

epati

1.03. Kurulum Kılavuzu

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı
Kılavuzlar

1.03. 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 Siber Güvenlik Teknolojileri tarafından yapıştırılmış 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.

Fiziksel ve Mantıksal Güvenlik

1. Antikor kurulu donanım, güvenliği sağlanmış olan sistem odasında bulunmalıdır. Odaya giriş ve çıkışlar yalnızca yetkili kişiler tarafından olmalıdır.
2. Antikor'un yedekleri düzenli olarak alınarak saklanmalıdır.
3. Antikor kurulu donanım üzerinde USB portları bulunuyorsa devre dışı bırakılmalıdır.
4. Antikor kurulu donanımının güç kaynağı, ethernet kabloları vb. parçaların sağlamlığı kontrol edilmelidir.
5. Antikor'a erişim sağlayacak kişilerin parola bilgileri admin parolası ile aynı olmamalı ve yetkileri kısıtlanmalıdır.
6. Antikor'a erişim sağlayan kullanıcılar, belirli zaman dilimlerinde parola değişikliği yapmalıdır.
7. Antikor'a erişim sağlayan sistem yöneticilerinin kullanıcı adı ve parola bilgilerinin güvenliği kendilerine aittir. İlgili sistem yöneticisi, bu yazılımı kullanarak, kullanıcı adı ve parola bilgilerinin güvenliğinin korunması ile ilgili gerekli önemleri aldığını kabul etmiş sayılır. Epati Siber Güvenlik Teknolojileri kullanıcı adı ve parola bilgilerinin güvenliğinden kaynaklanabilecek doğrudan veya dolaylı bir zarar doğması halinde borç, sorumluluk ve mükellefiyet kabul etmemektedir.

Donanım İhtiyaçları

Bilgisayarlar en yavaş bileşene göre çalışırlar. Aşağıdaki yazılarda da görülebileceği üzere her bir bileşen kendi içerisinde çok parametre taşımaktadır. Güvenlik Duvarlarında en önemli bileşenler CPU, Ram Hızı, Ethernet, Disktir. Bu bileşenler cihazdan geçen internet trafiğini belirler. Güvenlik Duvarlarında Throughput'u cihaza girişten(ethernet), paketlerin işlendiği yer olan (CPU-Ram) değerleri hatta kendine bağlı switch ve İnternet Bant

Genişliğine kadar tüm çevre bileşenleri etkilidir.

Tümleşik Siber Güvenlik Sistemi Antikor için gereken bileşenler;

1. En az 8 Core Xeon (mantıksal çekirdekler hariç)
2. En az 32 GB DDR4 2133 Mhz Ram
3. Multi queue (çok kuyruklu) ethernet kartı
4. En az 256GB SSD

Ethernet (Ağ) Kartı

Güvenlik Duvarlarında Ethernet Kartları kesinlikle multi queue (çok kuyruklu) ethernet kartları olmak zorundadır. Bu sayede Ethernet driverları birden fazla core üzerine yayılabilmektedir.

Tavsiye edilen ethernet kartları aşağıdaki gibidir.

- Intel i210 ethernet kartı 2 port 1Gbit/s (KOBİ lerde)
<https://www.intel.com/content/dam/www/public/us/en/documents/datasheets/i210-ethernet-controller-datasheet.pdf>
- Intel'in i350 ethernet kartı 4 port 1Gbit/s olup, her bir portta 8 TX/RX yola sahip, bu da toplam 32 core'a kadar ethernet driverin yayılacağı anlamına gelir. (Orta büyüklükteki işletmelerde)
<https://www.intel.com/content/www/us/en/products/sku/84805/intel-ethernet-server-adapter-i350t4v2/specifications.html>
- Yine Intel'in başka 2 portlu Intel x540 modelleri 10 Gbit/s olup her bir portu 128 kuyruğa dağıtabiliyor. (Büyük işletmelerde) <http://www.intel.com/content/dam/www/public/us/en/documents/datasheets/ethernet-x540-datasheet.pdf>
- Yine Intel'in başka 4 portlu Intel x710T modelleri 10 Gbit/s (Büyük işletmelerde)
<http://www.intel.com/content/www/us/en/support/network-and-i-o/ethernet-products/intel-10-gigabit-server-adapters/intel-ethernet-converged-network-adapter-x710-series/intel-ethernet-converged-network-adapter-x710-t4.html>

Disk (Depolama)

Kullanılacak Programın Disk ile işi çok oluyorsa ve devamlı diskden okuma/yazma yapıyorsa Disklerin önemi çok büyüktür. Diskler de kendi içinde büyüklük ve hıza göre ayrılırlar. Disk çeşitleri olarak SATA Diskler, SAS Diskler, SSD Diskler, şimdi de SSD NVMe Diskler piyasadadır.

Sistem yöneticisi bir servisi veya sistemi devreye alırken disk'le ilgili ihtiyaçlarını düşünürken sadece kapasite öngörüsünde bulunurlar. Doğal olarak orta ve uzun vadede yük artıkça dar boğazlar oluşmaya ve performans kaybı gözlemlenir. Bunun yegâne sebebi sistemin ihtiyaç duyacağı toplam IOPS ve Throughput doğru öngörülememesi veya hiç hesaba katılmamasıdır.

Peki nedir bu değerler ve ne işe yararlar?

IOPS (Input/output operations per second) adından da anlaşılacağı gibi bir diskin saniyede yapabileceği maksimum yazma veya okuma sayısıdır. Throughput ise belli bir zaman aralığında yapılan işi temsil eder. Genelde 1 saniyede kaç MB yazdığı veya okuyabildiği değerdir. Örneğin kamera programı ise daha çok boyut önemlidir. Programın diske yazma hızı sabittir. Bu sunucunun toplam iş yükünün %10'i okuma, %90'si yazma gibi düşünebiliriz. Genelde kamera görüntüleri yazılır. Çekilmiş görüntülere bakacağımızda okuma işlemi olur.

Başka bir örnek olarak FTP dosya sunucumuzu ele alalım. Bu sunucunun toplam iş yükünün %80'i okuma, %20'si yazma gibi düşünebiliriz. Genelde insanlar dosya sunucusundan indirme yaptığı için okuma, biz dosya atarsak yazma işlemi olur.

Fonksiyonel IOPS = ((Toplam IOPS *yazma yüzdesi)/(Raid penalty))+(Toplam IOPS *okuma yüzdesi)

Not: Formülde RAID 0 Raid Penalty 1, RAID 1 Raid Penalty 2, RAID 5 Raid Penalty 4, RAID 6 Raid Penalty 6 olarak hesaplanır. Görüldüğü üzere aynı diskler farklı raid yapıları ve okuma ve yazma oranlarıyla tamamen farklı sonuçlar vermektedir. Antikor içerisinde Veritabanı işlemleri ve Loglama olduğundan kapasitesi en az 256GB olan SSD tercih edilmelidir.

