epati

Kurulum Kılavuzu

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı

Yapılandırma Örnekleri

www.epati.com.tr

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 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.

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/

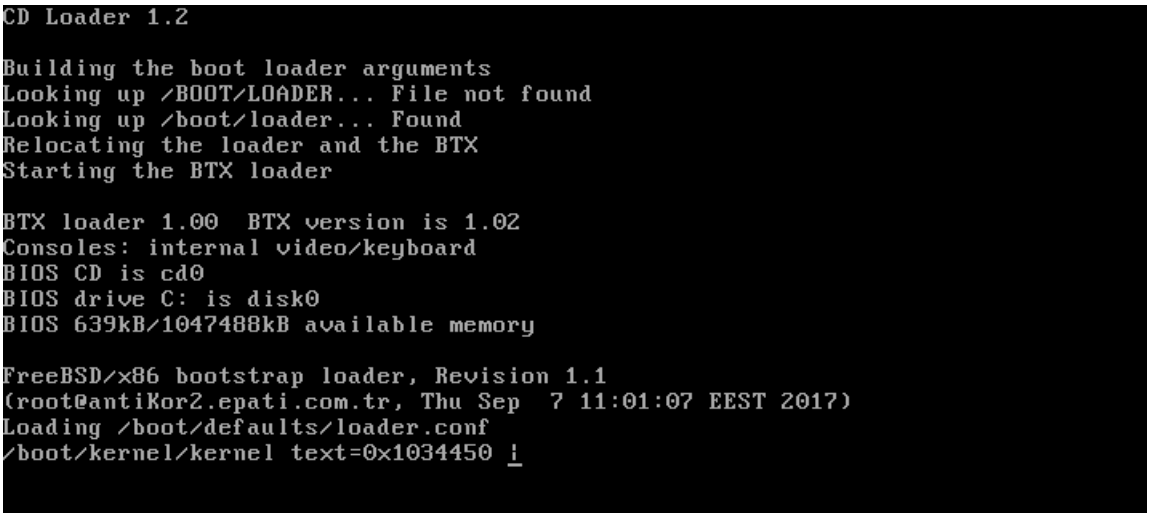
Not: Antikor'un kurulum yapılacağı ağ ortamda filtreleme yapan bir cihazın(firewall) arkasında ise; Antikor'un kurulu olduğu sunucu IP adresi için, 7001 ve 7002 portları lisans sunucusu ile haberleşebilmesi için açık olması gerekmektedir. Açık olmaması halinde lisans sunucusundan gelen paketler çekilmeyecek 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.



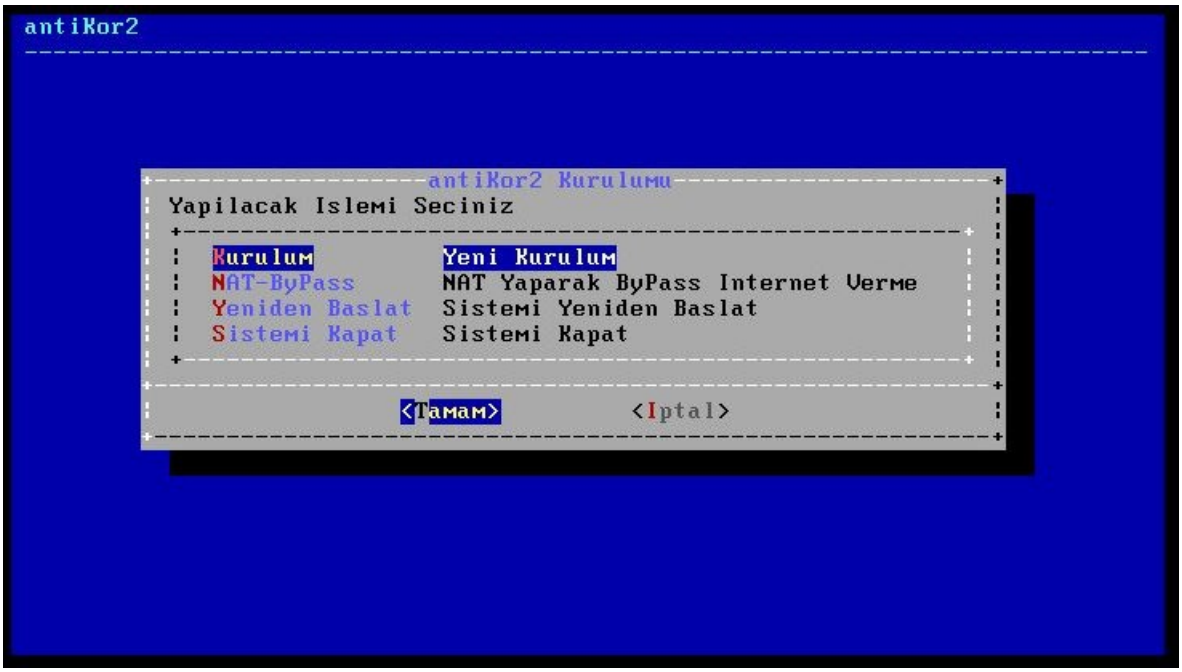
Yukarıdaki ekranda ilk satırda “CD Loader ” yazdığında kurulum başladığını belirtmektedir.

Dil Seçimi

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

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

Kurulum

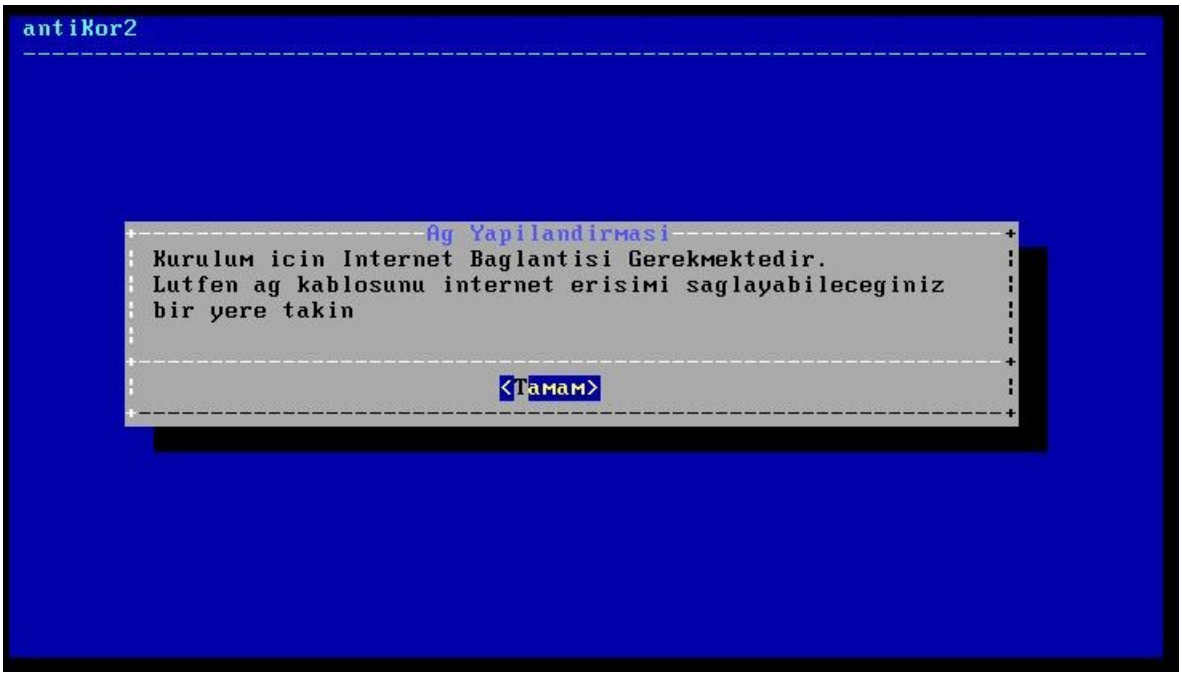


Yukarıdaki ekranda;

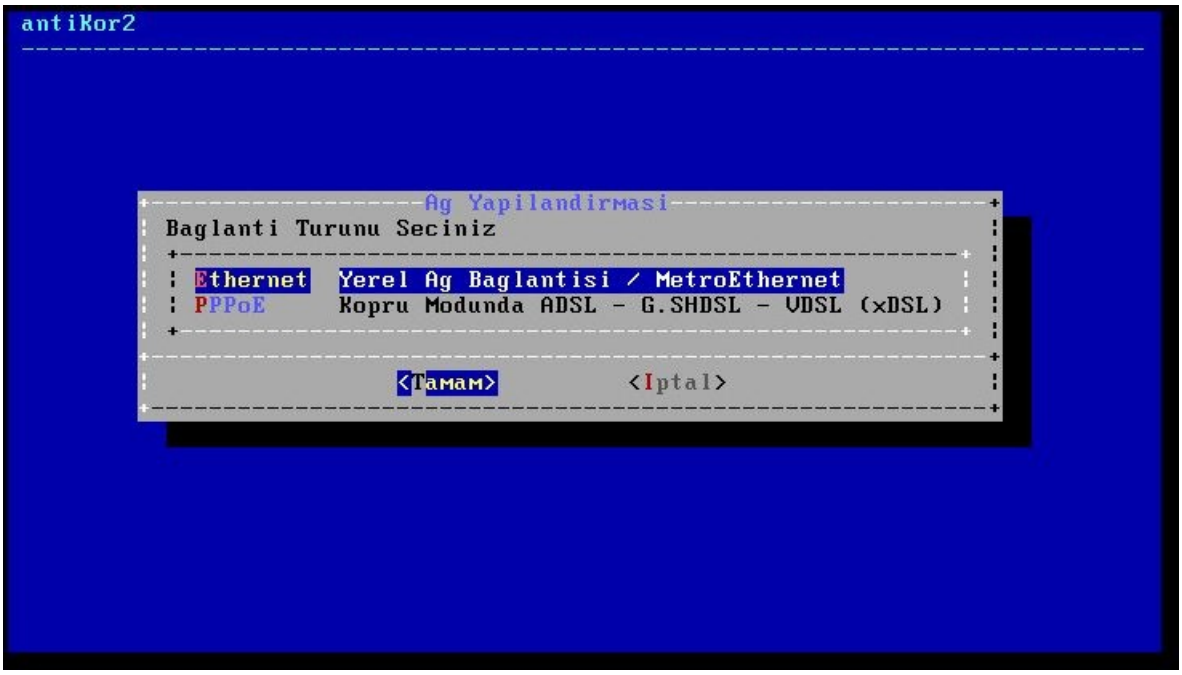
- `Kurulum` seçeneği yeni Antikor kurulumun başlatılması istendiğinde seçilmelidir.
- `Nat-Bypass` seçeneği kurulumu yapılmış Antikor'un bypass yapılarak internete çıkarılması için kullanılmalıdır.
- `Yeniden Başlat` seçeneği kurulumun tekrardan başlatılması için kullanılmalıdır.
- `Sistemi Kapat` seçeneği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

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

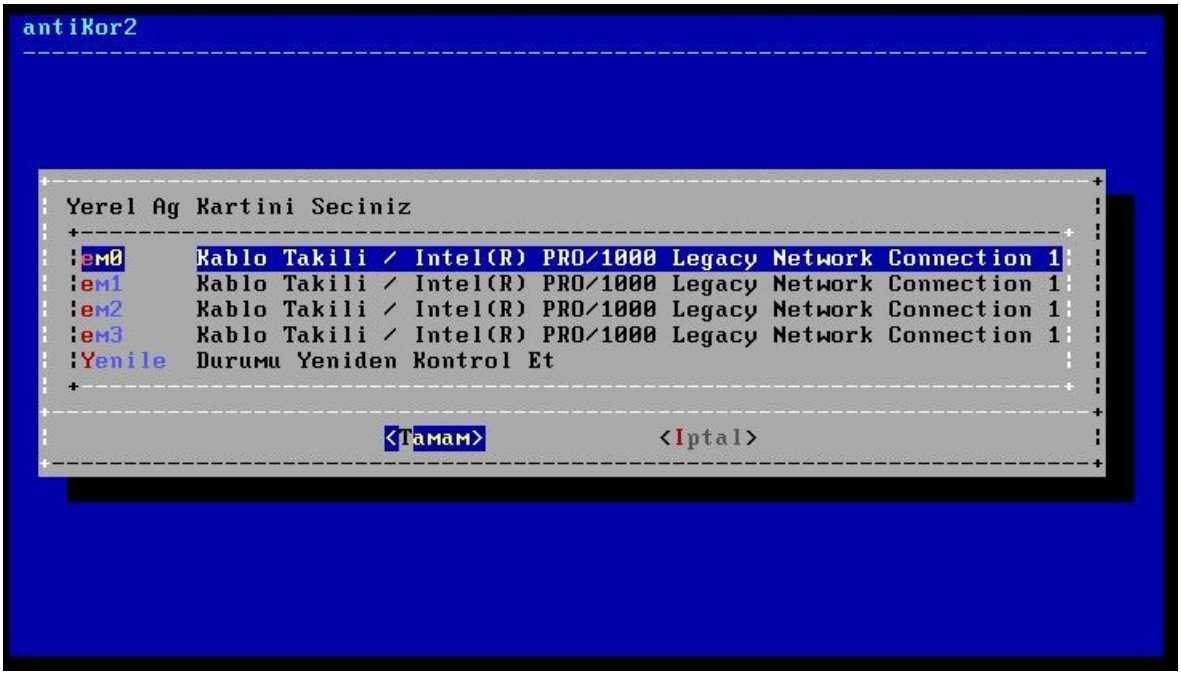
Ağ Yapılandırması



Kurulum için internet bağlantısı gerekmektedir.



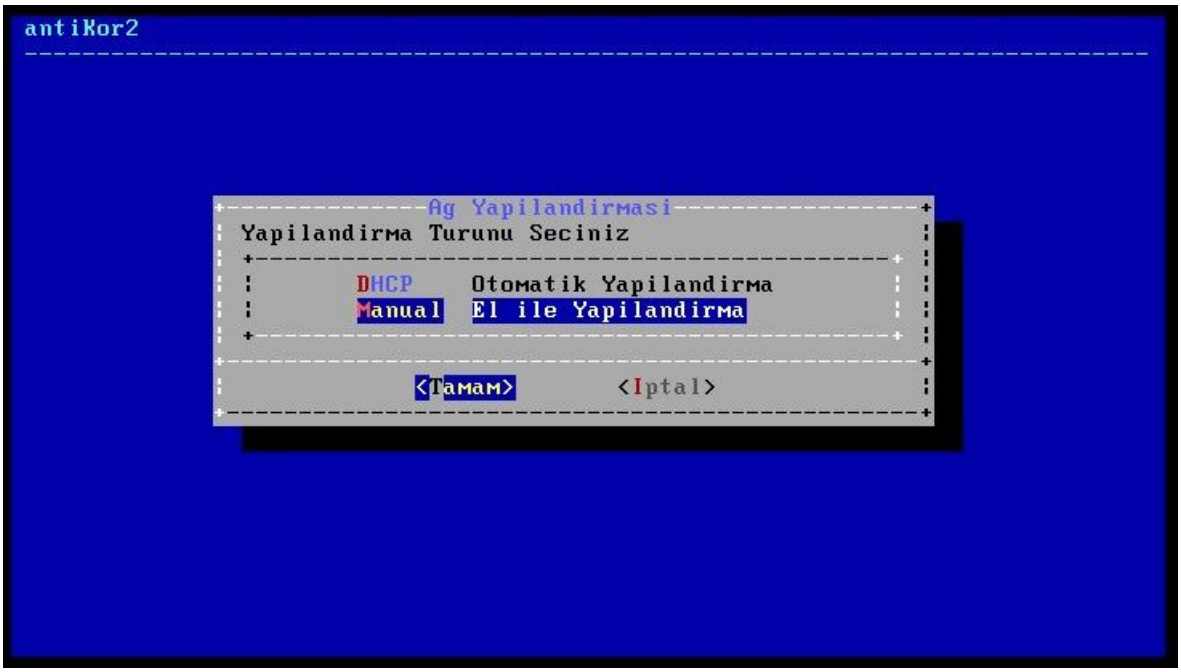
İnternet bağlantı türü seçimi yapılır.



