

# epati

## Kurulum Kılavuzu

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı

Yapılandırma Örnekleri

## Kurulum Kılavuzu

### Online İnceleme

Antikor NGFW'ı online incelemek için [tıklayınız](#).

Kullanıcı adı: demo

Parola: demo

## Kurulumdan Önce Yapılması Gereken Adımlar

### Ürün Doğrulama Prosedürleri

Alıcı tarafından doğrulama işlemi, alınan medyanın md5 toplamı ile karşılaştırılarak gerçekleştirilir. \

- Müşteri, medyanın üzerinde bulunan Epati Bilişim Teknolojileri tarafından yapılandırılmış mührün zarar görüp görmediğini doğrular. Mührün zarar görmüş olması halinde kurulum gerçekleştirilmemelidir. \
- Müşteri, ürünün adını ve sürümünü doğrular. \
- Müşteri, medyanın md5 toplamını üretir ve resmi web sayfasındaki ISO md5 toplamı ile karşılaştırır. \
- Hesaplanan md5 toplamı ve web sayfasında bulunan md5 toplamı aynı ise yükleme işlemi başlayabilir.

### Donanım İhtiyaçları

Kurulum yapılacak lisansa göre donanım değişiklik göstermektedir. Detaylara aşağıdaki sayfadan **Modeller Ve Ürün Detaylarından** ulaşabilirsiniz.

<https://www.epati.com.tr/tr/urunler/antikor-v2-yeni-nesil-guvenlik-duvari/>

**Not:** Antikor'un kurulum yapılacağı ağ ortamda filtreleme yapan bir cihazın(firewall) arkasında ise; Antikor'un kurulu olduğu sunucu IP adresi için, 7001 ve 7002 portları lisans sunucusu ile haberleşebilmesi için açık olması gerekmektedir. Açık olmaması halinde lisans sunucusundan gelen paketler çekilmeyecek ve kurulum başarısız olacaktır. Bu portlar(7001 ve 7002) sadece Antikor lisans sunucu IP adresinin erişimi için de açılabilir. Lisans sunucu IP adresi için Teknik Destek Ekibi ile iletişime geçebilirsiniz.

Test için;

```
telnet lisans.epati.com.tr 7001
telnet lisans.epati.com.tr 7002
```

## Kurulum Aşaması

ISO dosyasını edinmek için [tıklayınız](#).

```
CD Loader 1.2
Building the boot loader arguments
Looking up /BOOT/LOADER... File not found
Looking up /boot/loader... Found
Relocating the loader and the BTX
Starting the BTX loader

BTX loader 1.00 BTX version is 1.02
Consoles: internal video/keyboard
BIOS CD is cd0
BIOS drive C: is disk0
BIOS 639kB/1047488kB available memory

FreeBSD/x86 bootstrap loader, Revision 1.1
(root@antiKor2.epati.com.tr, Thu Sep  7 11:01:07 EEST 2017)
Loading /boot/defaults/loader.conf
/boot/kernel/kernel text=0x1034450 |
```

Yukarıdaki ekranda ilk satırda “CD Loader ” yazdığıında kurulum başladığını belirtmektedir.

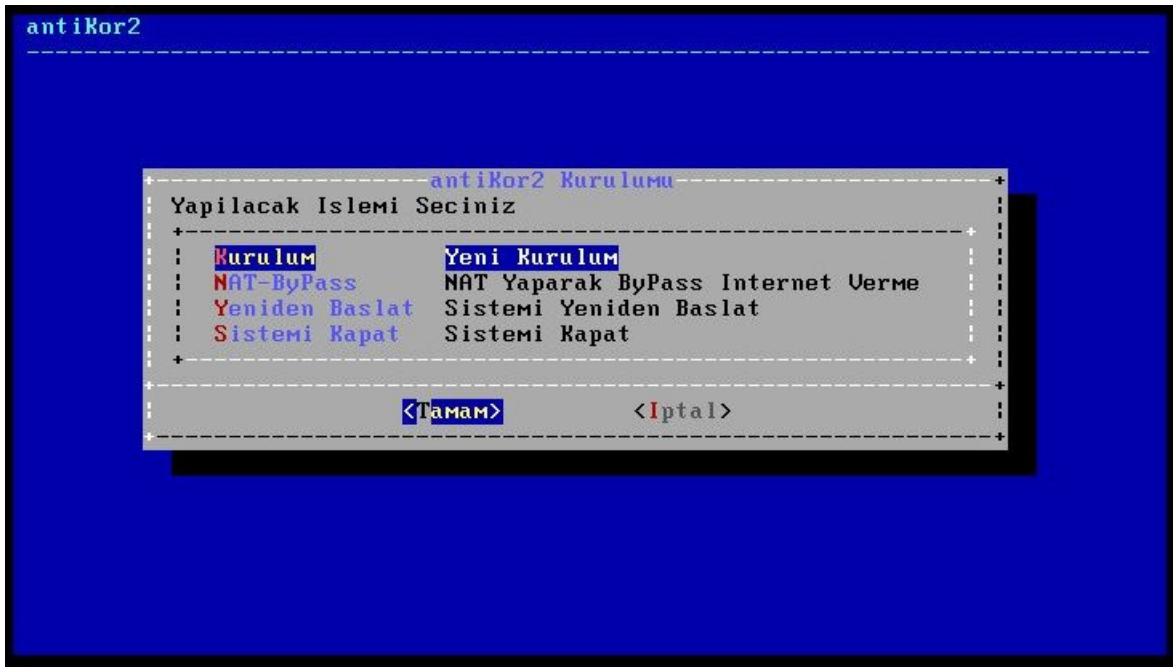
### Dil Seçimi

CD başarılı bir şekilde çalıştırılır ise, kurulumla başlama adımı karşımıza gelecektir.



İstenilen dil seçilerek **Tamam**’a tıklanır.

### Kurulum

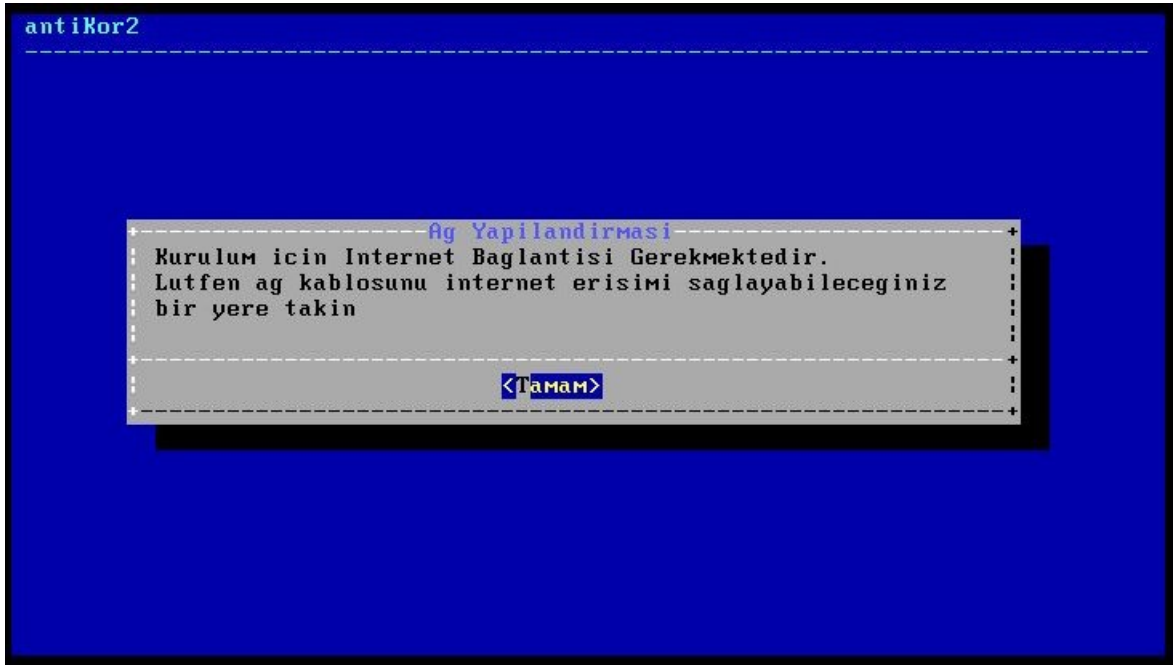


Yukarıdaki ekranda;

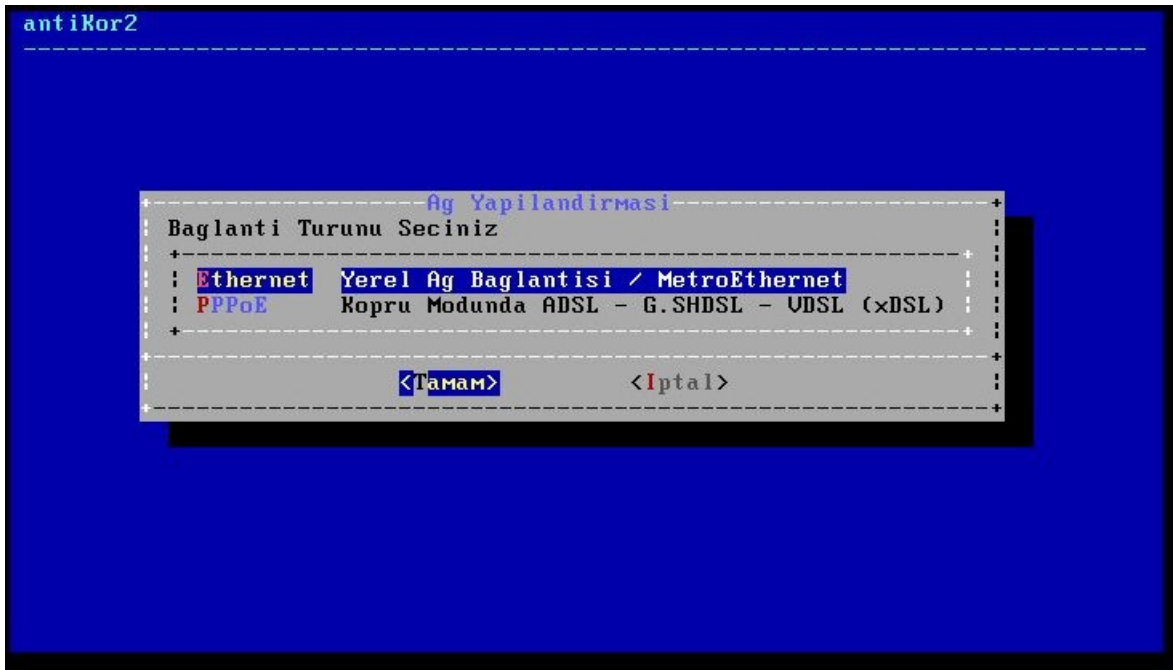
- **Kurulum** seçeneği yeni Antikor kurulumun başlatılması istendiğinde seçilmelidir.
- **Nat-ByPass** seçeneği kurulumu yapılmış Antikor'un bypass yapılarak internete çıkarılması için kullanılmalıdır.
- **Yeniden Baslat** seçeneği kurulumun tekrardan başlatılması için kullanılmalıdır.
- **Sistemi Kapat** seçeneği sistemin gücünü kapatmasını sağlamaktadır.