1. Kurulumun gerçekleştirileceği cihaz için, network yapısına uygun olarak ethernet kartı takılmalıdır veya sanal kurulum gerçekleştirilecek ise ethernet kartları açılmalıdır . örneğin, WAN, LAN ve DMZ kullanılacak ise 3 portlu ethernet kartı veya 3 tane ayrı ethernet kartları takılmalıdır. Sanallaştırma üzerinden kurulum yapılacak ise 3 tane ethernet portu açılmalıdır. Kurulum tamamlandıktan sonra ethernet kartı eklenmesi veya çıkarılması yapılmamalıdır.

2. Kurulumun gerçekleştirileceği cihaz için **Last State** ayarı sürekli açık yapılmalıdır. Bunun için BIOS ayarları kontrol edilmelidir.

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

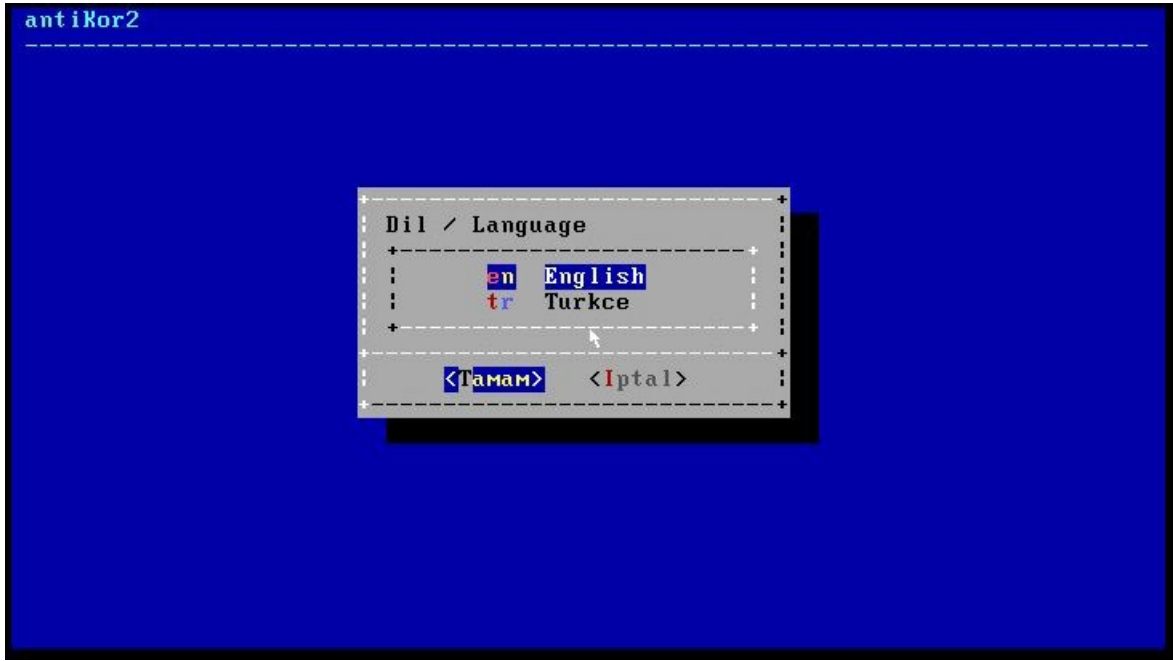
BTX loader 1.00 BTX version is 1.02
Consoles: internal video/keyboard
BIOS CD is cd0
BIOS drive C: is disk0
BIOS 639kB/1047488kB available memory

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 " yazdığı anda kurulum başladığını belirtmektedir.

