ilir.	na bölümünde tanım	ılı olan network		
Adres Ailesi	Tar	umlanacal	colan IP adres ailes	i seçilir.		
IP Adresi	Tar	umlanacal	colan IP adresi girili	r.		
Açıklama	Açı	klama giril	ir.			
	<u> </u>	111				0

ePati Siber Güvenlik Teknolojileri A.Ş. Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN



CONCICOURS Tümlesik Siber Güvenlik Sistemi



EPOTİ Sanal Ethernet Birleştirme

Bileştirme (Köprüleme - LACP): Bu bölümde Antikor L2 Tünel'in üstünden geçen hızı arttırmak veya**Cluster** olarak Antikor L2 Tünel çalıştırmak için kullanılmaktadır.

Sanal Ethernet - Link Birleştirme			🔁 Yenile 🛛 🕇 Ekle
XLS CSV PDF	I Göster/Gizle Sayfa Başı Kayıt Sayısı	Tamam	▼ Filtrele
# Adı 🎼 Sanal Ethern	et Türü 🕴 Üye Ethernetler	่ំា Açıklama	Jî İşlemler
	« c > »		Git
Sanal Ethernet Birleştirme Birleştirme türü olarak 7 seç Sanal Ethernet - Link Birleşt	e Yeni Kayıt enek mevcuttur. irme - Yeni Kayıt	×	
Adı	Otomatik üretilecektir		
Üye Ethernetler			
Sanal Ethernet Türü	Köprüleme	~	
Açıklama	Köprüleme Köprüleme - Rapid STP Failover Load Balance LACP		
	Round Robin ByPass	det	



ALAN	AÇIKLAMA
Adı	Sanal Ethernet Adı otomatik üretilir.
Üye Ether netle r	Fiziksel Ethernet seçilir.
Sanal Ether net Türü	
Köprü leme	İki TCP/IP ağını birbirine bağlayan bir donanımdır. İki veya daha fazla aynı protokolü kullanan ağları bağlamak için kullanılan bir cihazdır. Bağlama işlemi, iki ağdaki her mesajı birbirine tekrarlanarak sağlanır.
Köprü leme - Rapid STP	Spanning-tree protokolü, döngüleri (loop) engellemek için geliştirilmiş bir protokoldür.
Failo ver	Yapı içerisinde bulunan cluster üyesi sunucuların ve bu sunucular üzerinde çalışan rol ve servislerin kapalı olduklarında veya çevresel etkenlerden etkilenerek down duruma geldiklerinde (donanımsal arızalar gibi) cluster üyesi olan bir sunucudan diğer sunucuya aktarılmasına denilmektedir.
Load Balan ce (FEC)	Load Balance kelime anlamı olarak yük paylaşımı anlamına gelmektedir. İki adet farklı internet bağlantısını aynı anda kullanarak bant genişliği artar ve hız artırımı yapılmış olur.
LACP	Link Aggregation Control Protocol (LACP) mevcut bağlantıları kurmak için kümelenmiş bağlantıların iki ucunda kullanılan Layer-2 anlaşma protokolüdür. LACP içindeki bağlantılardan birinde sorun oluşması halinde iletim diğer bağlantılardan yapılmaya devam edecektir. Bağlantı tekrar aktif olduğunda yük tekrar dağıtılıp yük dengeleme sağlanacaktır. Bununla birlikte, iletimi sağlayan bağlantılar arasında yük dengelemesi yaparak, bant genişliği de yükselecektir.
Round Robin	Tek bir kaynak ve birden fazla kullanıcı olması durumunda kaynağı kullanıcılar arasında eşit zaman aralıkları ile paylaştırmaya yönelik algoritmaya verilen isimdir. Örneğin 3 adet DNS sunucusu varsa, ilk istek yapan kullanıcı birinciye, ikinci istek yapanı ikinci sunucuya, üçüncü istek yapan kullanıcıyı da üçüncü sunucuya yönlendirir.
ByPas s	-
Açıkl ama	Açıklama isteğe göre yazılır.

ePati Siber Güvenlik Teknolojileri A.Ş. Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN





EPOTÍ Sanal Ethernet Loopback

Antikor L2 Tünel'de kendi içinde yerel bir Ethernet oluşturmak için kullanılır.



epati Sanal Ethernet VLAN Etiketi Tabanlı

Belirli VLAN'lar ethernetlere dahil edilmek istendiğinde bu bölümdenSanal Ethernet oluşturulabilir. Bir ethernete istenildiği kadar VLAN atanabilir.

Sanal Ethernet - VLAN Etiketi Tabanlı Sayfa Başı Kayıt Sayısı 🥜 Filtreyi Temizle 👃 Ethernet Adı 1 VLAN ID 1 Açıklama 1 İşlemler Adı « < > »

Ekle butonuna tıklanır.

Sanal Ethernet - VLAN Etiketi Tabanlı Ağ Arayüzü Yeni Kayıt

Sanal Ethernet - VLAN Etiketi Tabanlı - Yeni Kayıt × Adı Otomatik üretilecektir Ethernet Adı ens35 VLAN ID Ör : 100 Açıklama

> Ø İptal 🖹 Kaydet

ALAN	AÇIKLAMA
Adı	Sanal Ethernet Adı otomatik üretilir.
Ethernet Adı	Ethernet arayüzü seçilir.
VLAN ID	Ethernet arayüzüne dahil olacak VLAN ID yazılır.
Açıklama	Açıklama isteğe göre yazılır.

ePati Siber Güvenlik Teknolojileri A.Ş. Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN







1/1 0.5	I Etikoti	Tabaali	Vani	Varut	



epati Network Monitörü

Anlık tüm trafiğin tcpdump parametreleri, belli filtreler ve/veya Layer bazında görüntülenebildiği sayfadır.

Tek seferde en fazla 25 satır gösterebilmektedir.

ametreler					
Çıktı	Sekran (PCAP Olarak Kaydet	Hazır Filtreler	Filtre Yok	~
Dns Çözümlemesi	Yapsın	Yapmasın	Protokol	Tûmû	
Ethernet Başlıkları	Göster (Gösterme		Tuniu	
Detaylı Sonuç	Göster (Gösterme	Ek Parametreler		
Network	Network		▼ Snapshot Boyutu	262144	Byte
	_				

Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN **\$** +90 324 361 02 33 🖶 +90 324 361 02 39

Tümlesik Siber Güvenlik Sistemi







Antikor L2 Tünel yazılımının kurulu olduğu sunucunun **gücünü kapatmak** veya **yeniden başlatmak** için kullanılır.

Güç Yönetimi				
	Antikoru Kapat	Antikoru Yeniden Başlat		
	டு	C		
<mark>ePati Siber Güvenlik Teknolo</mark> Mersin Üniversitesi Çiftlikköy Kar Teknopark İdari Binası Kat: 4 No: Posta Kodu: 33343 Yenişehir / <i>N</i>	<mark>ijileri A.Ş.</mark> mpüsü 411 IERSİN		 	٩

EPOTI IP Network Hesaplama

Bu bölümde **IP Network Hesaplama** yapılabilmektedir. Aşağıda örnek görülmektedir. Sağ tarafta IP adresleri kapsam içerisinde olup olmadığı kontrolleri yapılabilir.

IP & Network Hesaplama

IPv4 10.10.10.0 ske Bitleri 24 24 • Immediate Immediate Ağ Maskesi IPv4 IPv4 255.255.255.0 Islangıç IP IPv4 IPv4 10.10.10.1 iş IP IPv4 IPv4 10.10.10.254 Ivork Adres IPv4 IPv4 10.10.10.0	ork Hesaplayıcı		ł	Kapsam Kontrol	
ke Bitleri 24 v Im Hesapla IP v4 255.255.255.0 angıç IP IP v4 10.10.10.1 i IP v4 10.10.10.254 IP v4 work Adres IP v4 10.10.10.0	work	IPv4 10.10.10.0		Network	IPv4 10.10.10.0
imit Hesapla IP v4 255.255.255.0 ingrç IP IP v4 10.10.10.1 IP IP v4 10.10.10.254 indcast Adres IP v4 10.10.10.0	ke Bitleri	24	v	Maske Bitleri	24
Ağ Maskesi IPv4 255.255.255.0 Iangıç IP IPv4 10.10.10.1 ş IP IPv4 10.10.10.254 work Adres IPv4 10.10.10.0 adçast Adres IPv4 10.10.10.0		🖩 Hesapla		IP Adresi	IPv4 10.10.10.0
angiç IP IPv4 10.10.10.1 IP IPv4 10.10.10.254 vork Adres IPv4 10.10.10.0	ğ Maskesi	IPv4 255.255.255.0			🖌 Kontrol Et
IP IPv4 10.10.10.254 vork Adres IPv4 10.10.10.0 idcast Adres is is is is is is is is is is is is is i	angıç IP	IPv4 10.10.10.1			
dcast Adres	IP	IPv4 10.10.10.254			
cast Adres	ork Adres	IPv4 10.10.10.0			
IPv4 10.10.10.255	dcast Adres	IPv4 10.10.10.255			
	Mersin Üniver Teknopark İda	sitesi Çiftlikköy Kampüsü ri Binası Kat: 4 No: 411			✓ bilgi@epati.com.tr ↓ +90 324 361 02 33





ераті Tarih Saat Ayarları

Sistemin tarih ve saati ayarlamak için kullanılır. Sistemde bütün raporlar bu tarih ve saate göre raporlanır. Güncelle butonuna tıklanması saati düzeltmek için yeterlidir.

28 04 202	20	NTP Sunucular 2 Yenile +				
20.01.201		XLS CSV PDF BGöster/	Gizle 🗸 Sayfa Başı Kayıt Sayısı	Tamam Tiltrele		
11:39 33	+3	# Durum 🎼 Sunucu A	dresi 🕴 İşlemler			
Dtomatik Al		1 Aktif 0.tr.pool.r	ntp.org	il 🔁 Senkronize Et		
at Dilimleri +3	v					
C Kaydet			« (] > >	Gif		
# Kimlik Bilgileri	👫 Kullanıcı Adı	↓† İşlem Adı	र ↓† İşlem Zamanı	11		
1 Antikor Admin	admin	Güncelleme	2020-04-24 00:20:56.130152+03			
2 Antikor Admin	admin	Ekleme	2020-04-24 00:20:15+03			
				Git		

Tümlesik Siber Güvenlik Sistemi

🖶 +90 324 361 02 39

Teknopark Idari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN

epati Yardımcı Araçlar



Ping

İster yerel ağdan ister internetten bir ip ye ping atılabilir. Eğer ICMP yasağı yoksa bu IP adresinden yanıt dönecektir. Bu şekilde o IP adresine sahip bilgisayarın açık olduğunu anlaşılabilir.

Ping Trace Route DNS Sorgulama		
IPv4, IPv6 veya Alan Adı giriniz	Boyut(Byte) Kaynak Adres	► Başlat
En üsteki kayıt en son gelen çıktıdır. Çıktı geçmişinde maksir	mum 25 satır gösterilir.	
ALAN	AÇIKLAMA	
IPv4, IPv6 veya Alan Adı giriniz	Ping gönderilecek adres girilir.	

Trace Route

Yazılan bir hedef IP adresine erişmek için internette hangi yönlendiricilerden/routerlardan geçtiği ve IP adreslerini gösterir. İnternette veya herhangi bir dış IP adresinde sorun olduğunda hangi IP adresinden sonra cevapsız kaldığı bu araçtan öğrenilebilir.

Ping	Trace Route	DNS Sorgulama			
IPv4, II Adı gir	Pv6 veya Alan iniz			Kaynak Adres	► Başlat
_					🗎 Temizle
Area	üsteki kavıt on son ge	lan siktidir. Cikti gesmisinda maksin	num 25 catir göstarilir		
U En l	usteki kayit eri sori ge	ien çıktıdır. Çıktı geçmişinde maksır	num 25 satir gösteniir.		

ALAN	AÇIKLAMA
IPv4, IPv6 veya Alan Adı giriniz	Trace yapılacak adres girilir.

DNS Sorgulama

İster bir DNS IP adresini veya bir alan adını yazarak bunun Adres, Mail Exchanger ve Name Server bilgilerine ulaşılabilir.

Ping	Trace Route	DNS Sorgulama					
Türü	Seçiniz.		IPv4, IPv6 veya Alan Adı giriniz	Sunucu Adresi	193.255.128.2	2	► Başlat 會 Temizle
ALAN			AÇIKLAMA				
ALAN Türü			AÇIKLAMA DNS kayıt türleri	nden biri seçilir.			
ALAN Türü IPv4, girini	IPv6 veya iz	Alan Adı	AÇIKLAMA DNS kayıt türlerin Sorgulanacak ad	nden biri seçilir. İres yazılır.			

Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN www.epati.com.tr
 ilgi@epati.com.tr
 +90 324 361 02 33
 +90 324 361 02 39

epati Yedekle / Geri Yükle



AntiKor'daki bütün ayarlar bilgisayara alınıp istenildiği zaman yedekten geri dönülebilir.Yedekle butonuna basılarak yedek bilgisayara kaydedilir. (Not: indirme yapılırken Flashget tarzı download programları varsa kapatılması gerekmektedir.) Geri Yükle seçeneği ile daha önceden kayıt edilmiş olan yedek tekrar sisteme yüklenebilmektedir.

Yerel Ayarlar

Yedekle / Geri Yükl	le	
Yerel Ayarlar	Uzak Sunucu Ayarları	
	Yedek Kapasitesi	Seri Yükle
	Past	

Uzak Sunucu Ayarları

Antikorda uzak sunucuya kullanıcının belirleyeceği yedekleme aralığına göre yedeklenebilmektedir.

Yedekle / Geri Yükle	2			
Yerel Ayarlar	Uzak Sunucu Ayarları			
			Yedekleme Ayarları	
		Sunucuya Yedekleme	Pasil	
			醫 Kaydet	
Yedekle / Geri Yükle				
Yerel Ayarlar	Uzak Sunucu Ayarları			
			Yedekleme Ayarları	
		Sunucuya Yedekleme	Aker	
		Yedekleme Aralığı	1 Hafta 🔹	
		Gün	Pazartesi 🔻	
		Saat		
		Adres Ailesi	● IPv4 Pv6	
		Sunucu Adresi	IPv4	
		Dosya Paylaşım Türü	FTP	
		Sunucu Portu		
		Kullanıcı Adı		
		Parola		
		Hedef Klasör		
			🖺 Kaydet	

ePati Siber Güvenlik Teknolojileri A.Ş. Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN



epati Bildirim Geçmişi



Güncel

Güncel bildirimleri barındırmaktadır. Bir bildirim için Anlaşıldı butonuna tıklanırsa, o bildirim artık geçmiş sayfasında görülecektir.