Yeni kurulum yapılması için, "Kurulum" seçilerek devam edilmelidir.

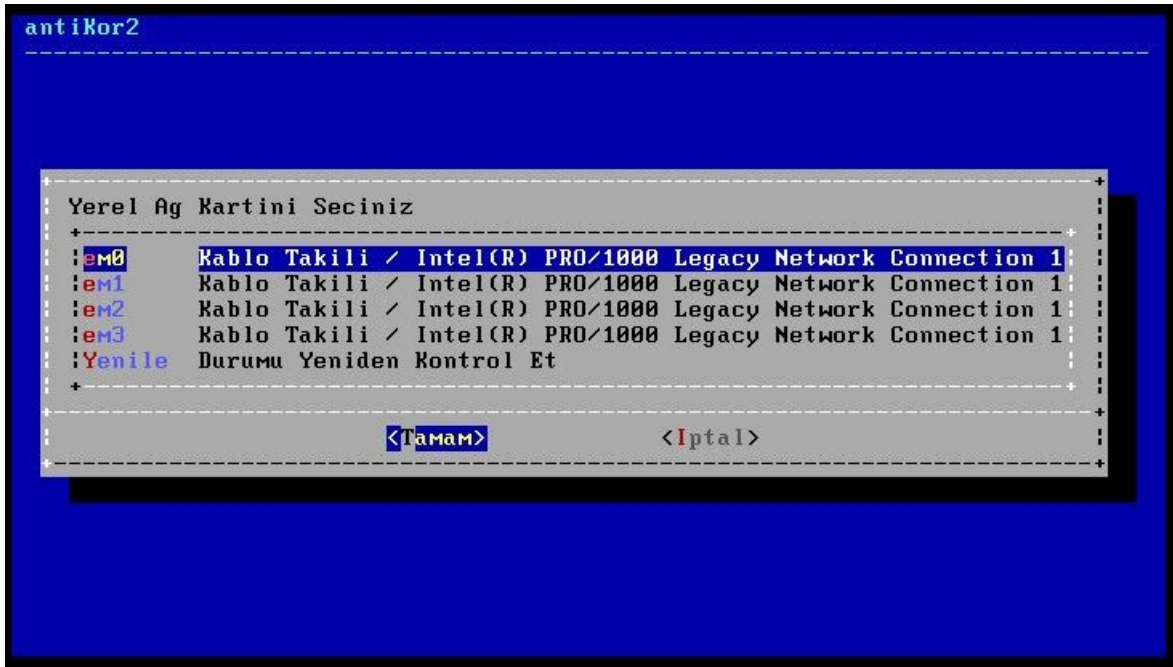
#### Ağ Yapılandırması



Kurulum için internet bağlantısı gerekmektedir.



İnternet bağlantı türü seçimi yapılır.



Bu ekranda 4 adet Intel Ethernet görülmektedir. Kurulum hangi Ethernet üzerinden yapılacaksa o Ethernet seçilerek kurulumla devam edilir.

**Not:** Ethernet kartları görünmediği takdirde, bağlantılar kontrol edilerek **Yenile Durumu Yeniden Kontrol Et** seçeneği seçilir.

#### DHCP - Manuel Seçimi

antiKor2

```
Ag Yapilandirmasi
Yapilandirma Turunu Seciniz
+
: DHCP Otomatik Yapilandirma
: Manual El ile Yapilandirma
+
+
: <Tamam> <Iptal>
```

Seçilen ethernetten internete manuel IP verilerek veya DHCP seçilerek otomatik IP alınması gerekir. Fakat DHCP için IP dağıtan bir sisteminizin olması gerekmektedir. Eğer DHCP sunucu yoksa manuel IP verilerek devam edilir.

Aşağıda manuel IP verilerek kurulumu devam edilmiştir.

antiKor2

```
Ag Yapilandirmasi
+
: IP Adresi
: Alt Ag Maskesi 255.255.255.0
: Ag Gecidi
: DNS Sunucusu 8.8.8.8
+
+
: <Tamam> <Iptal>
```

antiKor2

```
Ag Yapilandirmasi
+-----+
:IP Adresi          172.16.33.10
:Alt Ag Maskesi     255.255.255.0
:Ag Gecidi          172.16.33.2
:DNS Sunucusu      8.8.8.8
+-----+
<Tamam>           <Iptal>
```

antiKor2

```
Ag Yapilandirmasi
+-----+
em0: flags=8843<UP, BROADCAST, RUNNING, SIMPLEX, MULTICAST> metric 0 mtu
1500
options=81009b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM, VLAN
_HWFILTER>
ether 00:0c:29:fb:3d:7e
inet 172.16.33.10 netmask 0xfffff00 broadcast 172.16.33.255
media: Ethernet autoselect (1000baseT <full-duplex>)
status: active
nd6 options=29<PERFORMNUD, IFDISABLED, AUTO_LINKLOCAL>

Routing tables

Internet:
Destination      Gateway          Flags           Netif Expire
default          172.16.33.2     UGS             em0
127.0.0.1        link#4          UH              lo0
+-----+
<Evet >          <Hayir>          80%
```

antiKor2

```
Ag Yapilandirmasi
+-----+
172.16.33.2 - Ag Gecidine Ping Atiliyor...
Ag Gecidine Ulasilabiliyor
Sunucuya Erisim Kontrol Ediliyor...
Internete Ulasilabiliyor
Zaman Damgasi Aliniyor...
+-----+
```

Kurulum tipi seçilir. Online kurulumda sunucunun internete çıkması gerekmektedir. Kurumsal kurulum kapalı devre sistemlerde Merkezi Yönetim üzerinden kurulum için kullanılır.

antiKor2

```
Ag Yapilandirmasi
Kurulum Kaynagini Seciniz
:Online   Ureticinin Sunucularindan
:Kurumsal Antikor CFWM - Merkezi Yonetim Sunucusundan
<Tamam>   <Iptal>
```

Antikor'a erişim sağlanması istenen IP adresi girilir. 0.0.0.0/0 seçilmesi durumunda her yerden erişim sağlanabilecektir.

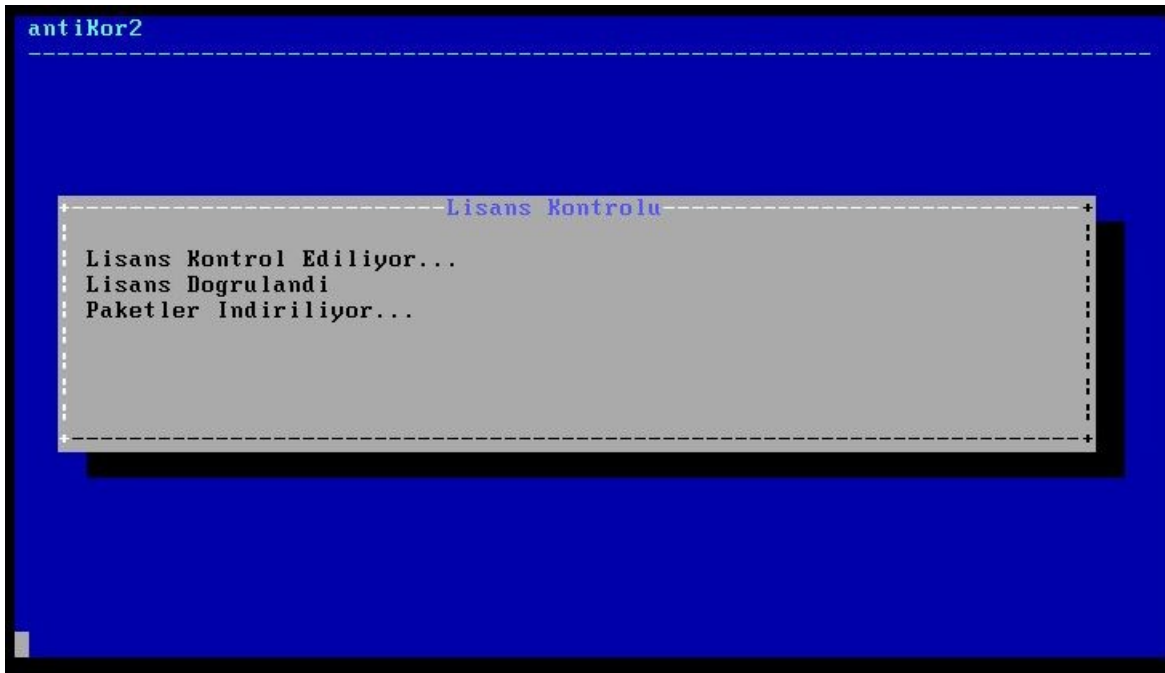
antiKor2

```
Ag Yapilandirmasi
:Yetkili IP Adresi   0.0.0.0/0
<Tamam>   <Iptal>
```





Epsti Siber Gvenlik tarafından saęlanan lisans anahtarı girilir.