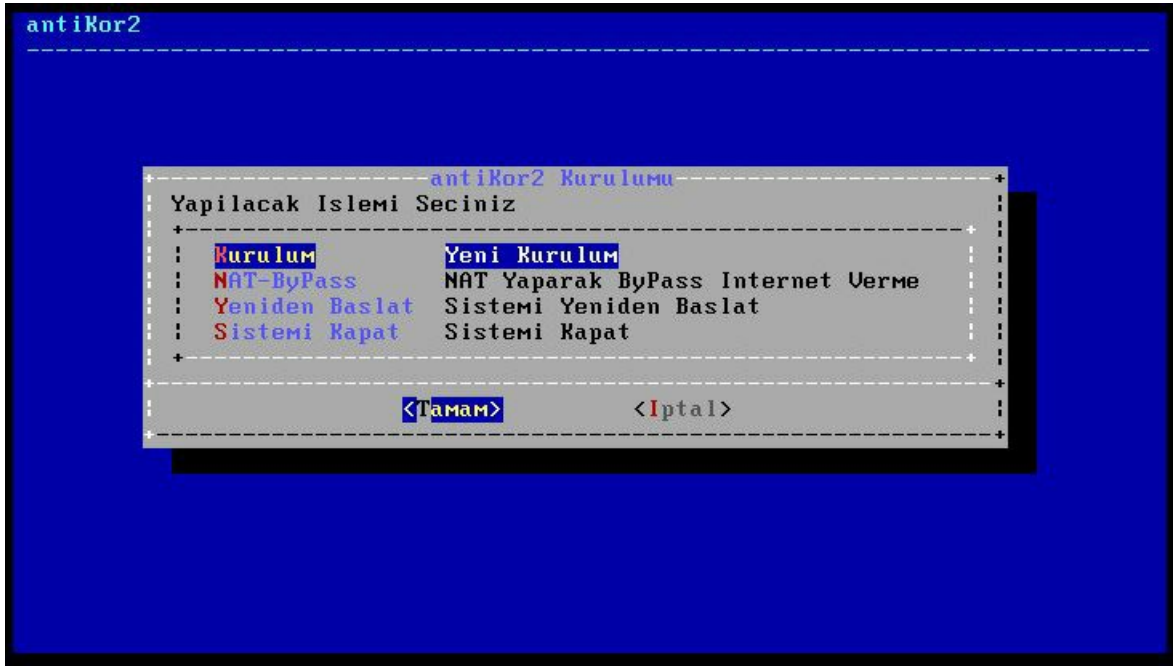
Dil Seçimi

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



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

Kurulum

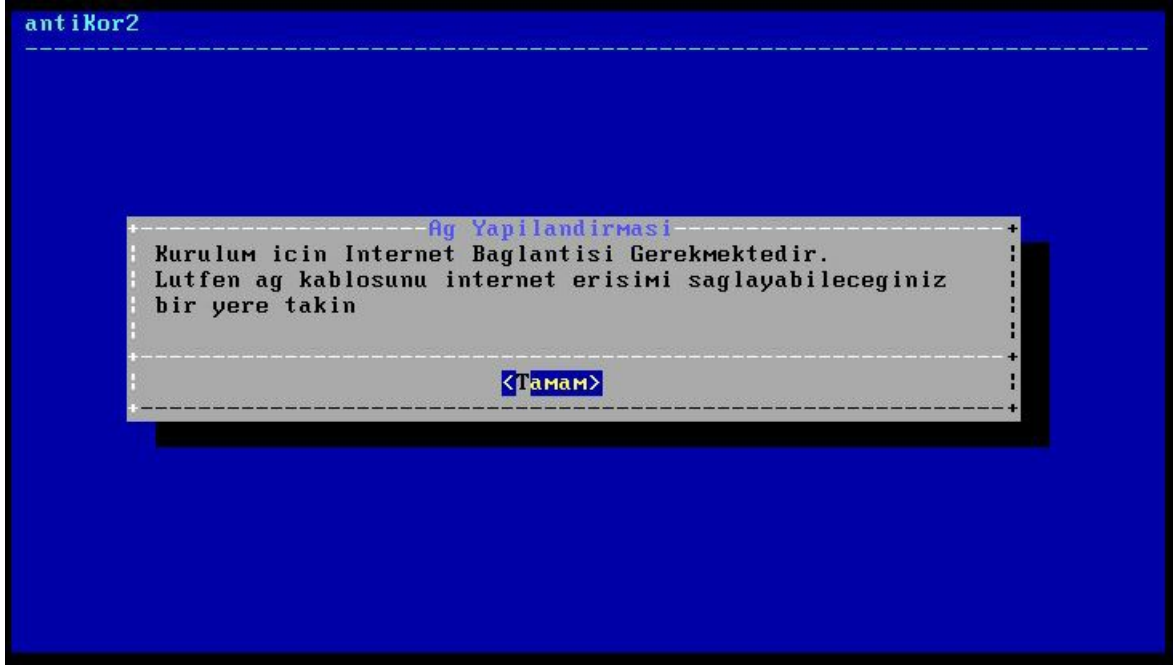


Yukarıdaki ekranda;

- **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.

antiKor2

----- Ag Yapilandirmasi -----

Baglanti Turunu Seciniz

+-----+
: Ethernet Yerel Ag Baglantisi / MetroEthernet :
: PPPoE Koprü Modunda ADSL - G.SHDSL - VDSL (xDSL) :
+-----+
+-----+
: <Tamam> <Iptal> :
+-----+

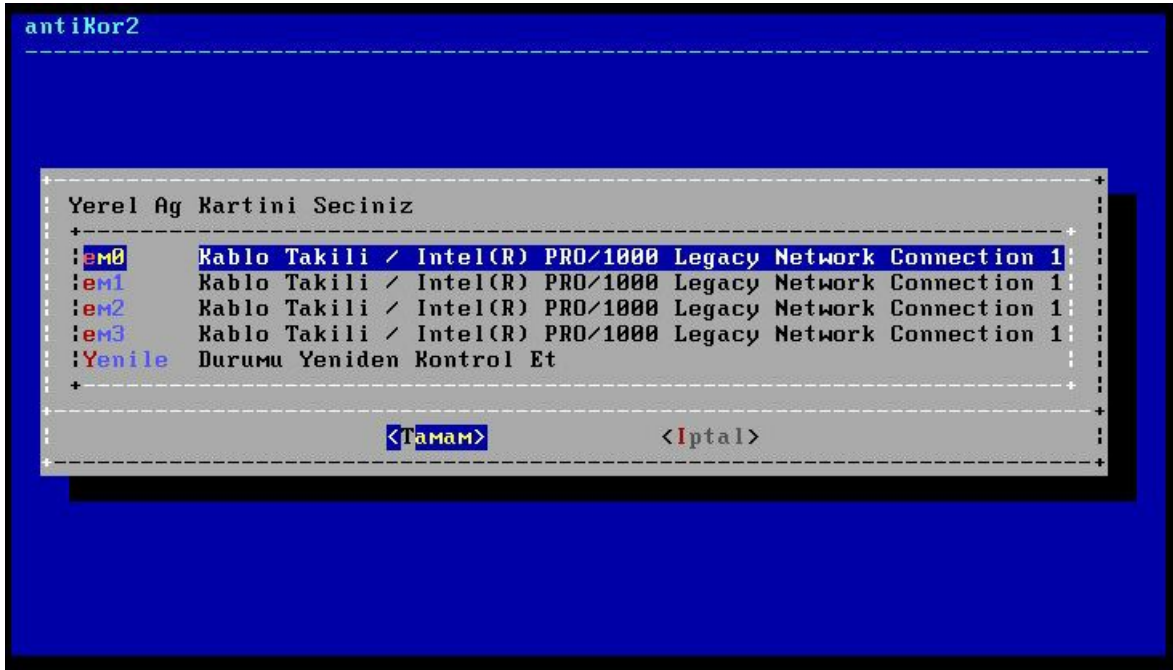
antiKor2

----- Ag Yapilandirmasi -----

Baglanti Turunu Seciniz

+-----+
: Ethernet Yerel Ag Baglantisi / MetroEthernet :
: PPPoE Koprü Modunda ADSL - G.SHDSL - VDSL (xDSL) :
+-----+
+-----+
: <Tamam> <Iptal> :
+-----+

İnternet bağlantı türü seçimi yapılır.

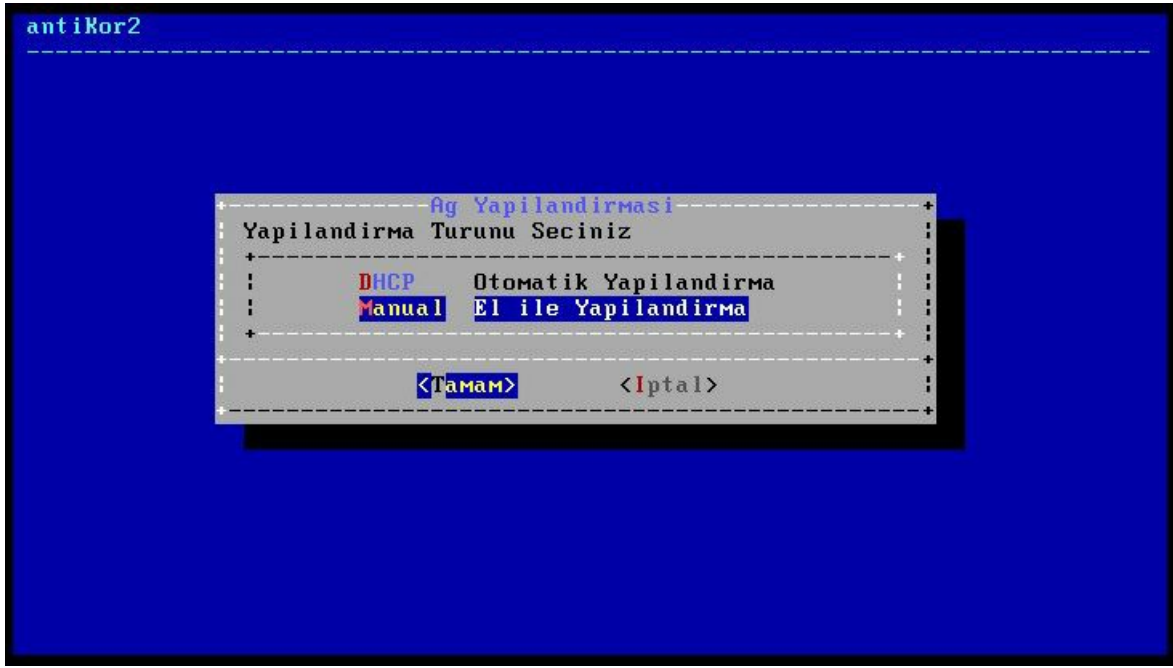


Bu ekranda 4 adet Intel Ethernet görülmektedir. Kurulum hangi Ethernet üzerinden yapılacaksa o Ethernet seçilerek kurulumla devam edilir.