CONCICOURSE Tümleşik Siber Güvenlik Sistemi

	çmişi						C Yeni
Güncel	Geçmiş						
XLS	CSV PDF				⊞ Göster	/Gizle - Sayfa Başı Kayıt Sayısı Tamam	🕇 Filtrele 🖌 Filtreyi Temizle
#	Tarih	↓₹ -	Seviye		Detay	👫 Kimlere Gönderildi	İşlemler
1	2020-01-19 05:46:22	1	Uyarı		RAM kullanımı 95 - 100 arasındadır. Kullanım Oranı: 96		Anlaşıldı
2	2020-01-19 05:46:17		Bilgilendirme		RAM kullanımı 0 - 95 arasındadır. Kullanım Oranı: 95		Anlaşıldı
3	2020-01-19 05:30:52	1	Uyarı		RAM kullanımı 95 - 100 arasındadır. Kullanım Oranı: 96		Anlaşıldı
4	2020-01-19 05:30:47		Bilgilendirme		RAM kullanımı 0 - 95 arasındadır. Kullanım Oranı: 95		Anlaşıldı
5	2020-01-19 05:29:36		Uyarı		RAM kullanımı 95 - 100 arasındadır. Kullanım Oranı: 96		Anlaşıldı
δ	2020-01-19 05:28:28	ſ	Bilgilendirme		RAM kullanımı 0 - 95 arasındadır. Kullanım Oranı: 95		Anlaşıldı
7	2020-01-19 05:22:59	ſ	Bilgilendirme		RAM kullanımı 95 - 100 arasındadır. Kullanım Oranı: 96		Anlaşıldı
8	2020-01-19 05:22:59	ſ	Uyarı		RAM kullanımı 95 - 100 arasındadır. Kullanım Orani: 96		Anlaşıldı
9	2020-01-12 09:50:09	ſ	Bilgilendirme		CPU kullanımı 0 - 95 arasındadır. Kullanım Oranı: 67		Anlaşıldı
10	2020-01-12 09:49:59	1	Uyarı		CPU kullanımı 95 - 100 arasındadır. Kullanım Oranı: 95		Anlaşıldı
eçm	niş						
irim Ge	çmişi						C Yeni
Güncel	ıçmişi Geçmiş						3 Yen
Güncel	csv PDF				III Göster/	<mark>/Gizle ↓</mark> Sayfa Başı Kayıt Sayısı <mark>Tamam</mark>	© Yeni ▼ Fitrele
Güncel XLS	csv PDF Farih	J# Se	viye		II Coster/ Detay	/Gizle • Sayfa Başı Kayıt Sayısı Tamam	₽ Yen T Filtrele
Güncel XLS # 1	csv Ppr. Tarih 2020-01-19 05:46:22	J≣ se ∪y	r viye		Detay RAM kullanımı 95 - 100 arasındadır. Kullanım Oranı: 96	XGide • Sayfa Başı Kayıt Sayısı Tamam الله لله Kimlere Gönderildi	€ Yen ▼ Fitrele ✓ Fitreyi Temble işlemler Anlaşıldı
Güncel XLS # 1 1 2 2 2	Geçmişi Gy PDF Tarih 2020-01-19 05:46:22 2020-01-19 05:46:17]₹ S€ U) BI	Wiye Jari 'gilendirme		Detay RAM kullanımı 95 - 100 arasındadır. Kullanım Oranı: 96 RAM kullanımı 0 - 95 arasındadır. Kullanım Oranı: 95	/Gide - Sayfa Başı Kayıt Sayısı Tamam	♥ Fitrele ✓ Fitreyi Temble işlemler Anlaşıldı Anlaşıldı
Güncel	Geçmiş CSV PDF Tarih 2020-01-19 05:46:22 2020-01-19 05:46:17	JF Se U) Bia	aviye yarı Igilendirme		Ill Göster Detay RAM kullanımı 95 - 100 arasındadır. Kullanım Oranı: 96 RAM kullanımı 0 - 95 arasındadır. Kullanım Orani: 95	/Gude - Sayfa Başı Kayıt Sayısı Tamam	♥ Yer ▼ Fitrele
Güncel XLS 4 1 2 2	cymişi Geçmiş CSV PDF Tarih 2020-01-19 05:46:22 2020-01-19 05:46:17 Pati Siber C	JF Se UJ BI	eviye yarı Igilendirme Vİİk Tekn	ti olo	Detay RAM kullanımı 95 - 100 arasındadır. Kullanım Oranı: 96 RAM kullanımı 0 - 95 arasındadır. Kullanım Oranı: 95	/Side → Sayfa Başı Kayıt Sayısı Tamam İî Kimlere Gönderildi	♥ Yer
Güncel	eçmişi Geçmiş CSV PDF Tarih 2020-01-19 05:46:22 2020-01-19 05:46:17 Pati Siber C Mersin Üniver	JF sr Uj BI SÜVER Sitesi	eviye yarı Igilendirme 1 lik Tekn Çiftlikköy	it Olo ' Kar	Tectay RAM kullanımı 95 - 100 arasındadır. Kullanım Oranı: 96 RAM kullanımı 0 - 95 arasındadır. Kullanım Oranı: 95	/Gizle - Sayfa Başı Kayıt Sayısı Tanının ☐ Kimlere Gönderildi	2º Yer ▼ Fitreele ✓ Fitreele/Tentizale işlemler Anlaşıldı Anlaşıldı Git Dati.com.tr pati.com.tr
Güncel	eçmişi Geçmiş CSV PDF Tarih 2020-01-19 05:46:22 2020-01-19 05:46:17 ePati Siber C Mersin Üniver Teknopark İda	JF sı u: BI SÜVER Sitesi (ıri Bina	viye yarı Igilendirme 1lik Tekn Çiftlikköy Əsı Kat: 4	II IOOO V Kar No:	Detay RAM kullanımı 95 - 100 arasındadır. Kullanım Oranı: 96 RAM kullanımı 0 - 95 arasındadır. Kullanım Oranı: 95 (< (1 >)) jileri A.Ş. npüsü 411	/Gude - Sayfa Başı Kayıt Sayısı Tamom	Preventione T Filtrele I Filtr

EPOTİ Bildirim Grupları



Alıcı gruplarına ait kayıtların girildiği sayfadır.

ipue	Фіриси							
Kimlik	Kimlik Tanımlarından yeni bir kişi ekleyebilirsiniz, var olan kişilerin telefon ve e-posta adreslerini güncelleyebilirsiniz.							
Bildirim	Grupları						C Yenile + Ekle	
XLS	CSV PDF			⊞ Göster/Gizle → S	Sayfa Başı Kayıt Sayısı	Tamam Tiltrele	🖌 Filtreyi Temizle	
#	Durum	🗯 Grup Adı	🕴 Grup Üyeleri			İşlemler		
1	Aktif	Developers	11111111111 - Antikor Admin 22222222222 - Test TEST			🕼 Düzenle 👔 Sil		

Bildirim Grupları Yeni Kayıt

Bildirim Grupları - Yeni Kayıt					
ktif					
Seçiniz					
	ayıt				



Alan	Açıklama
Durum	Aktif ve pasif durumu seçilmelidir
Grup Adı	Grup Adı girilmelidir.
Grup Üyeleri	Grup Üyeleri belirtilmelidir. Grup Üyelerine Kimlik Tanımları sayfasında kimliği bulunan kullanıcılar eklenebilir.

ePati Siber Güvenlik Teknolojileri A.Ş. Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN

EDUTÍ Bildirim Sağlayıcı Tanımları (SMS, Eposta)

Antikor2 kayıt servisi aktif olduğunda, kayıt formunu dolduran kullanıcılara, sistem otomatik olarak bir onay kodu (SMS) gönderebilmektedir.

Bild	ldirim Sağlayıcı Tanımları									
	SMS	S Sağlayıcıları SM	/IS Ayarları	Mail Ayarları						
							C Yenile + Ekle			
	#	Adı	Metod	Url	Başarılı Cevap Kodu	Geçersiz Karakterler	İşlemler			
	1	İleti Merkezi	XML_POST	http://api.iletimerkezi.com/v1/send-sms	200		🕼 Düzenle 👔 Sil			
	2	Posta Güvercini	GET	http://www.postaguvercini.com/api_http/sendsms.asp	200		C Düzenle			
	3	TTMesaj_GET	GET	http://xml.ttmesaj.com/SENDSMS/sendsmsget.aspx	ОК		CP Düzenle			
	4	TTMesaj_XML	XML_POST	http://ws.ttmesaj.com/service1.asmx?wsdl	ОК		C Düzenle			
	5	Dakik Sms	XML_POST	http://www.dakikapi.com/api/xml_api_ileri.php	ОК		C Düzenle			
	б	TELSAM	XML_POST	http://websms.telsam.com.tr/xmlapi/sendsms	OK		CP Düzenle			

Bu işlem sayesinde kayıt formu onayı istenirse Antikor2 yöneticisinden bağımsız olarak da çalışabilmektedir.

SMS Sağlayıcıları

API'si alınan SMS sağlayıcı ayarları bu menüye tanımlanmalıdır.

Bild	irim S	m Sağlayıcı Tanımları							
	SMS	S Sağlayıcıları SM	15 Ayarları	Mail Ayarları					
							🕄 Yenile 🛛 + Ekle		
	#	Adı	Metod	Url	Başarılı Cevap Kodu	Geçersiz Karakterler	İşlemler		
	1	İleti Merkezi	XML_POST	http://api.iletimerkezi.com/v1/send-sms	200		🕼 Düzenle 📄 Sil		
	2	Posta Güvercini	GET	http://www.postaguvercini.com/api_http/sendsms.asp	200		🕼 Düzenle 👔 Sil		
	3	TTMesaj_GET	GET	http://xml.ttmesaj.com/SENDSMS/sendsmsget.aspx	ОК		🕼 Düzenle 👔 Sil		
	4	TTMesaj_XML	XML_POST	http://ws.ttmesaj.com/service1.asmx?wsdl	ОК		🕼 Düzenle 👔 Sil		
	5	Dakik Sms	XML_POST	http://www.dakikapi.com/api/xml_api_ileri.php	ОК		🕼 Düzenle 👔 Sil		
	6	TELSAM	XML_POST	http://websms.telsam.com.tr/xmlapl/sendsms	ОК		🕼 Düzenle 📋 Sil		

SMS Sağlayıcıları Yeni Kayıt

Adı	
Metod	GET •
Url	http://
Gönderilen Bilgiler	
Gelen Bilgiler	
Başarılı Cevap Kodu	
Geçersiz Karakterler	

İptal 🖪 Kaydet

ALAN	AÇIKLAMA
Adı	SMS sağlayıcısının adının yazıldığı alan.
Metod	Sağlayıcının hangi metodu kullandığı seçilir.
URL	Sağlayıcıya ait URL yazılır.
Gönderilen Bilgiler	
Gelen Bilgiler	
Başarılı Cevap Kodu	
Geçersiz Karakterler	Geçerli olmayan karakterler yazılır.

SMS Ayarları

SMS sağlayıcısından alınan kullanıcı adı ve şifresi bu menüye tanımlanmalıdır.

Bildirim Sağlayıcı Tanımları			
SMS Sağlayıcıları SMS Ayarları	Mail Ayarları		
			2 Yenile + Ekle
# Sağlayıcı Adı	Kullanıcı Adı	Gönderici Başlığı	İşlemler
MS Ayarları Yeni Ka	yıt		
Bildirim Sağlayıcı Tan	ımları - Yeni Kayıt	×	
Sms Sağlayıcı	İleti Merkezi	v	
Kullanıcı Adı			
Parola			
Gönderici Başlığı			
		🖉 İptal 🖺 Kaydet	
ALAN	AÇIKLAMA		
SMS Sağlayıcı	SMS sağlayıcılarında bi	ulunan kayıtlardan biri seçilir.	
Kullanıcı Adı	SMS sağlayıcısına ait k	ullanıcı adı girilir.	
Şifre	SMS sağlayıcısına it ku	llanıcı adının şifresi girilir.	

Gönderici Başlığı girilir.

Mail Ayarları

Bildirim ayarlarında mail kullanılması için ayarların yapıldığı bölümdür.

Bildiri	m Sağlayıcı Tanımları							
	SMS Sağlı	avıcıları	SMS Avarları	Mail Avarları				
								€ Yenile + Ekle
		Supucu		Port	Kullanıcı Adı	Güvenlik Türü	İslamlar	
	1	smtp.mailtra	p.io	2525	f511b49760ff63	Yok	🕼 Düzenle 👔 Sil	

Mail Ayarları Yeni Kayıt

Bildirim Sağlayıcı Tanımları - Yeni Kayıt

Sunucu		465	Port
Güvenlik Türü	SSL TLS Vok	SMTP A	uth
Kullanıcı Adı			
Parola			
Gönderici Adı			
Gönderici Adresi			
Açıklama			

🖉 İptal 🛛 🖺 Kayde

ALAN	AÇIKLAMA
Sunucu	Sunucu ve port bilgileri girilir.
Güvenlik Türü	Güvenlik türü seçilir.
Kullanıcı Adı	Kullanıcı adı girilir.
Parola	Parola girilir.
Gönderici Adı	Gönderici adı girilir.
Gönderici Adresi	Gönderici adresi girilir.
Açıklama	Açıklama girilir.

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



EPOTİ Bildirim Yapılandırması

Bildirim yapılandırması ayarlarının yapıldığı sayfadır.

Bildirim Yapılandırması								
Ak	ttif SMS Ayarı	Seçiniz		• Aktif SMTP Ayarı Seçiniz	T			
XLS	GSV PDF			III Göster/Gide + Sayfa Başı Kayıt Sayısı	Tamam Tiltrele Filtreyi Temizle			
#	Durum	Bildirim Seviyesi	İçerik	Açıklama	↓ ↑ işlemler			
1	Aktif	Bilgilendirme	CPU Kullanım Oranı	CPU - 0-95 Bilgilendirme (Ön-tanımlı Bildirim Yapılandırması)	🕼 Düzenle 👔 Sil			
2	Aktif	Uyarı	CPU Kullanım Oranı	CPU - 95-100 Uyarı (Ön-tanımlı Bildirim Yapılandırması)	🕼 Düzenle 👔 Sil			
3	Aktif	Bilgilendirme	Disk Kullanım Oranı	Disk - 0-95 Bilgilendirme (Ön-tanımlı Bildirim Yapılandırması)	C Düzenle			
4	Aktif	Uyarı	Disk Kullanım Oranı	Disk - 95-100 Uyarı (Ön-tanımlı Bildirim Yapılandırması)	C Düzenle			
5	Aktif	Bilgilendirme	Ethernet Link Durumu	Ethernet Link Durumu Bilgilendirme (Ön-tanımlı Bildirim Yapılandırması)	🕼 Düzenle 👔 Sil			
6	Aktif	Bilgilendirme	RAM Kullanım Oranı	RAM - 0-95 Bilgilendirme (Ön-tanımlı Bildirim Yapılandırması)	C Düzenle			
7	Aktif	Uyarı	RAM Kullanım Oranı	RAM - 95-100 Uyarı (Ön-tanımlı Bildirim Yapılandırması)	🕼 Düzenle			
				c 1 > >	Git			

Not: Aktif SMS Ayarı ve Aktif SMTP Ayarı, Bildirim Sağlayıcı Tanımları sayfasından eklenmektedir.

Bildirim Yapılandırması Yeni Kayıt

Bildirim Yapılandırm	ası - Yeni Kayıt	×
Durum	Aktif	
Bildirim Seviyesi	Bilgilendirme •	
İçerik		
Alıcı Grupları	Seçiniz	
İletim Yolu	SMS Mail Tarayıcı Bildirimi	
Açıklama		
	Ø İptal 🖪 Kayd	et



Alan	Açıklama
Durum	Aktif ve Pasif durumu seçilebilir.
Bildirim Seviyesi	Bildirim seviyesi belirtilebilir.
İçerik	CPU, RAM, Disk Kullanım oranları seçilebilir ve ardından yüzde aralığı girişi yapılmalıdır. Ethernet Link Durumu, yalnızca açık veya kapalı durumları bildirilecektir.
Alıcı Grupları	Bildirimin iletileceği alıcı grubu seçilmelidir. Bildirim Grupları sayfasından Alıcı Grubu oluşturulabilir.
İletim Yolu	İletim yolu seçilmelidir.
Açıklama	Açıklama girilir.

ePati Siber Güvenlik Teknolojileri A.Ş. Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN

EPOTİ Kullanıcı Grupları



Kullanıcılara	ait gruplar Ekle butonu il	e tanımlanabilmektedir.		
Kullanıcı Grupları				27 Yenile + Ekle
XLS CSV PDF			🔀 Göster/Gizle 🔹 Sayfa Başı Kayıt Sayısı	famam 🛛 🕇 Filtrele 🖉 Filtreyi Temizle
# Adı 1 Hepsi	I≗ Açıklama Tüm Gruplar Işin	II İşlemler II Düzenle ∎ SI → Yetkiler ve Rolle	1	Git
Kullanıcı Gr	upları Yeni Kayıt			
Kullanıcı Gru	ıpları - Yeni Kayıt		×	
	Adı			
Açı	klama			
		Ø İptal	읍 Kaydet	
ALAN	AÇIKLAMA			
Adı	Grup adı verilir.			
Açıklama	Açıklama yazılır.			
Yetkiler ve F	Roller			
Yetkiler ve vapılabilmekt	Roller butonu ile tanım tedir.	ılanmış olan kullanıcı grup	larına rol ve yetki düzenlemesi	
,				4 Geri Dan
Rol Düzenle		Yetki Düzenle		

RLS CSW PDF Pointe				XLS CS	V PDF		▼ Filtrele 🗸 Filtreyi Temizle
#	Adı	↓ h Kapsam	lt işlemler	#	Adı	🎼 Kapsam	11 İşlemler
		K C D	Git			K ()	Git

Rol Düzenle

Kullanıcı Rolleri sayfasında tanımlanmış olan rollerden biri seçilir.

_				
D	0	L	0	٣
n	U		c	

۰.		

Roller			
	tst		
		Ø İptal	🖺 Kaydet

Yetki Düzenle

Detaylı olarak gruba verilmek istenen yetkiler düzenlenir.

Roller ve Yetkiler		×	
Yetkiler	🛓 🔲 🍉 Hepsi	×	
DF ↓ Kapsam ≪ ∢	 Tanımlamalar Tünel Yapılandırması Sistem Ayarları Ağ Yapılandırması Ağ Yapılandırması Anlık Gözlem Performans Araçlar Kullanıcı Yönetimi Servis Yönetimi Uygulanacak İşlem Listesi Bildirim Yönetimi 		
ePati Siber Gü Mersin Üniversit	venlik Teknolojileri A.Ş. resi Çiftlikköy Kampüsü		

Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN **\$** +90 324 361 02 33 +90 324 361 02 39



epati Kullanıcı Rolleri

Kullanıcılara ait roller Ekle butonu ile tanımlanabilmektedir.

Kullanıcı I	Rolleri													€Yenile +Ekle
XLS C	SV PDF							Göster/Gizl	le 🔻 S	ayfa Başı Kayıt Sayı	151	Tamam	▼ Filtrele	🖌 Filtreyi Temizle
#	Adu	Li. Acıklama	11 İslemler											
1	tst	test	C2 Düzenle	🗊 Sil 🖬 Yetki	iler 🖉 Yetkiler	eri Temizle								
					a c 1	> 20								
Yeni	Kayıt													
Kulla	anici Rolle	eri - Yeni Kayit							×					
		Adı												
	Acil	dama												
	Λţii													
						Øi	otal	🖪 Kavd	et					
AL	AN.	AÇIKLAMA												

Concicor.v2 Tümleşik Siber Güvenlik Sistemi

ALAN	AÇIKLAMA
Adı	Oluşturulacak rol adı girilir.
Açıklama	Açıklama yazılır.