### Disk Blmleme

Sunucu zerinde birden fazla disk var ise, Antikor Yazılımı ve Logları farklı diske kurulabilir. Tek disk var ise seęilen diske kurulum yapılacaktır.

antiKor2

```
-----Disk Yapilandirmasi-----+
:
: Disk Bolumleme Semasi Seciniz
:
: GPT GPT Legacy
: MBR Master Boot Record
:
:
: <Tamam> <Iptal>
:-----+

```

Diskinizin partition yapısına göre(GPT, MBR) seçim yapılır. Disklerin bir çoğu GPT uyumludur.

antiKor2

```
-----Disk Yapilandirmasi-----+
:
: Kurulum Diskini Seciniz
:
: da0 81920MB - VMware Virtual disk 1.0 RETRY_BUSY
:
:
: <Tamam> <Iptal>
:-----+

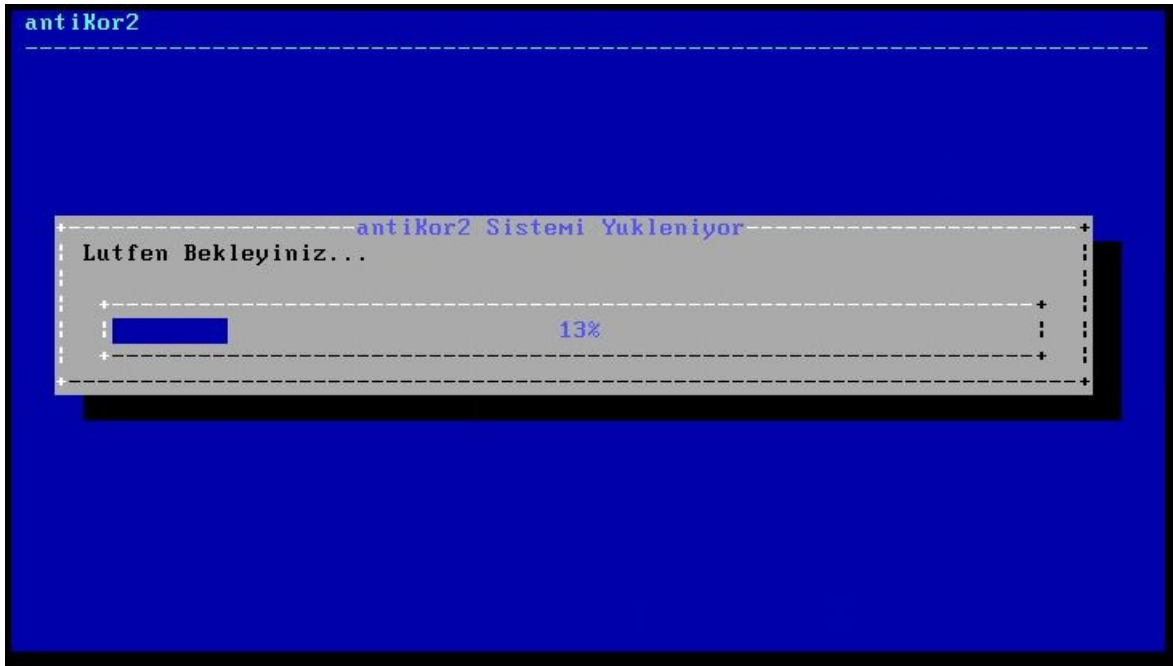
```

antiKor2

```
-----Disk Yapilandirmasi-----+
:
: Diskinizdeki tum veri silinecektir!
: Devam etmek istediginize emin misiniz?
:
:
: <Evet > <Hayir >
:-----+

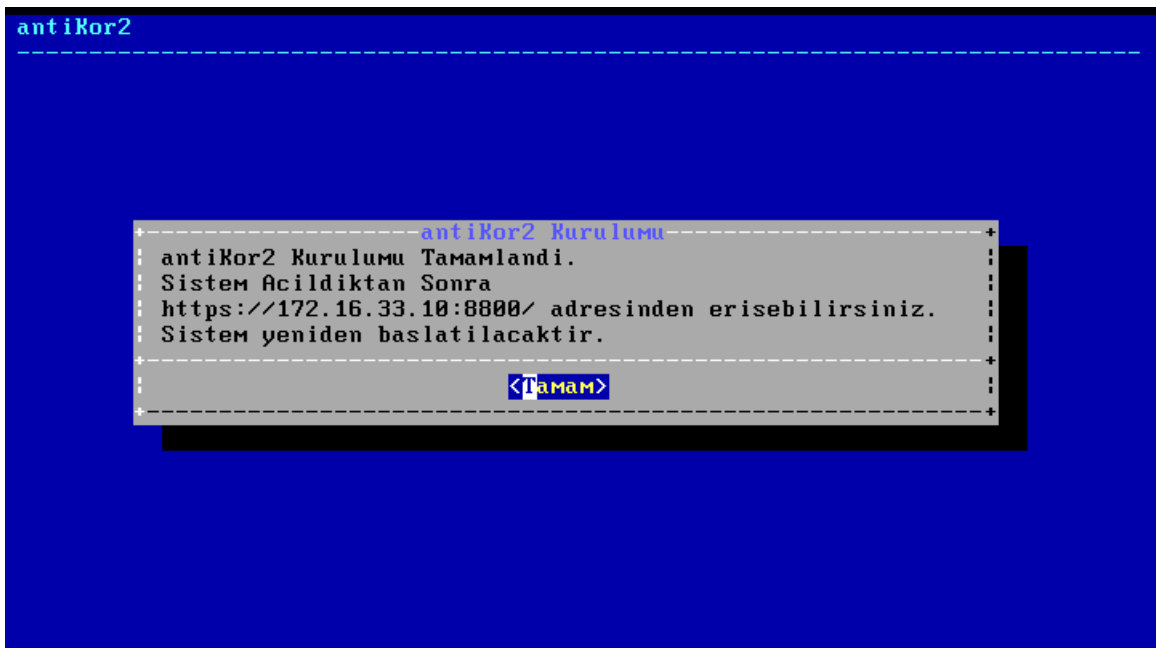
```

Kurulum için diskin biçimlendirilmesi gerekmektedir. **Evet** seçerek devam edilir.



The screenshot shows a blue terminal window with the title "antiKor2". A grey box contains a list of packages being installed, titled "PAKETLER KURULUYOR".

| Package Name            | Version  | Status           |
|-------------------------|----------|------------------|
| Arayuz Modulu           | 2.0.954  | Kurulmaya Hazir  |
| Arac Kutusu             | 2.0.19   | Kurulmaya Hazir  |
| Yonetimsel Araclar      | 2.0.12   | Kurulmaya Hazir  |
| Yapilandirma Yoneticisi | 2.0.357  | Kurulmaya Hazir  |
| Haberlesme Modulu       | 2.0.611  | Guncel           |
| Haberlesme Aracisi      | 2.0.15   | Kurulmaya Hazir  |
| URL Kategori Veritabani | 2.0.32   | Indiriliyor      |
| IPS Imza Veritabani     | 2.0.9221 | Sirada (Indirme) |
| Uygulama Tanimlayici    | 2.0.319  | Sirada (Indirme) |
| Web Erisim Loglari      | 2.0.23   | Sirada (Indirme) |
| Proxy Kimlik Dogrulama  | 2.0.4    | Sirada (Indirme) |
| Balkupu Modulu          | 2.0.18   | Sirada (Indirme) |
| Layer2 Anormallik       | RC-2.0.7 | Sirada (Indirme) |
| Modul Yoneticisi        | 2.0.15   | Guncel           |
| Yoneticici Konsolu      | 2.0.38   | Sirada (Indirme) |
| Bant Genisligi Monitoru | 2.0.0    | Sirada (Indirme) |
| Kamu SM - Zamane        | 2.0.5    | Sirada (Indirme) |
| Arayuz Modulu (Halka)   | 2.0.7    | Sirada (Indirme) |
| Haberlesme Yoneticisi   | 2.0.4    | Sirada (Indirme) |
| (Router)                |          |                  |





# antikor

antikor v2 NGFW Kurumsal  
Giriş yapmak için bilgileri giriniz.

ePati Siber Güvenlik © 2016 -2022  
Dil Seçiniz : tr en

- Giriş ekranı gelecektir. Kullanıcı adı "admin" ve parolayı "antikor" yazarak Giriş butonuna tıklanır.

Gösterge Paneli

Sistem Kullanımı

CPU 15% Bellek 35% Disk 6%

Arayüz Durumları

Gruplanmamış

em0 WAN1 100%281810134 Devrede 100%281810134 Devrede

em1 LAN1 100%281810134 Devrede 100%281810134 Devrede

em2 Altkonfig 100%281810134 Devrede 100%281810134 Devrede

em3 Altkonfig 100%281810134 Devrede 100%281810134 Devrede

em4 Altkonfig 100%281810134 Devrede 100%281810134 Devrede

em5 Altkonfig 100%281810134 Devrede 100%281810134 Devrede

em6 Altkonfig 100%281810134 Devrede 100%281810134 Devrede

Ethernet Bant Genişliği Kullanımı

Tümü

Servis Durumları

|                                       |                  |   |   |   |
|---------------------------------------|------------------|---|---|---|
| Balıkçısı Servisi                     | Kapalı           | ▶ | ⊞ | ⊞ |
| Karadeki Servisi                      | Kapalı           | ▶ | ⊞ | ⊞ |
| Anti-Spoof Servisi                    | Kapalı           | ▶ | ⊞ | ⊞ |
| Güvenlik Duvarı                       | ▲ Durdurulmadı   | ▶ | ⊞ | ⊞ |
| Sanal Kablo Motoru                    | Yapılandırılmadı | ▶ | ⊞ | ⊞ |
| Web Sunucusu Güvenliği                | Kapalı           | ▶ | ⊞ | ⊞ |
| Uygulama Kontrolü / IPS Motoru        | Yapılandırılmadı | ▶ | ⊞ | ⊞ |
| Uygulama Kontrolü Kuralları           | Yapılandırılmadı | ▶ | ⊞ | ⊞ |
| IPS Kuralları                         | Yapılandırılmadı | ▶ | ⊞ | ⊞ |
| AV Kuralları                          | Yapılandırılmadı | ▶ | ⊞ | ⊞ |
| Antivirus Motoru                      | Kapalı           | ▶ | ⊞ | ⊞ |
| Web Filtreleme Motoru                 | Kapalı           | ▶ | ⊞ | ⊞ |
| Forwarded For Bilgisi Gate            | ByPass           | ▶ | ⊞ | ⊞ |
| HTTP Denetim Servisi                  | ByPass           | ▶ | ⊞ | ⊞ |
| HTTPS Denetim Servisi                 | ByPass           | ▶ | ⊞ | ⊞ |
| Sayfa Yasaklama Servisi               | ByPass           | ▶ | ⊞ | ⊞ |
| Antivirus / İçerik Filtreleme Servisi | ByPass           | ▶ | ⊞ | ⊞ |
| Proxy Servisi                         | ByPass           | ▶ | ⊞ | ⊞ |
| DNS Denetleme Motoru                  | Kapalı           | ▶ | ⊞ | ⊞ |
| DNS Denetim Servisi                   | ByPass           | ▶ | ⊞ | ⊞ |

Arayüze giriş yapıldıktan sonra ilk adım olarak güvenlik amacı ile Parolanın değiştirilmesi gerekmektedir. Yönetim Paneli Ayarları menüsü altında bulunan Yönetim Paneli Kullanıcıları sekmesi açılır ve ilgili kullanıcı için detaylar butonuna tıklanır.