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

DHCP - Manuel Seçimi





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 kurulumla devam edilmiştir.



antiKor2

Ag Yapilandirmasi

:IP Adresi10.2.1.205

:Alt Ag Maskesi255.255.255.0

:Ag Gecidi10.2.1.253

:DNS Sunucusu8.8.8.8

<Tamam>

<Iptal>

antiKor2

```
Ag Yapilandirmasi
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu
1500
options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
ether 00:0c:29:5f:74:18
inet 10.2.1.205 netmask 0xfffff00 broadcast 10.2.1.255
nd6 options=29<PERFORMNUD, IFDISABLED, AUTO_LINKLOCAL>
media: Ethernet autoselect (1000baseT <full-duplex>)
status: active

Routing tables

Internet:
Destination      Gateway          Flags           Netif Expire
default          10.2.1.253      UGS             em0
10.2.1.0/24      link#1          U              em0
10.2.1.205       link#1          UHS             lo0
```

<Evet >

<Hayir>

84%

antiKor2

```
Ag Yapilandirmasi
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu
1500
options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
ether 00:0c:29:5f:74:18
inet 10.2.1.205 netmask 0xfffff00 broadcast 10.2.1.255
nd6 options=29<PERFORMNUD, IFDISABLED, AUTO_LINKLOCAL>
media: Ethernet autoselect (1000baseT <full-duplex>)
status: active

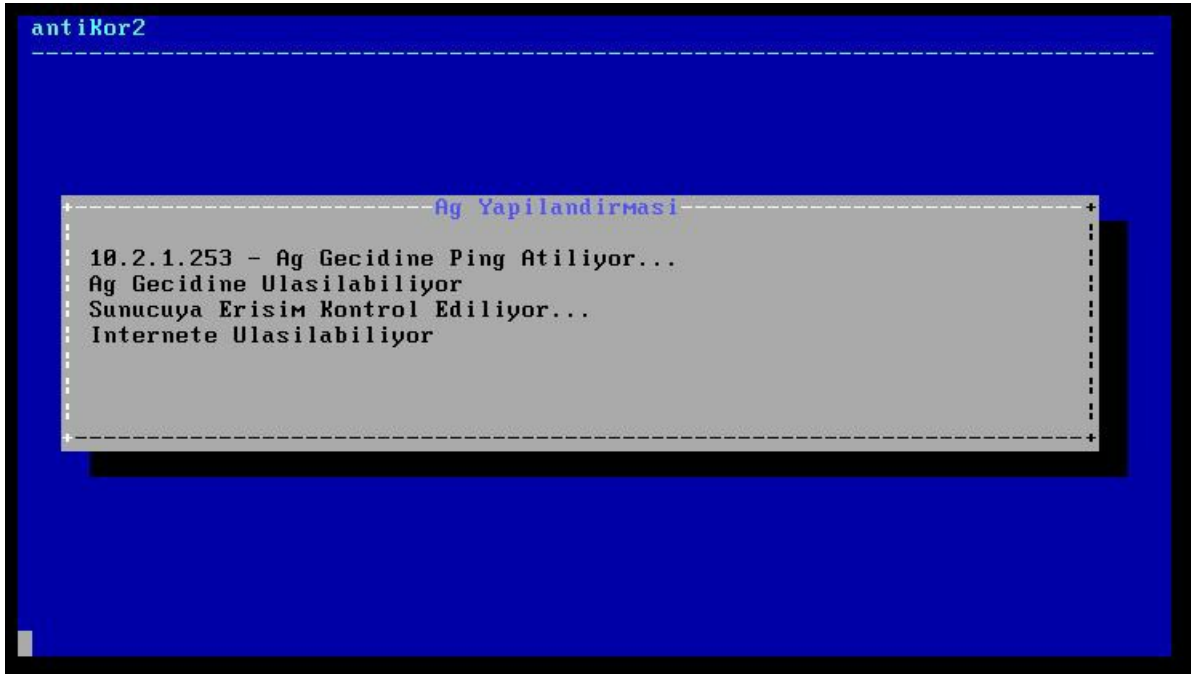
Routing tables

Internet:
Destination      Gateway          Flags           Netif Expire
default          10.2.1.253      UGS             em0
10.2.1.0/24      link#1          U              em0
10.2.1.205       link#1          UHS             lo0
```