Yetkiler

Yetki Ağacı	

Rollere ait yetki/ler kapsayacağı bölümler seçilebilmektedir.

Rollere ait tanımlar tek başına seçilebildiği gibi seçilen nesnenin (görüntüle, ekle, güncelle, sil) ayrıca detaylı olarak tanımlanabilmektedir.

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


EPOTİ Yasaklanan Kullanıcılar

CONCICOURSE SIDE CONCULTION CONCULTICO CONCULTICO CONCULTICO CONCULTICO CONCULTICO CONCULTICO CONCULTICO CONCULTICO CONCULTICO CONCULTURA CONCULA CONCULTURA CONCULTURA CONCULTURA CONCULTURA CONCULA CONCULTURA CONCULTURA CONCULTURA CONCULTURA CONCULTURA CONCULTURA

Web Yönetim Paneli'ne giriş esnasında Oturum Ayarları'nda belirlenen politikalara aykırı olarak giriş denemesi yapan kullanıcıların yasaklarının görüntülendiği bölümdür.

Yasaklanan Kullanıcılar								
								🛛 🕄 Yenil
#	IP Adresi	Giriş Deneme Sayısı	Denenen Kullanıcı Adları	Yasak Başlangıcı		Son 5 Oturum		Eylemler
					Kullanıcı Adı	Giriş Zamanı	Çıkış Zamanı	
	10.2.				.tr	2020-07-13 13:03:44+00	2020-07-13 13:09:31+00	
					.tr	2020-07-13 11:21:03+00	2020-07-13 11:31:09+00	
1		5	5 admin 2020-07-13 13:09:50 .tr 2020-07-13 10:55:29+00	2020-07-13 11:09:29+00	Yasağı Kaldır			
		.tr 2020-07-13 10:53:41+0	2020-07-13 10:53:41+00	2020-07-13 10:55:29+00				
					.tr	2020-07-13 10:39:36+00	2020-07-13 10:51:38+00	

Alan	Açıklama
Yasağı	Engellenen IP Adresinin yasağı
Kaldır	kaldırılır.

ePati Siber Güvenlik Teknolojileri A.Ş. Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN





EPOTİ Yönetim Paneli Ayarları

AntiKor2 web yönetim arabirimine hangi IP adres(ler)inden giriş yapılacağını gösterir. Kısıtlı erişim seçilirse erişilmesi istenen IP adres(ler)inin veya Network adres(ler)inin belirtilmesi gerekir.

Yönetim Paneli Ayarları		
Servis Ayarları	Oturum	Ayarları
Web Arayüzü Erişim Protokolü 🛛 💿 https 🔿 http	Trafiği Logla	Kapali
Servis Portu Numarası 8800	Sertifika Bazlı Kimlik Doğrulama	Kapah
😫 Kaydet	Harici Kaynaklardan Kimlik Doğrulama	Kapeli
	Eş Zamanli Oturum Açma	Açık
	Çalışma Modu	Her Yerden Erişim
	Giriş Feragatnamesi	Kapah
	SSH Karşılama Ekran Durumu	Карай
	B Ka	ydet

Çalışma Modu

ALAN	AÇIKLAMA
Her Yerden Erişim	IP adres kısıtlaması olmadan herhangi IP adresindenAntiKor2 arayüzüne erişilebilir durumdadır.
Kısıtlı Erişim	Sadece belirlenen IP adres(ler)i veya network adres(ler)inden erişilebilir durumdadır.
Trafiği Logla	Buton aktif edilerek yönetim paneli erişim logları Syslog sunucuya gönderilmesi sağlanabilir.
Sertifika Bazlı Kimlik Doğrulama	Yönetim Paneli Kullanıcılarında oluşturulan sertifika ile giriş yapılacak ise <i>Açık</i> olmalıdır. Açık olduğu takdirde sertifika bulunan yönetim paneli kullanıcıları haricinde kimse arayüze giriş yapamaz.

Yönetim Paneli Erişim Ayarları Yeni Kayıt

Yönetim Paneli Erişim Ayarları - Yeni Kayıt				
	IP Adresi	IPv4		
		و) İptal 🛛 🖺 Kaydet	
ALAN	AÇIKL	AMA		
IP	Erişim	izni verilecek olan IP adres(ler)i veya n	etwork adres(ler)i	

yazılır.

Adresi

Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN ➢ bilgi@epati.com.tr
 ✓ +90 324 361 02 33
 ➡ +90 324 361 02 39



epati Yönetim Paneli Kullanıcıları

AntiKor2 yönetimi için yeni kullanıcılar tanımlama ve var olan kullanıcılar için ise kullanıcı rolleri ve yetkileri tanımlanabilmektedir.

Yönetim I	Paneli Kullanıcıla	ırı									Yenile + Ekle
XLS	SV PDF							⊞ Göster/Gizle •	- Sayfa Başı Kayıt Sayısı	Tamam T Filtrele	🖌 Filtreyi Temizle
# Du	irum 🕸 A	Adı 👘	Soyadı 🚽	Kullanıcı Adı	🕴 İzinli IP Adresleri	11 İşlemler					
1 Ak	tif A	Antikor	Admin	admin	(Adet: 0)	C Düzenle	💼 Sil 🛛 😁 Grup Üyelikleri	→ Yetkiler ve Roller	★ Detaylar 🔷 Sertifika Yönetimi -		
						« < 1 > »					Git

Yönetim Paneli Kullanıcıları Yeni Kayıt

Yönetim Paneli Kullanıcıları - Yeni Kayıt × Durum Pasif Kimlik Bilgileri Kullanıcı Yok Ŧ Kullanıcı Adı Parola Þ İzinli IP Adresleri Admin Kullanıcısı SSH Erişimi Sms Dogrulama Yap Yetkili Olduğu İstemci Grupları Yetkili Filtreleme İçin Yetkili Olduğu İstemci Grupları olduğu gruplar ile aynı olsun

🛛 🖺 Kaydet



Durum	Aktif	
Kimlik Bilgileri	111*****11 - Antikor Admin	x =
Kullanıcı Adı	admin	
İzinli IP Adresleri		
	Admin Kullanıcısı Sms Dogrulama Yap SSH Erişimi	

Øİptal	🖺 Kaydet

ALAN	AÇIKLAMA
Kimlik Bilgileri	Kimlik Tanımlamaları sayfasında tanımlı bulunan kullanıcılardan seçilir.
Kullanıcı Adı	Kullanıcı adı yazılır.
Parola	Kullanıcıya ait parola yazılır.
İzinli IP Adresleri	Kullanıcının yönetim paneline giriş yapabileceği IP adresleri girilir. İsteğe bağlı olarak boş bırakılabilir.
Admin Kullanıcısı	Admin kullanıcıya ait yetkiler, oluşturulan kullanıcıya verilmiş olur.
SMS Doğrulama Yap	Tanımlı SMS sağlayıcısı mevcut ise, ilk kez oturum açıldığında, bir defaya mahsus SMS doğrulama yapılır.
Yetkili Olduğu İstemci Grupları	Yetkili olacağı istemci grup/ları seçilir.
Filtreleme İçin Yetkili Olduğu İstemci Grupları	Filtreleme için yetkili olacağı istemci grup/ları seçilir.

Yetkiler ve Roller

Kullanıcı A	dı : admin			← Geri Dön 🖉 Yenile
Rol Düzenl				
				▼ Fitrele ✓ Temizle
#	Adı	↓ iii Kapsam	Jî İşlemler	
Yetki Düze	ne			
				▼ Filtrele
#	Adı		↓ h Kapsam	å‡ İşlemler
1	Bellek Durumu / Görüntüleme / Performans / Hepsi		0.0.0.0/0 :::/0	Kapsam
2	Cpu Durumu / Görüntüleme / Performans / Hepsi		0.0.0.0/0 ::/0	Kapsam
3	Disk Durumu / Görüntüleme / Performans / Hepsi		0.0.0.0/0 ::/0	Kapsam
4	Ethernet Atama / Sil / Ağ Yapılandırması / Hepsi		0.0.0.0/0 ::/0	Kapsam
5	Ekle / Ethernet Atama / Ağ Yapılandırması / Hepsi		0.0.0.0/0 ::/0	Kapsam
б	Ekle / Hepsi / Kullanıcı Yönetimi / Yönetim Paneli Kullanıcıları		0.0.0.0/0 ::/0	Kapsam
7	Ekle / IP Havuzları / Ağ Yapılandırması / Hepsi		0.0.0.0/0 ::/0	Kapsam
8	Ekle / Kullanıcı Grupları / Hepsi / Kullanıcı Yönetimi		0.0.0.0/0 ::/0	Kapsam
9	Ekle / Kullanıcı Rolleri / Hepsi / Kullanıcı Yönetimi		0.0.0.0/0 ::/0	Kapsam
10	Ekle / Ağ Yapılandırması / Sanal Ethernet - Loopback / Hepsi		0.0.0.0/0 ::/0	Kapsam

Kullanıcı Rolleri tanımlı olan rollerden biri seçilir.

Roller	×
Roller	
	Ø İptal
etki Düzenle	
Roller ve Yetkiler	×
Ka	psam
Yetki	Ağacı Hepsi Tanımlamalar Tünel Yapılandırması Sistem Ayarları Ağ Yapılandırması Aşt Yapılandırması Anlık Gözlem Performans Araçlar Kullanıcı Yönetimi Yervis Yönetimi Uygulanacak İşlem Listesi Bildirim Yönetimi VPN Yönetimi Yönlendirme Yönetimi Yönlendirme Yönetimi
	Ø İptal
ALAN AÇI	(LAMA

ALAN	AÇIKLAMA
Kapsam	Yetkinin hangi IP adresleri için geçerli olacağı seçilir.
Yetki Ağacı	Yetki ağacında bulunan tanımlardan istenilen yetkiler ve yetkilere ait türler seçilir.

Sertifika Yönetimi - Yeni Sertifika Üret

Kullanıcı yeni sertifika üretimi için Sertifika Yönetimi butonuna tıklamalıdır. Daha sonra Yeni Bir Sertifika Üret'e basılmalıdır.

Not: Üretilecek olan sertifika veya sertifikalar Yönetim Paneli Erişim Ayarlarında Sertifika Bazlı Kimlik Doğrulama **Açık** durumda ise işe yarayacaktır.

Yönetim Paneli Kullanıcıları	C Yenile + Ekle
XLS CSV PDF # Durum &= Aai \$1 Soyaai \$1 Kuilanici Aai \$1	şiermer
1 Aktif Antikor Admin admin	Image: Complex Sile Image: Complex Sile
	« (1) »
Başarılı	
Kullanıcı anahtar ve sertifikası başarıyla	a oluşturuldu.
ОК	
Mevcut sertifika kullanıcı için indirilebilir v yükledikten sonra giriş yapabilmektedir. k	reya feshedebilmektedir. İndirilen sertifikaları kullanıcı tarayıcısına Kullanıcı sertifikayı feshedip yeni bir sertifika da üretilebilmektedir.
Yönetim Paneli Kullanıcıları	C Yenile + Ekle
XLS CSV PDF I Aktir Antikor Admin admin	T Filtreie ↓ Filtreie ↓ Filtreie ↓ Filtreie ↓ Filtreie ↓ Temizie ↓ Setonika Yohedmi ↓ ↓ Mevcut Settifikayi İndir

	- Mevcut Sertifikayı Feshet	
<u>«</u>	< 1 > »	
ePati Siber Güvenlik Teknolojileri A.Ş.	📀 www.epati.com.tr	
Mersin Üniversitesi Çiftlikköy Kampüsü	₩bilgi@epati.com.tr	1
Teknopark İdari Binası Kat: 4 No: 411	L +90 324 361 02 33	
Posta Kodu: 33343 Yenişehir / MERSIN	🖶 +90 324 361 02 39	

epati Bellek Durumu



çilmiş olan tarihler arasında bellek (RAM) kullanım ist	atistikleri gösteren	sayfadır.		
:k Durumu				
	Başlangıç Tarihi Bitis Tarihi	 22.12.2019 23.12.2019 	00:00	
	Diciş Fallılı	Göster	0 23.39	
lam Bellek : 7852 MB				
Göster butonuna tıkladıktan sonra belirtilen tarihler	arasında kullanılmı	ş bellek miktar	ının grafiği	
gösterilmektedir.				
ek Durumu				
	Başlangıç Tarihi	22.12.2019	© 00:00	
	Bitiş Tarihi	23.12.2019	Ø 23:59	
	Bitiş Tarihi	🗯 23.12.2019	© 23:59	
lam Bellek : 7852 MB	Bitiş Tarihi	23.12.2019	0 23:59	
lam Bellek : 7852 MB 00MB	Bitiş Tarihi	🗎 23.12.2019 Göster	0 23:59	
lam Bellek : 7852 MB	Bitiş Tarihi	dister	0 23:59	
lam Bellek : 7852 MB 00MB 00MB	Bitiş Tarihi	Cidater	© 23:59	00
lam Bellek : 7852 MB 00MB 00MB • <u>•••••••••••••••••••••••••••••••••</u> •	Bitiş Tarihi	23.12.2019 Göster	0 23:59	00@
Iam Bellek : 7852 MB 000MB 000MB 000MB	Bitiş Tarihi	23.12.2019 Göster	0 23:59	
Iam Bellek : 7852 MB 00MB 00MB 00MB 00MB	Bitiş Tarihi		<u>o</u> 23:59	
Iam Bellek : 7852 MB 00MB 00MB 00MB 00MB 00MB	Bitiş Tarihi	23.12.2019 Gidster	© 23:59	

epati CPU Durumu



pu Durumu Başlangıç Tarihi Bitiş Tarihi Bitiş Tarihi CPU Model : intel(R) Xeon(R) CPU E5-2603 v3 @ 1.60GHz ::::::::::::::::::::::::::::::::::::	 22.1 23.1 23.1 Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998) Control (1998)<th>2.2019 2.2019 Göster deleri grafik</th><th>a halinde</th><th>:59</th>	2.2019 2.2019 Göster deleri grafik	a halinde	:59
Başlangıç Tarihi Bitiş Tarihi PU Model : Intel(R) Xeon(R) CPU ES-2603 v3 @ 1.606Hz pu Çekirdek Sayısı : 6 Göster butonuna tıkladıktan sonra seçili tarihler arasında kullanılmış CPU gelmektedir. Başlangıç Tarihi Bitiş Tarihi PU Model : Intel(R) Xeon(R) CPU ES-2603 v3 @ 1.606Hz pu Çekirdek Sayısı : 6	 € 22.1 PU yüzce £ 22.12 	2.2019 2.2019 Gösser deleri grafik	c halinde	:59
Bitiş Tarihi PU Model : Intel(R) Xeon(R) CPU E5-2603 v3 @ 1.606Hz pu Çekirdek Sayısı : 6 Göster butonuna tıkladıktan sonra seçili tarihler arasında kullanılmış CPU gelmektedir. u Durumu Başlangıç Tarihi Bitiş Tarihi U Model : Intel(R) Xeon(R) CPU E5-2603 v3 @ 1.606Hz pu Çekirdek Sayısı : 6 30%	PU yüzc 22.12	coner Goner	o 23	:59
U Model : intel(R) Xeon(R) CPU E5-2603 v3 @ 1.60GHz a Çekirdek Sayısı : 6 Göster butonuna tıkladıktan sonra seçili tarihler arasında kullanılmış CPU gelmektedir. Durumu Başlangıç Tarihi Bitiş Tarihi U Model : intel(R) Xeon(R) CPU E5-2603 v3 @ 1.60GHz a Çekirdek Sayısı : 6	PU yüze 22.12	deleri grafik	c halinde	1
Göster butonuna tıkladıktan sonra seçili tarihler arasında kullanılmış CPU gelmektedir. Durumu Başlangış Tarihi Bitiş Tarihi I Model : Intel(R) Xeon(R) CPU E5-2603 v3 @ 1.60GHz C Çekirdek Sayısı : 6 V 55 V	PU yüze	deleri grafik	k halinde	ł
Durumu Başlangıç Tarihi Bitiş Tarihi Model : Intel(R) Xeon(R) CPU E5-2603 v3 @ 1.60GHz Çekirdek Sayısı : 6	1 22.12			
Model : Intel(R) Xeon(R) CPU E5-2603 v3 @ 1.60GHz Çekirdek Sayısı : 6	EE 22.12	2010	0 00	00
J Model : Intel(R) Xeon(R) CPU E5-2603 v3 @ 1.60GHz I Çekirdek Sayısı : 6 20%	前 23.12	2.2019	© 23:	59
% 5%		Göster		
5%				
15%		/		
5% ************************************				
0% -	02:00 23.1;	2.2019 06:00 23.12	2.2019 10:00	23.12.2019 14:0

