pfSense Captive Portal Entegrasyon Rehberi

Bu rehber, **pfSense** güvenlik duvarının Captive Portal özelliği ile Useroam Cloud arasındaki misafir hotspot entegrasyonunu adım adım anlatır. Misafir, pfSense'in misafir ağına bağlanır; telefonunda Useroam karşılama sayfası açılır (SMS, WhatsApp ve diğer giriş yöntemleri); kimlik doğrulaması RADIUS ile Useroam'da yapılır ve misafir internete çıkar. Hız, kota, oturum süresi ve günlük bitiş saati Useroam panelindeki gruptan pfSense'e otomatik gönderilir.

> **Başlamadan önce:** pfSense CE 2.7.0 / pfSense Plus 23.05 veya üstü, pfSense web arayüzüne yönetici erişimi ve pfSense'in internete çıktığı **genel (dış) IP adresi** gerekir. Menü adları sürüme göre küçük farklar gösterebilir.

> **Useroam sunucu adresi her yerde 104.247.174.120'dir.** RADIUS sunucusu, giriş öncesi izin listesi ve 5651 log hedefi bu IP ile yazılır. Başka bir adres kullanmayın.

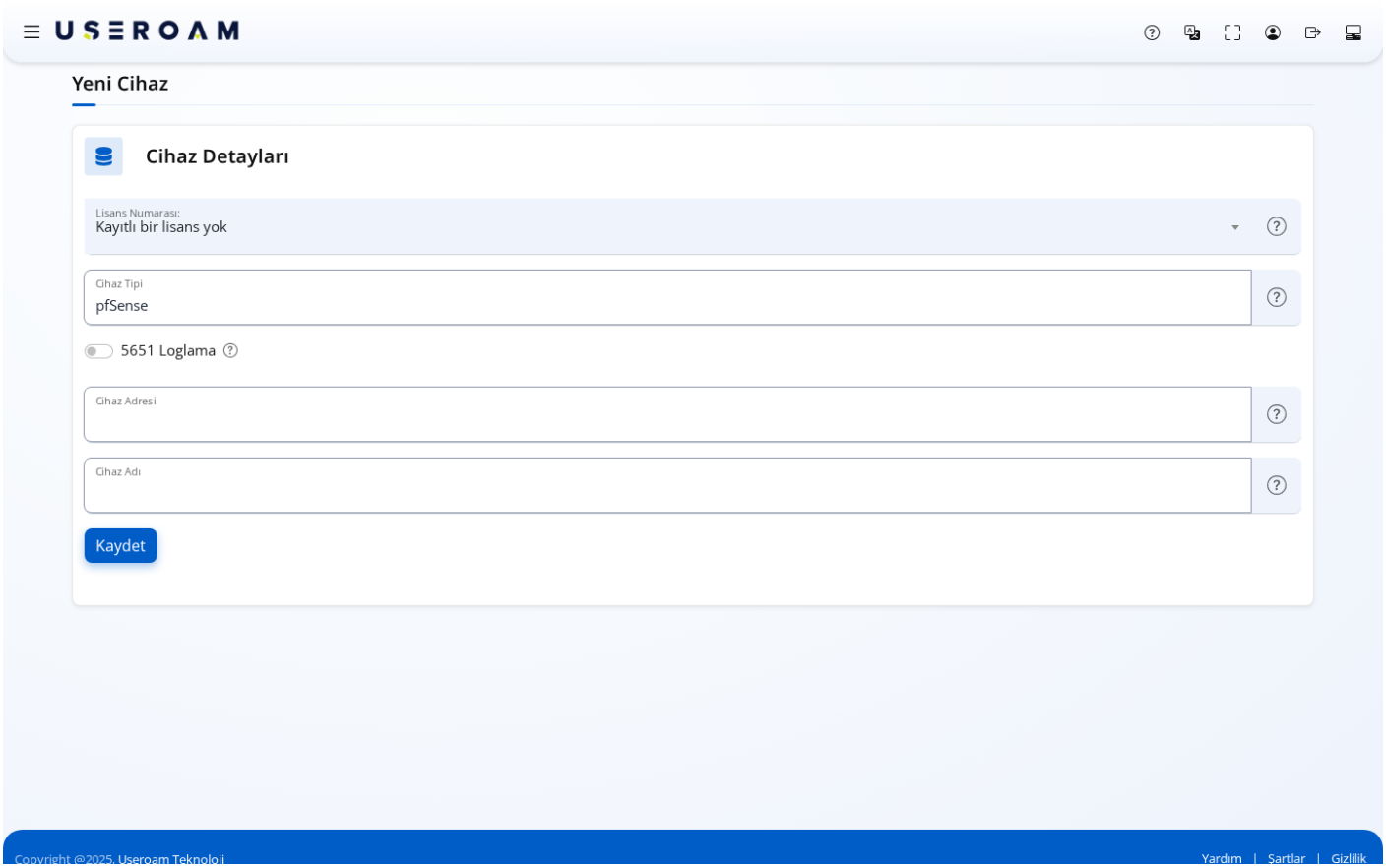
> **Nasıl çalışır?** pfSense'e Useroam'un hazırladığı küçük bir portal sayfası yüklenir. Bu sayfa misafiri Useroam karşılama sayfasına yönlendirir. Misafir giriş yaptıktan sonra kullanıcı adı ve şifre pfSense'e geri gönderilir, pfSense de bunları RADIUS ile Useroam'a sorar. pfSense'te ayrıca bir "harici portal" ayarı yoktur; yöntem budur.