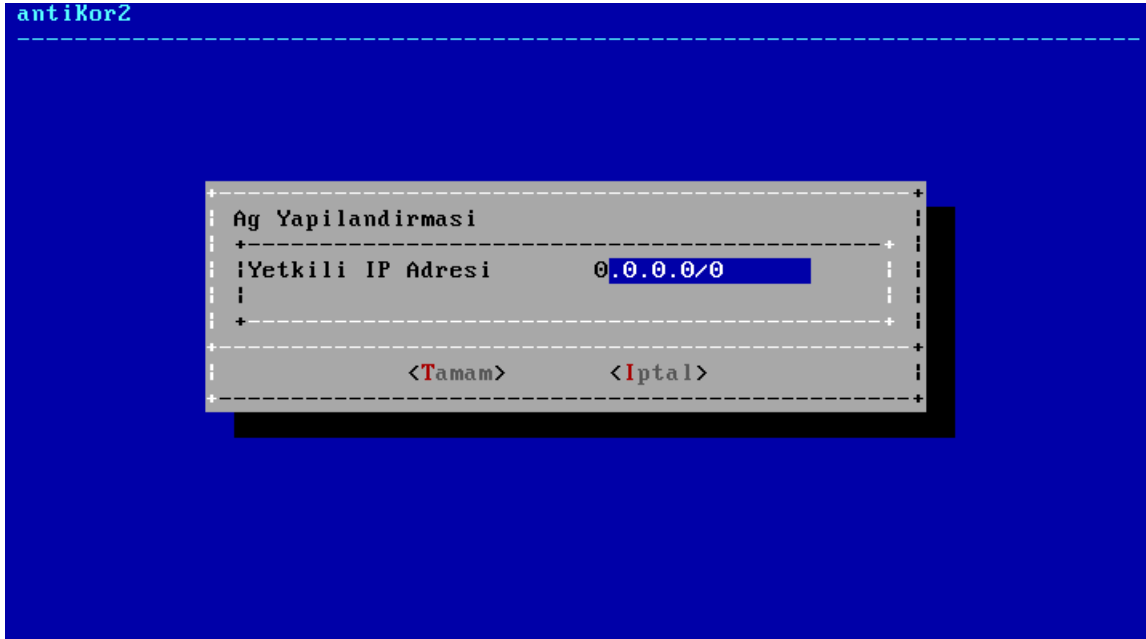
<Evet >

<Hayir>

84%

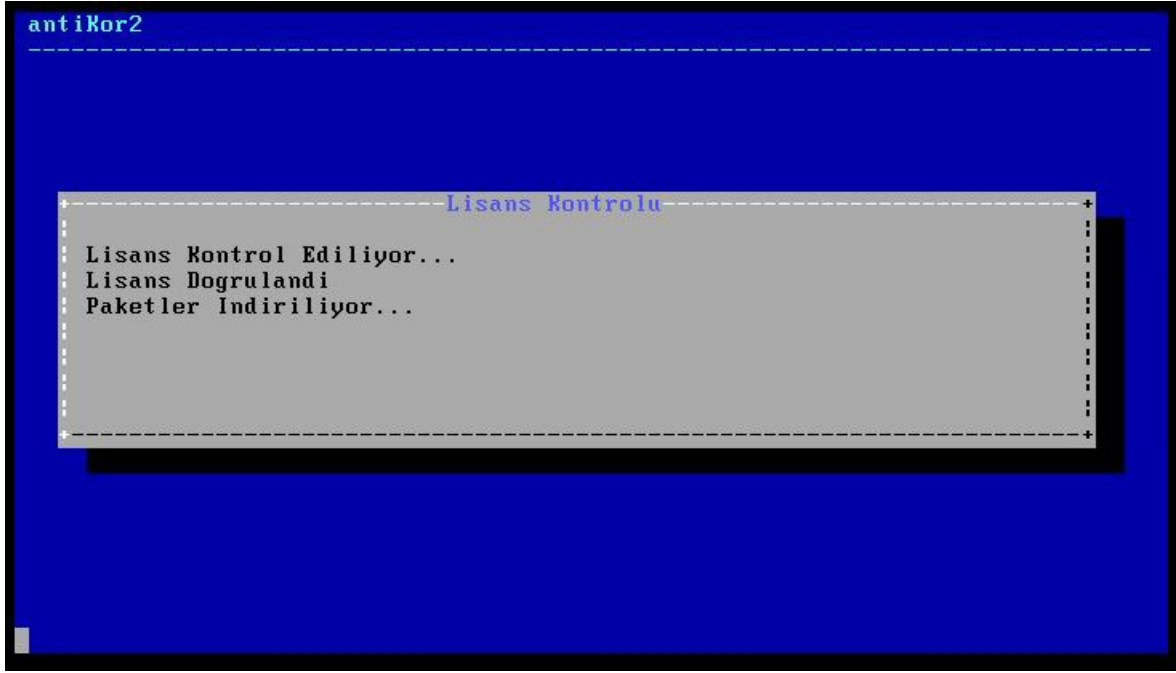


Antikor'a erişim sağlanması istenen IP adresi girilir. 0.0.0.0/0 seçilmesi durumunda her yerden erişim sağlanabilecektir.





Epsti Siber Gvenlik Teknolojileri tarafından saęlanan lisans anahtarı girilir.



Disk Blmleme

Sunucu zerinde 2-3 farklı disk var ise, Antikor Yazılımı ve Logları 2 farklı diske kurulabilir. Tek disk var ise seęilen diske kurulum yapılacaktır.