epati Disk Durumu



J

Counted Balange Tarrih 2122019 2000 2390 Sobster butonuna tikladıktan sonra belirtilen tarihler arasında kullanılmış disk miktarının grafiği gösterilmektedir.	çilmiş olan tarihler arasında disk kullan	m istatistikleri gösteren sayfadır.		
Biglangig Tarmi 2112.019 0 0.000 Bitly Tarmi 0 23.12.2019 0 23.9 plan Depo Alan: 109424 M8 Corumu 0 0.000 0	k Durumu			
Alam 1 103424 MB Coster butonuna tıkladıktan sonra belirtilen tarihler arasında kullanılmış disk miktarının grafiği gösterilmektedir. Korumu Başlangeş Tarihi Biş Tarihi<		Başlangıç Tarıhı Bitis Tarihi	22.12.2019	0 23:59
Alam Depo Alam: 103424 MB Göster butonuna tıkladıktan sonra belirtilen tarihler arasında kullanılmış disk miktarının grafiği gösterilmektedir.			Göster	
Göster butonuna tıkladıktan sonra belirtilen tarihler arasında kullanılmış disk miktarının grafiği gösterilmektedir. Durumu	iam Depo Alani : 103424 MB			
Göster butonuna tıkladıktan sonra belirtilen tarihler arasında kullanılmış disk miktarının grafiği gösterilmektedir. Arumu Başlangş Tarihi				
Durumu Başlangış Tarihi Imale 2.12.2019 Imale Imal	Göster butonuna tıkladıktan sonra be gösterilmektedir.	irtilen tarihler arasında kullanılm	nış disk miktarının	grafiği
Bitly Tarihi Diamondary Linking	Durumu	Raslange Tarihi	篇 22.12.2019	0.000
Im		Bitiş Tarihi	23.12.2019	© 23:59
Image: Sector				
Iam Depo Alan: 103424 MB 00MB 00MB 00MB 00MB 00MB 00MB 01MB 01MB			Chara	
00MB 00MB 00MB 00MB 00MB 00MB 00MB 00MB 00MB 22.12.2019 02:00 22.12.2019 06:00 22.12.2019 10:00 22.12.2019 18:00 22.12.2019 22:00 23.12.2019 06:00 23.12.2019 00:00 23.12.2019 10:00 23.			Göster	
00ME 00ME 22.12.2019 02.00 22.12.2019 10.00 22.12.2019 14.00 22.12.2019 18.00 22.12.2019 22.00 23.12.2019 06.00 23.12.2019 10.00 23.12.2019 14.00	lam Depo Alanı : 103424 MB		Göster	
00MB 	lam Depo Alani : 103424 MB 00MB		Göster	
00MB 	lam Depo Alani : 103424 MB 000MB •••••••••••••••••••••••••••••••		Göster	
OMMB	lam Depo Alanı : 103424 MB DOMB 		Göster	
OME 22.12.2019 02:00 22.12.2019 06:00 22.12.2019 16:00 22.12.2019 14:00 22.12.2019 18:00 22.12.2019 22:00 23.12.2019 02:00 23.12.2019 06:00 23.12.2019 10:00 23.12.2019 14:00	Jam Depo Alanı : 103424 MB 000MB 000MB		Göster	-0-0-0-0-0-0-0-0-0-0
OMB 22.12.2019 02:00 22.12.2019 06:00 22.12.2019 14:00 22.12.2019 18:00 22.12.2019 02:00 23.12.2019 06:00 23.12.2019 10:00 23.12.2019 10:00 23.12.2019 10:00	Dam Depo Alani : 103424 MB 0000MB 0000MB 0000MB	╸。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。	Göster	
	plam Depo Alani : 103424 MB	9	Göster	
	Ilam Depo Alanı : 103424 MB 00MB 00MB 00MB 00MB 00MB 00MB 22 12 2019 00200 22 12 2019 005 00 22 12 2019 10:00 22 12 2019 10:00	91400 22.12.2019 18.00 22.12.2019.22.00 23.12.201	Göster	23.12.2019 10.00 23.12.2019 14:00
	plam Depo Alanı : 103424 MB 000MB 500MB 00MB 22.12.2019 02.00 22.12.2019 02.00 22.12.2019 10.00 22.12.2019 10.00 22.12.2019 02.00 22.12.2019 10.00 22.12.2019 10.00 22.12.2019 10.00 22.12.2019 10.00	9 14 00 22 12 2019 18:00 22 12 2019 22:00 23 12 201 • . .	9 02:00 23:12:2019 06:00 2	23.12.2019 10:00 23.12.2019 14:00
Mersin Üniversitesi Çiftlikköy Kampüsü 🛛 bilgi@epati.com.tr	oplam Depo Alani : 103424 MB 2000MB 1500MB 500MB 2212.2019 02:00 22.12.2019 02:00 10.10 02:00	9 14.00 22.12.2019 18.00 22.12.2019 22.00 23.12.201 • Ş .	19 02.00 23.12.2019 06.00 2	23.12.2019 10.00 23.12.2019 14.00 v.epati.com.tr @epati.com.tr

Ethernet Bant Genişlikleri

Seçilmiş olan tarihler arasında, ethernet kartı seçimine göre, ethernet bant genişliğinin kullanım istatistikleri gösteren sayfadır.

Ethernet Bant Genişlikleri					
	Başlangıç Tarihi	=	22.12.2019	0	00:00
	Bitiş Tarihi	m	23.12.2019	0	23:59
	Ethernetler	Tür	nü		*
			Göster		

 Göster butonuna tıkladıktan sonra belirtilen tarihler arasında kullanılmış ethernet bant genişliği grafiği gösterilmektedir.

Ethernet Bant Genişlikleri						
	Başlangıç Tarihi	22.12.2019 Image: Object of the second sec				
	Bitiş Tarihi	23.12.2019				
	Ethernetler	Tümü 🔻				
		Göster				
3 Mbits						
2 Mb#s						
1 Mbits						
976Kbits						
0 ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;	22:00 00:00	02:00 04:00 06:00 08:00 10:00 12:00				
ePati Siber Güvenlik Teknolojileri A.Ş. 💮 www.epati.com.tr						

ePati Siber Güvenlik Teknolojileri A.Ş. Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN

-





epati Dinamik Raporlar



3 farklı rapor çeşidi dinamik olarak buradan görüntülenmekte ve listelenmektedir.

 Tünelleme Servisi Raporları Yasaklanan Kullanıcılar Raporları Yönetim Paneli Erişim Raporları 		
Dinamik Raporlar		
Tünelleme Servisi Raporları	Yasaklanan Kullanıcılar Raporları	Yönetim Paneli Erişim Raporları
Tünelleme Servis Raporları		
Tünelleme Servisi Raporları	Sa	
# Zaman Damgasi 会 令 分 ⇒		Mesaj ∉≎⊕ ∻
		Gald
Filtreleme	×	
Zaman Damgası	Temizle + Ekle	
Mesaj	Temizle + Ekle	
	Tanımları Uygula	

Yasaklanan Kullanıcılar

Yasakla	nan Kullanıcılar Raporları						🗲 Rap	orlara Di	ōn
🖹 CSV 🛛	PDF BXLS BHTML			Sayfa Başı 50	Kayıt Göster 🖉 Gö	ister/Gizle 👻 🗘 Sıralama 👻	▼ Filtreleme	-	0
#	Zaman Damgası ♦ \$ \$> \$>	İşlem ≪ ≑ Ø ⇒	Açıklama ≪ ≑ ≪ ⇒	Kullanıcı Adı ≪ ≎ ≪ ⇒		IP Adresi			
		a c	3					Git	ď

Filtreleme



Yönetim Paneli Erişim Raporları

SSV @ PDF @ XLS @ HTML					Sayfa Başı	50	Kayıt Göster	● Göster/Gizle ◄	¢ Sıralama ×	▼ Filtreleme	. 0
Zaman Damgası ≪ ≑ Ø ⇒	HTTP Kodu ≪ ≎ ≪ ⇒	IP Adresi	HTTP Metodu $\Leftarrow \Rightarrow \ll \Rightarrow$	URL ∉ ≑ ∞ ⊰	,		Tarayıcı Bilgisi €\$ Ø €		Yönlend €‡⊕ ÷	iren	
			x 1 3 9								Git 🗷
Filtreleme				3	¢						
Zaman Damgası			/ Tem	izle 🕇 Ekle							
HTTP Kodu			/ Tem	izle 🕇 Ekle							
IP Adresi			/ Tem	izle 🕇 Ekle							
HTTP Metodu			/ Tem	izle 🕇 Ekle							
URL			🖉 Tem	izle 🕇 Ekle							
Tarayıcı Bilgisi			/ Tem	izle 🕇 Ekle							
Yönlendiren			🝠 Tem	izle 🕇 Ekle							
			Tanıml	arı Uygula							
ePati Siber G	iüvenlik Tekno	olojileri A.Ş.					(www.ej	oati.cor	n.tr	

Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN



EPOTİ Sistem Yönetim Raporları

Sistem yönetim raporlarının gösterildiği bölümdür.

Siste	m Yönetim Raporla	arı					🕽 Son İşler	ni Geri Al 🛛 🛛 🕄	(enile
XL	5 CSV PDF		⊞ Göster/Gizle →	Sayfa Ba	aşı Kayıt Sayısı	\$	Tamam Tamam	🖌 Filtreyi Ten	nizle
#	Kimlik Bilgileri	👫 🛛 Kullanıcı Adı	🕴 İşlem Adı	Ψ J↑ s	Sayfa Adı	J1	İşlem Zamanı		1F
1	Antikor Admin	admin	Güncelleme	Y	/önetim Paneli Kullanıcıları		2020-04-17 17:19:55	i+03	
2	Antikor Admin	admin	Ekleme	K	Kullanıcı Grupları		2020-04-17 17:07:10	+03	
3	Antikor Admin	admin	Güncelleme	Т	Farih Saat Ayarları		2020-04-17 16:32:57	7.786873+03	
4	Antikor Admin	admin	Güncelleme	Т	Farih Saat Ayarları		2020-04-17 16:32:19	.335818+03	
			« < 1	> >>					Git

Not: **Son İşlemi Geri Al** butonuna tıklanıldığında sistem yönetim raporlarında son yapılan bir işlemi geri almaktadır.

Filtrele

Kimlik Bilgileri	İçeren	• Tersi
Kullanıcı Adı	İçeren	• Tersi
İşlem Adı	Görüntüleme	• Tersi
Sayfa Adı	Filtre Yok	• Tersi
İşlem Zamanı	m	Tersi

Filtrele

×

CONCICOURS Tümleşik Siber Güvenlik Sistemi

ALAN	AÇIKLAMA
Kimlik Bilgileri	Kimlik bilgisi girilir.
Kullanıcı Adı	Kullanıcı adı girilir.
İşlem Adı	Yapılan işlemin detayı girilir.
Sayfa Adı	Yapılan işlemin hangi menüde olduğu girilir.
İşlem Zamanı	Yapılan işlemin zamanı girilir.

ALAN	AÇIKLAMA
Tarih	Gösterilmek istenen sistem yönetim raporunun tarihi seçilir.
Tarihinde	Seçilen tarih günü için sistem yönetim raporunu filtreler.
Tarihinden Önce	Seçilen tarih gününe kadar olan sistem yönetim raporunu filtreler.
Tarihinden Sonra	Seçilen tarih gününden sonrası için sistem yönetim raporunu filtreler.

ePati Siber Güvenlik Teknolojileri A.Ş. Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN

EPOTİ Cluster Ayarları



Cluster, benzer bir amaç için belirli bir konfigürasyon yapılarak aynı görevi birlikte ya da yedekli çalışmasını sağlayan servistir.

Antikor, 2 sunucuya kadar cluster yapısını aktif/pasif olarak desteklemektedir. Antikor, yüksek erişilebilirlik cluster yapısına uygun çalışabilmektedir, yani clusterdaki bir sunucunun donanım ya da yazılım problemi oluştuğunda diğer bir sunucunun otomatik olarak devreye girmesidir. Bu durum network açısından sürekliliği sağlamaktadır.

Cluster Durumları



ALAN	AÇIKLAMA
Cluster Durumu	Master veya Slave sunucuda olduğunu belirtir.
Cluster Görevi	Cluster Ayarları sayfasında ayarlanan görevi.
Yedeğe Geç	Slave sunucunun devreye girmesini sağlar.

Cluster Durumu



ALAN	AÇIKLAMA
Cluster Durumu	Master veya Slave sunucuda olduğunu belirtir. Eğer Backup yazıyor ise Slave sunucu devrede demektir.
Cluster Görevi	Cluster Ayarları sayfasında ayarlanan görevi.
Yedeğe Geç	Slave sunucunun devreye girmesini sağlar.
Ceza Puanı	Slave sunucuya her geçiş yapıldığında Ceza Puanı artmaktadır. Bu ceza puanı Master sunucunun ne kadar sorun yaşadığını göstermektedir.

🛓 Dışarı Aktar 🔹 İçeri Aktar

		Cluster Ayarları	
Çalışma Modu	Bağımsız	O Master	◯ Slave
		🖺 Kaydet	

ALAN	AÇIKLAMA
Dışarı Aktar	Cluster konfigürasyonunun yedeğini almamızı sağlar.
İçeri Aktar	Cluster konfigürasyonunun alınmış yedeğini yüklememizi sağlar.
Bağımsız	Bağımsız durumunda çalışması.
Master	Öncelikli birincil sunucu durumunda çalışması.
Slave	Yedek ikincil sunucu durumunda çalışması.

Master

Cluster Ayarları										
	Çalışma Modu		🔿 Bağımsız	N	laster	🔵 sla	ave			
	Ön Tanıml	ı Anahtar								
	Ad	lres Ailesi	● IPv4 ○ II	■ IPv4 ○ IPv6						
	Slave	IP Adresi	IPv4							
	Kontrol	Periyodu	0 ms						Ŧ	
VHID Başlangıç Değeri										
Master SSH KEY										
Ssh-rsa AAAAB3NzaC1y YfwQlrot9AZrPbg38/IUOGI +fl8ZCPAoLrtaeltXyrG0yn0 bdp336x9WX9IYHypsg4tC3				AAAB3NzaC1yc2EAAAA irPbg38/IUOGDhLAhiUu taeltXyrG0yn0ghoAqNE X9IYHvpsg4tC3KgsIUo/I	ADAQABAAAB G9FyTxoTsK0 3YVxE0SvnLrL EpFAbpItAZo(AQDp6llEyPxYl2vcp! Ebmi9CVmtmmvkLL 4fM+53eMKxQlYHl2 DW7u9hff root@kur	534d/tZC1HWbMjb5lfjgPlK6 ygeO4XMUcCzJVw4YxSuezj xAdtqFFveNkldiUbmhtoFS4 ulum.antikor	RugdeR8Z2Nqj xZ6rvHI66SrpQ IA89qCRF+JhRł	lbOR2D/dqw2lRBxFMghx l6JPJqrTOF3wCkvdVChKa ı+79nB9Pxp2Apvsimlrfft	
Ax22017	Master Ethernet	Slave Etho	mot Ad	Cluster IPv4	Master	W4 Adrosi	Cluster IDv6	Master	Due Adrosi	
Adı	Adı	Slave Etile	met Au	Adresi	waster n	v4 Auresi	Adresi	Waster I	PV0 Auresi	
WAN1	bge1			10.2.1.42/24	IPv4			IPv6		
LAN1	bge0			192.168.2.1/24	IPv4			IPv6		
					🖺 Kaydet					

ALAN	AÇIKLAMA
Çalışm a Modu	Master
Ön Tanıml 1 Anahta r	Ön tanımlı anahtar girilir. Master ve Slave'de aynı olmak zorundadır.
Adres Ailesi	IPv4 veya IPv6 adres ailesi seçilir.
Slave TP	Slave sunucuva özel IP adresi girilir.

ALAN	AÇIKLAMA
Kontro l Periyo du	Sunucunun çalışma durumunu ne kadar sıklıkla kontrol edeceği seçilir. Master zorunlu olarak Slave'in ms değerinden küçük olmalıdır.
VHID Başlan gıç Değeri	
Master SSH Key	Master ve Slave arasındaki cluster senkronizasyonu için bu key kullanılmaktadır. Bu alandaki key Slave sunucudaki aynı alana kopyalanmalıdır.
Arayüz Adı	Master ve Slave arasındaki cluster senkronizasyonu için bu key kullanılmaktadır. Bu alandaki key Slave sunucudaki aynı alana kopyalanmalıdır.
Arayüz Adı	Fiziksel ethernet kartlarına atanmış arayüz adları bulunmaktadır. WAN1:WAN (Dış IP'miz) adresimiz. LAN1:LAN1 (İç IP'miz) adresimiz. LAN2:LAN2 (İkinci iç network) adresimiz. LAN3: Master ve Slave'in birebir kablo ile iletişim kuracağı porttur.
Master Ethern et Adı	Master Ethernet adlarının bulunduğu alandır.
Slave Ethern et Adı	Slave Ethernet adlarının bulunduğu alandır. Slave sunucuda olan fiziksel ethernet adları yazılır. Örneğin wan1 için Slave'de karşılık gelen fizksel ethernet adı igb0 ise, igb0 olarak girilir. Diğer fiziksel ethernet adları da aynı şekilde girilmelidir.
Cluste r IPv4 Adresi	Cluster IPv4 Adreslerinin bulunduğu alandır. Sunucular tarafından ortak kullanılacak IPv4 alanlarıdır.
Master IPv4 Adresi	Master IPv4 Adreslerinin bulunduğu alandır. Master sunucuya erişebilecek olan özel adresler girilir.
Cluste r IPv6 Adresi	Cluster IPv6 Adreslerinin bulunduğu alandır. Sunucular tarafından ortak kullanılacak IPv6 alanlarıdır.
Master IPv6 Adresi	Master IPv6 Adreslerinin bulunduğu alandır. Master sunucuya erişebilecek olan ikinci adresler girilir.