1 - Useroam Paneline Cihaz Ekleme

panel.useroam.com adresinden panelinize giriş yapıp **Yeni Cihaz** ekranını açın.

- **Cihaz Tipi:** `pfSense` seçin.
- **5651 Loglama:** pfSense loglarını Useroam'a göndereceksiniz (12. adım) açın.
- **Cihaz Adresi: [KRİTİK ADIM]** pfSense'in internete çıktığı genel (dış) IP adresini yazın. pfSense bir modem/NAT arkasındaysa NAT'ın çıkış IP'si yazılır. Useroam cihazı bu IP'den tanır; RADIUS istekleri de bu IP'den gelmelidir. İç IP'yi (192.168.x.x, 10.x.x.x) yazmayın.
- **Cihaz Adı:** panelde göreceğiniz ad (ör. "Otel pfSense").

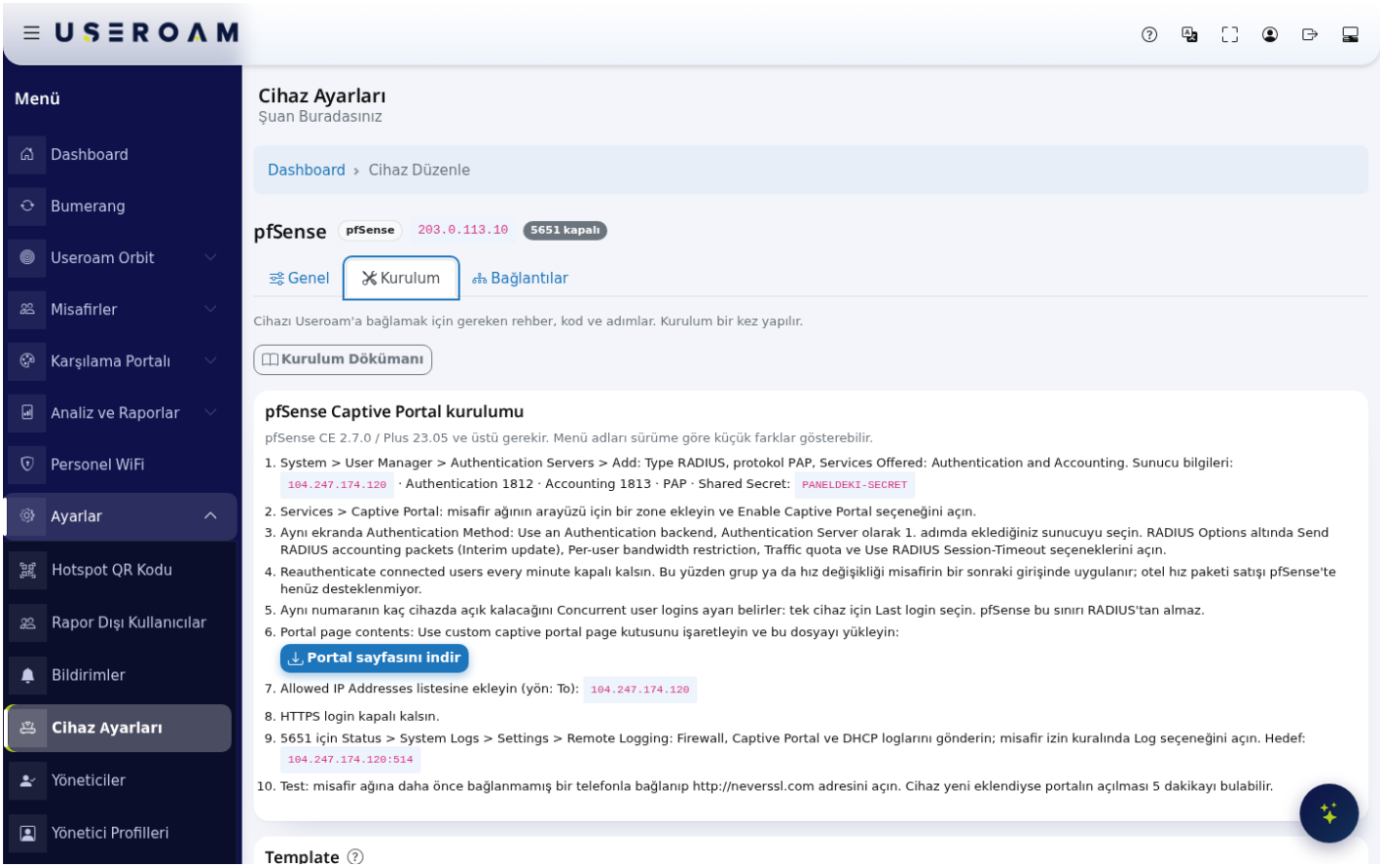
Kaydet düğmesine basın.