antiKor2

-----Disk Yapilandirmasi-----

Disk Bolumleme Semasi Seciniz

GPT	GUID Partition Table
UEFI	UEFI Boot
MBR	Master Boot Record

<Tamam> <Iptal>

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

antiKor2

-----Disk Yapilandirmasi-----

Kurulum Diskini Seciniz

1a0	81920MB - VMware Virtual disk 1.0 RETRY_BUSY
-----	--

<Tamam> <Iptal>

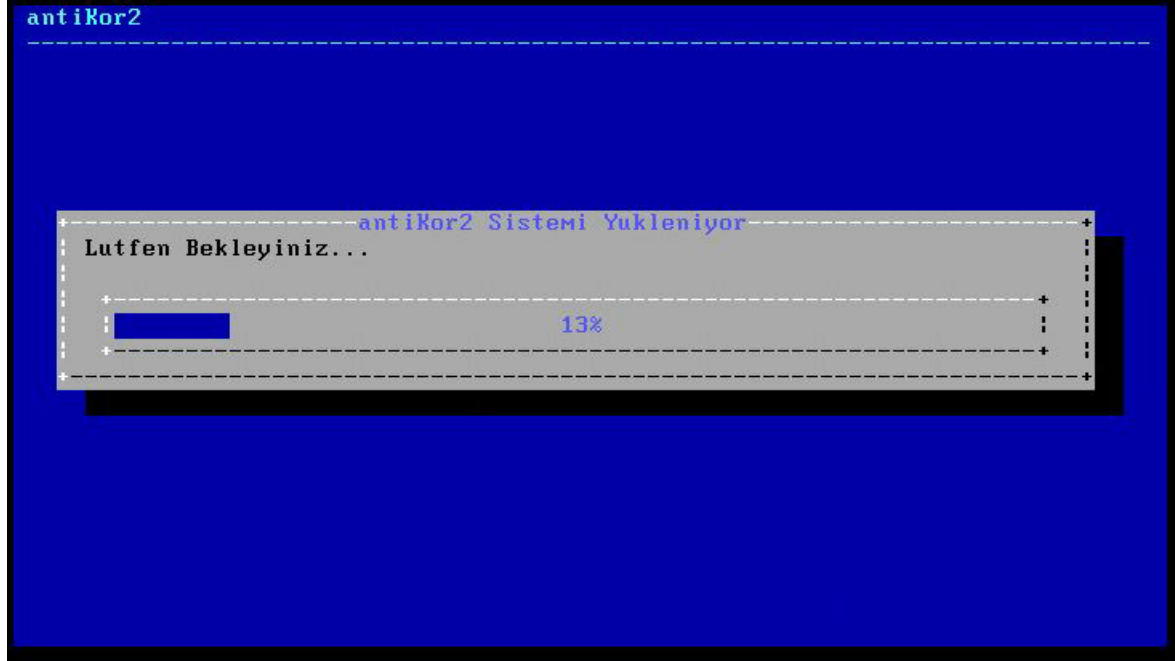
antiKor2

-----Disk Yapilandirmasi-----

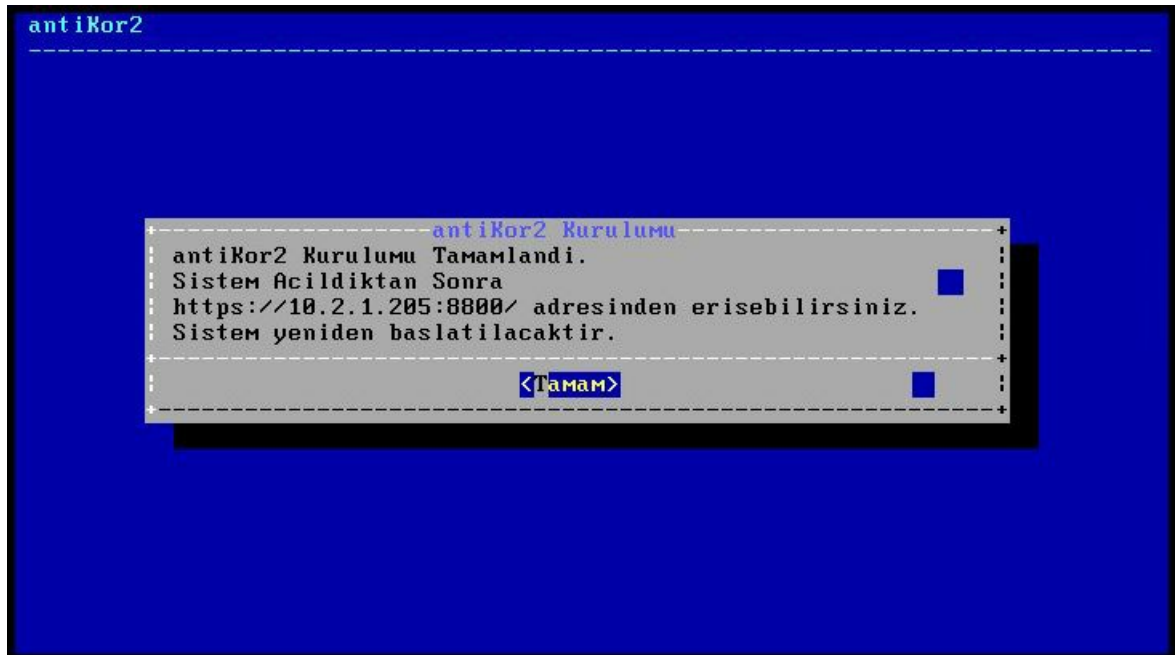
Diskinizdeki tum veri silinecektir!
Devam etmek istediginize emin misiniz?

<Evet > <Hayir>

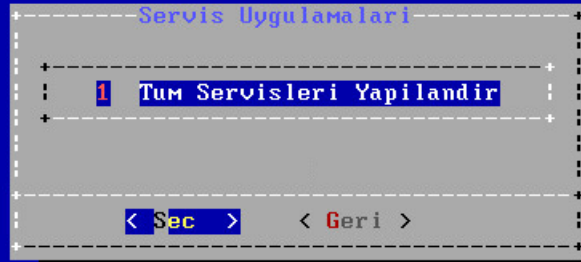
Kurulum için diskin biçimlendirilmesi gerekmektedir. **Evet** seçerek devam edilir.



PAKETLER KURULUYOR		
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
Yonetici 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)		



Antikor2 - Admin Konsolu



İşlem tamamlandıktan sonra Antikor bir defa yeniden başlatılır.

2. Admin konsolundan IP verilmesi gerekmektedir.

```
Kullanıcı adı: admin  
Parola: antikor
```

İlk olarak yapılması gerekenler, Network & IP Ayarları menüsü açılır.

Antikor2 - Admin Konsolu



Düzenlenmesi istenilen ethernet bacağı seçilir.



LAN Ayarlari menüsünü açıldığında;

İki alt menü görülecektir. Hiç bir kayıt bulunmuyorsa, "Yeni Kayıt Ekleme Sihirbazı" seçilir.



Yeni Kayıt Ekleme Sihirbazı seçildiğinde, cihazda bulunan ethernet portları görülecektir. LAN için kullanılacak ethernet portu seçilir.



IP alanına LAN IP bloğunda kullanılacak IP ve Alt Ağ Maskesi yazılır.



Network IP Ayarlari > LAN Ayarlari > Yeni Kayit Ekle

IP

192.168.2.1/24

<Tamam> <Iptal>

MTU değeri 1500 olarak bırakılır.

Network IP Ayarlari > LAN Ayarlari > Yeni Kayit Ekle

MTU

1500

<Tamam> <Iptal>

Bu işlemlerden sonra LAN bacağı için IP tanımlaması yapılmaktadır. Diğer ethernet bacakları için de aynı yol izlenerek IP adresleri verilebilir.

3. WEB arayüzüne girmek için LAN IP bloğunun kapsadığı bir IP'yi bilgisayara manuel olarak eklenebilir ve <http://192.168.2.1:8800> IP adresi ile WEB arayüzüne ulaşılabilir.

4. Ağ Yapılandırması menüsü altında bulunan IP Havuzları sayfasına gidilir.

⌕ Ağ Yapılandırması

IP Havuzları

IP Atama

Ethernet Atama

VLAN Yapılandırması

Sanal Ethernet - Link Birleştirme

Sanal Ethernet - Loopback

Sanal Ethernet - PPP

Sanal Ethernet - VLAN Etiketli Tabanlı

Sanal Ethernet - VXLAN

Sanal Ethernet - Ethernet Çifti

Ethernet Durumları

Ağ Geçidi İzleme

WAN Grupları

IPv6 6to4 Tünelleme

Sanal Kablo

Ekle butonuna tıklandığında, LAN bloğu için IP Havuzu belirlenecektir.

Ethernet

LAN1

Adres Ailesi



IPv4



IPv6

IP Bloğu

IPv4

192.168.2.0/24

Açıklama

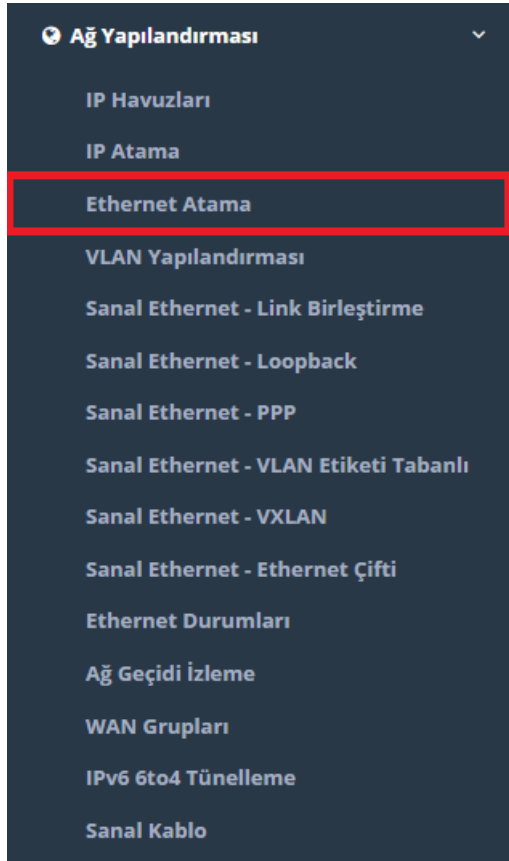
LAN için

İptal

Kaydet

Kaydet butonuna tıklanarak LAN bacağı için IP Havuzu belirlenmiş olur. Diğer ethernet bacakları için de aynı yol izlenerek IP Havuzları verilebilir.

5. Ağ Yapılandırması menüsü altında bulunan Ethernet Atama sayfasına gidilir.



LAN Ekle butonuna tıklanarak, LAN Ethernet Ataması gerçekleştirilir.