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

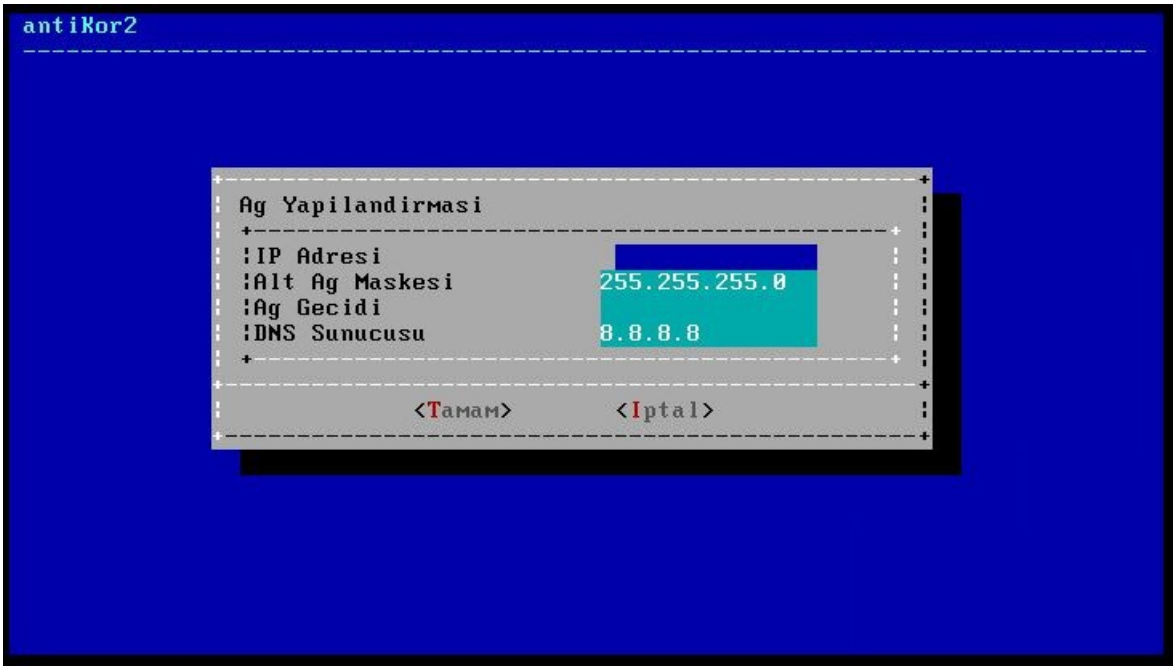
Not: Ethernet kartları görünmediği takdirde, bağlantılar kontrol edilerek**Yenile Durumu Yeniden Kontrol Et** seçeneği seçilir.

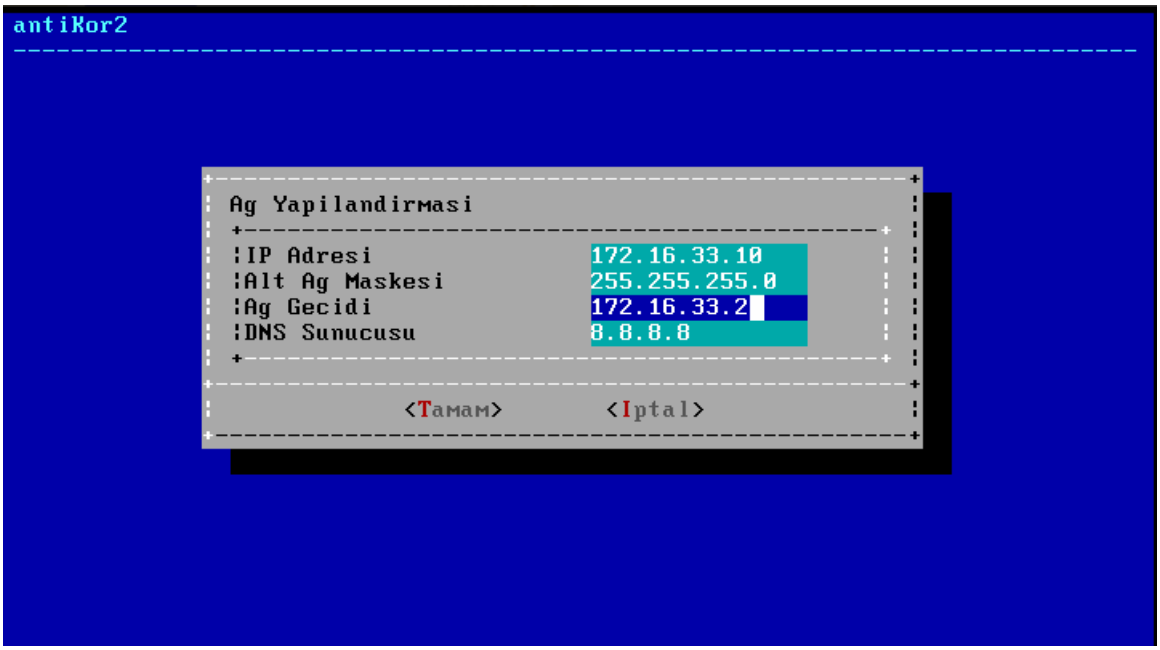
DHCP - Manuel Seçimi

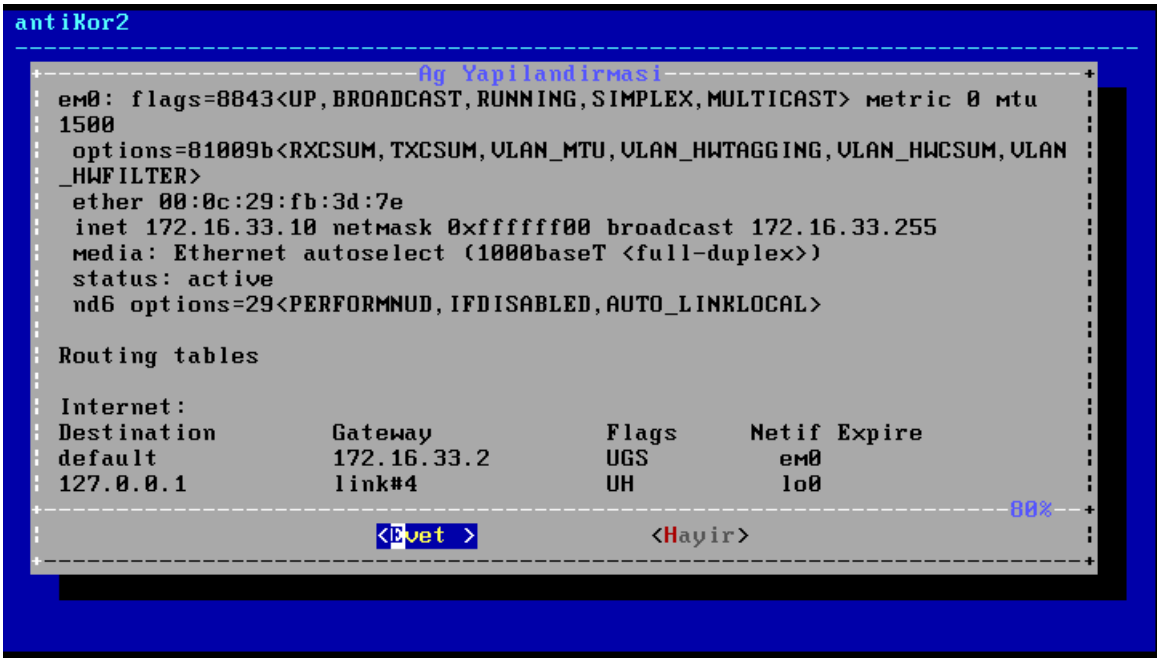


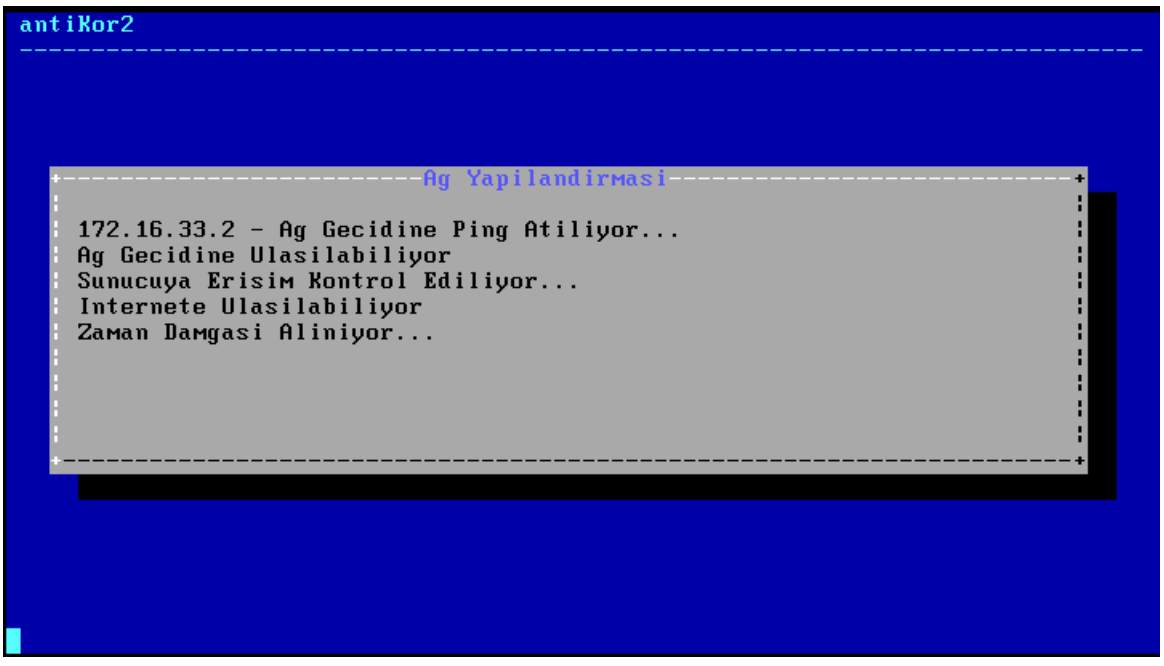
Seçilen ethernetten internete manuel IP verilerek veya DHCP seçilerek otomatik IP alınması gerekir. Fakat DHCP için IP dağıtan bir sisteminizin olması gerekmektedir. Eğer DHCP sunucu yoksa manuel IP verilerek devam edilir.

Aşağıda manuel IP verilerek kuruluma devam edilmiştir.

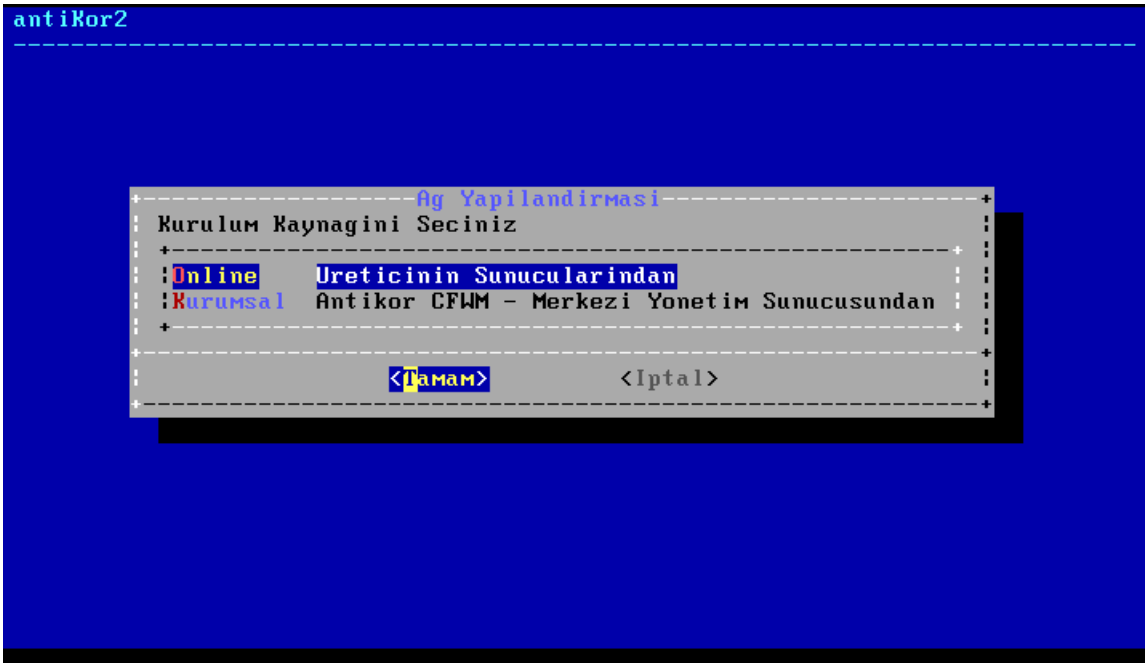




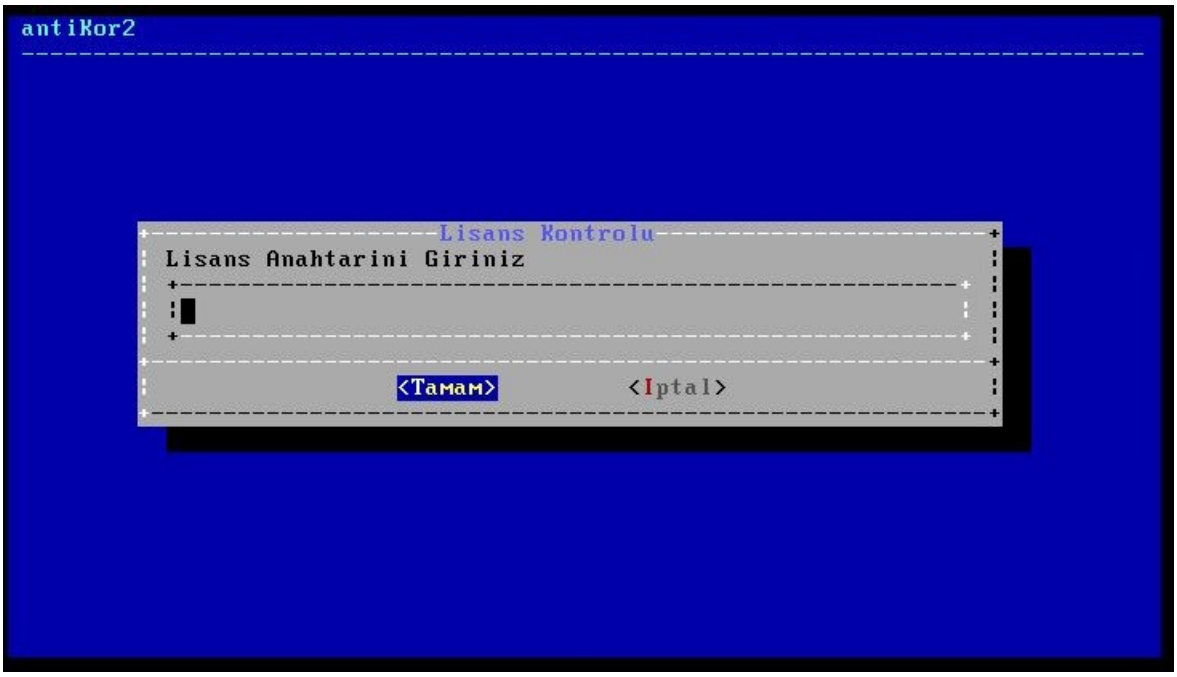




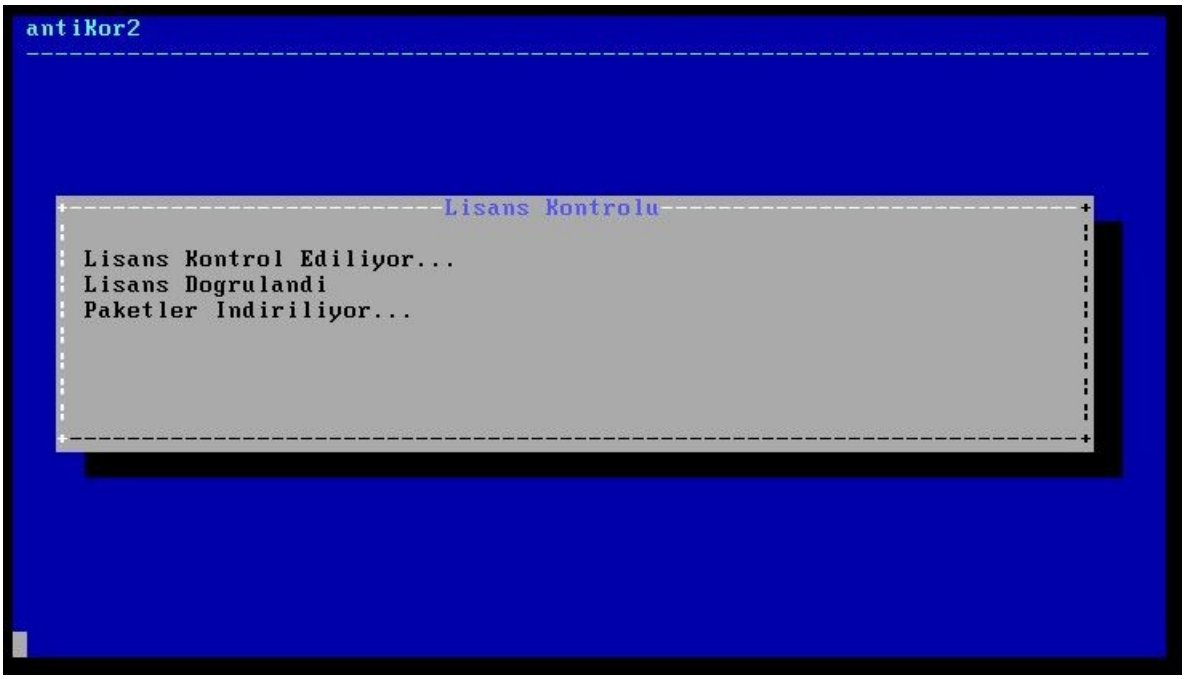
Kurulum tipi seçilir. Online kurulumda sunucunun internete çıkması gerekmektedir. Kurumsal kurulum kapalı devre sistemlerde Merkezi Yönetim üzerinden kurulum için kullanılır.