Yönetim Paneli Kullanıcıları

Yeni Ekle

ALS CSV PDF

Göster/Gütle Sayfa Başı Kayıt Sayısı Tamam Filtrele Filtreyi Temizle

| # | Durum | Adı     | Soyadı | Kullanıcı Adı | İzinli IP Adresleri | İşlemler  |
|---|-------|---------|--------|---------------|---------------------|---|
| 1 | Aktif | Antikor | Admin  | admin         | [Açma]              | [Düzenle] [Sil] [Grup Üyeleri] [Yetkiler ve Roller] [Detaylar] [Sertifika Yönetimi] |

< 1 >

GİT

Açılan sayfada "Düzenle" butonuna tıklanır.

Antikor Admin



Kullanıcı Adı : admin

## Kullanıcı Bilgileri

Adı Soyadı : Antikor Admin

Kullanıcı Adı : admin

E-Posta : bilgi@epati.com.tr

Oluşturma Tarihi :

Giriş Yapılan IP Adresi :

Giriş Yapılan Tarih :

Giriş Yapılan Son IP Adresi : 172.16.33.1

Giriş Yapılan Son Tarih : 2021-11-09 09:43:22+00

Giriş Sayısı : 3

Kim Tarafından Oluşturuldu :

## Profil Fotoğrafi Yükle

Profil Fotoğrafi : [Yükle](#)

## Kimlik Bilgileri

Adı

Antikor

Soyadı

Admin

ePosta

bilgi@epati.com.tr

## Kullanıcı Bilgileri

Kullanıcı Adı

admin

Kullanıcı Parolasını Değiştir.

[İptal](#)[Kaydet](#)

## Kullanıcı Parola Güncelleme

## Parolanızı Güncelleyin

Yeni Parola

Yeni Tekrar

Kaydet

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

## Yeni Kullanıcı Oluşturulması

Sistemi yöneten kullanıcıların her birinin kendi kullanıcı ve şifrelerini kullanarak arayüze giriş yapması güvenlik ve sistem yönetimi yönünden olumlu etki yaratacaktır.

Yeni bir kullanıcı oluşturmak için öncelikle **Yönetim Paneli Erişim Ayarları** menüsünden **Yönetim Paneli Kullanıcılarına** gidilir.



Yönetim Paneli Kullanıcılarında **Ekle** Butonuna tıklanır.

| # | Durum | Adı     | Soyadı | Kullanıcı Adı | İzinli IP Adresleri | İşlemler   |
|---|-------|---------|--------|---------------|---------------------|--|
| 1 | Aktif | Antikor | Admin  | admin         | [Adet:0]            | <a href="#">Düzenle</a> <a href="#">Sil</a> <a href="#">Grup Üyelikleri</a> <a href="#">Yetkiler ve Roller</a> <a href="#">Detaylar</a> <a href="#">Sertifika Yönetimi</a> |

Kullanıcı için gerekli bilgiler ve temel yetkileri (admin kullanıcısı, SSH Erişimi) girilerek **Kaydet** butonuna tıklanır ve tanımlar uygulanır.

Durum  Aktif

Kimlik Bilgileri 111\*\*\*\*\*11 - Antikor Admin x

Kullanıcı Adı epatisiberguvenlik

Parola Parola Tekrar İzinli IP Adresleri  Admin Kullanıcısı  Sms Doğrulama Yap  SSH Erişimi

SSH Yetkileri

adminKonsolu x arp x bootMesajlari x  
bufferTemizle x cluster-ceza-skoru x cluster-durumu x  
cluster-servisi x cluster-shell x df x dhcpTara x  
disk-bilgisi x disk-io x disk-listesi x  
donanim-bilgisi x drouter x ethernet x firewall x  
grep x http-loglari x ifconfig x iperf x ipsec x  
ipsec-debug x ipsecPolicy x kullanıcı x less x  
lisans x mgmt-servisi x mgmt-shell x more x  
ndp x netstat x nslookup x paket x passwd x  
pftop x pgsqServer x ping x ping6 x  
poweroff x radiusDebug x radtest x route x  
scp x servis x sistemLoglari x  
socket-yeniden-baslat x ssh x tabloListesi x tarih x  
tcpdump x tcpdump-any x telnet x top x  
traceroute x trafshow x tshark x uname x  
uptime x uygula x wc x webTarayici x  
yedek-olustur x yenidenBaslat x

Tümünü Seç

İptal

Kaydet

Uygulanacak İşlem Listesi

Güncelleştirmeler Hazır

Tanımları Uygula 1

| SSH Yetkileri                         |
|---------------------------------------|
| <input type="button" value="Uygula"/> |

**Not:** Kullanıcının eklenmesi için öncelikle menüde **Tanımlamalar** bölümünde bulunan **Kimlik Tanımlamaları**ndan kullanıcı ile ilgili bilgilerin eklenmesi(burada kimlik bilgisi bulunmuyorsa) gerekmektedir.

- Kullanıcı için yetki ve roller belirlenebilmektedir.

Yönetim Paneli Kullanıcıları

Yenile Ekle

| # | Durum | Adı     | Soyadı | Kullanıcı Adı      | İzinli IP Adresleri | İşlemler   |
|---|-------|---------|--------|--------------------|---------------------|--|
| 1 | Aktif | Antikor | Admin  | epatisiberguvenlik | (Adet: 0)           | <a href="#">Düzenle</a> <a href="#">Sil</a> <a href="#">Grup Üyelikleri</a> <a href="#">Yetkiler ve Roller</a> <a href="#">Detaylar</a> <a href="#">Sertifika Yönetimi</a> |
| 2 | Aktif | Antikor | Admin  | admin              | (Adet: 0)           | <a href="#">Düzenle</a> <a href="#">Sil</a> <a href="#">Grup Üyelikleri</a> <a href="#">Yetkiler ve Roller</a> <a href="#">Detaylar</a> <a href="#">Sertifika Yönetimi</a> |

[«](#) [1](#) [»](#)

Göt.



Rol Düzenle

Göster/Gizle

Sayfa Başı Kayıt Sayısı

Tamam

Filtrele

Filtreyi Temizle

| #      | Adı | Kapsam | İşlemler |
|--------|-----|--------|----------|
| < > >> |     |        |          |

Yetki Düzenle

Göster/Gizle

Sayfa Başı Kayıt Sayısı

Tamam

Filtrele

Filtreyi Temizle

| #      | Adı | Kapsam | İşlemler |
|--------|-----|--------|----------|
| < > >> |     |        |          |

## Roller ve Yetkiler

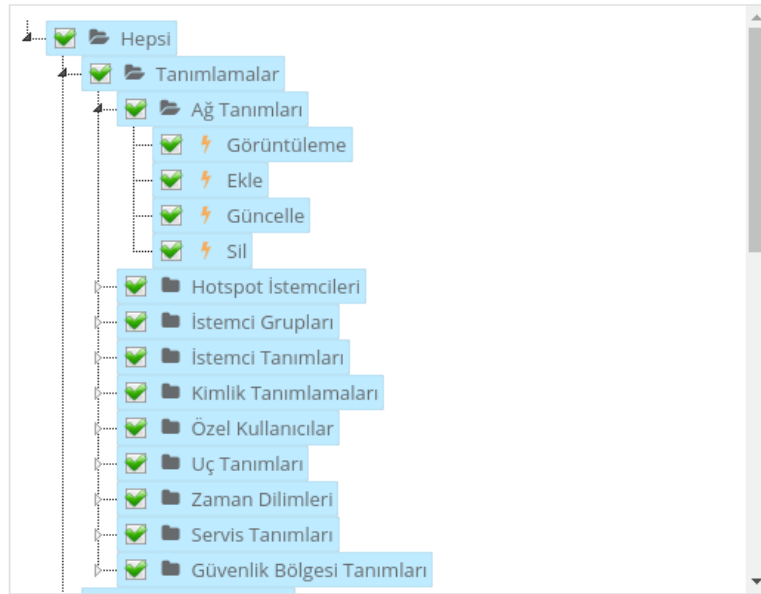
✕

Kapsam

0.0.0.0/0 ✕

::/0 ✕

Yetki Ağacı



İptal

Kaydet

- Antikor NGFW güvenlik önlemi olarak her kullanıcının kendi sertifikasını kullanarak giriş yapabilmesini de sağlamaktadır. Kullanıcının doğrulama sertifikası tarayıcıda yüklü değil ise arayüze giriş yapamayacaktır.

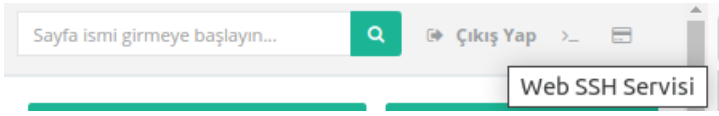
Detaylı Bilgi İçin: <http://kitaplik.epati.com.tr/kilavuzlar/antikor-v2-yeni-nesil-guvenlik-duvari/kullanici-yonetimi/yonetim-paneli-kullanicilari/>

- İşlemleri tamamladıktan sonra **Tanımları Uygulayarak** yeni kullanıcı ile giriş yapabilirsiniz.

**Not:** Kullanıcı ilk girişinde sözleşmeyi okuyup onaylaması ve şifreyi değiştirmesi istenir. Bu işlemlerden sonra kullanıcı başarılı bir şekilde giriş yapabilmektedir.

### Kullanıcıların SSH ile Bağlantısı

- Yönetim Paneli Kullanıcılarında oluşturulan kullanıcı ile Web SSH kullanılabilir.
- Gösterge Panelinin sağ üst köşesinde bulunan >\_ Web SSH Servisi simgesine tıklanır ve gelen ekranda yeni oluşturduğumuz kullanıcı adı ve şifreyle Web SSH servisi kullanılabilir.