Ethernet Atama

Yenile

WAN Ekle

LAN Ekle

DMZ Ekle

PPPoE Ekle

LAN bacağı için ilgili ayarlar girilmiştir. Diğer ethernet bacakları içinde aynı yol izlenerek Ethernet Atama işlemi gerçekleştirilebilir.

Ethernet Durumları

Durum Aktif

Arayüz LAN1

Ethernet Adı bge1

MTU 1500

IPv6 Ayarları

☐ Otomatik IPv6 Al

IPv6 Adresi IPv6 ffff::1/8

DHCPv6 Başlangıç IPv6

DHCPv6 Bitiş IPv6

DHCPv6 Relay Adresi IPv6

IPv4 Ayarları

☐ Otomatik IPv4 Al

IPv4 Adresi IPv4 192.168.2.1/24

DHCPv4 Başlangıç IPv4 192.168.2.10

DHCPv4 Bitiş IPv4 192.168.2.254

DHCPv4 Ağ Geçidi IPv4 192.168.2.1

DHCPv4 Relay Adresi IPv4

Global NAT IPv4 10.2.1.22

Seçenekler

☐ MAC Eşleme ☒ NAT

☐ Kayıt Al ☐ Anons Yap

☐ DHCPv6 Sunucusu ☒ DHCPv4 Sunucusu

☐ DHCPv6 Relay ☐ DHCPv4 Relay

☐ Managed Bayrağı ☐ Other Bayrağı

İptal

Kaydet

Ethernet atama işlemi yapılırken seçenekler bölümünde “DHCPv4 Sunucusu” işaretlenmiş ise; gösterge panelinde servis durumlarının altında bulunan DHCPv4 Servisi başlatılmalıdır.

Not: Kurulum gerçekleştikten sonra ethernet kartı eklenmemelidir ve çıkarılmamalıdır.

6. admin kullanıcısının varsayılanda gelen şifresinin(antikor) değiştirilmesi gerekmektedir.

- Kullanıcı Ayarları sayfasına gidilir.

admin

Kullanıcı Ayarları

Gösterge Paneli

Sistem Kullanımı

CPU: 20%

Bellek: 33%

Disk: 4%

Arayüz Durumları

Servis Durumları

Bakip Servisi	Kapalı	▶ ■ ⌂
Karadelik Servisi	Kapalı	▶ ■ ⌂
Anti-Spoof Servisi	Kapalı	▶ ■ ⌂
Güvenlik Duvarı	Çalışıyor	▶ ■ ⌂

- Kullanıcı Ayarları sayfasında **Kullanıcı Parolasını Değiştir** butonuna tıklanır.

antikor
antikor v2 NGFW Staging - STAGING
antikor v2 NGFW Staging

admin
Antikor Admin

Gösterge Paneli

Tanımlamalar

Sistem Ayarları

Ağ Yapılandırması

Duyuru ve Form Yönetimi

Raporlar

Kimlik Doğrulama Kuralları

Hotspot İşlemleri

Anlık Gözetim

Güvenlik Ayarları

Güvenlik Profilleri

E-posta Güvenliği

NAT Yapılandırması

Kullanıcı Ayarları

Profil Resmi


Kullanıcı Adı : admin

Kullanıcı Bilgileri

Adı : Antikor
Soyadı : admin
Kimlik Numarası : 11111111111
Telefon : 3243610233
E-Posta : bilgi@epati.com.tr
Doğum Tarihi : 2008-06-08
İlk Giriş Tarihi : 2022-12-05 17:06:37.769877+03
Son Giriş Tarihi : 2022-12-12 10:25:07.651087+03
Kim Tarafından oluşturuldu : Antikor

Profil Fotoğrafı Yükle

Profil Fotoğrafı : [Yükle](#)

Dil Ayarları
☒ tr ☐ en

Üst-Menü Konumu
☒ Sabit ☐ Statik

Parola Değiştir
[Kullanıcı Parolasını Değiştir](#)

İki Adımlı Kimlik Doğrulama
[İki Adımlı Kimlik Doğrulama Ayarları](#)

Gösterge Panelini Sıfırla

- Parola değiştirilir.

Parolanızı Güncelleyin

Eski Parola

Yeni Parola

Yeni Tekrar

[Kaydet](#)

Parolanızı Güncelleyin

Eski Parola

Yeni Parola

Yeni Tekrar

[Kaydet](#)

- Parola değiştirildikten sonra admin kullanıcısına atanmış yeni parola ile giriş yapılır.



antikor v2 NGFW Staging

Giriş yapmak için bilgileri giriniz.

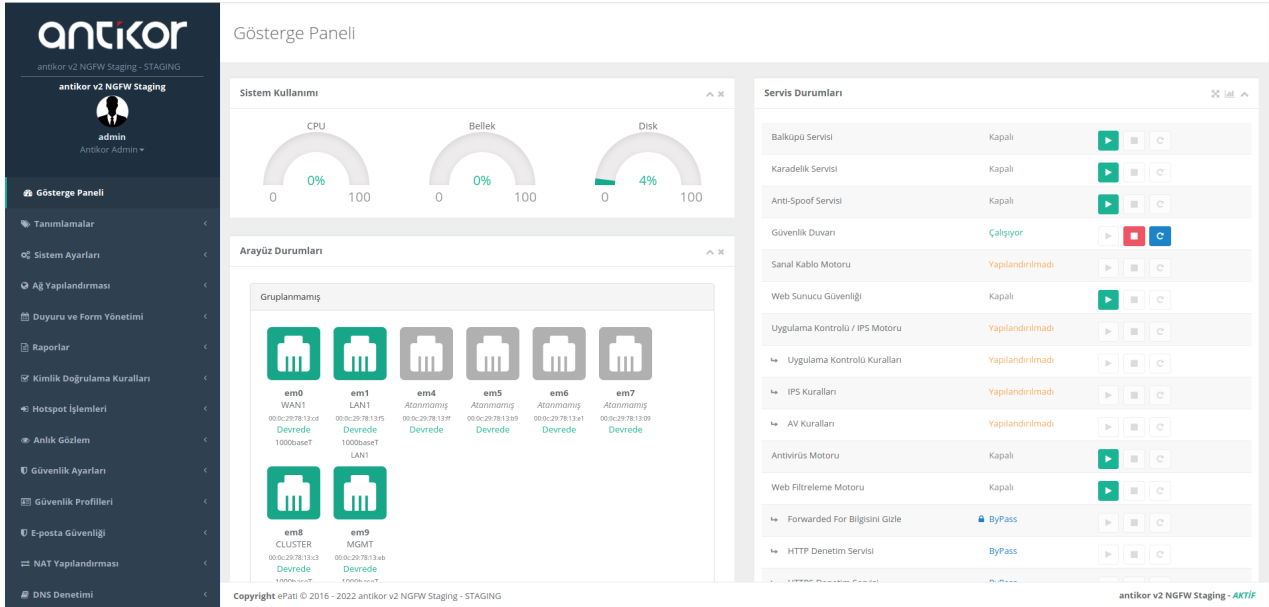
admin

.....