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



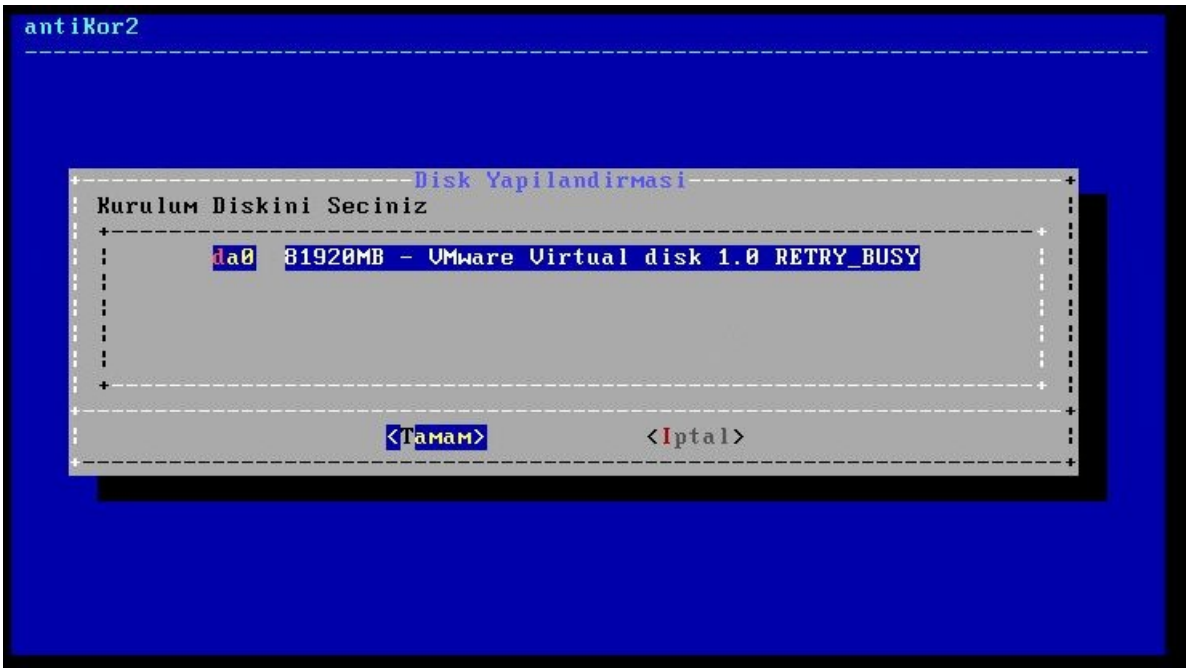
Epati Siber Güvenlik tarafından sağlanan lisans anahtarı girilir.

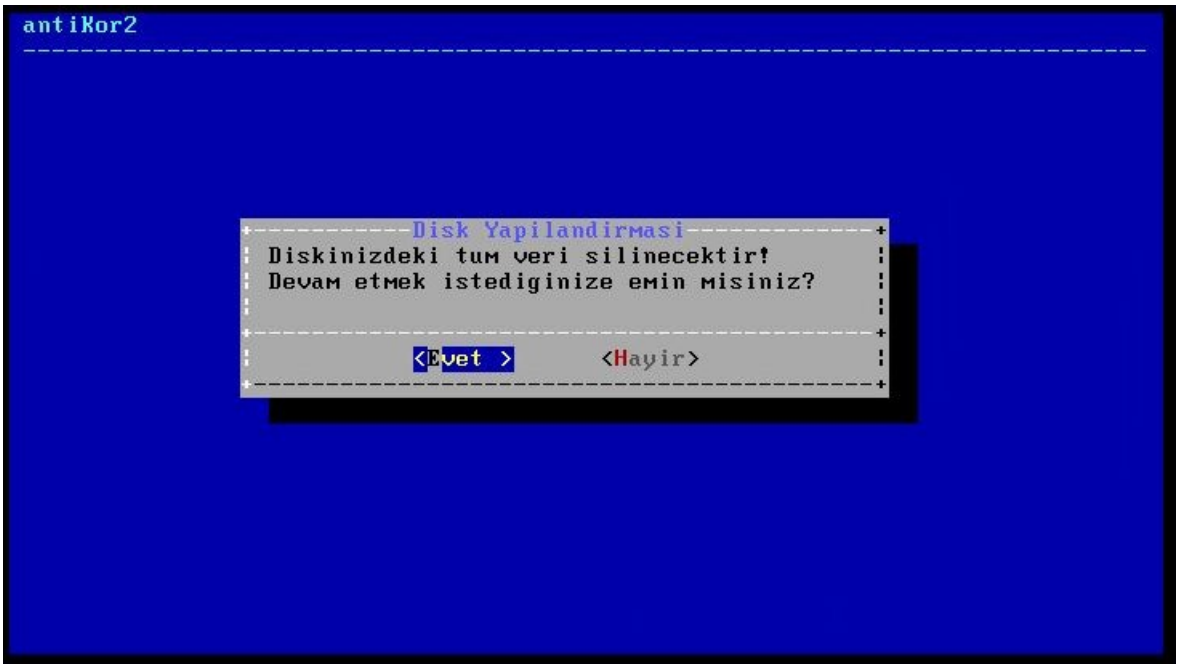


Disk Bölümleme

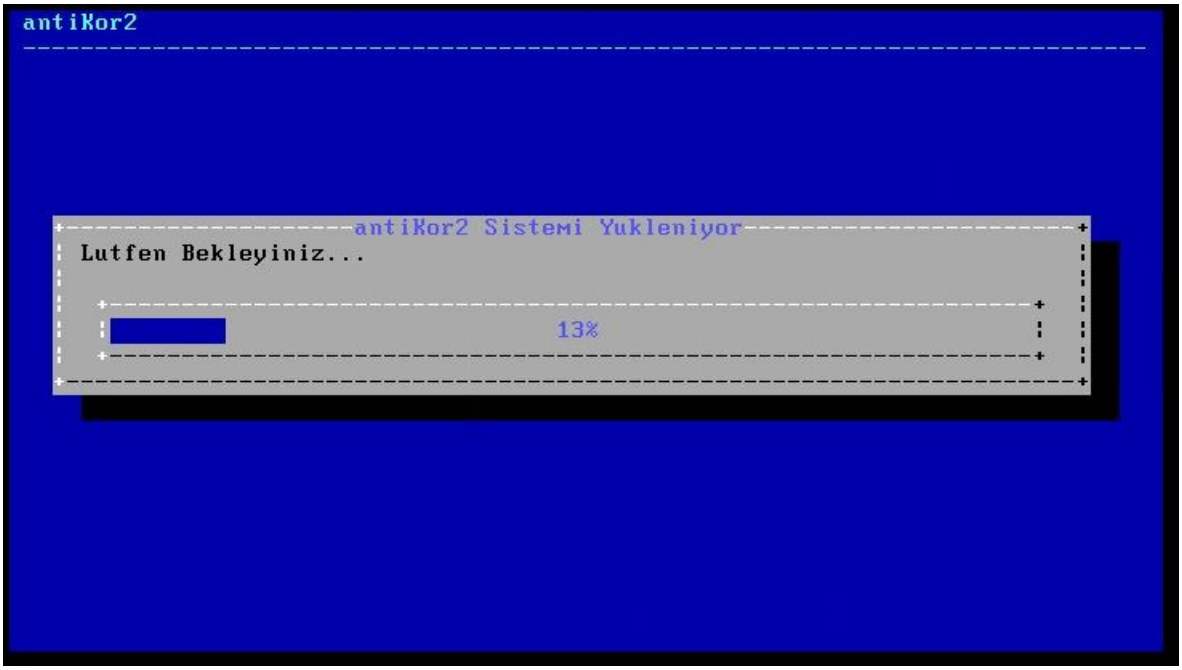
Sunucu üzerinde birden fazla disk var ise, Antikor Yazılımı ve Logları farklı diske kurulabilir. Tek disk var ise seçilen diske kurulum yapılacaktır.

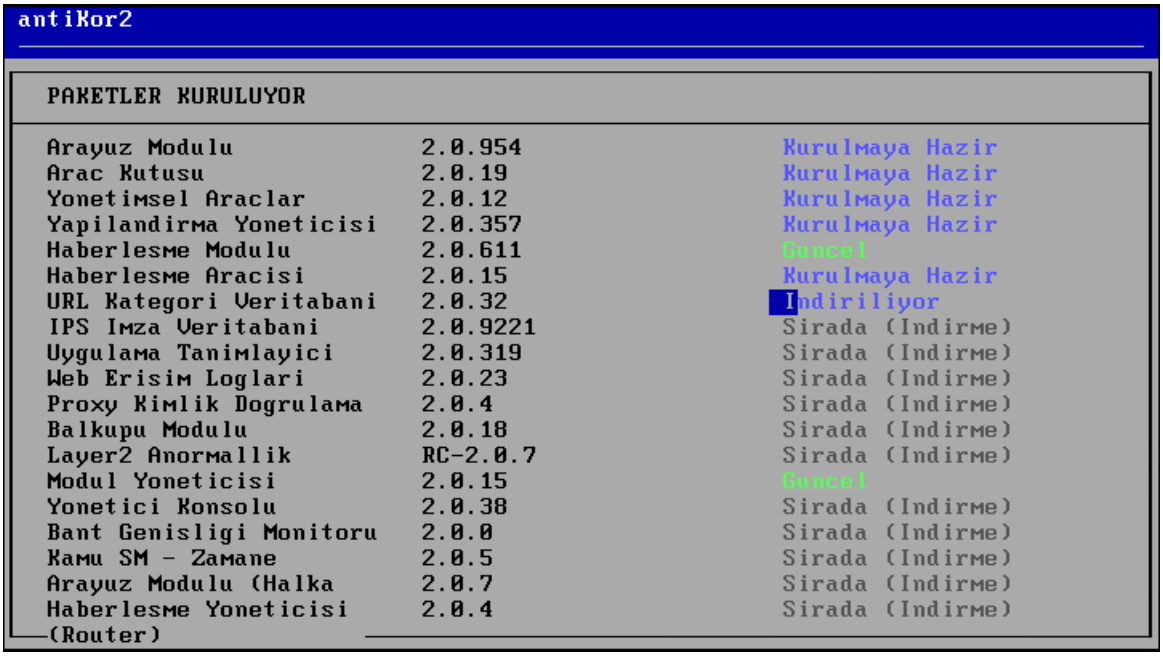
Diskinizin partition yapısına göre(GPT, MBR) seçim yapılır. Disklerin bir çoğu GPT uyumludur.

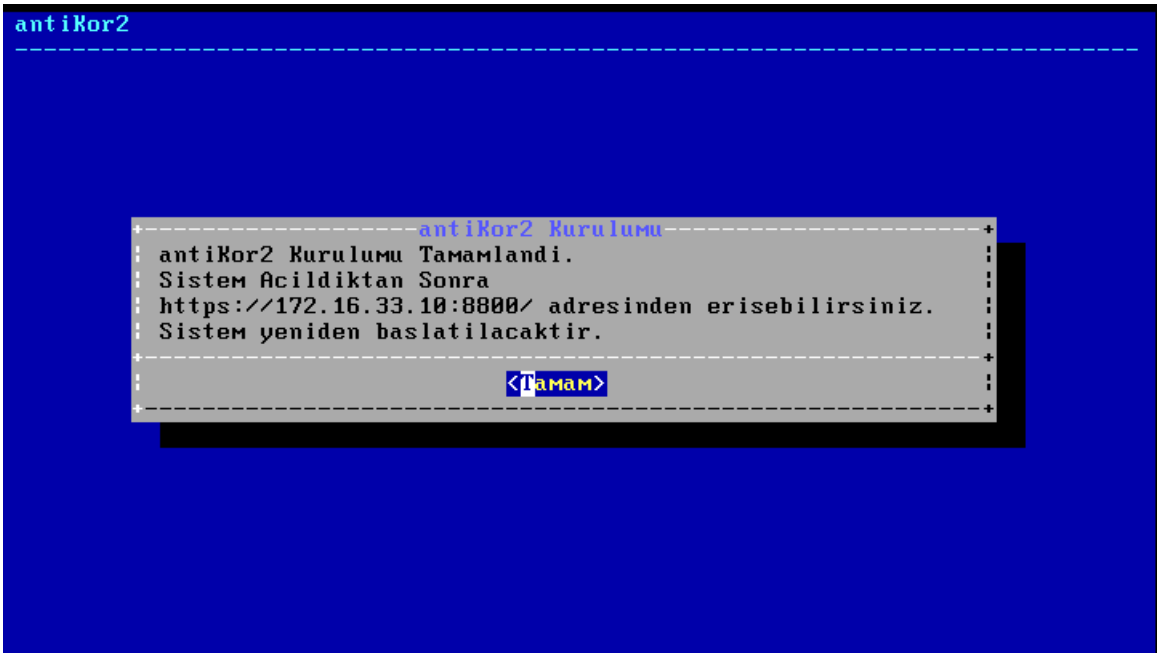




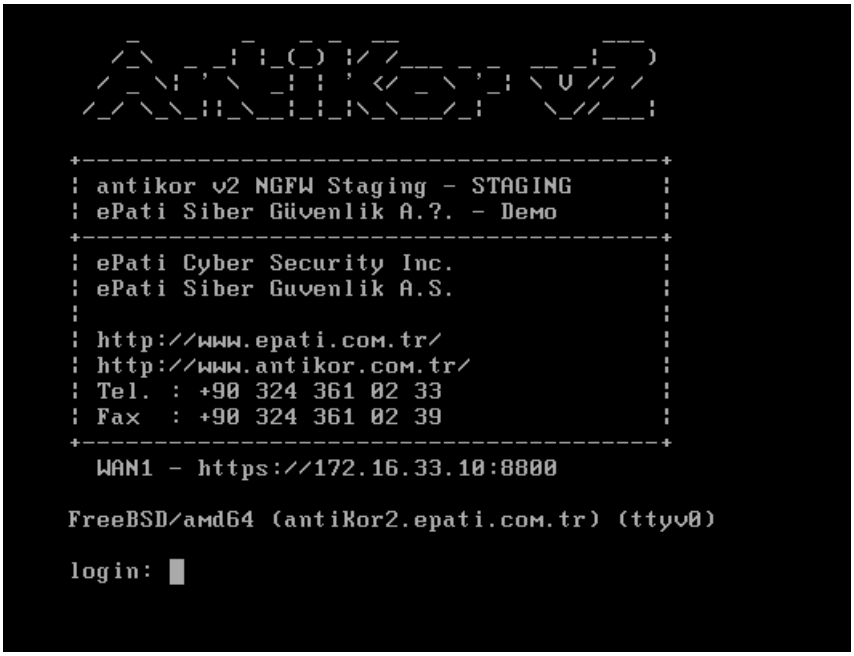
Kurulum için diskin biçimlendirilmesi gerekmektedir. Evet seçerek devam edilir.







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



İşlem tamamlandıktan sonra Antikor bir defa yeniden başlatılır.

`Not:` Kurulum gerçekleştikten sonra RAM haricinde herhangi bir donanım eklenmemeli veya çıkarılmamalıdır.

`Not:` Kurulum sonrası firewall varsayılan engelli modda çalışacağı için ICMP isteklerine yanıt vermeyecektir. `https://172.16.33.10:8800` IP adresi üzerinden arayüze erişebilirsiniz.