Cluster ayarları tamamladıktan sonra, öncelikle Slave sunucuda tanımlar uygulanır, daha sonra Master sunucuda cluster senkronizasyonu hariç tanımları uygula yapılır, en son olarak masterda yapılan ayar değişiklikleri, Cluster Senkronizasyonu butonuna tıklanarak bütün ayarlar Slave sunucuya aktarılır. Master sunucuda yapılacak olan değişikler her tanımlar uygulandığında Slave sunucuya aktarılacaktır. Master sunucuda donanım, network veya yazılım bir sorun oluştuğunda Slave sunucu devreye girecektir.

Slave

Cluster Ayarları					
Çalışma Modu	Bağımsız	O Master	Slave		
Ön Tanımlı Anahtar					
Adres Ailesi	● IPv4 ○ IPv6				
Master IP Adresi	IPv4				
Kontrol Periyodu	0 ms				Ŧ
VHID Başlangıç Değeri					
Master SSH KEY					
Proxy IP Adresi	IPv4				
Proxy Port					
Proxy Kullanıcı Adı					
Proxy Parola					
Arayüz Adı Cluster IPv4 Adresi	Slave IPv4 Adresi		Cluster IPv6 Adresi	Slave IPv6 Adresi	
WAN1 10.2.1.42/24	IPv4			IPv6	
LAN1 192.168.2.1/24	IPv4			IPv6	

🖺 Kaydet

ALAN	AÇIKLAMA
Çalış ma Modu	Master
Ön Tanım lı Anaht ar	Ön tanımlı anahtar girilir. Master ve Slave'de aynı olmak zorundadır.
Maste r IP Adres i	IP adresi girilir.
Kontr ol Periy odu	Sunucunun çalışma durumunu ne kadar sıklıkla kontrol edeceği seçilir. Minimum 50ms olmalıdır.
Maste r SSH Key	Master sunucudan alınan SSH Key girilir.
Proxy IP Adres i	Bu özellik, kullanılmayan bir WAN IP mevcut değil ise, slave sunucunun master sunucu devrede iken Antikor güncellemelerini alması için hazırlanmıştır. Proxy IP Adresi verilerek slave sunucu master sunucu üzerinden Proxy ile güncelleme alabilecektir.
Proxy Port	Proxy portu girilmelidir.
Proxy	

KUIIA ALAN NICI	Remulanda girilmelidir.
Adı	
Proxy Kulla nıcı Parol a	Proxy kullanıcı parolası girilmelidir.
Ether net Adı	Fiziksel ethernet kartlarına atanmış arayüz adları bulunmaktadır. WAN1: WAN (Dış IP'miz) adresimiz. LAN1: LAN1 (İç IP'miz) adresimiz. LAN2: LAN2 (İkinci iç network) adresimiz. LAN3: Master ve Slave'in birebir kablo ile iletişim kuracağı porttur.
Clust er IPv4 Adres i	Cluster IPv4 Adreslerinin bulunduğu alandır. Ortak kullanılan IP adreslerinin bulunduğu kısımdır.
Slave IPv4 Adres i	Slave IPv4 Adreslerinin bulunduğu alandır. Slave sunucuya erişebilmek için verilecek IP adreslerini barındırır. Mutlaka LAN ve iletişim kurduğu portlara IP verilmelidir. LAN'a verilen IP üzerinden erişim sağlanır. İletişim kurduğu bağlantı ile Cluster'ın çalışması sağlanır.
Clust er IPv6 Adres i	Cluster IPv6 Adreslerinin bulunduğu alandır. Ortak kullanılan IP adreslerinin bulunduğu kısımdır.
Slave IPv6 Adres i	Slave IPv6 Adreslerinin bulunduğu alandır. Slave sunucuya erişebilmek için verilecek IP adreslerini barındırır. Mutlaka, LAN ve iletişim kurduğu portlara IP verilmelidir. LAN'a verilen IP üzerinden SSH veya arayüz erişimleri sağlanır. İletişim kurduğu bağlantı ile Cluster'ın çalışması sağlanır.

Master ve Slave sunuculara içeriden erişmek için LAN IP'si (IPv4 veya IPv6) girilmelidir. Dışarıdan erişimek için Master sunucunun WAN arayüzüne ait olan IP bloğundan IP adresi verilmelidir.

Not: Master sunucuda ve Slave sunucuda aynı güncelleme versiyonları yüklenmelidir.

Cluster Gereksinimleri

- Slave Antikor, Master Antikorun minimum gereksinimlerini karşılamalıdır.
- Slave Antikorun ethernet kartı sayısı en az masterin ethernet kartı sayısı kadar olmalıdır.
- Master ve Slave arasında senkronizasyon amaçlı kullanılmak üzere doğrudan bir kablo bağlantısı olması tavsiye edilir.
- Senkronizasyon için kullanılan ethernet üzerinde ortak IP adresi dışında master ve slave Antikorlara doğrudan erişmek için IP adresleri atanmalıdır.



EPOTİ Dil Ayarları



Antikor'da dil ayarlarının yapıldığı alandır.

Dil Ayarları

İstemci Arayüz Dil Ayarları		
Yönetim Paneli Girişi	tr	¥
	器 Kaydet	

Alan	Açıklama
Yönetim Paneli Girişi	Yönetim Paneli Girişi aşamasında ekranın dil ayarlarının belirlendiği bölümdür.

ePati Siber Güvenlik Teknolojileri A.Ş. Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN



EPOTİ DNS Ayarları

Sistemin kullandığı DNS bilgileridir. Yerel ağdaki bilgisayarlara da DHCP servisi üzerinden DNS bilgileri dağıtılır.

DNS Ayarları				C Yenile + Ekle
XLS CSV PDF	⊞ Göster/Gizle →	Sayfa Başı Kayıt Sayısı	Tamam T Filtr	ele 🖌 Filtreyi Temizle
Sıra	🎼 Dns Adresi	🕼 Açıklama	Jî İşler	nler
		« < > »		

CONCICOURS Tümlesik Siber Güvenlik Sistemi

Ekle butonundan DNS adresleri IPv4 veya IPv6 olarak eklenebilir.

DNS Ayarı - Yeni Kayıt			×		
Adres Ailesi Dns Adresi Açıklama	IPv4 IPv6 IPv4				
DNS Ayarı - Yeni Kayıt		Ø İptal	Kaydet		
Adres Ailesi Dns Adresi	 IPv4 IPv6 IPv4 8.8.8.8 				
Açıklama	DNS	Ø İptal	Kaydet		
DNS Ayarları XLS CSV PDF Sıra III Dıns Adresi	lit Aş	jklama 👔 İşleri	≣ Góner/Gizle → Sayfa Başı Kayı nler	© Yen Sayısı Təməm ▼Fikrele ✔Fik	le 🕇 Ekle reyi Temizle
0 8.8.8	DN	NS (20)	üzenle 📋 Sil 🛧 🗸		

Eklenen DNS kayıtları Excel, CSV veya PDF formatında indirilebilir.

ALAN	AÇIKLAMA
Adres Ailesi	IPv4 veya IPv6 adres türü seçilir.
DNS Adresi	DNS adresi yazılır.
Açıklama	Açıklama yazılır.

ePati Siber Güvenlik Teknolojileri A.Ş. Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN



EPOTİ Log Ayarları



Antikor Tünelleme ürünü üzerinden bulunan tüm loglar için cihazda tutulup tutulmayacağı ile ilgili ayarlamalar burada yapılmaktadır.

og Ayarları	
Log Ayarları	
Web Oturum Logları	📀 Cihazda Tut 💿 Cihazda Tutma
Web Arayüzü Logları	🧭 Cihazda Tut 🔷 Cihazda Tutma
Cluster Servisi Logları	🥑 Cihazda Tut 📄 Cihazda Tutma
Ethernet Durum Logları	🥑 Cihazda Tut 📄 Cihazda Tutma
Tünelleme Servisi Logları	🥑 Cihazda Tut 📄 Cihazda Tutma
Arayüze Erişimi Yasaklanan IPler	🥑 Cihazda Tut 📄 Cihazda Tutma
Yönetim Paneli Erişim Logları	🗌 Cihazda Tut 📀 Cihazda Tutma
Từmũnũ Seç	Cihazda Tut Cihazda Tutma
	🖹 Kajatet

Not: Varsayılan olarak Cihazda Tut seçili gelmektedir.

ePati Siber Güvenlik Teknolojileri A.Ş. Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN



epati Oturum Ayarları



Antikor L2 Tünel kullanıcılarının parola ve oturum politikalarının tanımlandığı sayfadır.

Asgari Büyük Karakter Sayısı	0	~
Asgari Küçük Karakter Sayısı	0	~
Asgari Rakam Sayısı	0	~
Asgari Noktalama İşareti Sayısı	0	~
Asgari Karakter Sayısı	4	÷
Parola Ömrü	Yok	~
urum Politikaları		
Azami Oturum Süresi	10 Dakika	~
Azami Başarısız Giriş Sayısı	10 Defa	~
Azami Giriş Engelleme Süresi	1 Saat	~

Parola Politikaları

Oturum Ayarları

ALAN	AÇIKLAMA
Büyük Karakter Sayısı	AntiKor2 kullanıcısına ait belirlenecek parolada kullanılacak olan, minimum büyük karakter sayısı girilir.
Küçük Karakter Sayısı	AntiKor2 kullanıcısına ait belirlenecek parolada kullanılacak olan, minimum küçük karakter sayısı girilir.
Rakam Sayısı	AntiKor2 kullanıcısına ait belirlenecek parolada kullanılacak olan, minimum rakam sayısı girilir.
Noktalama İşareti Sayısı	AntiKor2 kullanıcısına ait belirlenecek parolada kullanılacak olan, minimum noktalama işareti sayısı girilir.
Asgari Karakter Sayısı	AntiKor2 kullanıcısına ait belirlenecek parolada kullanılacak olan, minimum karakter sayısı girilir.
Parola Ömrü	Kullanıcıya ait belirlenecek parola için, geçerlilik süresi girilir. Süre sonunda parola güncellenir.

Oturum Politikaları

ALAN	AÇIKLAMA
Azami Oturum Süresi	AntiKor oturumunudan çıkış gerçekleştirilmeden en fazla oturum süresi tanımlanır.
Azami Başarısız Giriş Sayısı	AntiKor giriş ekranında en fazla kaç kez kullanıcı adı veya şifrenin üst üste yanlış girilebileceği tanımlanır.
Azami Giriş Englelleme Süresi	Azami başarısız giriş sayısına ulaşıldığında tekrar giriş yapabilmek için geçecek süre tanımlanır.

ePati Siber Güvenlik Teknolojileri A.Ş. Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN



EPOTİ SNMP Ayarları



SNMP (Simple Network Management Protocol) Ağ cihazlarının yönetimini ve izlenmesini kolaylaştıran bir uygulama katmanı protokolüdür.

SNMP'nin üç temel bileşeni vardır. Bunlar:

- NMS (Network Management System): Yönetici tarafında çalışan SNMP yazılımıdır.
- Agent: Yönetilen cihaz tarafında çalışan yazılımdır.
- MIB (Management Information Base): Her cihazın yerelinde bulunan, cihazdaki agent tarafından erişim sağlanan ve cihazla ilgili bilgileri bulunduran bir veri tabanıdır.

Antikor üzerinde SNMPv2 veya SNMPv3 tanımları yapılarak ağ izleme programlarından Antikora ait ethernet aryüzlerine ait istatistiklere erişilebilmektedir.

SNMP-V2

SNMP Ayarları				
Sistem Adı				
Sistem Açıklaması				
İletişim				
Konum				
SNMP Versiyon	SNMP-V2	~		
Hizmet IP Adresi	Arama Yapabilirsiniz	~		
Adres Tablosu 🔷 Açık 🥑 Kapalı	Arayüzler	🗌 Açık 🥑 Kapalı	IP Bilgileri	🗌 Açık 🥪 Kapalı
ICMP Bilgileri 💦 Açık 🤜 Kapalı	TCP Bilgileri	🔵 Açık 🤜 Kapalı	UDP Bilgileri	🔵 Açık 🥑 Kapalı
SCTP Bilgileri 🔷 Açık 🕑 Kapalı	Yönlendirme Tablosu	🔵 Açık 🥑 Kapalı		

SNMP-V3

SNMP Ayarları				
Sistem Adı				
Sistem Açıklaması				
İletişim				
Konum				
SNMP Versiyon	SNMP-V3	~	,	
Hizmet IP Adresi	Arama Yapabilirsiniz	~		
Adres Tablosu 💦 Açık 🤜 Kapal	Arayüzle	r 📄 Açık 🥪 Kapalı	IP Bilgileri	🗌 Açık 🕑 Kapalı
ICMP Bilgileri 🛛 Açık 📀 Kapal	TCP Bilgile	i 🔷 Açık 🕑 Kapalı	UDP Bilgileri	🔷 Açık 🥪 Kapalı
SCTP Bilgileri 🔷 Açık 🥑 Kapal	Yönlendirme Tablos	u 🔷 Açık 🕑 Kapalı		
	_			

ALAN	AÇIKLAMA				
Sistem Adı	Sisteme verilecek ad belirlenir.				
Sistem Açıklaması	Sistem için gerekli açıklama girilir.				
İletişim	İletişim bilgileri girilir.				
Konum	Konum bilgisi girilir.				
SNMP Versiyon	SNMP versiyonu v2 veya v3 seçilir.				
Hizmet IP Adresi	SNMP sunucusuna hizmet verecek arayüz seçimi yapılır.				

SNMPv2 Ayarları Yeni Kayıt

SNMP Ayarları - Yeni H	Cayıt	×
Durum	Aktif	
Modu	Salt Okunur 🗸	
Erişecek Ağ	0.0.0/0 ×	
Grup Adı		



ALAN	AÇIKLAMA			
Durum	Aktif ya da pasif olma durumu seçilir.			
Modu	Salt okunur ya da (okuma - yazma) modu seçilir.			
Erişecek Ağ	Erişecek ağ kapsamı girilmelidir.			
Grup Adı	SNMPv2 grup adı yazılır.			

SNMPv3 Ayarları Yeni Kayıt

Durum	Aktif	
Modu	Salt Okunur	v
Erişecek Ağ	0.0.0.0/0 ×	
Kullanıcı Adı		
Parola		
Doğrulama Türü	MD5	Ŧ
Gizlilik Protokolü	Yok	Ŧ
Anahtar		

Ø İptal 🛛 🖺 Kayde

ALAN	AÇIKLAMA				
Durum	Aktif ya da pasif olma durumu seçilir.				
Modu	Salt okunur ya da (okuma -yazma) modu seçilir.				
Erişecek Ağ	Erişecek ağ kapsamı girilmelidir.				
Kullanıcı Adı	SNMPv3 kullanıcı adı yazılır.				
Parola	SNMPv3 kullanıcısı için parola belirlenir.				
Doğrulama Türü	Şifreleme algoritmalarından birisi seçilmelidir.				
Gizlilik Protokolü	İsteğe bağlı olarak simetrik şifreleme algoritması seçilir.				
Anahtar	Simetrik algoritma seçilmesi halinde anahtar belirlenebilir. Bu anahtar, karşı anahtar bilgisi ile aynı olmalıdır.				

ePati Siber Güvenlik Teknolojileri A.Ş. Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN

EPOTİ SSL Sertifikası Yönetimi

Antikorda SSL işlemlerinin yürütüldüğü bölümdür.

SSL Ser	tifikası Yönetin	ni				2 Yenile + Ekle 2 Yükle
XLS #	CSV PDF	斗 Alan Adı (CN)	11 Bitiş Tarihi	1 Açıklama	Sayfa Başı Kayıt Sayısı	Tamam Tiltrele Filtreyi Temizle
						Git

SSL Sertifikası Yönetimi Yeni Kayıt

SSL	Sertifikası Yönetin	ni - Yeni Kayıt	×
	Adı		
	Ülke Kodu (C)		
	İl Adı (ST)		
	İlçe Adı (L)		
	Kurum Adı (O)		
	Departman Adı (OU)		
	Eposta (E)		
	Alan Adı (CN)		
	Bitiş Tarihi		
	Açıklama		
	IPsec VPN için		



Øİptal 🕒 Kaydet

ALAN	AÇIKLAMA					
Adı	Sertifikaya ait ad girilir.					
Ülke Adı (C)	Sertifikanın hangi ülkede olduğu girilir.					
İl Adı (ST)	Sertifikanın hangi ilde olduğu girilir.					
İlçe Adı (L)	Sertifikanın hangi ilçede olduğu girilir.					
Kurum Adı (O)	Sertifikanın hangi kuruma ait olduğu girilir.					
Departman Adı(OU)	Sertifikanın hangi departman için kullanılacağı girilir.					
E-posta (E)	Sertifikanın hangi e-posta adresine kayıtlı olduğu girilir.					
Alan Adı (CN)	Sertifikanın hangi alan ad/larında geçerli olduğu girilir.					
Bitiş Tarihi	Sertifikanın bitiş tarihi seçilir.					
Açıklama	Açıklama girilir.					
IPsec VPN için	IPsec VPN kullanılacaksa kutucuk işaretlenir.					