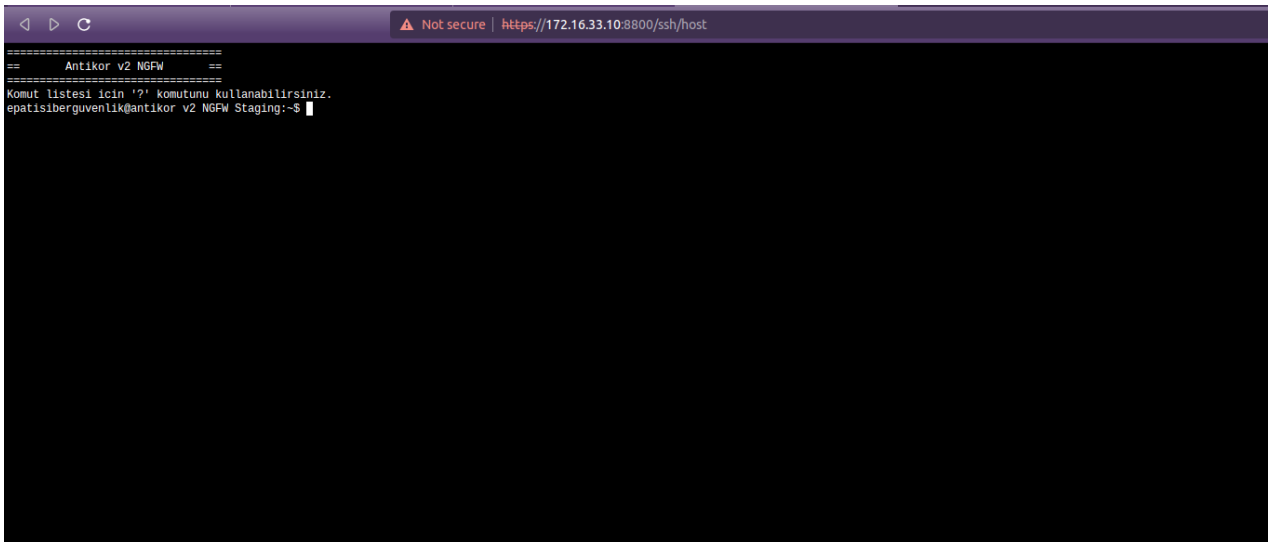


Sign in

https://172.16.33.10:8800

Username

Password



- Üçüncü parti uygulamalar ile giriş sağlanacaksa(PuTTY, Mobaxterm vb...) kullanıcılarının SSH'a erişebilmesi için ilk önce ssh-key üretilmelidir.

SSH key üretimi ve SSH erişiminin nasıl yapılacağına dair yapılandırma örneği için :

<http://kitaplik.epati.com.tr/yapilandirma-ornekleri/antikor-v2-yeni-nesil-guvenlik-duvari/kullanici-ssh-yapilandirilmesi/>

## IP Havuzları

Yönetilecek olan ağ(lar)ın IP adres aralıkları bu menüde tanımlanır. Bu aralıklar, AntiKor'un denetleme mekanizmalarında kullanılacaktır.

IP adres havuzlarına kullanılmak istenen IP adresleri önceden eklenmelidir. Bazı işlemler (İstemci Tanımları, Statik NAT gibi) IP havuzlarına IP adreslerini eklemeyi gerektirir.

| # | Ethernet | IP Bloğu       | Açıklama | İşlemler  |
|---|----------|----------------|----------|---|
| 1 | DMZ1     | 172.29.0.0/24  | DMZ      | <input type="checkbox"/> Düzenle <input type="checkbox"/> Sil |
| 2 | LAN1     | 172.28.0.0/24  | LAN1     | <input type="checkbox"/> Düzenle <input type="checkbox"/> Sil |
| 3 | WAN1     | 172.16.33.0/24 | WAN1     | <input type="checkbox"/> Düzenle <input type="checkbox"/> Sil |

## IP Havuzları Yeni Kayıt

### IP Havuzları - Yeni Kayıt

×

|              |  |
|--------------|--|
| Ethernet     | LAN1   |
| Adres Ailesi | <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 |
| IP Bloğu     | IPv4   |
| Açıklama     |  |

İptalKaydet

## Güvenlik Bölgesi Tanımları

AntiKor'da yönetilecek ethernet arayüzleri için Güvenlik Bölgesi Tanımı oluşturulur.

### Güvenlik Bölgesi Tanımları

| # | Makine Adı | Adı       | Varsayılan Politika | Açıklama  | İşlemler                              |
|---|------------|-----------|---------------------|-----------|---------------------------------------|
| 1 | dmz-zone   | dmz-zone  | izinli              | dmz-zone  | <span>Düzenle</span> <span>Sil</span> |
| 2 | lan1-zone  | LAN1-Zone | izinli              | LAN1-Zone | <span>Düzenle</span> <span>Sil</span> |
| 3 | wan-zone   | WAN Zone  | izinli              | WAN Zone  | <span>Düzenle</span> <span>Sil</span> |

Yenile Ekle

« < 1 > »

### Güvenlik Bölgesi Tanımları Yeni Kayıt

#### Güvenlik Bölgesi Tanımları - Yeni Kayıt

×

|                     |           |
|---------------------|-----------|
| Makine Adı          | lan1-zone |
| Adı                 | LAN1-Zone |
| Varsayılan Politika | izinli    |
| Açıklama            | LAN1-Zone |

İptalKaydet

## Ethernet Atama

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

| # | Durum | Arayüz | Ethernet Adı    | Hız        | MTU  | IPv4 Adresi       | IPv6 Adresi | Global NAT | Kull./Top. | Seçenekler   | İşlemler                                    |
|---|-------|--------|-----------------|------------|------|-------------------|-------------|------------|------------|--|---|
| 1 | Aktif | WAN1   | igb0 - Fiziksel |            | 1500 | 10.2.1.45/24      |             |            |            |  | <a href="#">Düzenle</a> <a href="#">Sil</a> |
| 2 | Aktif | LAN2   | igb2 - Fiziksel | autoselect | 1500 | 1.1.1.100/24      |             |            | 0/254      |  | <a href="#">Düzenle</a> <a href="#">Sil</a> |
| 3 | Aktif | LAN1   | igb1 - Fiziksel | autoselect | 1500 | 192.168.33.100/24 |             | 10.2.1.45  | 0/254      | <a href="#">NAT</a> <a href="#">DHCPv4 Sunucusu</a> <a href="#">Kayıt AI</a> | <a href="#">Düzenle</a> <a href="#">Sil</a> |
| 4 | Aktif | LAN3   | igb3 - Fiziksel | autoselect | 1500 | 192.168.100.1/24  |             | 10.2.1.45  | 0/241      | <a href="#">NAT</a> <a href="#">DHCPv4 Sunucusu</a>                          | <a href="#">Düzenle</a> <a href="#">Sil</a> |

## LAN Ekle Yeni Kayıt

### Ethernet Atama - LAN - Yeni Kayıt



#### Ethernet Durumları

**Durum**  Aktif

**Güvenlik Bölgesi** LAN1-Zone (lan1-zone) ▼

**Arayüz** LAN1 ▼

**Ethernet Adı** em1 ▼

**Hız** autoselect ▼

**MTU** 1500

**Web Arayüzü Erişimi**  Aktif

**Cluster Üyeligi**  Pasif

**Cluster Ethernet Adı**

**Açıklama** LAN1

#### IPv4 Ayarları

Otomatik IPv4 AI

**IPv4 Adresi** IPv4 172.28.0.1/24

**DHCPv4 Havuzu Modu** Tüm İstemcilere IP Dağıt x ▼

**DHCPv4 Başlangıç** IPv4 172.28.0.10

**DHCPv4 Bitiş** IPv4 172.28.0.254

**DHCPv4 Ağ Geçidi** IPv4 172.28.0.1

**DHCPv4 Relay Adresi** IPv4

#### Seçenekler

MAC Eşleme  Anti-Spoof

Kayıt AI  Anons Yap

DHCPv6 Sunucusu  DHCPv4 Sunucusu

DHCPv6 Relay  DHCPv4 Relay

Managed Bayrağı  Other Bayrağı

#### IPv6 Ayarları

Otomatik IPv6 AI

**EUI64**  Pasif

**IPv6 Adresi** IPv6 ffff::1/8

**DHCPv6 Başlangıç** IPv6

**DHCPv6 Bitiş** IPv6

**DHCPv6 Relay Adresi** IPv6

## Cihazda log tutma ayarları

Logların, firewall üzerinde görüntülenmesi isteniyorsa sırasıyla, **Sistem Ayarları -> Log Ayarları** sayfasından logları **Cihazda tut** seçilir. Tüm logların cihazda tutulması isteniyorsa sayfanın en altında **Tümünü Seç**,

cihazda tut olarak ayarlanır.

| Log Ayarları  |   |  |
|---|---|--|
| HTTP(S) Sunucu Yönlendirme Logları                  | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| Kararlılık Servisi Logları                          | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| SSH ve Konsol Oturum Logları                        | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| VPN - SSL VPN Logları                               | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| VPN - PPTP / L2TP Logları                           | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| RADIUS Logları                                      | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| VPN - IPsec VPN Logları                             | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| DHCP Olay Logları                                   | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| Hotspot Logları                                     | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| Cluster Logları                                     | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| Web Filtreleme - İçerik ve Antivirüs Tarama Logları | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| Antispam Logları                                    | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| SSH Koruma Servisi Logları                          | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| Web Filtreleme - Sayfa Yasaklama Logları            | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| Web Erşim Logları                                   | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| Web Oturum Logları                                  | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| Web Arayüzü Logları                                 | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| Arayüze Erşimi Yasaklanan IPler                     | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| SSH Denetimi Logları                                | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| Web Uygulama Güvenliği Logları                      | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| AV, AppID, IPS, DDoS Logları                        | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| DNS Filtreleme Logları                              | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| PPP Logları   | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| PPP Debug Logları                                   | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| Sanal Kablo Logları                                 | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| Paket Filtreleme Logları                            | <input checked="" type="checkbox"/> Cihazda Tut | <input type="checkbox"/> Cihazda Tutma |
| Tümünü Seç  | <input type="checkbox"/> Cihazda Tut            | <input type="checkbox"/> Cihazda Tutma |

## Web Filtreleme Profilleri

Sistemde 3 milyon 600 binin üzerinde site ön tanımlı kategorilerde gelmektedir. Bu kategorilere ek, manuel olarak da izinli ve engelli sayfalar tanımlanabilmektedir. HTTPS adresleri de bu bölümden yasaklanabilmektedir. ( Facebook, Youtube vs.) Engelli adresler alanında eklenecek uzantılar da sistem tarafından yasaklanacaktır.