Sistemde Oluşan Hata Sonrasında Gerçekleştirilecek Eylemler

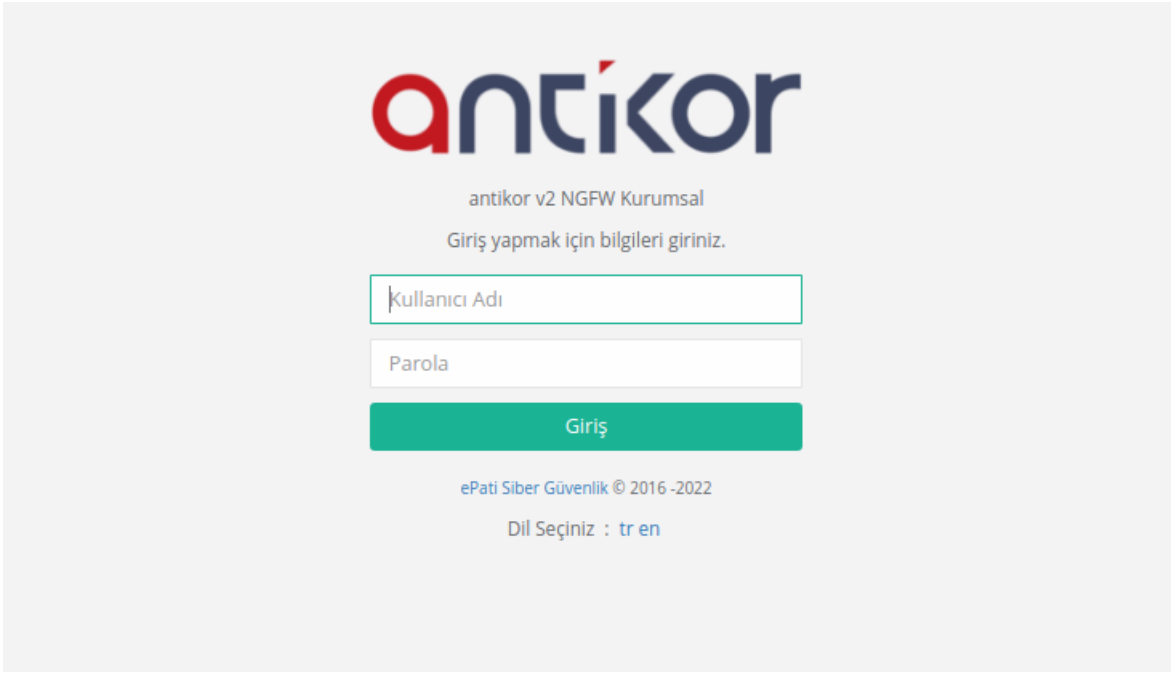
Sistemde herhangi bir arıza yaşanması durumunda lütfen aşağıdaki adımları takip ediniz. \
1. Yaşanan arıza ile ilgili olarak, arızanın ne zaman ve hangi işlemden sonra ortaya çıktığı, karşılaşılan detaylar ve varsa hata çıktısı ile birlikte teknik destek talep edilmelidir. \
2. Yaşanan arıza sadece belli servisleri etkiliyorsa, ilgili servis kapatılmalıdır. \
3. Sistem Bilgileri sayfasında, Sistem Tanılama Paketi ile birlikte teknik destek talep edilmelidir. \
4. Yaşanan arıza tüm sistemi olumsuz etkiliyor ve yedek sistemin mevcut olması halinde yedek sistem devreye alınmalıdır.

Kurulum Sonrası Temel Yapılandırmalar

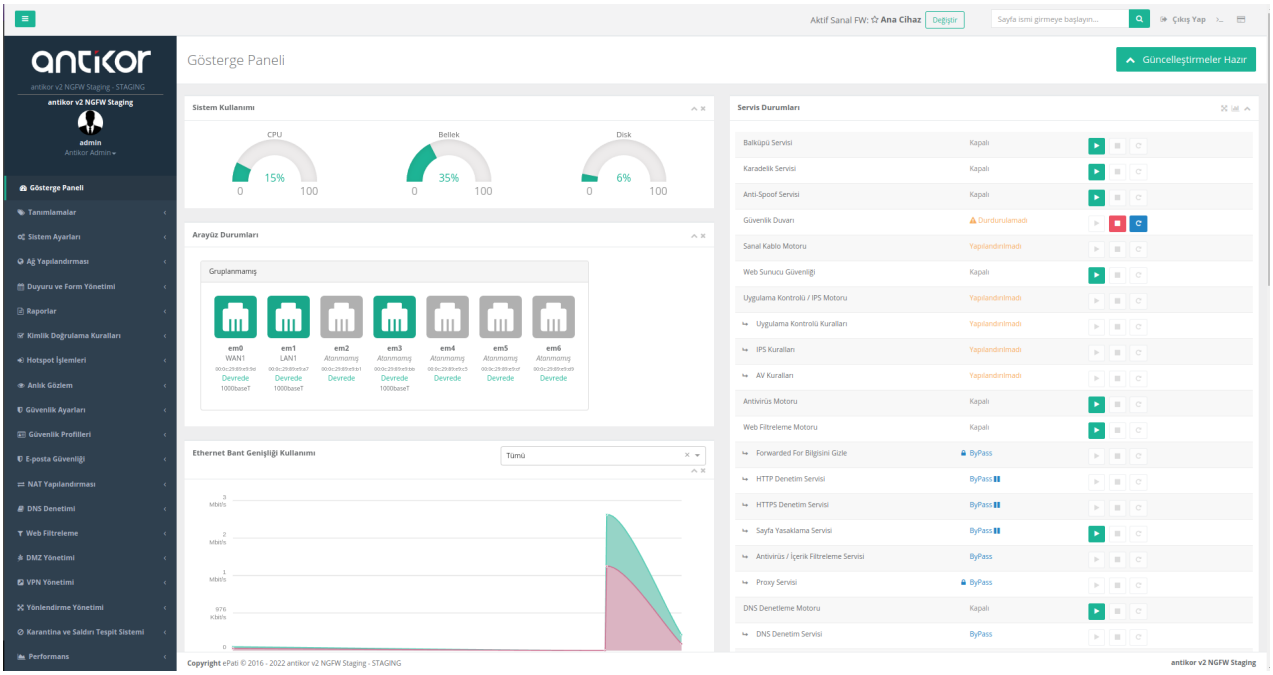
Antikor Güvenlik Duvarının WEB arayüzüne nasıl girilir?

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;

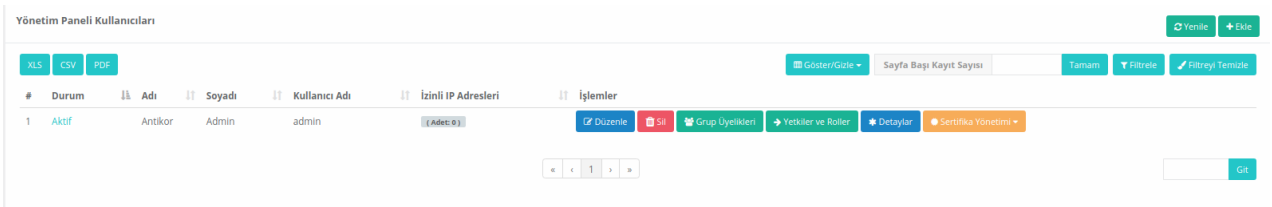
- Tarayıcının adres kısmına sunucuya verilmiş olan IP adresihttps://172.16.33.10:8800 girilir. Port 8800 olduğu için “https://” nin yazılması unutulmamalıdır.



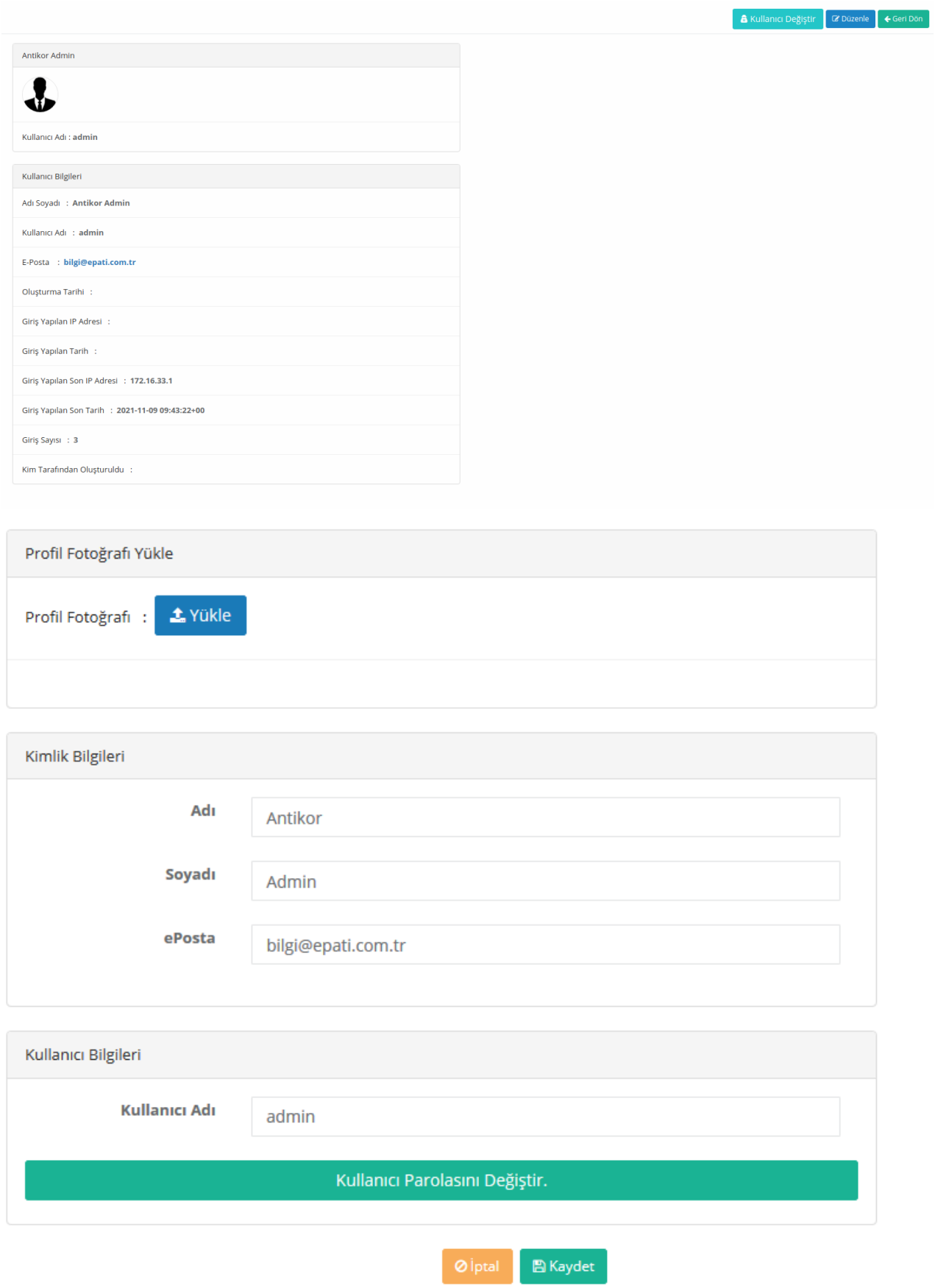
- Giriş ekranı gelecektir. Kullanıcı adı “admin” ve parolayı “antikor” yazarak`Giriş` butonuna tıklanır.



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.



Açılan sayfada “Düzenle” butonuna tıklanır.



Kullanıcı Parola Günceleme

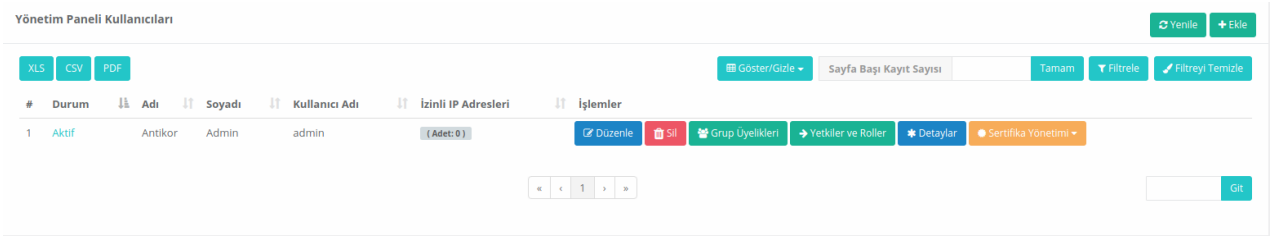
Kullanıcı bilgileri bölümünde yeni Parola belirlenerek “Kaydet” butonuna tıklanır.

Yeni Kullanıcı Oluşturulması

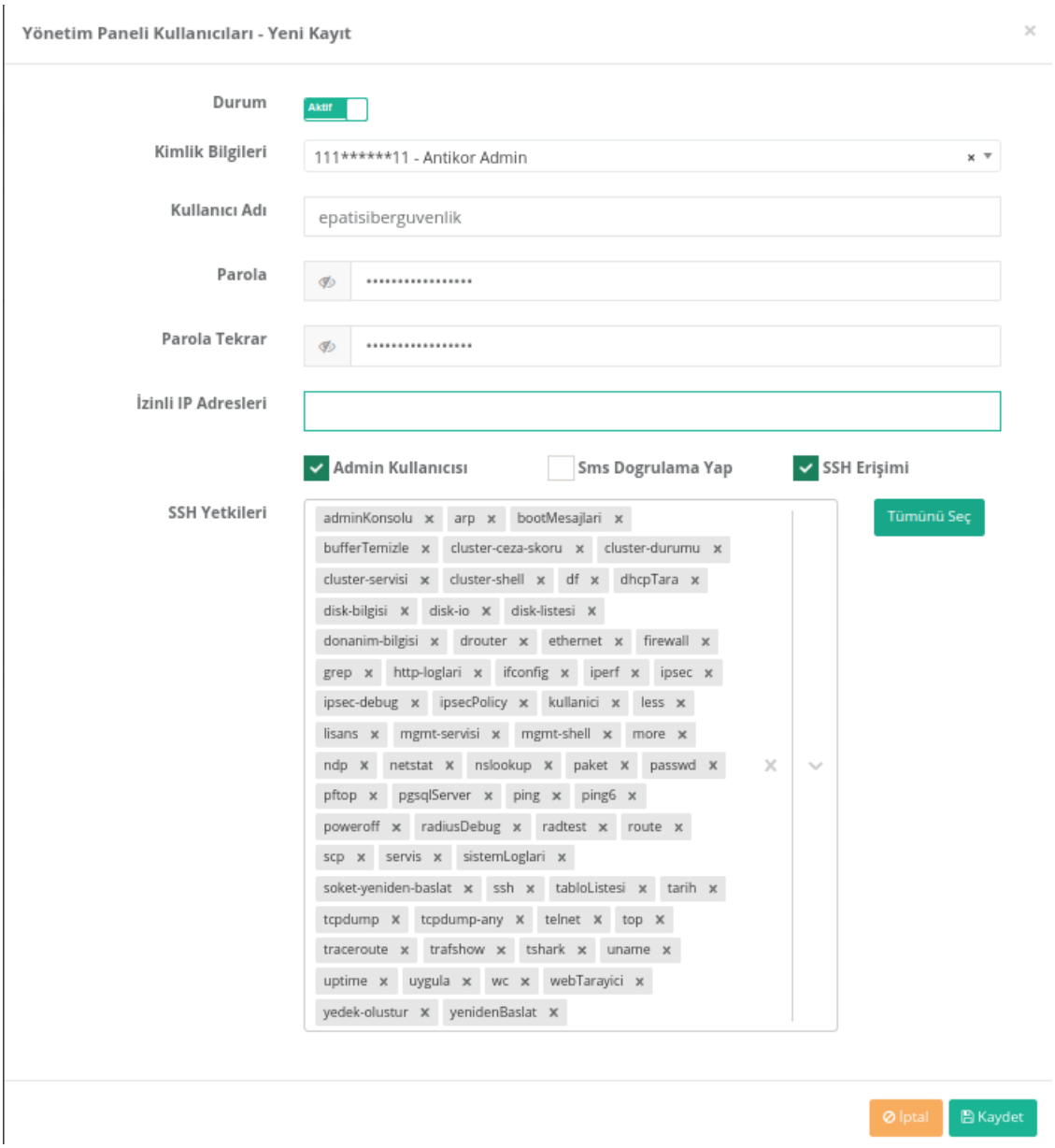
Sistemi yöneten kullanıcıların her birinin kendi kullanıcı ve şifrelerini kullanarak arayüze giriş yapması güvenlik ve sistem yönetimi yönünden olumlu etki yaratacaktır.

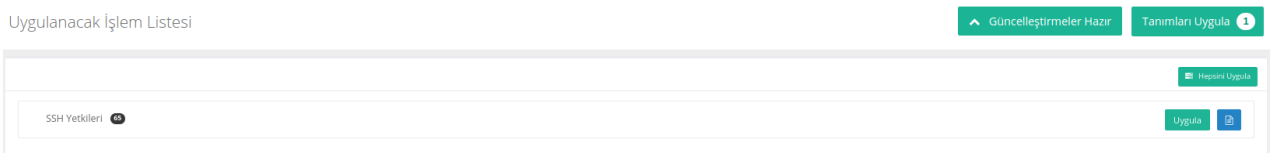
Yeni bir kullanıcı oluşturmak için öncelikle **Yönetim Paneli Erişim Ayarları** menüsünden **Yönetim Paneli Kullanıcıları**na gidilir.

Yönetim Paneli Kullanıcılarında **Ekle** Butonuna tıklanır.