SSL Sertifikası Yönetimi Yükle

Dosya Yükleme Formu

 \times



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

epati SysLog Ayarları



Sunucu sistem loglarının kayıt edileceği sunucunun/sunucuların eklendiği bölümdür.

Syslog Ayarları				🛛 🎜 Yenile 🚺 🕇 Ek	de
XLS CSV PDF		⊞ Göster/Gizle →	Sayfa Başı Kayıt Sayısı	Tamam 🛛 🕇 Filtrele 🛃 Filtreyi Temizl	e
# Durum ↓ii Log Çe	şitleri 🕴 Gönderim Formatı	👫 🛛 Sunucu Adresi	👫 Protokol	↓† Port ↓† İşlemler	
		C C D		G	it
SysLog Ayarları - Yeni	Kayıt	×			
Durum	Aktir				
Log Çeşidi	Web Erişim Logları	~			
Adres Ailesi	● IPv4 ○ IPv6				
Server Adresi	IPv4				
Protokol	тср	~			
Port		•			

🛛 İptal 🛛 🖺 Kaydet

ALAN	AÇIKLAMA				
Log Çeşidi	Log çeşidi seçilir ve seçilen log çeşidi Syslog sunucuya gönderilir.				
Adres Ailesi	IPv4 ya da IPv6 adres ailesi seçilir.				
Server Adresi	Logların tutulacağı sunucuya ait IP adresi yazılır.				
Protokol	Logların gönderilmesinde kullanılacak protokolün seçildiği alandır.				
Port	Logun hangi port numarasını kullanacağı yazılır.				

ePati Siber Güvenlik Teknolojileri A.Ş. Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN



epati Ağ Tanımları



Ağ tanımlarının bulunduğu bölümdür.

Bu bölüm içinde Ağ Grupları oluşturup, bu gruplara IP adresi veya network tanımlanabilir. Bu tanımlar erişim izinlerinde ve özel kullanıcılar bölümünde kullanılabilir. Ağ grubu eklemek için Ekle butonuna basıldıktan sonra gelecek olan Ağ Tanımları – Yeni Kayıt penceresinden oluşturmak istenilen IP Adres(Ier)i/Network(Ier) tanımlanabilir.

Ağ Tan	ımları											
A	ğ Grupları	Sil Ekle Düzenle	Ağ Grup	Üyeleri						Gün	celle 🛛 🎗 Yenile	+ Ekle 🕹 Yükle
	→ ■ # (0) ↓ ■ Botnet IP List (0) ↓ ■ Geo IP (0)		XLS #	CSV PDF Grup Adı	↓≟ Açıkla	ma		Sayfa Başı Kayıt Sayı si	isi İî Kaynak	Tamam	▼ Filtrele J† İşlemi	🖌 Filtreyi Temizle ler
							« () »					Git

Ağ Grupları

Ağ Grupları	Sil Ekle Düzenle
# # (0)	
🖿 Alpemix Uygulaması (0)	
📟 🖿 Ammyy Admin Uzak Masasütü Uy	/gulaması (0)
🖿 Anydesk Uzak Masaüstü Uygulam	1asi (0)
🖿 AOL Uygulaması (0)	
🖿 BotNet - Feodo (0)	
🖿 BotNet - Palevo (0)	
🖿 BotNet - Palevo (0)	
🖿 Browsec Uygulaması (0)	
🖳 🖿 China - Kore IP Adresleri (0)	
🖿 deneme (0)	
📟 🖿 Spamhaus - Drop List (0)	
🖿 Spamhaus - Extended Drop List (0))
🖿 Teamviewer Uyulaması (0)	
🖿 Telegram Uygulaması (0)	
🖿 Tor Tarayıcı Uygulaması (0)	
🖿 Türkiye IPleri (0)	
🖿 USOM (0)	
🖿 WannaCry CnC Sunucuları (0)	
🖿 🖿 Zenmate Uygulaması (0)	

Ağ Grupları Yeni Kayıt

Ağ Tanım	ları -	Yeni	Kayıt
----------	--------	------	-------

Kaynak	Elle Veri Girişi	Ŧ
Adı		

ALAN	AÇIKLAMA
Kaynak	Kaynak seçimi yapılır. (Elle veri Girişi, İnternetten Otomatik Al, Referans Grup)
Adı	Ağ Grubu adı verilir.

Ağ Grupları Kayıt Düzeltme

Düzenle tuşu ile kayıt ile ilgili bilgiler düzenlenebilmektedir.

Ağ Tanımları - Kayıt Düzeltme			×
	Kaynak	İnternetten Otomatik Al	
	Adı	Spamhaus - Drop List	
	Url	http://www.spamhaus.org/drop/drop.txt	
		Ø İptal	let

ALAN	AÇIKLAMA
Kaynak	Kaynak seçimi değiştirilebilir.
Adı	Ağ Grubu adı değiştirilebilir.
URL	URL düzenlenebilir.

Ağ Grup Üyeleri

Tanımlanan ağ grubuna, ağ grup üyeleri eklemek için Ekle butonuna basıldıktan sonra gelecek olan Ağ tanımları-Yeni kayıt sayfasından yapılır.

×

🖹 Kaydet

Ağ Gr	up Üyeleri				Güncelle 🕻 🔁 Yenile 🕇 🕇 El	kle 🛃 Yükle
XLS	CSV PDF		⊞ Göster/Gizle → Sayfa Başı k	(ayıt Sayısı	Tamam Tiltrele	ltreyi Temizle
#	IP Adresi	🎼 🛛 Grup Adı	🅼 Açıklama	Kimlik Bilgileri	11 İşlemler	
1	216.58.206.161	Test	blogspot.com1		🕼 Düzenle 🕅 Sil	
2	216.58.206.169	Test	blogspot.com2		🕼 Düzenle 🕅 🕅 Sil	
3	216.58.212.1	Test	blogspot.com3		🕼 Düzenle 🕅 Sil	
			« < 1 >	>>		

🖺 Kaydet

Ağ Grup Üyeleri Yeni Kayıt

Ağ Tanımları - Yeni Kayıt	
Adres Ailesi	● IPv4 ○ IPv6
IP Adresi	IPv4
Açıklama	

ALAN	AÇIKLAMA
Adres Ailesi	Adres ailesi seçilir. (IPv4 veya IPv6)
IP Adresi	Eklenecek olan IP adres(ler)i eklenir.
Açıklama	Açıklama yazılır.

Ağ Grup Üyeleri Kayıt Düzeltme

Düzenle tuşu ile kayıt ile ilgili bilgiler düzenlenebilmektedir.

Ağ Tanımları - Kayıt Düzeltme		
Adres Ailesi	● IPv4 ○ IPv6	
IP Adresi	IPv4 216.58.212.1	
Açıklama	blogspot.com3	
	Ø İptal 🖺 Kaydet	
ALAN	AÇIKLAMA	
-----------------	--	
Adres Ailesi	Adres ailesi seçilir. (IPv4 veya IPv6)	
IP Adresi	Eklenecek olan IP adres(ler)i düzenlenir.	
Açıklama	Açıklama düzenlenebilir.	

ePati Siber Güvenlik Teknolojileri A.Ş. Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN ٢

EPOTİ Kimlik Tanımlamaları



İstemciler için kimlik tanımlarının yapıldığı bölümdür.

Kimli	k Tanımlamalar	1							2 Yenile + Ekle
XLS	CSV PDF					⊞ Göster/Gizle → Sa	yfa Başı Kayıt Sayısı	Tamam Tiltre	le 🖌 Filtreyi Temizle
#	Uyruk	🎼 Kimlik No	lt Adı	lî Soyadı	👫 Oluşturulma Tarihi	11 ePosta	1 işlemler		
1	Türkiye	111*****11	Antikor	Admin	2018-12-13 20:07:24.568756	bilgi@epati.com.tr	🕼 Düzenle 👘 Sil	🔺 İstemciler	
					« < 1 > »				

Kimlik Tanımlamaları Yeni Kayıt

Yeni kimlik eklemek için Ekle tuşuna basıldıktan sonra açılan Kimlik Tanımlamaları – Yeni Kayıt penceresinde bilgiler doldurularak manuel kayıt yapılabilir.

Cinsiyet Kadın ● Erkek Uyruk Türkiye Kimlik No Adı Soyadı Telefon C +90 ▼ 501 234 56 78 ePosta Doğum Tarihi	Kimlik Tanımlamaları - Yeni Kayıt					
Kimlik No Adı Soyadı Telefon €Posta Doğum Tarihi	Cinsiyet Uyruk	◯ Kadın ● Erkek				
AdıSoyadıTelefon€PostaDoğum Tarihi	Kimlik No					
Soyadı Telefon €Posta Doğum Tarihi	Adı					
Telefon ePosta Doğum Tarihi	Soyadı					
ePosta Doğum Tarihi	Telefon	C +90 ▼ 501 234 56 78				
Doğum Tarihi	ePosta					
	Doğum Tarihi					
Ø İptal		Ø İptal	/det			

ALAN	AÇIKLAMA
Cinsiyet	Cinsiyet (Kadın/Erkek) seçilir.
Uyruk	Eklenecek olan kimlik kaydının uyruğu (Türkiye veya Yabancı Uyruklu) seçilir.
Kimlik No	Kimlik numarası yazılır.
Adı	Adı yazılır
Soyadı	Soyadı yazılır
Telefon	Telefon numarası yazılır.
E-posta	E-posta adresi yazılır.
Doğum Tarihi	Doğum tarihi seçilir.

Kimlik Tanımlamaları Kayıt Düzeltme

Düzenle tuşu ile kayıt ile ilgili bilgiler düzenlenebilmektedir.

Kimlik Tanımlamaları - Kayıt Düzeltme			
Cinsiyet	🔿 Kadın 🔘 Erkek		
Uyruk	Türkiye 🔻		
Kimlik No			
Adı	Antikor		
Soyadı	Admin		
Telefon	C +90 ▼ 324 361 02 33		
ePosta	bilgi@epati.com.tr		
Doğum Tarihi	08.06.2008		

ALAN	AÇIKLAMA
Cinsiyet	Cinsiyet değiştirilebilir.
Uyruk	Eklenecek olan kimlik kaydının uyruğu değiştirilebilir.
Kimlik No	Kimlik numarası değiştirilebilir.
Adı	Adı değiştirilebilir.
Soyadı	Soyadı değiştirilebilir.
Telefon	Telefon numarası değiştirilebilir.
E-posta	E-posta adresi değiştirilebilir.
Doğum Tarihi	Doğum tarihi değiştirilebilir.

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



epati Port Tanımları



Port Tanımları

Port Tanımları			
Port Grupları Ekle Si Güncelle	Port Grup Üyeleri		3 Yenile + Ekle
→ 😓 # 🖿 Personeller Portian - TCP	XLS CSV PDF	🖩 Göster/Gizle 👻 Sayfa Başı Kayıt Sayısı	Tamam Tiltrele Filtreyi Temizle
🏜 Yöneticiler Portları - ICMP 🖿 Kamera Portları - IP	# Port Başlangıç	Port Bitiş Açıklama	lî İşlemler
	2 200	300 Hepsi Üye Portu - 2	C Düzenle 🗍 Sil

🖹 Kaydet

Port Grupları

Port Grupları	Ekle Sil Güncelle
 # Personeller Portları - TCP Yöneticiler Portları - ICMP Kamera Portları - IP 	

Port Grupları Yeni Kayıt

Port Tanımları - Yeni I	(ayıt	×
Protokolu	IP	v
Referans Grup	Pasif	
Grup Adı		

ALAN	AÇIKLAMA
Protokolu	İstenilen protokol türü seçilir. (TCP, UDP, vb.)
Grup Adı	Grup adı verilir.

Port Grupları Kayıt Düzeltme

Protokolu Referans Grup Grup Adı	IP Bu tanımın kullanıldığı kurallarda problemi ön protokol değişimine izin verilmemektedir. Pasif Kamera Portları	▼ lemek amacıyla,	
Port Grup Üyeleri	٩) İptal 🖪 Kaydet	
Port Grup Uyeleri XLS CSV PDF # Port Başlangıç		Tamam ↓† Açıklama	Yenile + Ekle ▼ Filtrele Filtreyi Temizle ↓↑ İşlemler Git

Port Grup Üyeleri Yeni Kayıt

Port Tanımları - Yeni K	ayıt			×
Port Başlangıç			* *	
Port Bitiş			•	
Açıklama				
		Ø İptal	🖺 Kayde	t

ALAN	AÇIKLAMA
Port Başlangıç	Tanımlanmış olan Port Grubunun başlangış port numarası yazılır. (1- 65535 arasında olmalıdır)
Port Bitiş	Tanımlanmış olan Port Grubunun bitiş port numarası yazılır. (1- 65535 arasında olmalıdır)
Açıklama	Açıklama yazılır.

Port Tanımları - Kayıt Düzeltme

Port Başlangıç	12000	•	
Port Bitiş	13000	*	
Açıklama	test		
		🖉 İptal 🛛 🖺 Kaydet	
ePati Siber Güv Mersin Üniversite	r <mark>enlik Teknolojileri A.Ş.</mark> si Çiftlikköy Kampüsü		

epati Tünel Ayarları



Tünelleme: Layer 2 seviyesinde iletişim sağlayarak, kapalı bir ağ ve ağlar arası şifreli iletişim sağlamaktadır. Tüneller arası MAC adresi bilgileri taşınacak, çoklu VLAN veya access VLAN taşınabilecektir. Uç ağların tünel sayesinde internet trafiği merkeze gelecek ve merkezde bulunan güvenlik duvarındaki politikalara tabi olacaktır, bu sayede merkezi yönetim ve homojen güvenlik de sağlanmış olacaktır.

Tünel Ayarları

İlk olarak Tünel Yapılandırması menüsü altında bulunan Tünel Ayarlarına tıklanır.



Açılan sayfada Sanal Switch yaratılır. Switch Ekle butonuna tıklanır.

Tünel Ayarları		Switch Ekle
Switch - Yeni Kayıt		×
Adı		
Açıklama		
Spanning Tree Servisi	Kapalı	*
LLDP Servisi	Pasif LLDP Sistemi Adı bilgisi, SNMP Ayarlarından alınmaktadır.	
		🖉 İptal 🛛 🖺 Kaydet

Adı		
Açıklama		
Spanning Tree Servisi	Kapalı	`
LLDP Servisi	Kapalı Rapid STP	
	STP Lectro Sistem Auroligisi, Sixivi Ayanan ann naktaur.	_

) İptal	🖹 Kaydet
---------	----------

Alan	Açıklama
Adı	Switch Adı yazılır.
Açıklama	Açıklama yazılır.
Spanning Tree Servisi	Eklenecek olan sanal switch için spanning-tree servisi kullanılacaksa Rapid-STP veya STP servisi seçilir.
LLDP Servisi	LLDP servisi kullanılacaksa aktifleştirilir. LLDP sistem adı bilgisi, SNMP ayarlarından alınmaktadır.

Ardından Tünel Ekle butonuna tıklanır.

İnternet Ağı

Genel Ayarlar		
	Durum	Attif

Tünel Ayarları	
Port Türü	● Tek Port ○ LACP
Grup Adı	*
Tünel Adı	
Tünelleme Modu	Layer 2 Tünel 🗸
Layer 2 Tünel	
DF Biti'ni Tünelle	Aktif

VLAN Ayarları		
VLAN Modu	Etiketsiz	~
VLAN ID		
VLANIar (Trunk)		
Native VLAN		Temizle



Alan	Açıklama
Durum	Aktif/Pasif durumunu belirtme.
Port Türü	Tek Port ya da LACP seçilir.
LACP Adı	Port Türü LACP seçilir ise, LACP Adı yazılır.
Grup Adı	Port Türü Tek Port seçilir ise, Grup Adı yazılır.
Tünel Adı	Tünel Adı yazılır.
Tünelle me Modu	Layer 2 Tunnel, Layer 2 Tunnel over IPsec modlarının yanı sıra NAT arkasında çalışacak sunucu ve istemciler için Layer 2 Tünel over IPsec NAT-T Sunucu ve Layer 2 Tünel over IPsec NAT-T İstemci seçilebilir.
IPsec VPN Profili	Tünelleme modunda <i>over IPsec</i> seçilmişse burada VPN Yönetimi/IPSec VPN Profilleri Menüsünde oluşturulmuş olan profiller seçilmektedir.
DF Biti'ni Tünelle	Layer 2 Tunnel, Layer 2 Tunnel over IPsec modlarında kullanıcı DF biti'ni tünelleyecekse aktifleştirilir.
VLAN Modu	Etiketsiz: Tek VLAN taşınacaksa bu seçenek seçilir ve VLAN ID girilir. Etiketli ve Etiketsiz: Birden fazla VLAN ve Native VLAN taşınacaksa bu seçenek seçilir. Native VLAN belirtme zorunluluğu bulunmamaktadır.
VLAN ID	Taşınması istenen tek VLAN'ın ID bilgisi girilir. VLAN Modu Etiketsiz olarak seçildiğinde aktifleşir.
VLANlar (Trunk)	Taşınacak olan VLAN'ların ID bilgisi girilir.(Etiketli ve Etiketsiz seçili olmalıdır.)
Native VLAN	Taşınacak olan Native VLAN'ın ID bilgisi girilir.