### Web Filtreleme Profilleri

| Ayarlar                             |            |  |  |  |  |
|-------------------------------------|------------|--|--|--|--|
| Dinamik Proxy Tünel Tespiti         | Devre Dışı |  |  |  |  |
| Engellenen Trafik Logları           | Aktif      |  |  |  |  |
| İzinli Trafik Logları               | Pasif      |  |  |  |  |
| Loglarda URL Parametrelerini Kaydet | Pasif      |  |  |  |  |

| Web Filtreleme Profilleri |       |                                 |                     |                     |   |
|---------------------------|-------|---------------------------------|---------------------|---------------------|---|
| #                         | Durum | Adı                             | Oluşturma Tarihi    | Güncelleme Tarihi   | İşlemler  |
| 1                         | Aktif | Genel Web Filtreleme Politikası | 31.10.2022 10:46:07 | 31.10.2022 10:46:07 | <a href="#">Düzenle</a> <a href="#">Sil</a> <a href="#">Yeni</a> <a href="#">Ekle</a> |

Düzenle butonuna tıklayarak ilgili profildeki yapılandırmalar ayarlanır ve kaydet butonu ile tanımlar uygulanır.

| Web Filtreleme Profilleri - Kayıt Düzenleme |  |   |   |  |  |      |      |   |   |       |       |   |   |                   |       |  |  |  |
|---|--|---|---|--|--|------|------|---|---|-------|-------|---|---|-------------------|-------|--|--|--|
| Adı   | Genel Web Filtreleme Politikası  |   |   |  |  |      |      |   |   |       |       |   |   |                   |       |  |  |  |
| Durum                                       | Aktif  |   |   |  |  |      |      |   |   |       |       |   |   |                   |       |  |  |  |
| İnceleme Yöntemi                            | Trafik Tabanlı   |   |   |  |  |      |      |   |   |       |       |   |   |                   |       |  |  |  |
| Servis Ayarları                             | <table><tr><td>HTTP</td><td>HTTP</td><td>X</td><td>+</td></tr><tr><td>HTTPS</td><td>HTTPS</td><td>X</td><td>+</td></tr><tr><td>Protokol Algılama</td><td colspan="4">Pasif</td></tr></table> |   |   |  |  | HTTP | HTTP | X | + | HTTPS | HTTPS | X | + | Protokol Algılama | Pasif |  |  |  |
| HTTP  | HTTP   | X | + |  |  |      |      |   |   |       |       |   |   |                   |       |  |  |  |
| HTTPS                                       | HTTPS  | X | + |  |  |      |      |   |   |       |       |   |   |                   |       |  |  |  |
| Protokol Algılama                           | Pasif  |   |   |  |  |      |      |   |   |       |       |   |   |                   |       |  |  |  |
| IP Adresi ile Gözlenen URL'leri Engelle     | Pasif  |   |   |  |  |      |      |   |   |       |       |   |   |                   |       |  |  |  |
| Antivirüs Taraması                          | Pasif  |   |   |  |  |      |      |   |   |       |       |   |   |                   |       |  |  |  |
| İçerik Filtreleme                           | Pasif  |   |   |  |  |      |      |   |   |       |       |   |   |                   |       |  |  |  |
| Varsayılan Erşim İzni                       | Varsayılan Tüm Siteler Serbest   |   |   |  |  |      |      |   |   |       |       |   |   |                   |       |  |  |  |
| Aktif Saat Dilimi                           | Şablonları düzenlemek için Zaman Dilimleri Sayfasını Kullanabilirsiniz.  |   |   |  |  |      |      |   |   |       |       |   |   |                   |       |  |  |  |
| Yönlendirme Adresi                          | Varsayılan Yönlendirme   |   |   |  |  |      |      |   |   |       |       |   |   |                   |       |  |  |  |

| #                        | Kategori Adı     | Tür        | İşlemler         |
|--------------------------|------------------|------------|------------------|
| <input type="checkbox"/> | Agresif          | On Tanımlı | İzin Ver Engelle |
| <input type="checkbox"/> | Alışveriş Yapmak | On Tanımlı | İzin Ver Engelle |
| <input type="checkbox"/> | Alkol            | On Tanımlı | İzin Ver Engelle |
| <input type="checkbox"/> | Anlık Mesajlaşma | On Tanımlı | İzin Ver Engelle |
| <input type="checkbox"/> | Anonim Ypn       | On Tanımlı | İzin Ver Engelle |
| <input type="checkbox"/> | Anti Spyware     | On Tanımlı | İzin Ver Engelle |
| <input type="checkbox"/> | Araba            | On Tanımlı | İzin Ver Engelle |
| <input type="checkbox"/> | Arama Motorları  | On Tanımlı | İzin Ver Engelle |
| <input type="checkbox"/> | Askeri           | On Tanımlı | İzin Ver Engelle |

| # | Durum | Adres Durumu | Filtreleme Türü          | Eşleme Türü | İfade        | İşlemler         |
|---|-------|--------------|--------------------------|-------------|--------------|------------------|
| 1 | Aktif | Engelli      | HTTP ve HTTPS Filtreleme | Alan Adı    | facebook.com | İzin Ver Engelle |

Web Filtreleme > Kategori Yönetimi sayfasında manuel olarak bir kategori oluşturulabilir ve Web Filtreleme Profilinde bu kategori izinli/engelli olarak kullanılabilir.

| Ön Tanımlı Kategoriler |                 | Kullanıcı Tanımlı Kategoriler |  |
|------------------------|-----------------|-------------------------------|--|
| #                      | Kategori Adı    | İşlemler                      |  |
| 1                      | Manuel Kategori | İzinli Engelli                |  |

| # | İfade        | Eşleme Türü | Filtreleme Türü          | İşlemler         |
|---|--------------|-------------|--------------------------|------------------|
| 1 | abc.com      | Alan Adı    | HTTP ve HTTPS Filtreleme | İzin Ver Engelle |
| 2 | facebook.com | Alan Adı    | HTTP ve HTTPS Filtreleme | İzin Ver Engelle |

| #                        | Kategori Adı    | Tür               | İşlemler         |
|--------------------------|-----------------|-------------------|------------------|
| <input type="checkbox"/> | Manuel Kategori | Kullanıcı Tanımlı | İzin Ver Engelle |
| <input type="checkbox"/> | Siyaset         | On Tanımlı        | İzin Ver Engelle |
| <input type="checkbox"/> | Taki            | On Tanımlı        | İzin Ver Engelle |
| <input type="checkbox"/> | Spam            | On Tanımlı        | İzin Ver Engelle |
| <input type="checkbox"/> | Radio-TV        | On Tanımlı        | İzin Ver Engelle |
| <input type="checkbox"/> | Sigorta         | On Tanımlı        | İzin Ver Engelle |
| <input type="checkbox"/> | Blog            | On Tanımlı        | İzin Ver Engelle |
| <input type="checkbox"/> | Tatil           | On Tanımlı        | İzin Ver Engelle |
| <input type="checkbox"/> | Reklamlar       | On Tanımlı        | İzin Ver Engelle |

| # | Durum | Adres Durumu | Filtreleme Türü          | Eşleme Türü | İfade        | İşlemler         |
|---|-------|--------------|--------------------------|-------------|--------------|------------------|
| 1 | Aktif | Engelli      | HTTP ve HTTPS Filtreleme | Alan Adı    | facebook.com | İzin Ver Engelle |

## DNS Ayarları

DNS (Domain Name System), internet ortamında alan adından IP'ye, IP'den alan adına dönüşümlerini gerçekleştiren sistemdir. Sistemin kullandığı DNS bilgileridir. Yerel ağdaki bilgisayarlara da DHCP servisi üzerinden DNS bilgileri dağıtılır.

Antikor da DNS ayarı için sırasıyla **Sistem Ayarları -> DNS Ayarları** sayfasında ekle butonuna tıklanır.

Adres Ailesi  IPv4  IPv6

Dns Adresi IPv4 8.8.8.8

Açıklama DNS Sunucusu

İptal

Kaydet

DNS Ayarları

Yenile Ekle

XLS CSV PDF

Göster/Gizle

Sayfa Başı Kayıt Sayısı

Tümünü

Filtrele

Filtreyi Temizle

| Sıra | Dns Adresi | Açıklama     | İşlemler    |
|------|------------|--------------|-------------|
| 0    | 8.8.8.8    | DNS Sunucusu | Düzenle Sil |

## DNS Filtreleme Profilleri

Sistemde 3 milyon 600 binin üzerinde site ön tanımlı kategorilerde gelmektedir. Bu kategorilere ek, manuel olarak da izinli ve engelli sayfalar tanımlanabilmektedir

DNS Filtreleme Profilleri

| # | Adı   | Açıklama | Ötipe Ayarı | Ötipe Seçimler | İşlemler    |
|---|-------|----------|-------------|----------------|-------------|
| 1 | Genel |          | Engelli     |                | Düzenle Sil |

Düzenle butonuna tıklayarak ilgili profildeki yapılandırmalar ayarlanır ve kaydet butonu ile tanımlar uygulanır.

DNS Filtreleme Profilleri - Kayıt Düzeltme

Yenile

Adı Genel

Açıklama

Aktif Saat Dilimi

Şablonları düzenlemek için Zaman Dilimleri Sayfasını Kullanabilirsiniz.

DNS Tünel Engelle

Engelli

Tünel Filtre Ayarlarını Düzeltilir

Kaydet

| #                        | Kategori Adı     | Tür        | İşlemler         |
|--------------------------|------------------|------------|------------------|
| <input type="checkbox"/> | Ağresit          | Ön Tanımlı | İzin Ver Engelle |
| <input type="checkbox"/> | Alışveriş Yapmak | Ön Tanımlı | İzin Ver Engelle |
| <input type="checkbox"/> | Alkol            | Ön Tanımlı | İzin Ver Engelle |
| <input type="checkbox"/> | Anlık Mesajlaşma | Ön Tanımlı | İzin Ver Engelle |
| <input type="checkbox"/> | Anonim Uçun      | Ön Tanımlı | İzin Ver Engelli |
| <input type="checkbox"/> | Arızi Spyware    | Ön Tanımlı | İzin Ver Engelle |
| <input type="checkbox"/> | Araba            | Ön Tanımlı | İzin Ver Engelle |
| <input type="checkbox"/> | Arama Motorları  | Ön Tanımlı | İzin Ver Engelle |
| <input type="checkbox"/> | Askeri           | Ön Tanımlı | İzin Ver Engelle |

| # | Adres Durumu | İfade        | İşlemler    |
|---|--------------|--------------|-------------|
| 1 | Engelli      | haberler.com | Düzenle Sil |

Web Filtreleme > Kategori Yönetimi sayfasında manuel olarak bir kategori oluşturulabilir ve DNS Filtreleme Profiline bu kategori izinli/engelli olarak kullanılabilir.