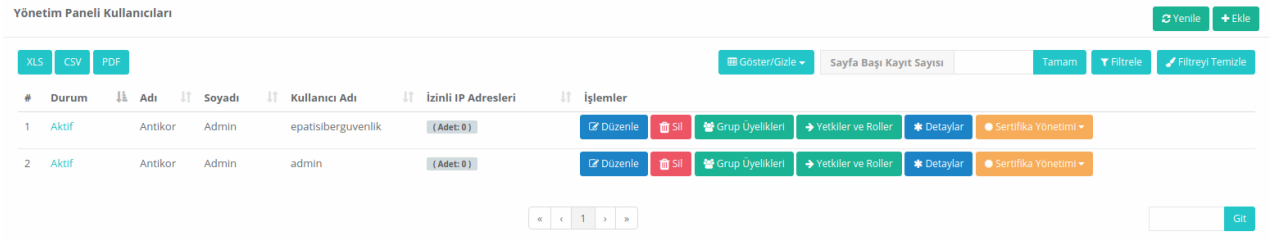
Kullanıcı için gerekli bilgiler ve temel yetkileri (admin kullanıcısı, SSH Erişimi) girilerek**Kaydet** butonuna tıklanır ve tanımlar uygulanır.

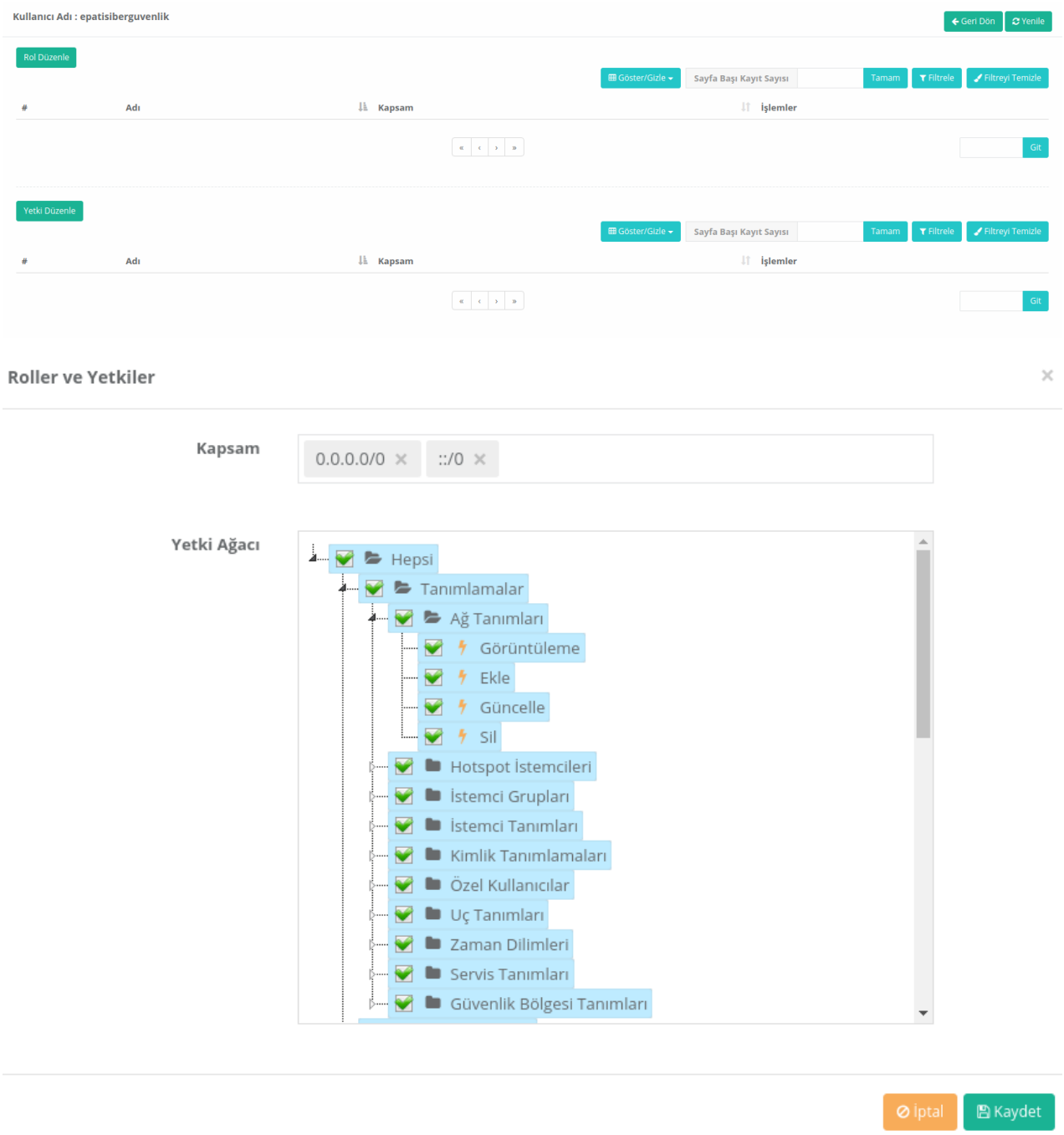




Not: Kullanıcının eklenmesi için öncelikle menüde **Tanımlamalar** bölümünde bulunan **Kimlik Tanımlamaları**ndan kullanıcı ile ilgili bilgilerin eklenmesi(burada kimlik bilgisi bulunmuyorsa) gerekmektedir.

- Kullanıcı için yetki ve roller belirlenebilmektedir.





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

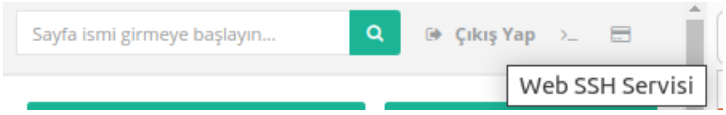
Detaylı Bilgi İçin: http://kitaplik.epati.com.tr/kilavuzlar/antikor-v2-yeni-nesil-guvenlik-duvari/kullanici-yonetimi/yonetim-paneli-kullanicilari/

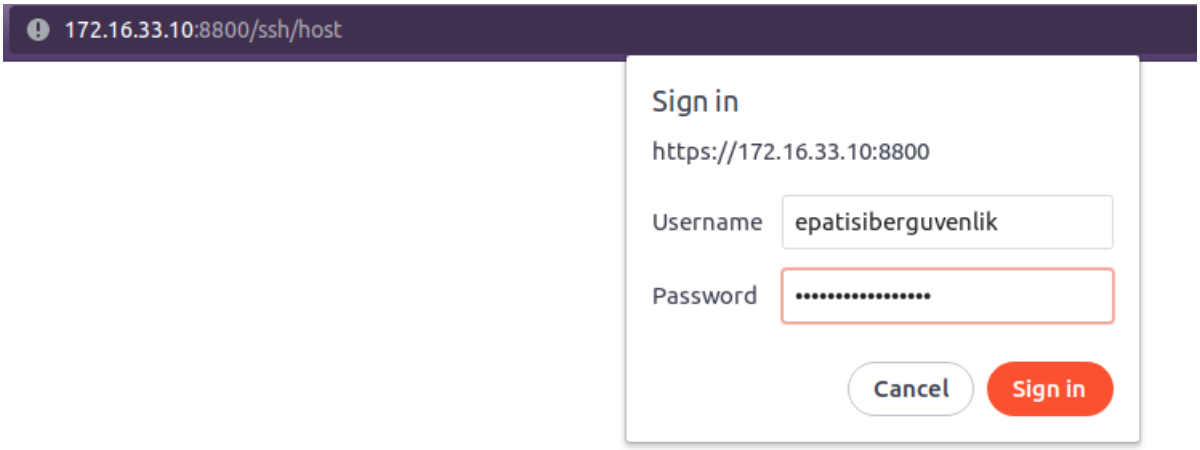
- İşlemleri tamamladıktan sonra **Tanımları Uygulayarak** yeni kullanıcı ile giriş yapabilirsiniz.

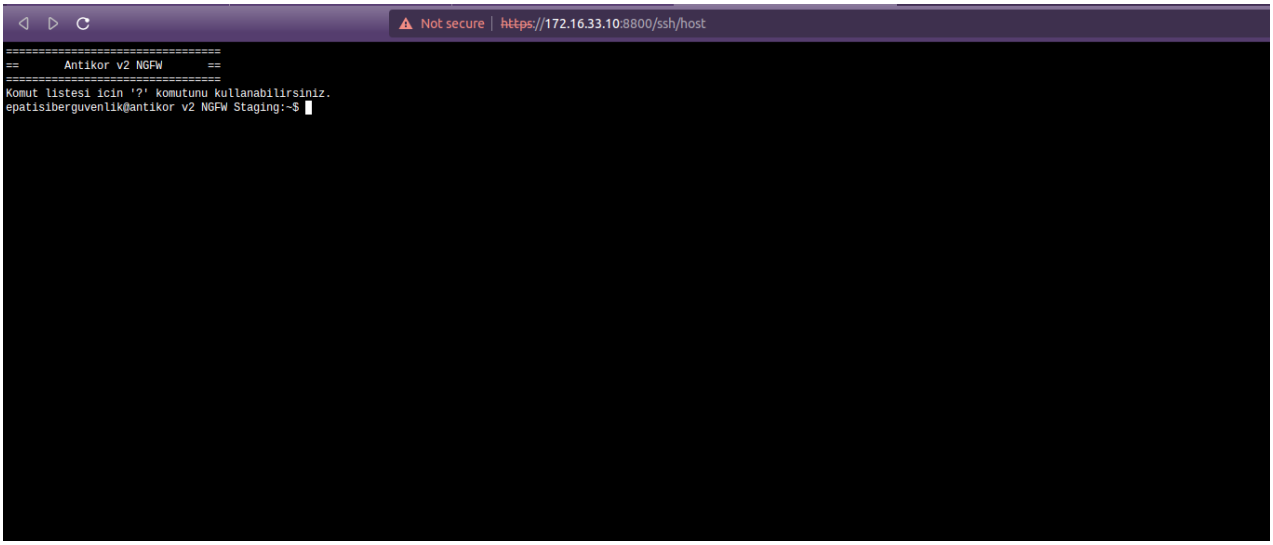
`Not:` Kullanıcı ilk girişinde sözleşmeyi okuyup onaylaması ve şifreyi değiştirmesi istenir. Bu işlemlerden sonra kullanıcı başarılı bir şekilde giriş yapabilmektedir.

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.







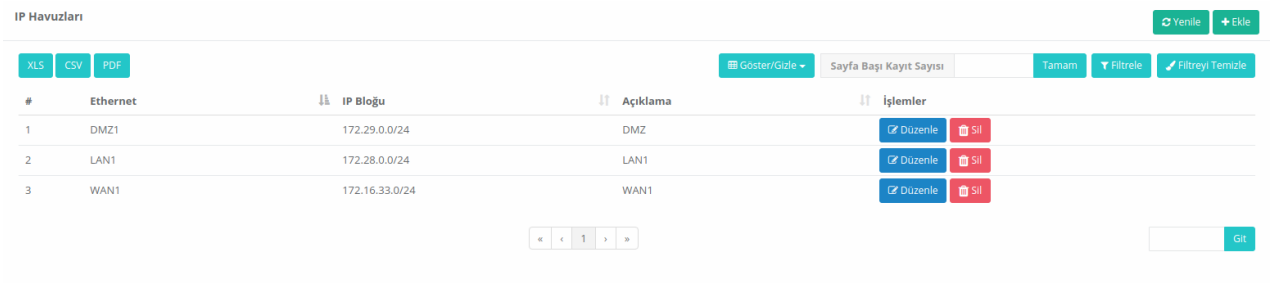
- Üçüncü parti uygulamalar ile giriş sağlanacaksa(PuTTy, Mobaxterm vb…) kullanıcılarının SSH'a erişebilmesi için ilk önce ssh-key üretilmelidir.

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-yapilandirilmasi/

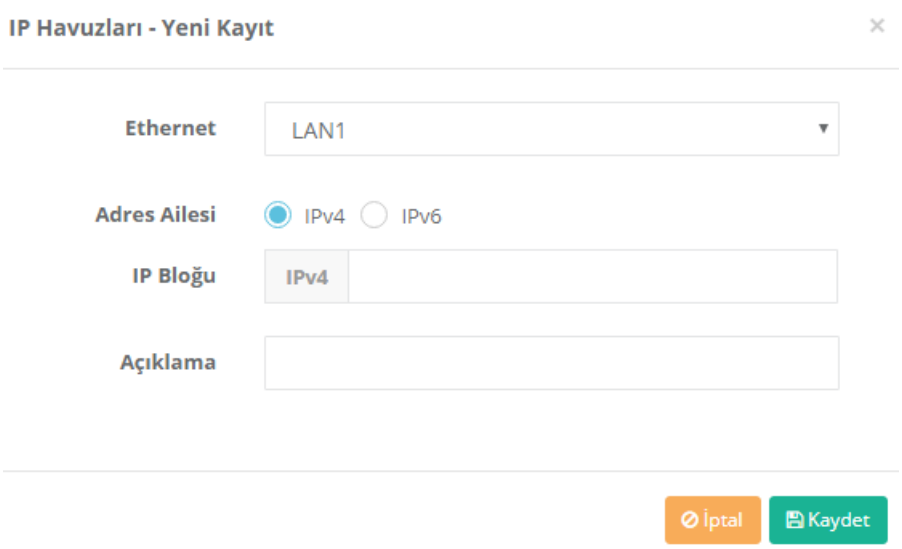
IP Havuzları

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 eklemeden yapılamamaktadır.