Giriş

ePati Siber Güvenlik © 2016 -2022

Dil Seçiniz : tr en



Antikor Güvenlik Duvarının WEB arayüzüne nasıl girilir?

Bilgisayarda bulunan herhangi bir web tarayıcısı (Internet Explorer, Chrome, Firefox, vb.) ile cihaza erişip gerekli ayarlar yapılabilmektedir. Yazılım ayarlarını yapmadan önce yukarıdaki gibi Antikorun kurulum IP adreslerinin doğruluğundan ve kabloların takılı olduğundan emin olunuz. Antikor sunucusu açıldıktan sonra;

- Tarayıcının adres kısmına sunucuya verilmiş olan IP adresi <https://10.2.1.205:8800> girilir. Port 8800 olduğu için “https://” nin yazılması unutulmamalıdır.

antikor

antikor v2 NGFW

Giriş yapmak için bilgileri giriniz.

Kullanıcı Adı alanı boş bırakılamaz.

Giriş

ePati Siber Güvenlik © 2016 -2022

Dil Seçiniz : tr en

- Giriş ekranı gelecektir. Kullanıcı adı “admin” ve parolayı “antikor” yazarak **Giriş** butonuna tıklanır.

antikor

admin
Antikor Admin

- Gösterge Paneli
- Tanımlamalar
- Sistem Ayarları
- Ağ Yapılandırması
- Duyuru ve Form Yönetimi
- Raporlar
- Kimlik Doğrulama Kuralları
- Hotspot İşlemleri
- Anlık Gözetim
- Güvenlik Ayarları
- E-posta Güvenliği
- NAT Yapılandırması
- DNS Denetimi
- Web Filtreleme
- DMZ Yönetimi
- VPN Yönetimi
- Yönlendirme Yönetimi
- Karantina ve Saldırı Tespit Sistemi

antikor v2 NGFW Staging - STAGING

Sayfa ismi girmeye başlayın...

Q

Çıkış Yap

Gösterge Paneli

Sistem Kullanımı

CPU

8%

0 100

Bellek

30%

0 100

Disk

2%

0 100

Arayüz Durumları

Gruplanmamış

em0 WAN1

em1 LAN1

em2 LAN2

em3 DMZ1

em4 Alınmamış

em5 Alınmamış

Ethernet Bant Genişliği Kullanımı

Tümü

488 Kbps

366 Kbps

Servis Durumları

Balkıpu Servisi	Kapalı	▶	■	⊞
Karadellik Servisi	Kapalı	▶	■	⊞
Anti-Spoof Servisi	Kapalı	▶	■	⊞
Güvenlik Duvarı	Çalışıyor	▶	■	⊞
Web Sunucu Güvenliği	Kapalı	▶	■	⊞
Uygulama Güvenliği / IPS Motoru	Kapalı	▶	■	⊞
Uygulama Güvenliği Kuralları	Kapalı	▶	■	⊞
IPS Kuralları	Kapalı	▶	■	⊞
Antivirüs Motoru	Kapalı	▶	■	⊞
Web Filtreleme Motoru	Kapalı	▶	■	⊞
Forwarded For Bilgisini Gizle	ByPass	▶	■	⊞
HTTP Denetim Servisi	ByPass	▶	■	⊞
HTTPS Denetim Servisi	ByPass	▶	■	⊞
Sayfa Yasaklama Servisi	ByPass	▶	■	⊞
Antivirüs / İçerik Filtreleme Servisi	ByPass	▶	■	⊞
Proxy Servisi	ByPass	▶	■	⊞
DNS Denetleme Motoru	Kapalı	▶	■	⊞

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

Yönetim Paneli Kullanıcıları

XLS CSV PDF

Filtrele Temizle

#	Durum	Adı	Soyadı	Kullanıcı Adı	İşlemler
1	Aktif	Antikor	Admin	admin	Düzenle Sil Grup Üyelikleri Yetkiler ve Roller Detaylar

«

<

1

>

»

Ardından “Detaylar” 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 : 10.2.1.12

Giriş Yapılan Tarih : 2019-07-29 11:45:37+00

Giriş Yapılan Son IP Adresi : 192.168.100.10

Giriş Yapılan Son Tarih : 2019-08-01 09:43:54+00

Giriş Sayısı : 22

Açılan sayfada “Düzenle” butonuna tıklanır.

Profil Fotoğrafı Yükle

Profil Fotoğrafı :  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.

Kurumsal Güvenlik Politikası

Kurulum tamamlandıktan sonra, kurulum sırasında **Yetkili IP Adresi** alanına girilen istemciden başka yetkili istemci var ise Antikor ürünü web arayüzünden bu yetkiler tanımlanmalıdır. Bunun için **Yönetim Paneli Ayarları** > Erişim / Oturum Ayarları menüsünden arayüze erişmeye yetkili diğer istemcilerin IP adresleri tanımlanabilir. Tanımlanan yetkili istemcilerin IP adreslerinin ağıınızda kullanılan mimariye bağlı olarak değişmediğinden emin olunuz.

Erişim/Oturum Ayarları

Oturum Ayarları

Trafiği Logla

Kapalı

Sertifika Bazlı Kimlik Doğrulama

Kapalı

Harici Kaynaklardan Kimlik Doğrulama

Kapalı

Eş Zamanlı Oturum Açma

Açık

Çalışma Modu

Kısıtlı Erişim

Giriş Feragatnamesi

Kapalı

SSH Karşılama Ekran Durumu

Kapalı

Kaydet

Erişebilen Ağlar

Yenile

Ekle

XLS

CSV

PDF

#	IP Adresi	Açıklama	İşlemler
1	0.0.0.0/0	Arayüz Erişim	Düzenle Sil

<<

<

1

>

>>

Git

Güvenli Mod

Antikor kurulumu gerçekleştirildikten sonra RAM haricinde herhangi bir donanım(ethernet kartı, harddisk vb.) eklenildiği zaman, Antikor güvenlik amacıyla “Güvenli Moda” geçiş yapacak ve işlevini yerine getirmeyecektir. Bu durumda, Antikor’un Güvenli Moddan önceki işlevine devam edebilmesi için eklenen donanım sökülmalıdır. Eklenen donanımın Antikorla uyumlu bir şekilde çalışabilmesi için yeniden kurulum yapılması gerekmektedir.

Sistemde Oluşan Bir Failure Sonrasında Gerçekleştirilecek Eylemler

Sistemde herhangi bir arıza yaşanması durumunda lütfen aşağıdaki adımları takip ediniz.

- Yaşanan arıza ile ilgili olarak, arızanın ne zaman ve hangi işlemten sonra ortaya çıktığı, karşılaşılan detaylar ve varsa hata çıktısı ile birlikte teknik destek talep edilmelidir.
- Yaşanan arıza sadece belli servisleri etkiliyorsa, ilgili servis kapatılmalıdır.
- Yaşanan arıza tüm sistemi olumsuz etkiliyor ve yedek sistemin mevcut olması halinde yedek sistem devreye alınmalıdır.