| Ön Tanımlı Kategoriler   |                 | Kullanıcı Tanımlı Kategoriler  |              |              |                          |             |
|--|-----------------|--|--------------|--------------|--------------------------|-------------|
| Yeni Ekle  |                 | Kapat Güncelle Yeni Ekle   |              |              |                          |             |
| Göster/Gizle Sayfa Başlı Kayıt Sayısı 25 Tamam Filtrele Filtreyi Temizle |                 | Göster/Gizle Sayfa Başlı Kayıt Sayısı 25 Tamam Filtrele Filtreyi Temizle |              |              |                          |             |
| #  | Kategori Adı    | #  | İfade        | Eşleşme Türü | Filtreleme Türü          | İşlemler    |
| 1  | Manuel Kategori | 1  | abc.com      | Alan Adı     | HTTP ve HTTPS Filtreleme | Düzenle Sil |
|  |                 | 2  | facebook.com | Alan Adı     | HTTP ve HTTPS Filtreleme | Düzenle Sil |

| Kategoriler              |                                      |                   |                  |
|--------------------------|--------------------------------------|-------------------|------------------|
| Tümünü Seç               | Toplu İşlem Seçiniz İzin Ver Engelle |                   |                  |
| #                        | Kategori Adı                         | Tür               | İşlemler         |
| <input type="checkbox"/> | Manuel Kategori                      | Kullanıcı Tanımlı | İzin Ver Engelle |
| <input type="checkbox"/> | Siyaset                              | Ön Tanımlı        | İzin Ver Engelle |
| <input type="checkbox"/> | Taki                                 | Ön Tanımlı        | İzin Ver Engelle |
| <input type="checkbox"/> | Spam                                 | Ön Tanımlı        | İzin Ver Engelle |
| <input type="checkbox"/> | Radio-TV                             | Ön Tanımlı        | İzin Ver Engelle |
| <input type="checkbox"/> | Sigorta                              | Ön Tanımlı        | İzin Ver Engelle |
| <input type="checkbox"/> | Blog                                 | Ön Tanımlı        | İzin Ver Engelle |
| <input type="checkbox"/> | Tatil                                | Ön Tanımlı        | İzin Ver Engelle |
| <input type="checkbox"/> | Reklamlar                            | Ön Tanımlı        | İzin Ver Engelle |

| Adresler   |              |              |             |
|--|--------------|--------------|-------------|
| Yeni Ekle  |              |              |             |
| Göster/Gizle Sayfa Başlı Kayıt Sayısı 10 Tamam Filtrele Filtreyi Temizle |              |              |             |
| #  | Adres Durumu | İfade        | İşlemler    |
| 1  | Engelli      | haberler.com | Düzenle Sil |

## Uygulama Kontrolü Profilleri

Uygulama kontrolü için profillerin belirlendiği sayfadır. Yeni profil girmek için Ekle butonuna tıklanmalıdır ve kaydet butonuna basılır.

### Uygulama Kontrolü Profilleri

| Uygulama Kontrolü Profilleri   |       |     |          |                  |                   |          |
|--|-------|-----|----------|------------------|-------------------|----------|
| Yeni Ekle  |       |     |          |                  |                   |          |
| Göster/Gizle Sayfa Başlı Kayıt Sayısı 25 Tamam Filtrele Filtreyi Temizle |       |     |          |                  |                   |          |
| #  | Durum | Adı | Açıklama | Oluşturma Tarihi | Güncelleme Tarihi | İşlemler |
|  |       |     |          |                  |                   |          |



Uygulama Kontrolü Profilleri - Kayıt Düzelme < Profiller

Durum Aktif

Adı Uygulama Kontrolü Profili

İzinli Uygulamalar Select...

Engelli Uygulamalar Facebook x Twitter x Instagram x LinkedIn x X |

Bağıntılı Limitli Uygulamalar Select...

QoS Kuyruğu

Açıklama Uygulama Kontrolü Profili

Kaydet

| Kategoriler   | İzin Ver   | Engelle  | QoS   |   |
|---|--|--|---|---|
| <input type="checkbox"/> instant messaging          | <span style="background-color: green; color: white; padding: 2px 5px;">On Tanımlı</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">İzin Ver</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">Engelle</span>   | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">QoS</span> |
| <input type="checkbox"/> messaging queues           | <span style="background-color: green; color: white; padding: 2px 5px;">On Tanımlı</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">İzin Ver</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">Engelle</span>   | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">QoS</span> |
| <input type="checkbox"/> mobile application         | <span style="background-color: green; color: white; padding: 2px 5px;">On Tanımlı</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">İzin Ver</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">Engelle</span>   | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">QoS</span> |
| <input type="checkbox"/> multimedia (music/audio)   | <span style="background-color: green; color: white; padding: 2px 5px;">On Tanımlı</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">İzin Ver</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">Engelle</span>   | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">QoS</span> |
| <input type="checkbox"/> multimedia (other)         | <span style="background-color: green; color: white; padding: 2px 5px;">On Tanımlı</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">İzin Ver</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">Engelle</span>   | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">QoS</span> |
| <input type="checkbox"/> multimedia (TV/video)      | <span style="background-color: green; color: white; padding: 2px 5px;">On Tanımlı</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">İzin Ver</span> | <span style="background-color: green; color: white; padding: 2px 5px;">Engelle</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">QoS</span> |
| <input type="checkbox"/> network protocols/services | <span style="background-color: green; color: white; padding: 2px 5px;">On Tanımlı</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">İzin Ver</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">Engelle</span>   | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">QoS</span> |
| <input type="checkbox"/> network utilities          | <span style="background-color: green; color: white; padding: 2px 5px;">On Tanımlı</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">İzin Ver</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">Engelle</span>   | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">QoS</span> |
| <input type="checkbox"/> news                       | <span style="background-color: green; color: white; padding: 2px 5px;">On Tanımlı</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">İzin Ver</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">Engelle</span>   | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">QoS</span> |
| <input type="checkbox"/> PACS                       | <span style="background-color: green; color: white; padding: 2px 5px;">On Tanımlı</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">İzin Ver</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">Engelle</span>   | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">QoS</span> |
| <input type="checkbox"/> peer to peer               | <span style="background-color: green; color: white; padding: 2px 5px;">On Tanımlı</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">İzin Ver</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">Engelle</span>   | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">QoS</span> |

Güvenlik Ayarları > Uygulama Kategori Yönetimi sayfasında manuel olarak bir kategori oluşturabilir ve Uygulama Kontrolü Profillerinde bu kategoriye izinli/engelli olarak kullanabilirsiniz.

Uygulama Kategori Yönetimi - Yeni Kayıt x

Kategori Adı

Uygulama Adı

İptal Kaydet

Uygulama Kontrolü Profilleri - Kayıt Düzelme < Profiller

Durum Aktif

Adı Uygulama Kontrolü Profili

İzinli Uygulamalar Select...

Engelli Uygulamalar Facebook x Twitter x Instagram x LinkedIn x X |

Bağıntılı Limitli Uygulamalar Select...

QoS Kuyruğu

Açıklama Uygulama Kontrolü Profili

Kaydet

| Kategoriler              |                  | Toplu İşlem Seçiniz  |  |   |   |
|--------------------------|------------------|--|--|---|---|
| #                        | Kategori Adı     | İl TÜR   | İşlemler   |   |   |
| <input type="checkbox"/> | ad portal        | <span style="background-color: green; color: white; padding: 2px 5px;">On Tanımlı</span>         | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">İzin Ver</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">Engelle</span>   | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">QoS</span> |
| <input type="checkbox"/> | anonymizer/proxy | <span style="background-color: green; color: white; padding: 2px 5px;">On Tanımlı</span>         | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">İzin Ver</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">Engelle</span>   | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">QoS</span> |
| <input type="checkbox"/> | AppID-Manuel     | <span style="background-color: orange; color: white; padding: 2px 5px;">Kullanıcı Tanımlı</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">İzin Ver</span> | <span style="background-color: green; color: white; padding: 2px 5px;">Engelle</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">QoS</span> |
| <input type="checkbox"/> | browser plugin   | <span style="background-color: green; color: white; padding: 2px 5px;">On Tanımlı</span>         | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">İzin Ver</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">Engelle</span>   | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">QoS</span> |
| <input type="checkbox"/> | business         | <span style="background-color: green; color: white; padding: 2px 5px;">On Tanımlı</span>         | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">İzin Ver</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">Engelle</span>   | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">QoS</span> |
| <input type="checkbox"/> | collaboration    | <span style="background-color: green; color: white; padding: 2px 5px;">On Tanımlı</span>         | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">İzin Ver</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">Engelle</span>   | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">QoS</span> |
| <input type="checkbox"/> | database         | <span style="background-color: green; color: white; padding: 2px 5px;">On Tanımlı</span>         | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">İzin Ver</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">Engelle</span>   | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">QoS</span> |
| <input type="checkbox"/> | download manager | <span style="background-color: green; color: white; padding: 2px 5px;">On Tanımlı</span>         | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">İzin Ver</span> | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">Engelle</span>   | <span style="background-color: #ccc; color: #000; padding: 2px 5px;">QoS</span> |

Copyright ePati © 2016 - 2022 antikor v2 NGFW Staging - STAGING antikor v2 NGFW Staging

## IPS Profilleri

IPS, saldırı tespit ve önleme sistemidir. İnternet trafiğinden geçen paketleri inceler ve imzaları ile eşleşen trafiği tespit edip loglayabilir ve engelleyebilir.

## IPS Profilleri

| ID | Durum | Adı                   | Açıklama              | Ön Tanımlı İmzalar | Kullanıcı Tanımlı İmzalar | Oluşturma Tarihi    | Güncelleme Tarihi   | İşlemler   |
|----|-------|-----------------------|-----------------------|--------------------|---------------------------|---------------------|---------------------|--|
| 1  | Aktif | Balanced IPS Drop     | Balanced IPS Drop     | 8068               | 0                         | 31.10.2022 10:46:07 | 21.11.2022 13:12:36 | <a href="#">Düzenle</a> <a href="#">Sil</a> <a href="#">Ön Tanımlı İmzalar</a> <a href="#">Kullanıcı Tanımlı İmzalar</a> |
| 2  | Pasif | Connectivity IPS Drop | Connectivity IPS Drop | 366                | 0                         | 31.10.2022 10:46:08 | 21.11.2022 13:12:40 | <a href="#">Düzenle</a> <a href="#">Sil</a> <a href="#">Ön Tanımlı İmzalar</a> <a href="#">Kullanıcı Tanımlı İmzalar</a> |
| 3  | Pasif | Max Detect IPS Drop   | Max Detect IPS Drop   | 32318              | 0                         | 31.10.2022 10:46:08 | 21.11.2022 13:12:43 | <a href="#">Düzenle</a> <a href="#">Sil</a> <a href="#">Ön Tanımlı İmzalar</a> <a href="#">Kullanıcı Tanımlı İmzalar</a> |
| 4  | Pasif | Security IPS Drop     | Security IPS Drop     | 14747              | 0                         | 31.10.2022 10:46:08 | 21.11.2022 13:12:47 | <a href="#">Düzenle</a> <a href="#">Sil</a> <a href="#">Ön Tanımlı İmzalar</a> <a href="#">Kullanıcı Tanımlı İmzalar</a> |

Aşağıdaki görüntüde kırmızı alan ile belirlenmiş Ön Tanımlı İmzalar butonuna tıklanıldığında, imzaların detayları ve imzalara özel "İşlemler" belirlenebilmektedir.

| ID | Durum | Adı               | Açıklama          | Ön Tanımlı İmzalar | Kullanıcı Tanımlı İmzalar | Oluşturma Tarihi    | Güncelleme Tarihi   | İşlemler   |
|----|-------|-------------------|-------------------|--------------------|---------------------------|---------------------|---------------------|--|
| 1  | Aktif | Balanced IPS Drop | Balanced IPS Drop | 8068               | 0                         | 31.10.2022 10:46:07 | 21.11.2022 13:12:36 | <a href="#">Düzenle</a> <a href="#">Sil</a> <a href="#">Ön Tanımlı İmzalar</a> <a href="#">Kullanıcı Tanımlı İmzalar</a> |

### IPS Profilleri

[Geri Dön](#)

Filtreler

Sınıf Tipi: Seçiniz...  
İmza Durumu: Seçiniz...  
Platform: Seçiniz...  
İmza Gösterimi: Devrede

CVE: Seçiniz...  
Kategori: Seçiniz...  
Politika: Seçiniz...