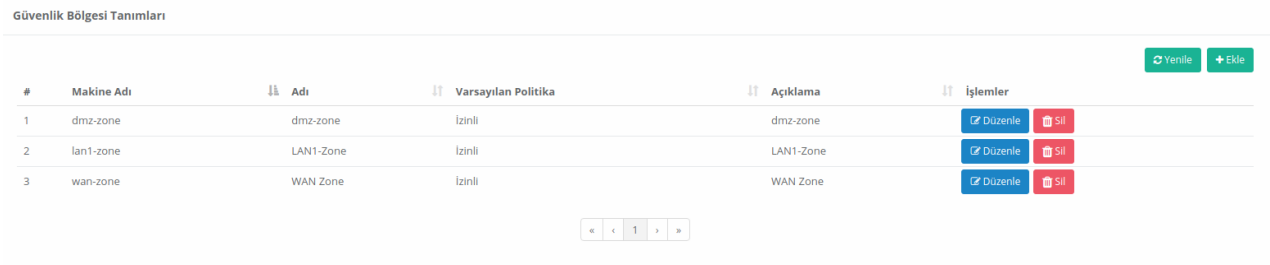


IP Havuzları Yeni Kayıt

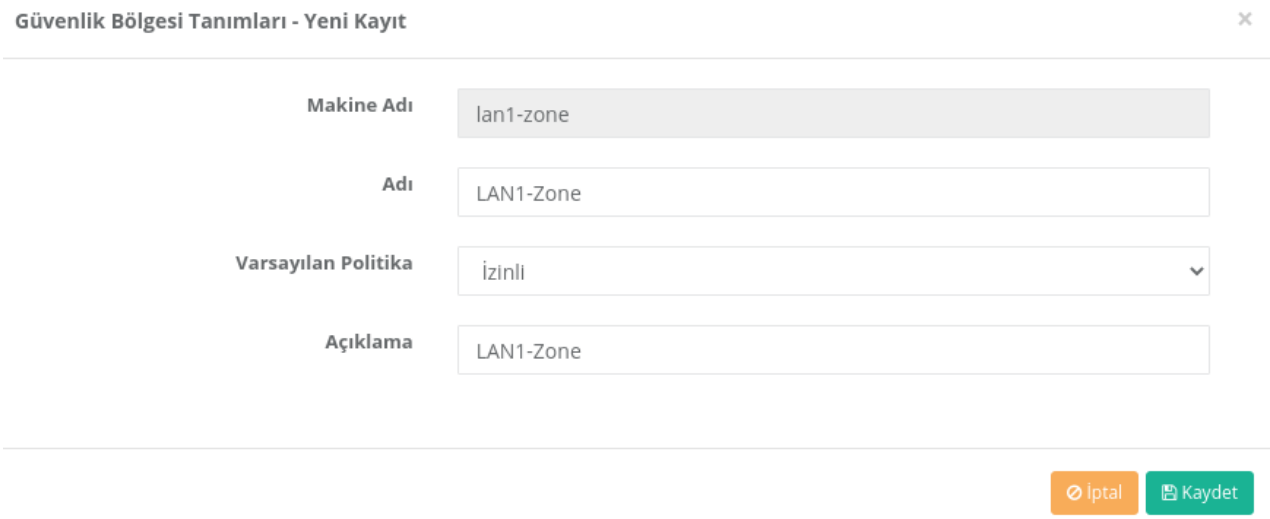


Güvenlik Bölgesi Tanımları

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

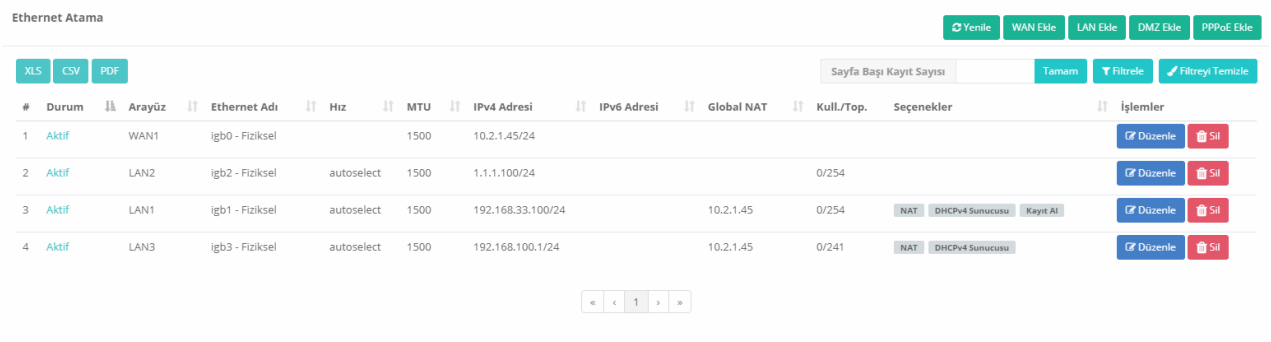


Güvenlik Bölgesi Tanımları Yeni Kayıt

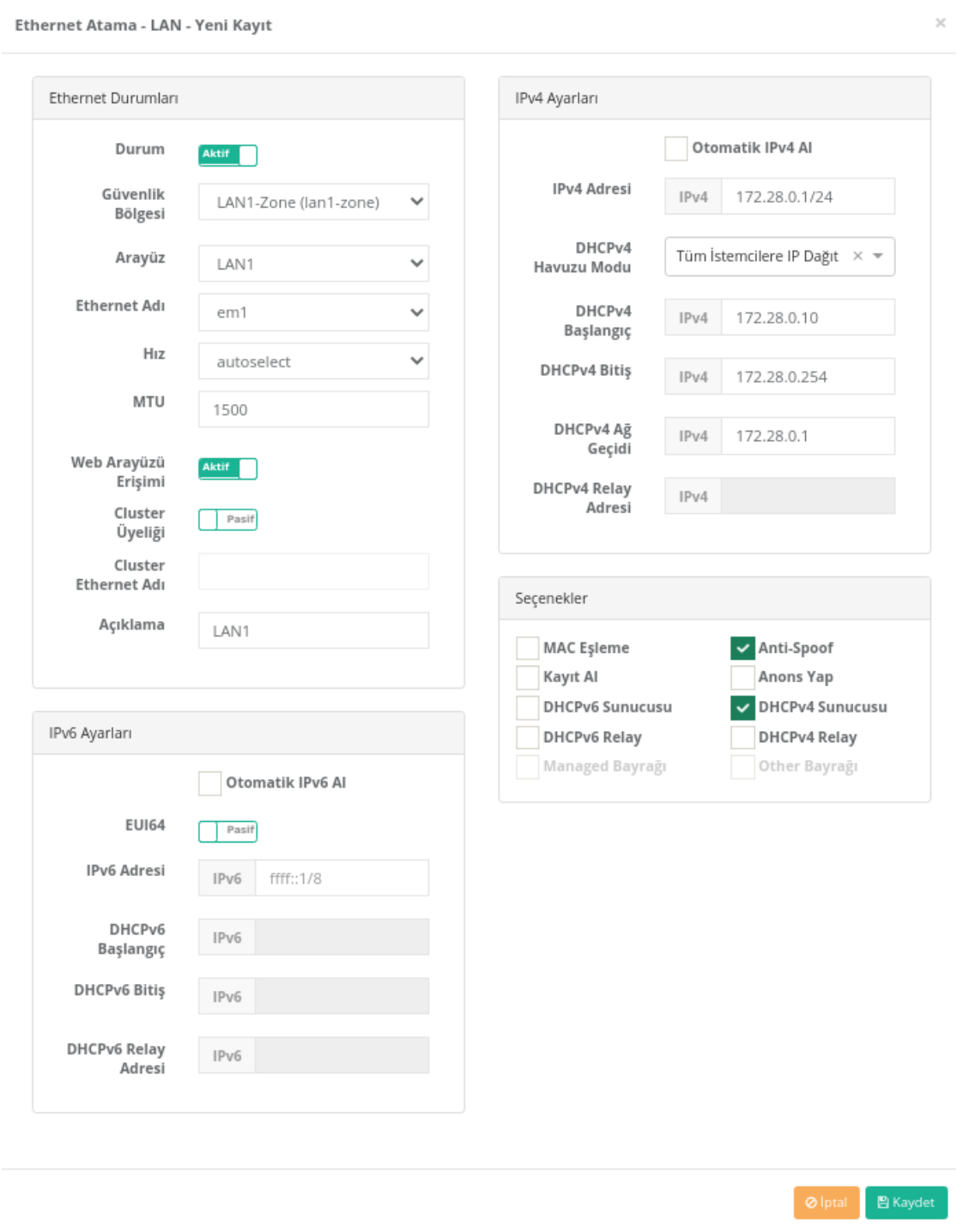


Ethernet Atama

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.



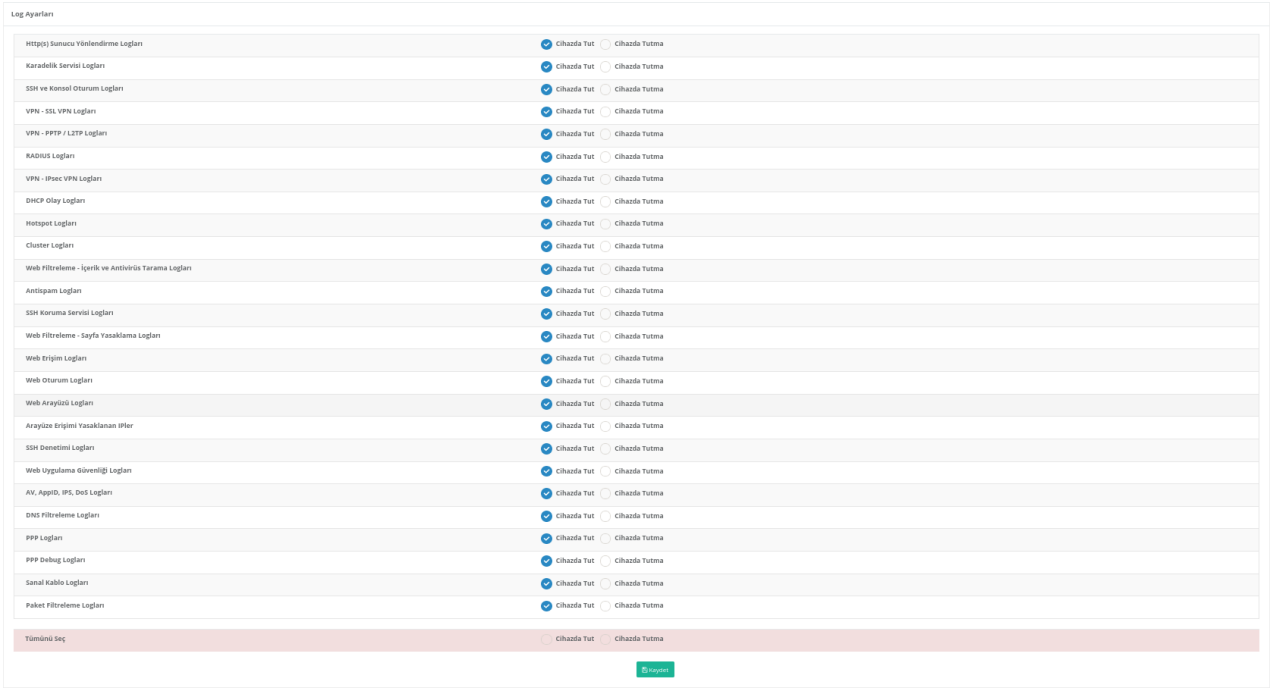
LAN Ekle Yeni Kayıt



Cihazda log tutma ayarları

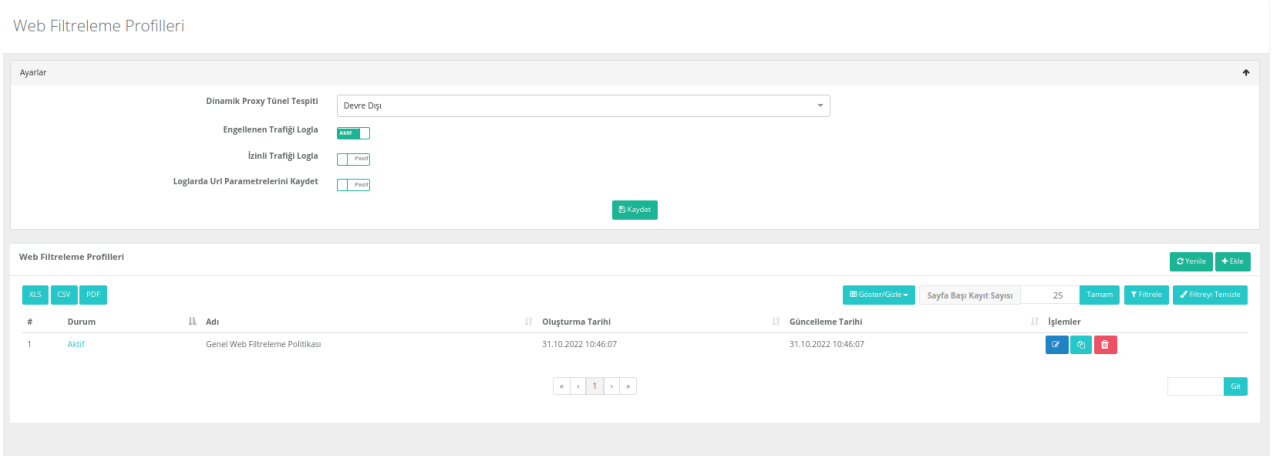
Logların, firewall üzerinde görüntülenmesi isteniyorsa sırasıyla,**Sistem Ayarları -> Log Ayarları** sayfasından logları **Cihazda tut** seçilir. Tüm logların cihazda tutulması isteniyorsa sayfanın en altında**Tümünü Seç,**

cihazda tut olarak ayarlanır.

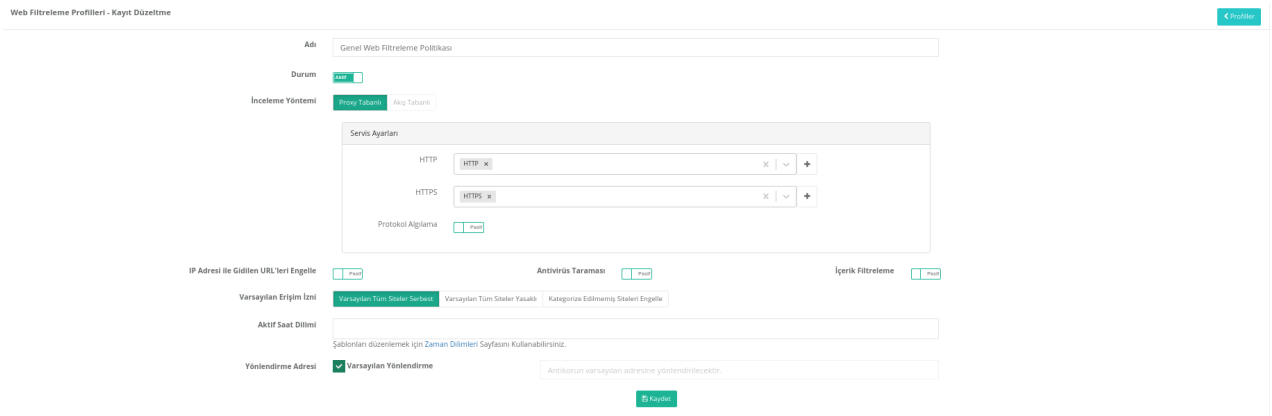


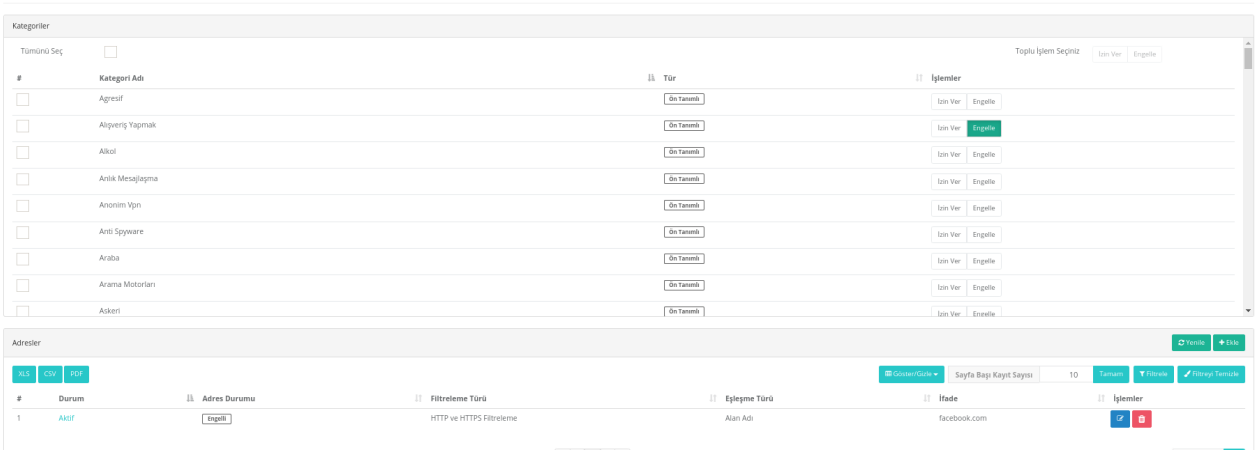
Web Filtreleme Profilleri

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.

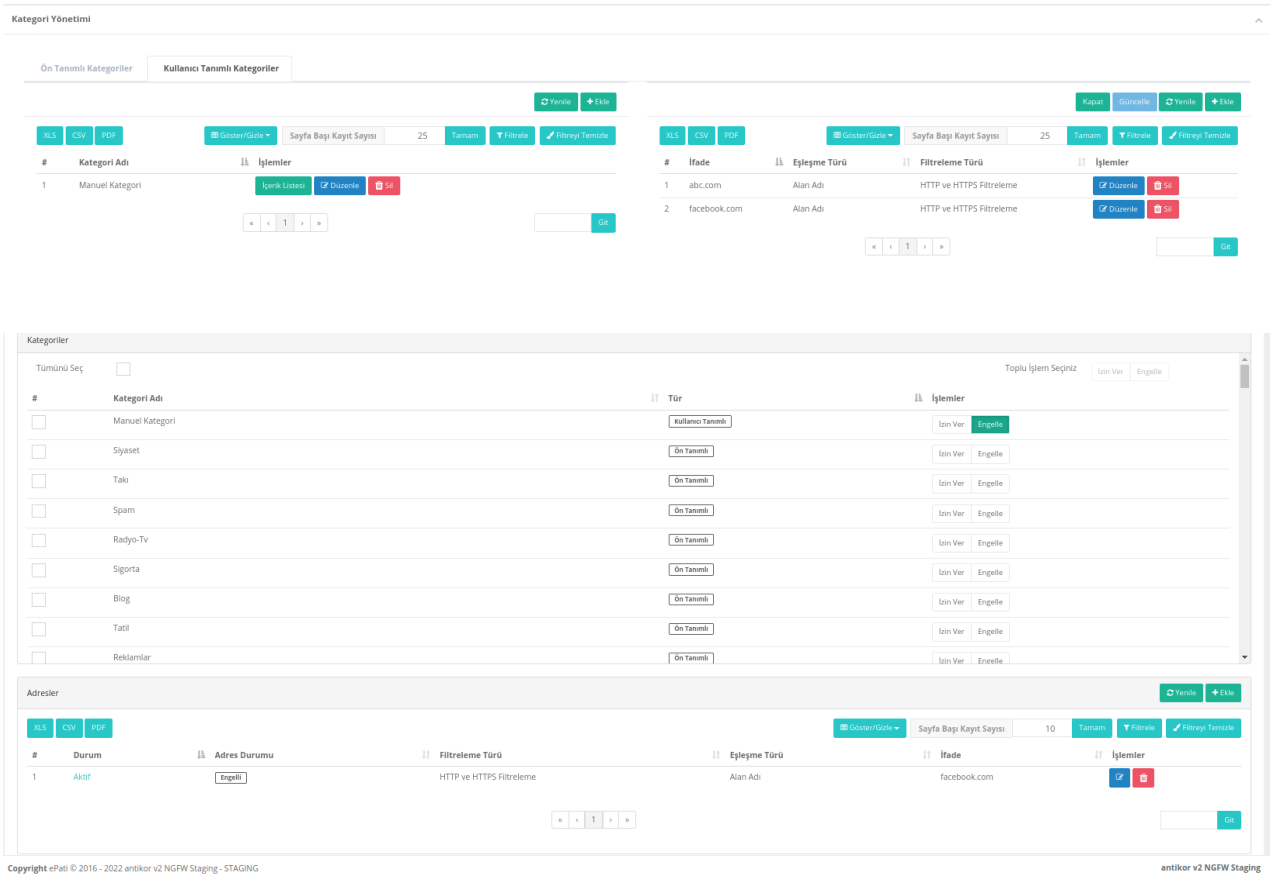


Düzenle butonuna tıklayarak ilgili profildeki yapılandırmalar ayarlanır ve kaydet butonu ile tanımlar uygulanır.