Tünelleme Modu



Layer 2 Tünel

Tünelleme Modu Layer 2 Tünel seçilmesi durumunda Layer 2 Tünel bölümü;

Tünelleme Modu	Layer 2 Tünel	~
Layer 2 Tünel		
DF Biti'ni Tünelle	IPv4 IPv6 Karşı Tünel IP Adresi	
	IPv4 WAN Arayüzü	
	WAN1 - 10.2.1.178	~
	Ekle	

Alan	Açıklama
Karşı Tünel IP Adresi	Layer 2 Tünel yapılacak tarafın IP adresi girilir.
WAN Arayüzü	Mevcuttaki tünelin WAM IP adresi varsayılan olarak gelir.

Layer 2 Tünel over IPsec

Tünelleme Modu Layer 2 Tünel over IPsec seçilmesi durumunda;

Tünelleme Modu	Layer 2 Tünel over IPsec	~
IPsec VPN Profili	AES128GCM16 - PRFSHA1 - MODP2048	~
Layer 2 Tünel		
	● IPv4 ○ IPv6	
	Karşı Tünel IP Adresi	
	IPv4	
	WAN Arayüzü	
	WAN1 - 10.2.1.178	~
	Ekie	
IPsec VPN Profili		
IPsec VPN Profili	AES128GCM16 - PRFSHA1 - MODP2048	~
	AES128GCM16 - PRFSHA1 - MODP2048 aes256gcm	

IPsec VPN Profili Tünelleme modunda *Layer 2 Tünel over IPsec, Layer 2 Tünel over IPsec NAT-T Sunucu ve Layer 2 Tünel over IPsec NAT-T İstemci* seçilmişse burada VPN Yönetimi/IPSec VPN Profilleri Menüsünde oluşturulmuş olan profiller seçilmektedir.

Tünelleme Modu	Layer 2 Tünel over IPsec	~
IPsec VPN Profili	AES128GCM16 - PRFSHA1 - MODP2048	~
Layer 2 Tünel		
	● IPv4 ○ IPv6	
	Karşı Tünel IP Adresi	
	IPv4	
	WAN Arayüzü	
	WAN1 - 10.2.1.178	~
	Ekle	

Alan	Açıklama
Karşı Tünel IP Adresi	Layer 2 Tünel yapılacak tarafın IP adresi girilir.
WAN Arayüzü	Mevcuttaki tünelin WAN IP adresi varsayılan olarak gelir.

Layer 2 Tünel over IPsec NAT-T Sunucu

Tünelleme Modu Layer 2 Tünel over IPsec NAT-T Sunucuseçilmesi durumunda;

Tünelleme Modu	Layer 2 Tünel over IPsec NAT-T Sunucu	~
IPsec VPN Profili	AES128GCM16 - PRFSHA1 - MODP2048	~
Layer 2 Tünel		
	● IPv4 ○ IPv6	
	Sunucu Dış IP Adresi	
	IPv4	
	Karşı Tünel IP Adresi	
	IPv4	
	WAN Arayüzü	
	WAN1 - 10.2.1.178	~
	Ekle	

Layer 2 Tünel

Alan	Açıklama	
Sunucu Dış IP Adresi	Merkezdeki tünelin NAT IP adresi girilir.	
Karşı Tünel IP adresi	Layer 2 Tünel yapılacak tarafın IP adresi girilir.	
WAN Arayüzü	Mevcuttaki tünelin WAN IP adresi varsayılan olarak gelir.	

Layer 2 Tünel over IPsec NAT-T İstemci

Tünelleme Modu Layer 2 Tünel over IPsec NAT-T İstemci seçilmesi durumunda;

Tünelleme Modu	Layer 2 Tünel over IPsec NAT-T Istemci	~
IPsec VPN Profili	AES128GCM16 - PRFSHA1 - MODP2048	~
Layer 2 Tünel		
	● IPv4 ○ IPv6	
	Sunucu Dış IP Adresi	
	IPv4	
	Karşı Tünel IP Adresi	
	IPv4	
	WAN Arayüzü	
	WAN1 - 10.2.1.178	~
	Ekle	

Alan	Açıklama
Sunucu Dış IP Adresi	Merkezdeki Tünelin NAT IP adresi girilir. İstemci tarafı, sunucu tarafındaki tünelin NAT IP adresini girmelidir.
Karşı Tünel IP adresi	Layer 2 Tünel yapılacak tünel cihazının IP adresi girilir.
WAN Arayüzü	Mevcuttaki tünelin WAN IP adresi varsayılan olarak gelir.

Tünel ayarları tamamlandıktan sonra, Fiziksel Port ekle butonuna tıklanır.



Durum	Aktif	
Port Türü	● Tek Port ○ LACP	
Grup Adı		-
Ethernetler		X -
MTU	1500	-
VLAN Modu	Etiketsiz	~
VLAN ID		×
VLANIar (Trunk)		
Native VLAN		Temizie

Tek Port

Alan	Açıklama
Durum	Aktif/Pasif durumunu belirtme.
Port Türü	Tek Port seçilir.
Grup Adı	Grup Adı girilir.
Ethernetl er	Bu alanda IP'siz bacak seçilir.
MTU	MTU Değeri defaultta 1500 olarak gelmektedir, istenildiği takdirde değiştirilebilir.
VLAN Modu	Etiketsiz: Tek VLAN taşınacaksa bu seçenek seçilir ve VLAN ID girilir. Etiketli ve Etiketsiz: Birden fazla VLAN ve Native VLAN taşınacaksa bu seçenek seçilir. Native VLAN belirtme zorunluluğu bulunmamaktadır.
VLAN ID	Taşınması istenen tek VLAN'ın ID bilgisi girilir. VLAN Modu Etiketsiz olarak seçildiğinde aktifleşir.
VLANlar (Trunk)	Taşınacak olan VLAN'ların ID bilgisi girilir.(Etiketli ve Etiketsiz seçili olmalıdır.)
Native VLAN	Taşınacak olan Native VLAN'ın ID bilgisi girilir.

🖺 Kaydet

Alan	Açıklama
Durum	Aktif/Pasif durumunu belirtme.
Port Türü	LACP seçilir.
LACP Adı	LACP Adı girilir.
Ethernetl er	Bu alanda IP'siz bacaklar seçilir.
MTU	MTU Değeri defaultta 1500 olarak gelmektedir, istenildiği takdirde değiştirilebilir.
VLAN Modu	Etiketsiz: Tek VLAN taşınacaksa bu seçenek seçilir ve VLAN ID girilir. Etiketli ve Etiketsiz: Birden fazla VLAN ve Native VLAN taşınacaksa bu seçenek seçilir. Native VLAN belirtme zorunluluğu bulunmamaktadır.
VLAN ID	Taşınması istenen tek VLAN'ın ID bilgisi girilir. VLAN Modu Etiketsiz olarak seçildiğinde aktifleşir.
VLANlar (Trunk)	Taşınacak olan VLAN'ların ID bilgisi girilir.(Etiketli ve Etiketsiz seçili olmalıdır.)
Native VLAN	Taşınacak olan Native VLAN'ın ID bilgisi girilir.

İnternet Ağı

	Akdeniz Bölgesi	Omurga Switch (LACP)
e 🔒	VianiD: 33 Mersin 💭 🗨	🗨 🗢 Omurga Switch (LACP)
ø	VianiD: 7 Antalya 🗅 🖝	🖜 🛤 ens33 100 mb/s MTU: 1500 T 🗙 🖋
	İç Anadolu	ens36 100 mb/s MTU: 1500 T 🗙 🖋
e 🔒	VianiD: 6 Ankara Şube 🖕 🖝	
1	VianiD: 42 Konya 💭 🖝	

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

× 1

EPOTI IPSec VPN Ayarları



 \mathbf{x}

IPSec VPN modülü, hem IPSec Transport hem de IPSec Tünel modunda çalışabilmektedir. Oluşturulan IPSec bağlantısının Faz1 ve Faz2 ayarlarını kolaylıkla tek ekrandan ayarlanabilir, erişmeye yetkili IP adreslerinin listelerini ve iletim esnasında kullanılacak protokolü kullanıcı dostu arayüzü ile yapılandırılabilir.

IPsec VP	N Ayarları					
						G*Yenile + Elde > IPsec Durumlari
XLS	CSV PDF				🖽 Göster/Gizle 🛩	Sayfa Başı Kayıt Sayısı 🛛 Tamam 🝸 Filtrele 🍠 Filtreyi Temizle
#	Durum	🕸 Bağlantı Adı	🕼 Kaynak IP	1 Yedek Hat Kaynak IP	1 Hedef IP	11 İşlemler
1	Aktif	epati	10.2.1.199		10.0.0.30	2 C Düzenle 🛱 Sil Erişimler
				6 C 1 5 9		Git

IPSEC Durumları

IPsec tünel bağlantı durumunun terminal çıktısını vermektedir.

IPsec Durumları

```
IPsec Status:
uptime: 21 days, since Feb 25 18:00:26 2021
malloc: sbrk 3401600, mmap 0, used 1692256, free 1789344
worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
Listening IP addresses:
10.2.1.199
Connections:
ipsec-transport-1-1: local: [10.2.1.199] uses pre-shared key authentication
ipsec-transport-1-1: local: [10.2.1.199] uses pre-shared key authentication
ipsec-transport-1-1: remote: [10.0.0.30] uses pre-shared key authentication
ipsec-transport-1-1: remote: [10.0.10] uses pre-shared key authentication
ipsec-transport-1-1: child: 10.2.1.199/32 === 10.0.0.30/32 TRANSPORT, dpdaction=restart
Security Associations (1 up, 0 connecting):
ipsec-transport-1-1[203]: IKEV2 SPIs: 70412971ab2b11d4_i 70e4abe196dabece_r*, pre-shared key reauthenti
ipsec-transport-1-1[203]: IKEV2 SPIs: 70412971ab2b11d4_i 70e4abe196dabece_r*, pre-shared key reauthenti
ipsec-transport-1-1[203]: IKE proposal: AES GCM_16_256/MEP_MAC_SHA2_256/MOP_2048
ipsec-transport-1-1[834]: INSTALLED, TRANSPORT, reqid 202, ESP SPIs: c2f77524_i c6cbded6_0
ipsec-transport-1-1[834]: 10.2.1.199/32 === 10.0.0.30/32
```

IPSEC VPN Ayarları Yeni Kayıt

Bağlantı Adı					Kaynak ID Türü	0	IP Adresi Domain(FQDN)	
Durum	Aktif				Kaynak ID			
Kaynak IP	Seçiniz			-	Hedef ID Türü		ID Advanti	
redek Hat Kaynak IP	Seçiniz			•	Hertef ID	0	Domain(FQDN)	
Hedef IP	IPv? •				neactio			
	IPv4							
	IPv6							
I F	llo Avarla					~		
	lie Ayana	0	Profil Ku	ıllan	Profil Seçiniz	Ť		
Faz 1	ne Ayana	0	Profil Ku	ıllan	Profil Seçiniz	÷		
Faz 1	/ersiyonu	○ IKEv1 ●	IKEv2	illan	Profil Seçiniz Faz 2 PFS Gru	bu	(14) modp2048	~
Faz 1 IKE V Kr Alj	/ersiyonu riptolama goritması	 IKEv1 aes128gcrr 	IKEv2	•	Profil Seçiniz Faz 2 PFS Gru Kriptolaı Algoritm	bu ma ası	(14) modp2048 aes128gcm16 (aes'	~
Faz 1 IKE V Kr Alų Pseudo	/ersiyonu riptolama goritması o Random Function	 IKEv1 aes128gcm prfsha1 	IKEv2	✓	Faz 2 Faz 2 PFS Gru Kriptolai Algoritm Pseudo Rando Functi	bu ma ası om ion	(14) modp2048 aes128gcm16 (aes' prfsha1	~ ~
Faz 1 IKE V Kr Alı Pseudo	/ersiyonu riptolama goritmasi o Random Function DH Grubu	 IKEv1 aes128gcm prfsha1 (14) modp2 	IKEv2 IKEv2 116 (aes ⁻	v v	Profil Seçiniz Faz 2 PFS Gru Kriptolaı Algoritm Pseudo Rande Functi	bu ma ası om ion	(14) modp2048 aes128gcm16 (aes ⁻ prfsha1	~
Faz 1 IKE V Kr Alş Pseudo	/ersiyonu riptolama goritması D Random Function DH Grubu Kimlik oğrulama Metodu	 IKEv1 aes128gcm prfsha1 (14) modp2 Ön Paylaşı 	IKEv2 n16 (aes ⁻ 2048 mlı Anař	• • •	Profil Seçiniz Faz 2 PFS Gru Kriptolaı Algoritm Pseudo Randı Functi Ölü Bağlantı Sapta	ibu ma ası oom ion	(14) modp2048 aes128gcm16 (aes ⁻ prfsha1	~
Faz 1 IKE V Kr Alş Pseudo I Do Ön P	Versiyonu riptolama goritması D Random Function DH Grubu Kimlik oğrulama Metodu Paylaşımlı Anahtar	 IKEv1 aes128gcm prfsha1 (14) modp2 Ön Paylaşı 	IKEv2 n16 (aes ⁻ 2048 mlı Anař	• •	Profil Seçiniz Faz 2 PFS Gru Kriptolaı Algoritm Pseudo Randı Functi Ölü Bağlantı Sapta Ölü Bağla Saptaı Davrar	bu ma ası om ion ma ama ntı ma nışı	(14) modp2048 aes128gcm16 (aes ⁻ prfsha1 Kapan (Trap)	•