Akış: Seçiniz...  
MS Zafiyeti: Seçiniz...  
Önem Derecesi: Seçiniz...

[Filtreleri Uygula](#)

İmzalar - 8655

Tümünü Seç

# İmza Adı Etiketler İşlemler

BROWSER-CHROME Google Chrome blink webaudio module use after free attempt  
Sınıf Tipi: attempted-user | CVE: CVE-2019-13720 | Akış: to\_client | İmza Durumu: default-enabled | Kategori: browser-chrome  
Platform: Linux | Politika: balanced-ips-drop | Politika: connectivity-ips-drop | Politika: max-detect-ips-drop | Politika: security-ips-drop  
Önem Derecesi: high

Engelle

Güvenlik Ayarları > IPS Kategori Yönetimi sayfasında manuel olarak bir kategori oluşturulabilir ve IPS Profilleri sayfasında bu kategoriye izinli/engelli olarak kullanabiliriz.

### Kategoriler - Yeni Kayıt



Kaynak

Elle Veri Girişi

Kategori Adı

Manuel IPS

Varsayılan kapalı imzaları da getir

[İptal](#)

[Kaydet](#)

|   |       |            |            |   |   |                     |                     |  |
|---|-------|------------|------------|---|---|---------------------|---------------------|--|
| 1 | Aktif | manuel-ips | manuel-ips | 0 | 0 | 21.11.2022 15:49:12 | 21.11.2022 15:49:12 | <a href="#">Düzenle</a> <a href="#">Sil</a> <a href="#">Ön Tanımlı İmzalar</a> <a href="#">Kullanıcı Tanımlı İmzalar</a> |
|---|-------|------------|------------|---|---|---------------------|---------------------|--|

Filtreler

Kullanıcı Tanımı  
Manuel IPS

İmza Gösterimi  
Devrede

Kullanıcı Tanımı: Manuel IPS

Filtreleri Uygula

## Güvenlik Kuralları

Ağdan çıkan paketlerin veya ağa gelen paketlerin izin veya engel kuralları oluşturulduğu alanlardır. Kuralların stateless sadece kaynak veya hedef adrese göre yazılabileceği gibi, statefull uçtan uca trafik inceleme yöntemiyle de yazılabilmektedir. Trafik incelemede syn, ack, fin gibi bayraklar da incelenebilmektedir. Kural için Hit Sayısı, Toplam Byte ve Geçerli State Sayısı da incelenebilmektedir. Ekle butonuna basıldıktan sonra, açılan pencerede işlemler gerçekleştirilir.

Antikor, ilk kurulumdan sonra **Güvenlik Duvarı Ayarlarında Varsayılan Kural Engelli** olarak gelecektir. Varsayılan Kural engelli olarak devam edilecekse, istemcilerin internete çıkabilmesi için güvenlik kuralı yazılması gerekecektir. Varsayılan kural izinli olarak ayarlanacaksa ek bir güvenlik kuralı yazmamıza ihtiyaç bulunmamaktadır.

Güvenlik Politikası

Varsayılan Kural  İzinli  Engelli

Varsayılan Kuralı Logla  Açık  Kapalı

Ağ Geçidi Saklama (Stealth) Modu  Açık  Kapalı

Multicast Akış İzni  Açık  Kapalı

Anti-Spoof Modu  Simetrik  Asimetrik

TCP Paketleri İçin İnceleme Yöntemi

TCP Oturum Zaman Aşımı  saniye

UDP Oturum Zaman Aşımı  saniye

ICMP Oturum Zaman Aşımı  saniye

Diğer Oturum Zaman Aşımı  saniye

## Güvenlik Kuralları Paketleri

Kurulum sonrası, varsayılanda bir kural seti gelecektir. Kuralları bu set veya oluşturacağımız başka setler içerisinde yazabiliriz. Resimde örnek olarak bir kural seti oluşturulmuştur.

Güvenlik Kuralları

Güvenlik Kuralları Paketleri

Yeni Ekle

İzle

Yeni Ekle

Sayfa Başı Kayıt Sayısı 25 Tanımı Filtreli Filtre Temele

| Sıra | Durum | Adı              | Kaynak Adres                | Hedef Adres                 | Sanal Kabiolar | İşlemler   |
|------|-------|------------------|-----------------------------|-----------------------------|----------------|--|
| 1    | Aktif | Ana Kural Seti   | [192.168.1.1] [0.0.0.0] [0] | [192.168.1.1] [0.0.0.0] [0] |                | [Kuralı Sil] [Kuralı Ekle] [Kuralı Sil] [Kuralı Ekle] [Kuralı Sil] [Kuralı Ekle] |
| 2    | Pasif | Yedek Kural Seti | [192.168.1.1] [0.0.0.0] [0] | [192.168.1.1] [0.0.0.0] [0] |                | [Kuralı Sil] [Kuralı Ekle] [Kuralı Sil] [Kuralı Ekle] [Kuralı Sil] [Kuralı Ekle] |

[1] [2] [3] [4] [5] [6] [7] [8] [9] [10]

[Sil]

## Güvenlik Kuralları Yeni Kayıt

Ana Kural Setinde **Kurallar** butonuna tıkladıktan sonra açılan sayfada **ekle** butonu ile yeni kural oluşturulur ve tanımlar uygulanır.

Güvenlik Kuralları - Yeni Kayıt

Genel Kurallar

Grubu: GENELKURALLAR GRUBU

Sıra No:

Durum:  Aktif  Pasif

İşlem: Engelle  Reddet  İzin Ver

Loglama:  Açık  Kapat

Ağ Geçidi: Varsayılan

Açıklama: LAN1 İnternet Kuralı

İnceleme Yöntemi:  STATEFULL  STATELESS

IP Kuralları

Kaynak Güvenlik Bölgesi:  Temu

Kaynak Adres:  Listedekiler Hariç

Hedef Güvenlik Bölgesi:  Temu

Hedef Adres:  Listedekiler Hariç

Servisler:  HTTP  HTTPS  DNS

Zaman Dilimleri:  Seçiniz

Güvenlik Profilleri

Du5 / Bağlantı Limitleme:  Pasif

Web Filtreleme:  Aktif Genel Web Filtreleme Politikası

Antivirus:  Pasif

DNS Filtreleme:  Aktif Genel

Uygulama Kontrolü:  Aktif Uygulama Kontrolü Profili

IPS:  Aktif Balanced IPS Drop

SSH Denetimi:  Pasif

WAF:  Pasif

NAT

Kapat  Çıkış Adres  NAT Havuzu  Global NAT

## Genel Kuralllar

| ALAN             | AÇIKLAMA  |
|------------------|---|
| Sıra No          | Kuralın sıra numarasını belirler veya kuralları aşağı yukarı taşıyarakta sıra numarası düzenlenebilir |
| Durum            | Aktif ya da pasif olma durumu seçilir.  |
| İşlem            | İşlem türü seçilir.   |
| Trafiği Logla    | Buton aktif edilirse loglar cihaz üzerinde tutulacaktır.  |
| Ağ Geçidi        | Kural için ağ geçidi seçilir. Defaultta varsayılan ağ geçidini kullanır.                              |
| Paket Yönü       | Kuralın hangi yönde çalışacağı seçilir.   |
| Açıklama         | Kuralların açıklamalarının yazıldığı bölümdür.  |
| İnceleme Yöntemi | Statefull veya stateless inceleme yöntemi seçilir.  |

## NAT

| ALAN        | AÇIKLAMA  |
|-------------|---|
| Kapalı      | Bu seçenekte istemciler NAT işlemi uygulanmayacaktır.   |
| Çıkış Adres | Bu seçenekte istemciler, internete doğru trafiği Firewall'un kullanmış olduğu WAN IP adresiyle yapacaktır.  |
| NAT Havuzu  | Bu seçenekte istemciler, sistem yöneticisinin belirlemiş olduğu NAT havuzu ile internet trafiği yapacaktır. (NAT Havuzları sayfasına erişim için; NAT Yapılandırması - NAT Havuzları) |
| Global NAT  | Bu seçenekte istemciler, Global NAT sayfasında tanımlanmış IP adresiyle internet trafiği yapacaktır. (Global NAT sayfasına erişim için; NAT Yapılandırması - Global NAT)              |

## IP Kuralları

| ALAN                          | AÇIKLAMA   |
|-------------------------------|--|
| Kaynak<br>Güvenlik<br>Bölgesi | Kaynak IP adresi için güvenlik bölgesi seçimi yapılır.   |
| Kaynak Adres                  | Kuralın kapsanacağı kaynak IP adresleri yazılır. (Not: Listedikiler hariç butonuna tıklandığında Kaynak bölüme yazılan IP adresi hariç herkesi kapsayacaktır.) |
| Hedef<br>Güvenlik<br>Bölgesi  | Hedef Adres için güvenlik bölgesi seçimi yapılır.  |
| Hedef Adres                   | Kuralın kapsanacağı hedef IP adresi yazılır.(Not: Listedikiler hariç butonuna tıklandığında hedef bölüme yazılan IP adresi hariç herkesi kapsayacaktır.)       |
| Servisler                     | Kuralda izin verilecek protokoller seçilir. HTTP, HTTPS, DNS gibi.   |

### Zaman Dilimleri

| ALAN           | AÇIKLAMA   |
|----------------|--|
| Saat<br>Dilimi | Bir hafta içerisinde hangi gün içerisinde ve gün içerisinde hangi saatte girilen güvenlik kuralının çalışacağı belirlenir. |

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](http://www.epati.com.tr)  
[bilgi@epati.com.tr](mailto:bilgi@epati.com.tr)  
+90 324 361 02 33  
+90 324 361 02 39