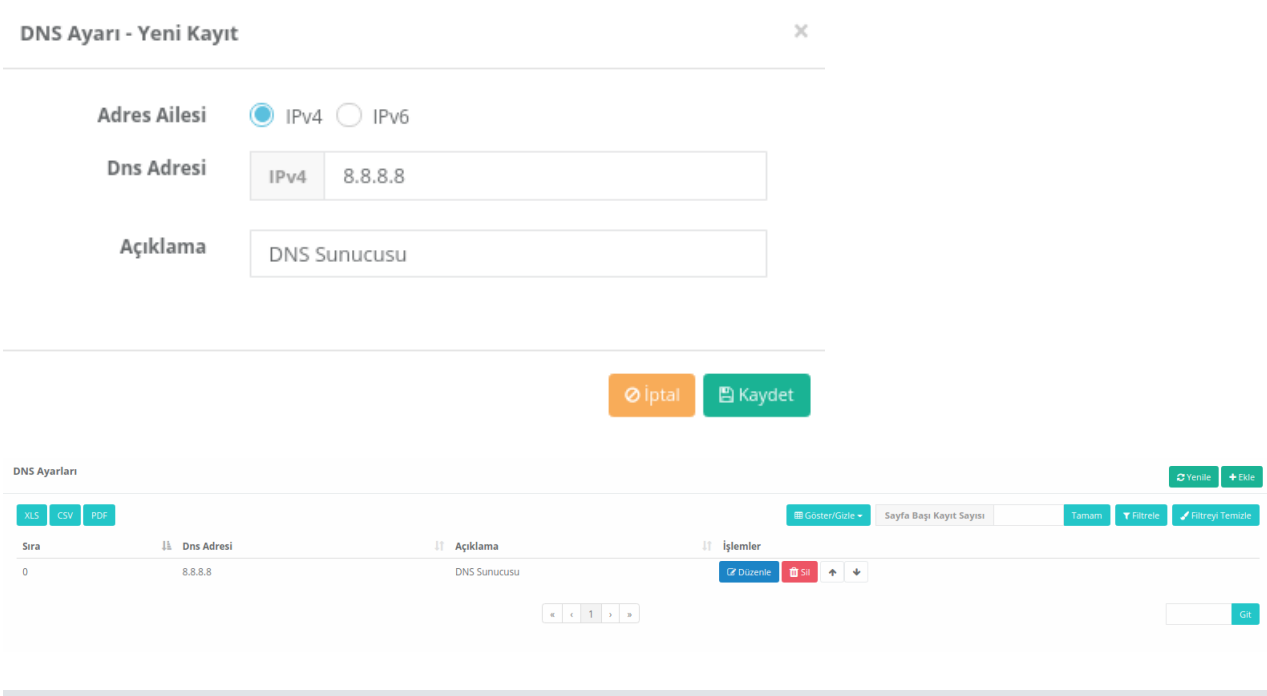
Web Filtreleme > Kategori Yönetimi sayfasında manuel olarak bir kategori oluşturulabilir ve Web Filtreleme Profilinde bu kategori izinli/engelli olarak kullanılabilir.



DNS Ayarları

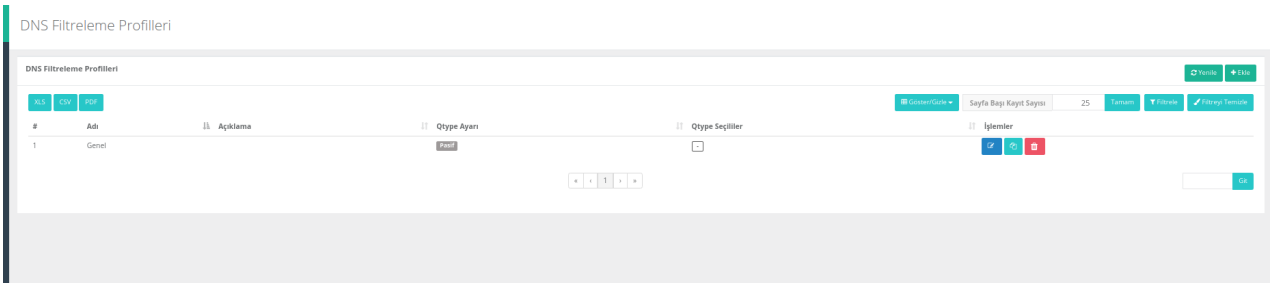
DNS (Domain Name System), internet ortamında alan adından IP'ye, IP'den alan adına dönüşümlerini gerçekleştiren sistemdir. Sistemin kullandığı DNS bilgileridir. Yerel ağdaki bilgisayarlara da DHCP servisi üzerinden DNS bilgileri dağıtılır.

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

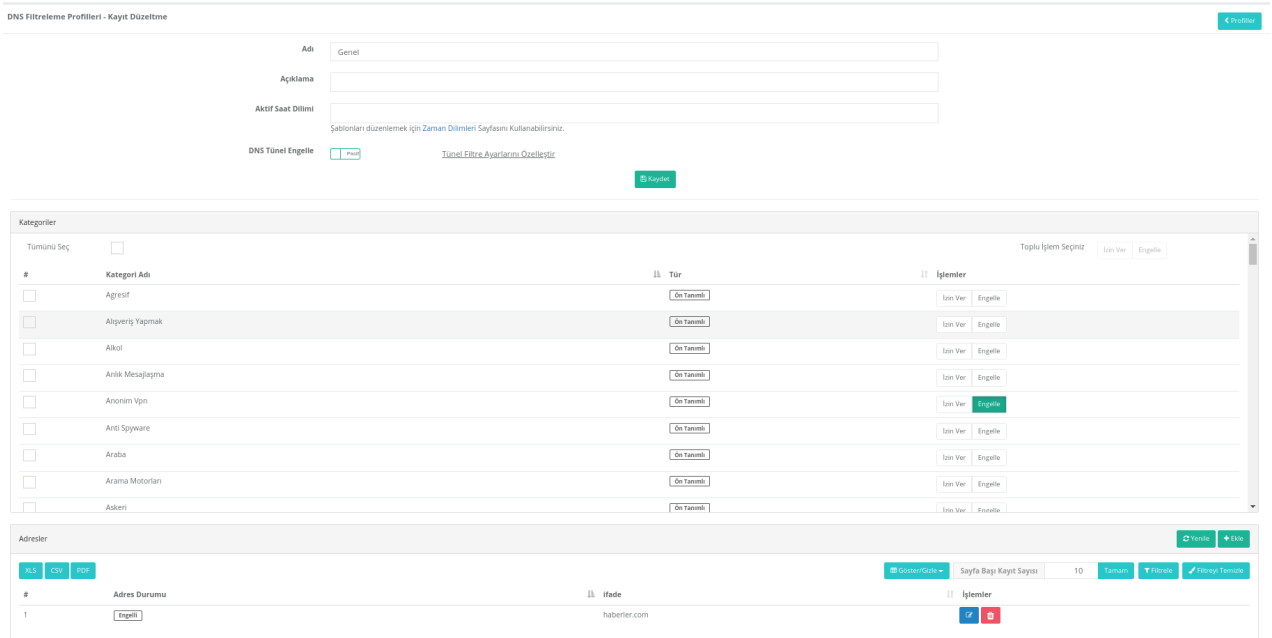


DNS Filtreleme Profilleri

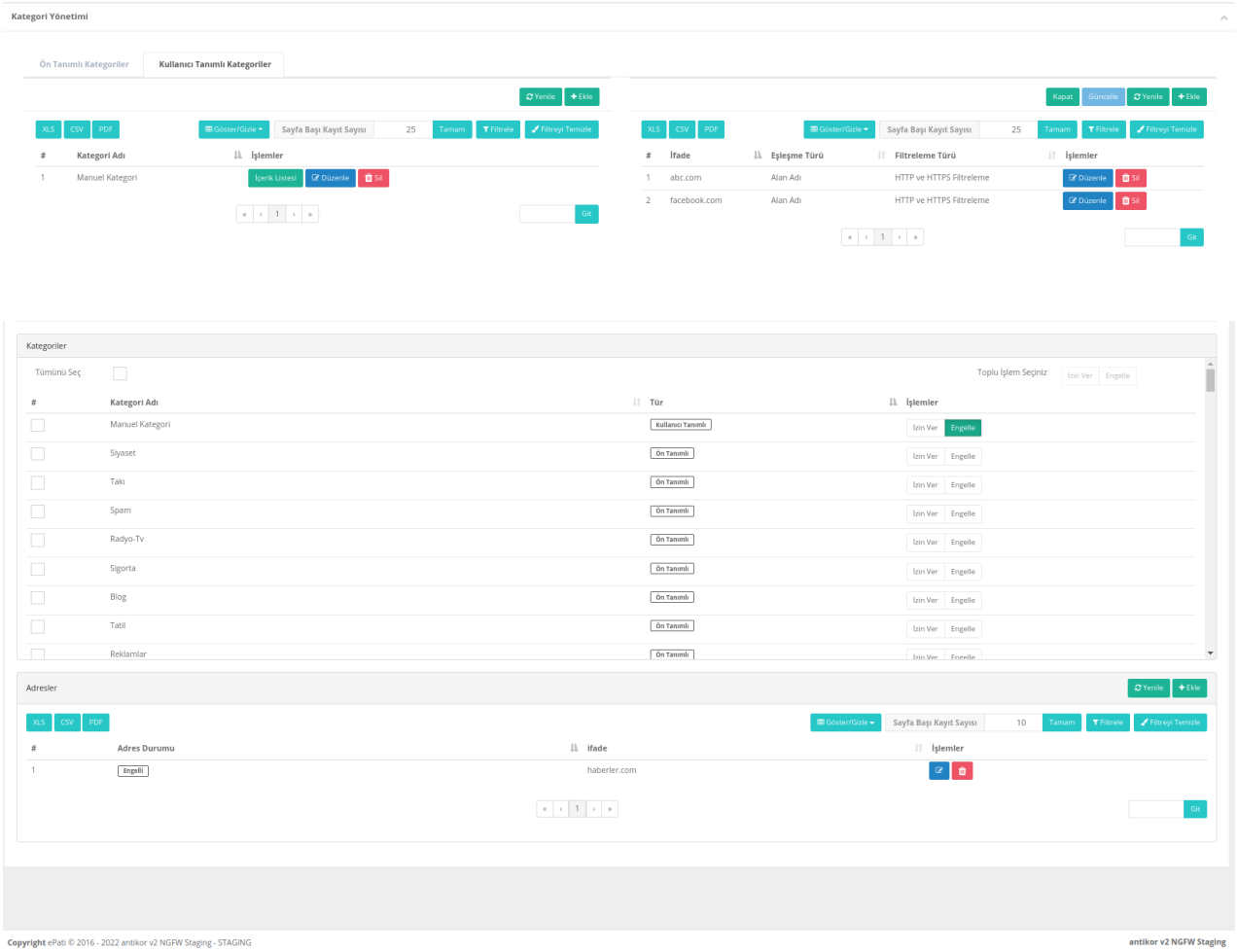
Sistemde 3 milyon 600 binin üzerinde site ön tanımlı kategorilerde gelmektedir. Bu kategorilere ek, manuel olarak da izinli ve engelli sayfalar tanımlanabilmektedir



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

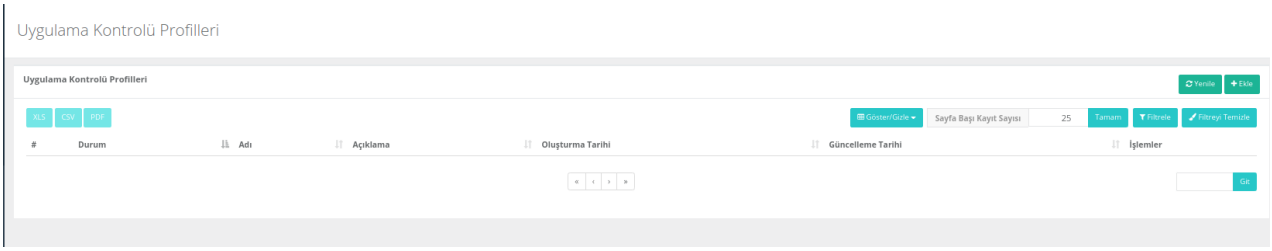


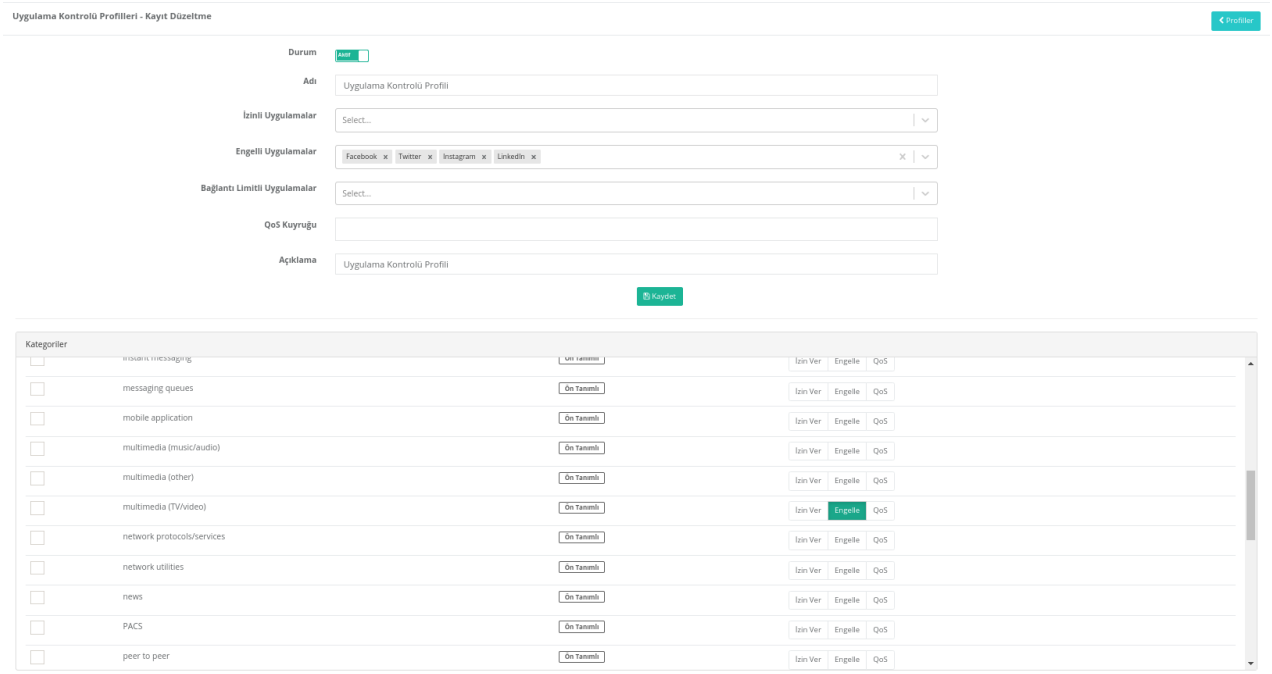
Web Filtreleme > Kategori Yönetimi sayfasında manuel olarak bir kategori oluşturulabilir ve DNS Filtreleme Profilinde bu kategori izinli/engelli olarak kullanılabilir.