Elle Ayarla	🔘 Profil Kullan	Profil Seçiniz 🛛 💙		
Faz 1		Faz 2		
IKE Versiyonu	IKEv1 🔿 IKEv2	PFS Grubu	(14) modp2048 🗸 🗸	
Takas Modu	aggressive 🗸	Kriptolama	aes128gcm16 (aes' 💙	
Kriptolama Algoritması	aes128gcm16 (aes' 💙	Pseudo Random	prfsha1 🗸	
Pseudo Random Function	prfsha1 🗸	Function		
DH Grubu	(14) modp2048 🗸 🗸	Ölü Bağlantı Saptama		
Kimlik Doğrulama Metodu	Ön Paylaşımlı Anat 💙	Ölü Bağlantı Saptama Davranısı	Kapan (Trap) 🗸 🗸	
Ön Pavlasımlı	- Ali	Ölü Bağlantı	5	
Anahtar	42	Saptama Suresi		
Anahtar		Saptama Suresi Ölü Bağlantı Saptama Zamanaşımı	0	
Anahtar Anahtar	II Kaynak (P II Yede 10.2.1.199	Saptama Suresi Ölü Bağlantı Saptama Zamanaşımı tak Hat Keynak IP II Hedel 1000	0 Eccloser/Colfe = Sayta Bay Kayt Saysts IP II Iptemier 30 Q IZ Duterk 05 51 54	CYronie ♦Elic Ir_UPare Tanues VEitree ØFire
Ayarları Ayarları Cot Tof Durum İl Bağlantı Adı Aktr cpoti	Т Каулак (Р Уеd 10.21.1199	saptama suresi Ölü Bağlantı Saptama Zamanaşımı ek Hat Keynak IP II Hedel 1000	Control of the series of the	Taman Three In Per-
Ayarları Ayarları Ayarları Durum II Bağlantı Adı Aktr opoti	II Kaynak IP II Yedd 10.21.1199	saptama suresi Ölü Bağlantı Saptama Zamanaşımı « « ۱ • » • • • • • • • • • • • • • • • • • •	Construction Sayta Bap Kayıt Sayta P II Işlemler 30 C IZ Duarela S C IZ DUARELA S C IZ DUAR	QYeelle +Elle 1. Eve Tanum Trittele ∠fitte genter
Ayarları Ayarları Ayarları Ayarları IPsec VPN Aya	II KaynakiP II Yedd 10.2.1.199 rlarında Erişimler kısmına	saptama suresi Ölü Bağlantı Saptama Zamanaşımı «kHat Kaynak IP I Hedel 1000 •••••••••••••••••••••••••••••••••	0 Ekdentide - Sayta Bap Kayit Sayaa 19 I Islember 30 0 2 2 Church 0 1 fe listesi gelmektedir.	CYmrib +Exe 1. Per Izman Tritete Zitte print
Ayartarı Ayartarı Ayartarı Ayartarı Ayartarı IPsec VPN Ayalı C VPN Erişim Li	rlarında Erişimler kısmına istesi	saptama suresi Ölü Bağlantı Saptama Zamanaşımı ** Hat Kaynak IP II Hedel 10.00	C Construction Sayla Basis Kayrt Sayrs P Listensi gelmektedir.	C) Yenda ↓ €Ea 5Daw Tanum ▼Tittela ↓ Daw prime
Ayartar Ayartar Durum 11 Bağlantı Adı Akti epsti IPsec VPN Ayal c VPN Erişim Li c VPN bağlantışı	rlarında Erişimler kısmına is tesi ına dahil olan veya olaca	k erişimler girilmektedi	0 Contrologie Sayla Bayi Kayit Sayis 1P Islemer 30 Q Course 25 Ect listesi gelmektedir. r.	C Yould ♦ Elic L. Pict Turnum ▼ Filters ✓ Pict printe
Ayarları Ayarları Ayarları Cv roz Durum IL Bağlantı Adı Aktr cpati IPsec VPN Ayal c VPN Erişim Li c VPN bağlantışı	rlarında Erişimler kısmına istesi ına dahil olan veya olaca	saptama suresi Ölü Bağlantı Saptama Zamanaşımı • • • • • • • • • • • • • • • • • • •	Constructor Sayta Bapi Kayt Sayts P I I Isterier C C C C C C C C C C C C C	Tanuns Thicele In the
Ayarları Anahtar Ayarları Ayarları IPsec VPN Ayal C VPN Erişim Li C VPN bağlantısı Ayarları	rlarında Erişimler kısmına istesi ına dahil olan veya olaca	saptama suresi Ölü Bağlantı Saptama Zamanaşımı ««Hat Kaynak IP I Hedel 1000 « • ۱ • » a tıklanıldığında <i>Erişim</i> k erişimler girilmektedi	C C Constrait= Sayfa Bap Kayt Sayss P Listesi gelmektedir. r.	Tanum Threes Inverse yours
Ayarları Cv ro Durum IL Bağlantı Adı Aktr cpati IPsec VPN Ayal c VPN Erişim Li c VPN bağlantışı Ayarları tı Adı: epati (Köynek IP: 10.2.1.199) Cv ro	rlarında Erişimler kısmına istesi ına dahil olan veya olaca	saptama suresi Ölü Bağlantı Saptama Zamanaşımı • • • • • • • • • • • • • • • • • • •	Constructor Sayta Bapi Kayit Sayis I Sayta Bapi Kayit Sayis r. Sayta Bapi Kayit Sayis Sayta Bapi Kayit Sayis	Create File Interes Tanum Trittele Create Control Contro Control Control
Ayarları Ayarları Ayarları IPsec VPN Ayarl C VPN bağlantısı Ayarları tı Adı: epati (Koynak IP: 10.2.1.199/2	rlarında Erişimler kısmına istesi ına dahil olan veya olaca	saptama suresi Ölü Bağlantı Saptama Zamanaşımı •••••••••••••••••••••••••••••••••••	Controller Sayla Bapi Kayi Sayası P Listesi gelmektedir. r. Controller Sayla Bapi Kayi Sayası P Listesi gelmektedir. r. P Listesi gelmektedir.	CYenis +Exe L.Proc Tarum Tittels Inter junior Tarum Cittels Inter Citter Inte

Erişim Listesi - Yeni Kayıt

Kaynak IP	IPv? •	
	Geçersiz IP adresi! CIDR kullanımı zorunlu!	
Hedef IP	IPv? -	
	Geçersiz IP adresi! CIDR kullanımı zorunlu!	
Mod	Aktarım (Transport)	~
Başlatma Davranışı	Konfigürasyonun yüklenmesinden sonra yerine geti eylem.	irilecek
	Başlat (Start)	~
	Bağlantıyı hemen başlatır, herhangi bir trafik isteği bel	demez.
Bağlantı Kopma Davranısı	Karşı tarafın bağlantısının kapanması durumunda y getirilecek eylem.	erine
Davranışı	Yok (None)	~
	Herhangi bir eylemde bulunmaz.	
IPComp	Şifreleme öncesi IPComp sıkıştırma. Etkinleştirilirse, şifreleme öncesi ESP taşıma yükü verisini sıkıştırma IPComp sıkıştırma üzerinde anlaşmayı deneyecektir	IKE, k için
	Hayır, etkinleştirme	~
Açıklama		

Erişim Listesi - Kayıt Düzeltme

Kaynak IP	IPv4 ▼ 10).2.1.199/32	
HedefID			
Hedel IP	IPv4 ▼ 10	0.0.30/32	
Mod	Aktarım (Tr	ansport)	~
Başlatma Davranışı	Konfigürasyonı eylem.	un yüklenmesinden sonra yerine getiri	ilecek
	Başlat (Star	t)	~
	Bağlantıyı heme	n başlatır, herhangi bir trafik isteği bekl	emez.
Bağlantı Kopma Davranısı	Karşı tarafın ba getirilecek eyle	ğlantısının kapanması durumunda ye m.	rine
Davranışı	Yok (None)		~
	Herhangi bir eyl	emde bulunmaz.	
IPComp	Şifreleme önce şifreleme önce IPComp sıkıştır	si IPComp sıkıştırma. Etkinleştirilirse, I si ESP taşıma yükü verisini sıkıştırmak ma üzerinde anlaşmayı deneyecektir.	KE, için
	Hayır, etkin	leştirme	~
Açıklama			

ALANAÇIKLAMAKaynak IPKaynak IPv4 adresi yazılır.Hedef IPHedef IPv4 adresi yazılır.ModAktarım (Transport) veya Tünel modundan biri
seçilir.AçıklamaYazılan erişim listesi kaydı için açıklama yazılır.

Uç Bilgileri

 \times

ALAN	AÇIKLAMA
Bağlantı Adı	Bağlantı adı yazılır.
Durum	Aktif ya da pasif olma durumu seçilir.
Kaynak IP	Kaynak IPv4 adresi yazılır
Yedek Hat Kaynak IP	Yedek IPv4 adresi yazılır.
Hedef IP	Hedef IPv4 adresi yazılır

ID Yapılandırması

ALAN	AÇIKLAMA
Kaynak ID Türü	Kaynak ID türü seçilir.
Kaynak ID	Kaynak ID yazılır.
Hedef ID Türü	Hedef ID türü seçilir.
Hedef ID	Hedef ID yazılır.

Profil Ayarları

ALAN	AÇIKLAMA
Elle Ayarla	Faz 1 ve Faz 2 ayarlarının manuel ayarlanması için kullanılmaktadır.
Profil Kullan	Faz 1 ve Faz 2 ayarlarının profil yardımıyla ayarlanması için kullanılmaktadır.
Profil Seçiniz	Profil Kullan seçilmesi halinde, daha önce girişi yapılmış profil seçilmelidir.
Profil Üzerinden Elle Ayarla	Seçilen profilin manuel olarak değişiklik yapılması için kullanılmaktadır.

Faz 1

ALAN	AÇIKLAMA
IKE Versiyonu	Internet Key Exchange(İnternet anahtar değişimi) versiyonu seçilir.
Takas Modu	Takas modu seçilir. (IKEv2 seçilmesi halinde takas modu seçilmemektedir.)
Kriptolama Algoritması	Kullanılacak olan kriptolama algoritması seçilir.
Hash Algoritması	Kullanılacak olan hash algoritması seçilir.
DH Grubu	DH grubu seçilir.
Kimlik Doğrulama Metodu	Kimlik doğrulama metodu seçilir.
Ön Paylaşımlı Anahtar	Ön paylaşımlı anahtar yazılır. (Kimlik doğrulama metodu olarak <i>Ön Paylaşımlı</i> <i>Anahtar</i> seçilmiş ise)
Sertifika	SSL sertifika seçilir. (Kimlik doğrulama metodu olarak Sertifika seçilmiş ise)
Karşı Sertifika	Karşı SSL sertifika seçilir. (Kimlik doğrulama metodu olarak Sertifika seçilmiş ise)

Faz 2

ALAN	AÇIKLAMA
PFS Grubu	PFS grubu seçilir.
Kriptolama Algoritması	Kullanılacak olan kriptolama algoritması seçilir.
Kimlik Doğrulama Algoritması	Kullanılacak olan kimlik doğrulama algoritması seçilir.
Sıkıştırma Algoritması	Sıkıştırma algoritması seçilir.

Ölü Bağlantı Saptama

ALAN	AÇIKLAMA
Ölü Bağlantı Saptama Süresi	IPSec bağlantısı kesildiğinde tekrar bağlantının kurulması için geçecek süredir.
Ölü Bağlantı Saptama Süresi Zaman Aşımı	Zaman aşımı 0 seçilmesi durumunda, ölü bağlantı davranışı, ölü bağlantı saptama süresince davranış tekrarlanacaktır. Zaman aşımına süre girilmesi durumunda zaman aşımı süresi dolduğunda ölü bağlantı saptama işlemi yapılmayacaktır.

ePati Siber Güvenlik Teknolojileri A.Ş. Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN



EPOTÍ IPSec VPN Profilleri

CONCICOURS Sistemi Tümleşik Siber Güvenlik Sistemi

IPSec VPN ayarları için oluşturulan profil bölümüdür.

IPsec VPN Profilleri Sayfa Başı Kayıt Sayısı 👫 🛛 Profil Adı İsle AES128GCM16 - PRFSHA1 - MODP2048 epati « < 1 > » Yeni Kayıt Ekle IPsec VPN Profilleri - Yeni Kayıt × Genel Profil Adı Durum Aktif Faz 1 Faz 2 IKE Versiyonu ◯ IKEv1 ◯ IKEv2 PFS Grubu (14) modp2048 ~ Kriptolama aes128gcm16 (aes12 ~ Kriptolama Algoritması aes128gcm16 (aes12 × Algoritması Pseudo Random prfsha1 \mathbf{v} Pseudo Random Function prfsha1 v Function DH Grubu (14) modp2048 v Kimlik Doğrulama Ön Paylaşımlı Anahta \sim Ölü Bağlantı Saptama Metodu Ön Paylaşımlı Ø) Ölü Bağlantı Kapan (Trap) ~ Anahtar Saptama Davranışı Ölü Bağlantı 5 Saptama Süresi

🥥 İptal 🛛 🖺 Kaydet

Genel	AÇIKLAMA
Profil Adı	IPSec VPN için profil adı girilir.
Durum	Aktif/Pasif durum seçilir.

Faz 1

ALAN	AÇIKLAMA
IKE Versiyonu	Internet Key Exchange(İnternet anahtar değişimi) versiyonu seçilir.
Takas Modu	Takas modu seçilir. (IKEv2 seçilmesi halinde takas modu seçilmemektedir.)
Kriptolama Algoritması	Kullanılacak olan kriptolama algoritması seçilir.
Hash Algoritması	Kullanılacak olan hash algoritması seçilir.
DH Grubu	DH grubu seçilir.
Kimlik Doğrulama Metodu	Kimlik doğrulama metodu seçilir.
Ön Paylaşımlı Anahtar	Ön paylaşımlı anahtar yazılır. (Kimlik doğrulama metodu olarak <i>Ön Paylaşımlı</i> Anahtar seçilmiş ise)

Faz 2

ALAN	AÇIKLAMA
PFS Grubu	PFS grubu seçilir.
Kriptolama Algoritması	Kullanılacak olan kriptolama algoritması seçilir.
Kimlik Doğrulama Algoritması	Kullanılacak olan kimlik doğrulama algoritması seçilir.
Sıkıştırma Algoritması	Sıkıştırma algoritması seçilir.

Ölü Bağlantı Saptama

ALAN	AÇIKLAMA
Ölü Bağlantı Saptama Süresi	IPSec bağlantısı kesildiğinde tekrar bağlantının kurulması için geçecek süredir.
Ölü Bağlantı Saptama Süresi Zaman Aşımı	Zaman aşımı 0 seçilmesi durumunda, ölü bağlantı davranışı, ölü bağlantı saptama süresince davranış tekrarlanacaktır. Zaman aşımına süre girilmesi durumunda zaman aşımı süresi dolduğunda ölü bağlantı saptama işlemi yapılmayacaktır.

Not: IPSec VPN Profil kaydını, IPSec VPN Yeni kayıt eklerken Profil Kullan'ı seçerek kullanabiliriz.



.

epati Statik Yönlendirme

Statik yönlendirmenin (static routing) yapıldığı bölümdür.

Statik Yö	nlendirme					🗗 Yeniden Uygula	€ Yenile + Ekle
XLS 0	CSV PDF			III Göster/Gizle 👻 Sa	ıyfa Başı Kayıt Sayısı Ta	imam T Filtrele	🖌 Filtreyi Temizle
#	Durum	↓ Hedef Ağ	👫 Ağ Geçidi	🕴 Açıklama	11 İşlemler		
1	Aktif	10.100.0.0/16	10.200.201.253	Yenişehir Route	🕼 Düzenle 👔 Sil		
2	Aktif	10.102.0.0/16	10.200.201.253	Uç Nokta Route	🕼 Düzenle 👔 Sil		
			-4C <	1 > >			

Statik Yönlendirme Yeni Kayıt

Statik Yönle	ndirme - Y	'eni Kayıt				×
I	Durum	Aktif				
He	edef Ağ					
Ağ	; Geçidi	IPv4				
Aç	iklama					
				Ø İptal	🖺 Kay	/det
ALAN	AÇIKL/	AMA				
Durum	Aktif ya da pasif olma durumu seçilir.					
Hedef Ağ	Hedef Ağ Yönlendirilecek hedef ağ yazılır.					
Ağ						

ePati Siber Güvenlik Teknolojileri A.Ş. Mersin Üniversitesi Çiftlikköy Kampüsü Teknopark İdari Binası Kat: 4 No: 411 Posta Kodu: 33343 Yenişehir / MERSİN

Ağ geçidi yazılır.

Açıklama yazılır.

Geçidi

Açıklama



CONCICOURSE Tümlesik Siber Güvenlik Sistemi

epati Yönlendirme Tablosu

Antikor'daki yönlendirmelerin IPv4 veya IPv6 bazlı, tablo halinde görülebildiği bölümdür.

Yönlendirme Tablosu								
IPv4	● IPv4 ○ IPv6							
Sayfada	50 v kayıt	göster			Ara :	CSV I	xcel PD	OF Print
5 kayıttan 1	- 5 arasındaki l	kayıtlar gösteriliyor						
#	11	Hedef Ağ	Ağ Geçidi 🕴	Bayraklar	l1	Network		
1		default	10.2.2.253	UGS		em0		
2		10.2.2.0/24	link#1	U		em0		
3		10.2.2.40	link#1	UHS		lo0		
4		127.0.0.1	link#6	UH		lo0		
5		127.0.0.2	link#6	UH		lo0		
						Önce	ki 1	Sonraki
Yönlendirm	ne Tablosu							
O IPv4	IPv6							
Sayfada	50 v kayıt	göster			Ara :	CSV E	xcel PD	IF Print
9 kayıttan 1	- 9 arasındaki l	ayıtlar gösteriliyor						
#	11	Hedef Ağ 11	Ağ Geçidi 🕴	Bayraklar		Network		
1		::/96	::1	UGRS		100		
2		::1	link#6	UH		lo0		
3		::ffff:0.0.0.0/96	::1	UGRS		lo0		
4		fe80::/10	::1	UGRS		lo0		
5		fe80::%lo0/64	link#6	U		100		
6		fe80::1%lo0	link#6	UHS		100		
7		ff01::%lo0/32	::1	U		100		
8		ff02::/16	::1	UGRS		100		
0		ff02::%lo0/32	c1	U		00		

Önceki 1 Sonraki

Tümlesik Siber Güvenlik Sistemi

Yönlendirme tablosunun altında bayrakların açıklamaları tablo halinde bulunmaktadır.

	Bayraklar	Açıklama
в	RTF_BLACKHOLE	Paketler karadeliğe atılıyor. Bu hedefe giden paketler düşürülür.
b	RTF_BROADCAST	Yönlendirme, broadcast adresi temsil ediyor
D	RTF_DYNAMIC	Dinamik protokoller (RIP,OSPF,BGP gibi) tarafından oluşturulan yönlendirme
G	RTF_GATEWAY	Ağ geçidi
Н	RTF_HOST	Yönlendirme tek bir host'u işaret ediyor (Bu bayrak yoksa networku temsil ediyor demektir)
L	RTF_LLINFO	Link adresi dönüşümü için geçerli protokol
М	RTF_MODIFIED	Dinamik protokoller (RIP,OSPF,BGP gibi) tarafından modiye edildi
R	RTF_REJECT	Hedef Erişilemez
S	RTF_STATIC	Statik Yönlendirme
U	RTF_UP	Yönlendirme Kullanılabilir
х	RTF_XRESOLVE	Harici Servis (External daemon) protokolü link adresine çeviriyor