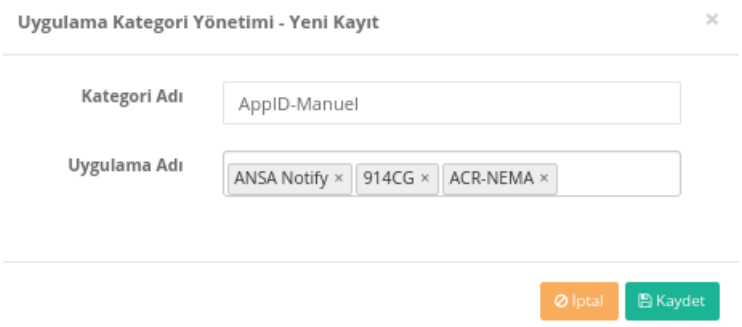
Uygulama Kontrolü Profilleri

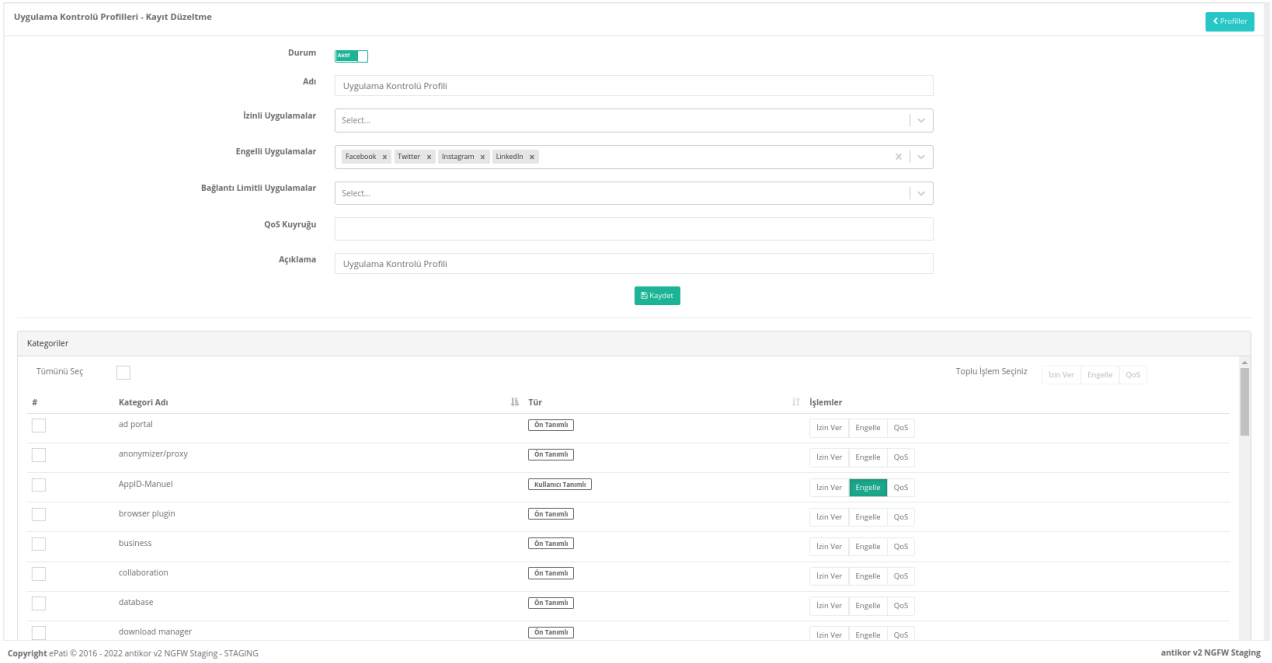
Uygulama kontrolü için profillerin belirlendiği sayfadır. Yeni profil girmek için Ekle butonuna tıklanmalıdır ve kaydet butonuna basılır.





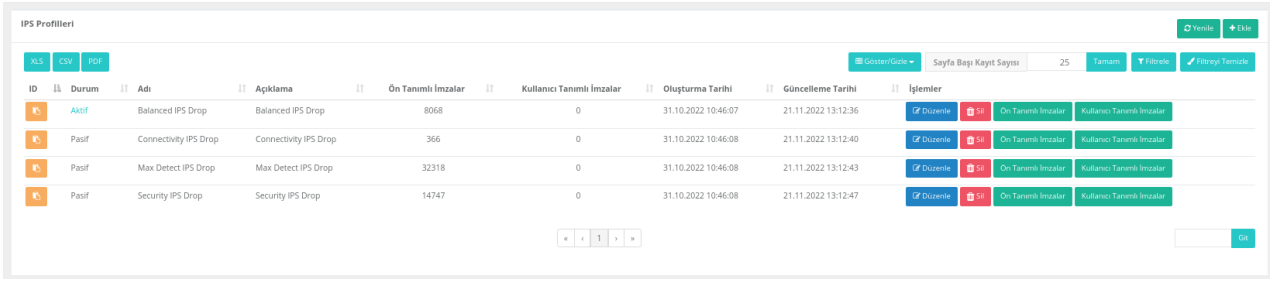
Güvenlik Ayarları > Uygulama Kategori Yönetimi sayfasında manuel olarak bir kategori oluşturabilir ve Uygulama Kontrolü Profillerinde bu kategoriyi izinli/engelli olarak kullanabilirsiniz.



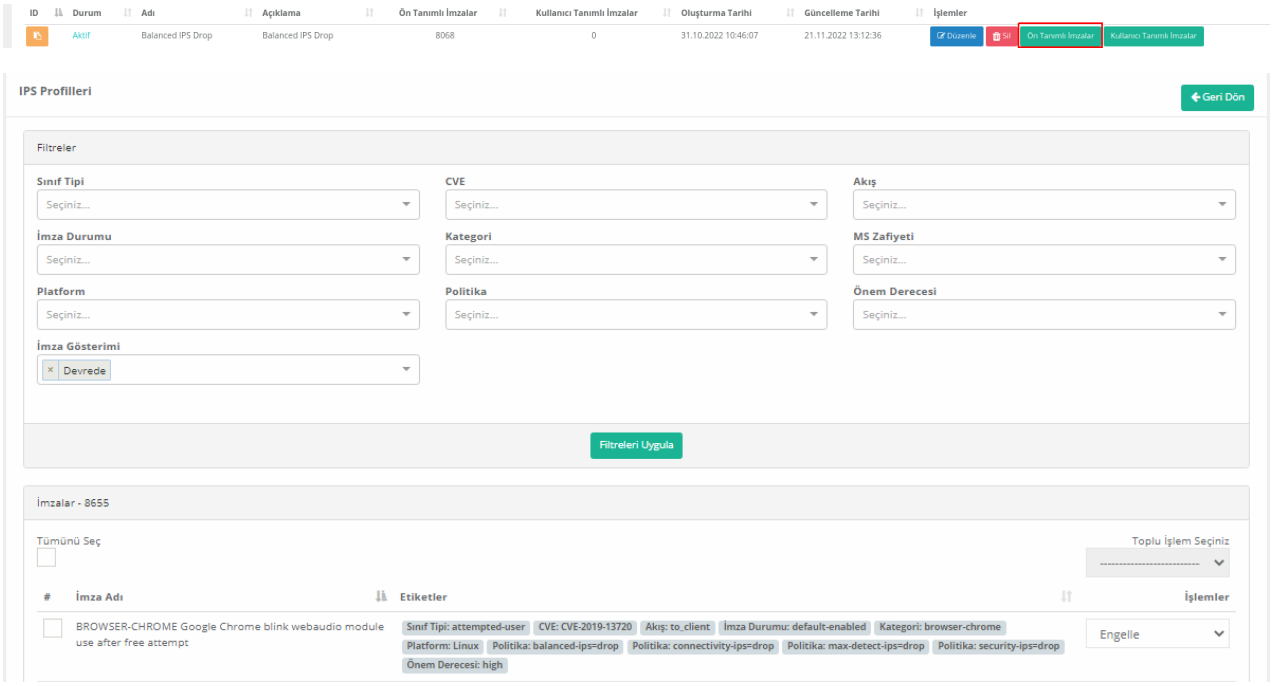


IPS Profilleri

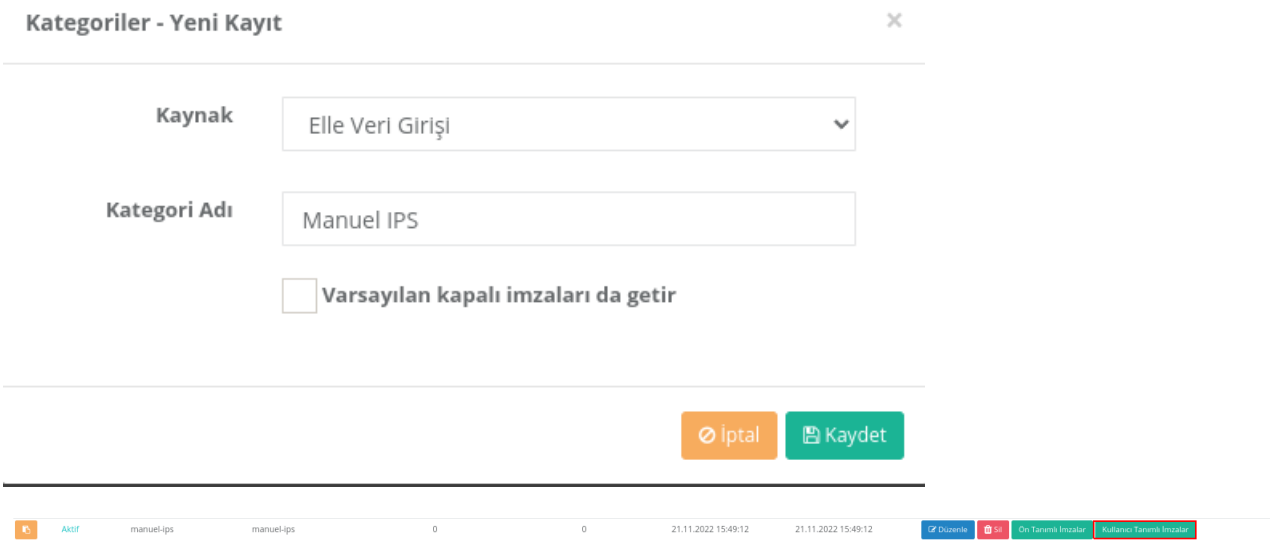
IPS, saldırı tespit ve önleme sistemidir. İnternet trafiğinden geçen paketleri inceler ve imzaları ile eşleşen trafiği tespit edip loglayabilir ve engelleyebilir.

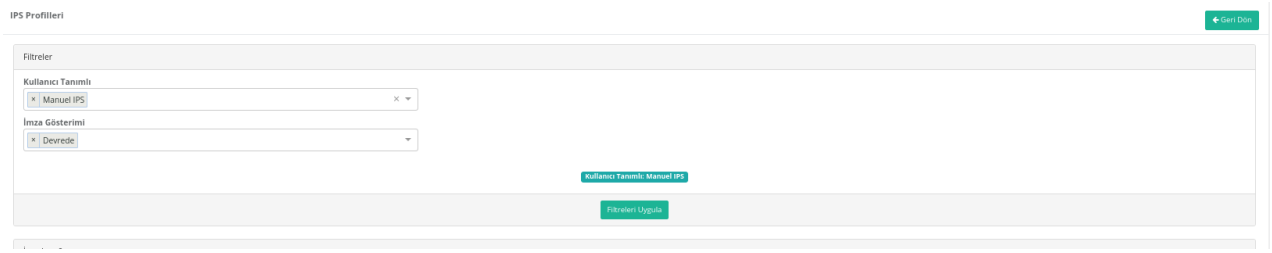


Aşağıdaki görüntüde kırmızı alan ile belirlenmiş Ön Tanımlı İmzalar butonuna tıklanıldığında, imzaların detayları ve imzalara özel “İşlemler” belirlenebilmektedir.



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

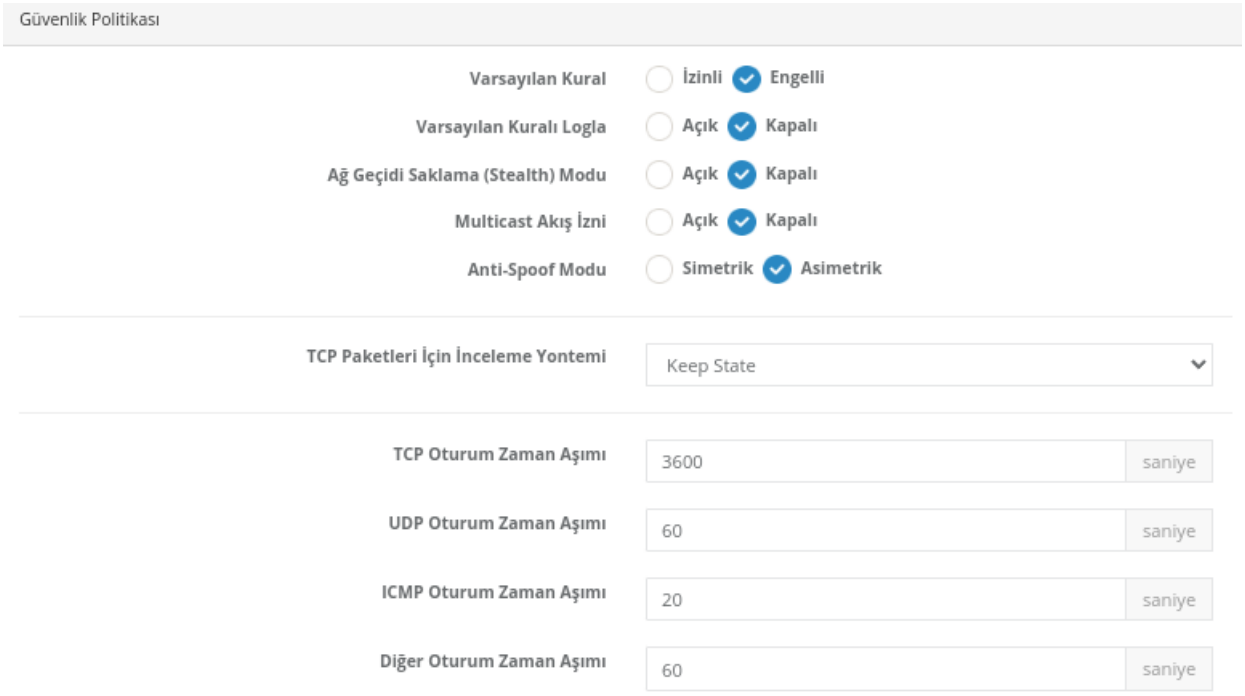




Güvenlik Kuralları

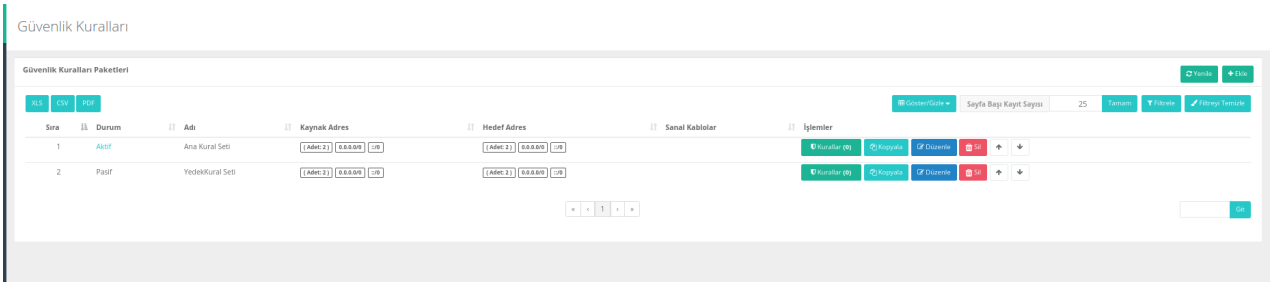
Ağdan çıkan paketlerin veya ağa gelen paketlerin izin veya engel kuralları oluşturulduğu alanlardır. Kuralların stateless sadece kaynak veya hedef adrese göre yazılabileceği gibi, statefull uçtan uca trafik inceleme yöntemiyle de yazılabilmektedir. Trafik incelemede syn, ack, fin gibi bayraklar da incelenebilmektedir. 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.



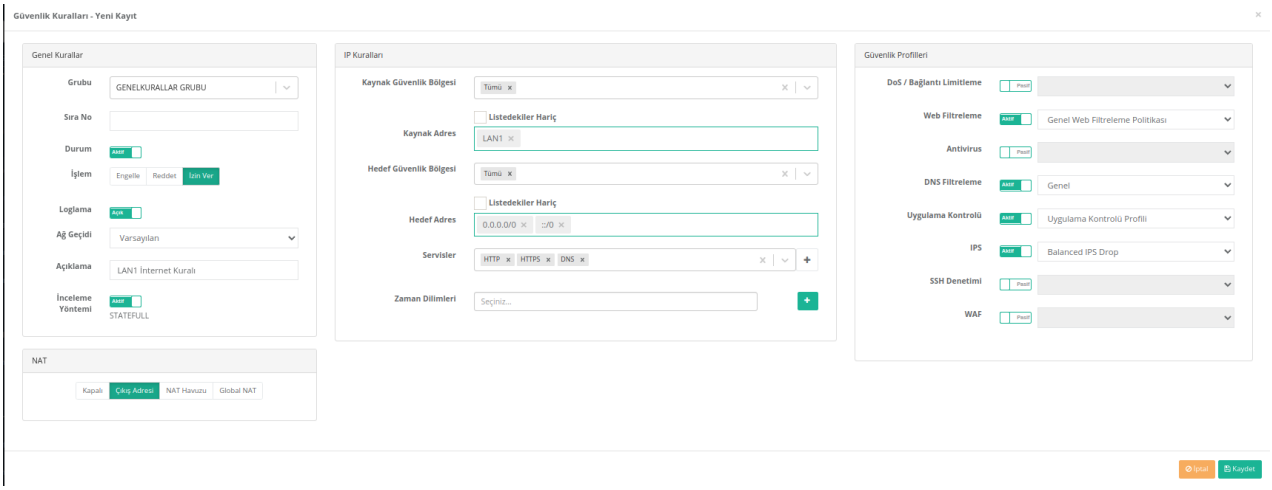
Güvenlik Kuralları Paketleri

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 Yeni Kayıt

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



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 Güvenlik 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 Güvenlik 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 Dilimi	Bir hafta içerisinde hangi gün içerisinde ve gün içerisinde hangi saatte girilen güvenlik kuralının çalışacağı belirlenir.