2 - Kurulum Bilgilerini Panelden Alma

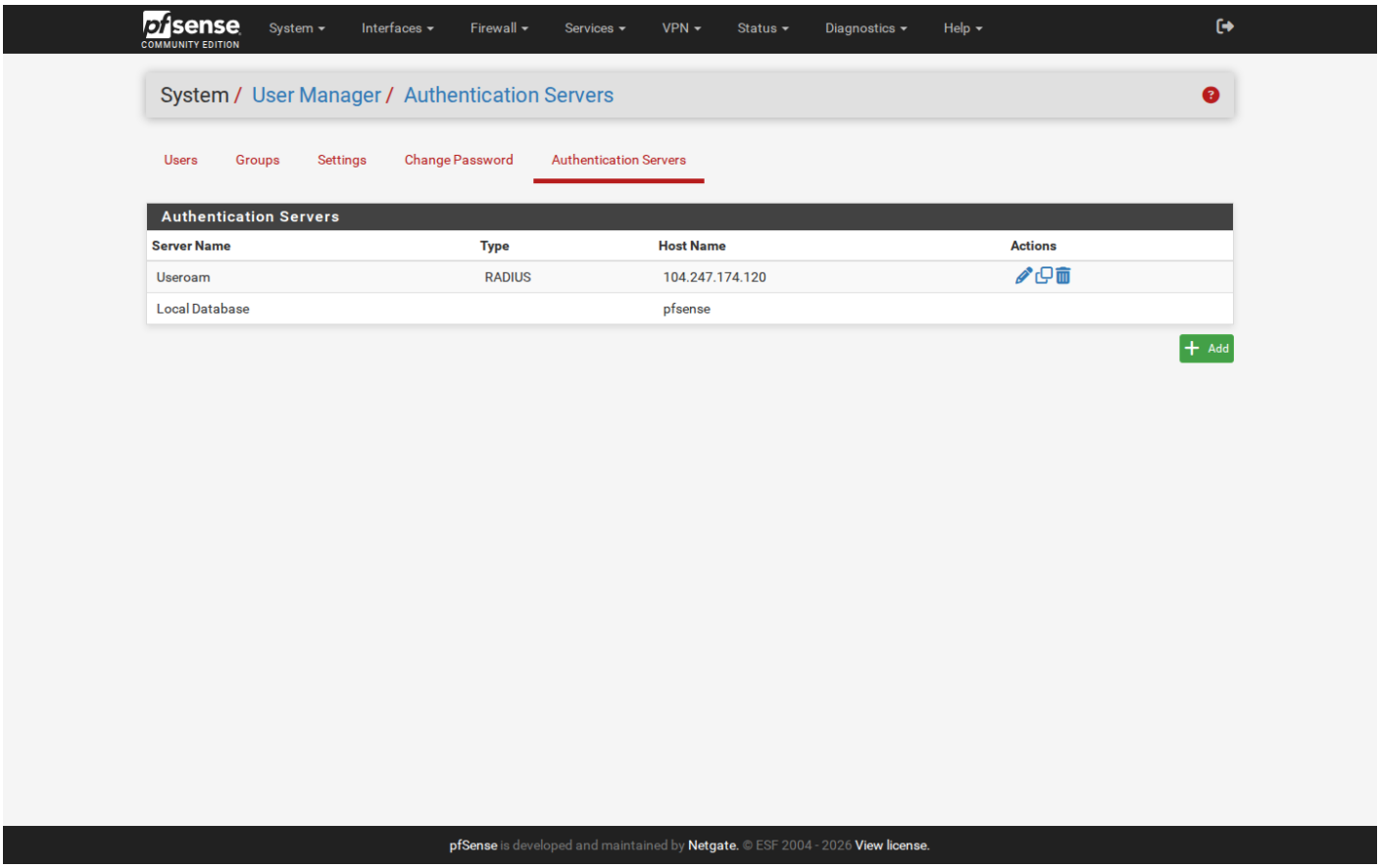
Cihaz kaydedildikten sonra **Ayarlar > Cihaz Ayarları** sayfasında **Kurulum** sekmesini açın. Burada iki şey alınır:

- **Shared Secret:** RADIUS sunucusu tanımlarken kullanılacak parola. Kartta yazan değeri kopyalayın.
- **Portal sayfasını indir:** bu düğme, cihazınızın kimliği içine yazılmış portal dosyasını (`portal.html`) indirir. Dosyanın içini değiştirmeyin; 6. adımda pfSense'e yüklenecek.

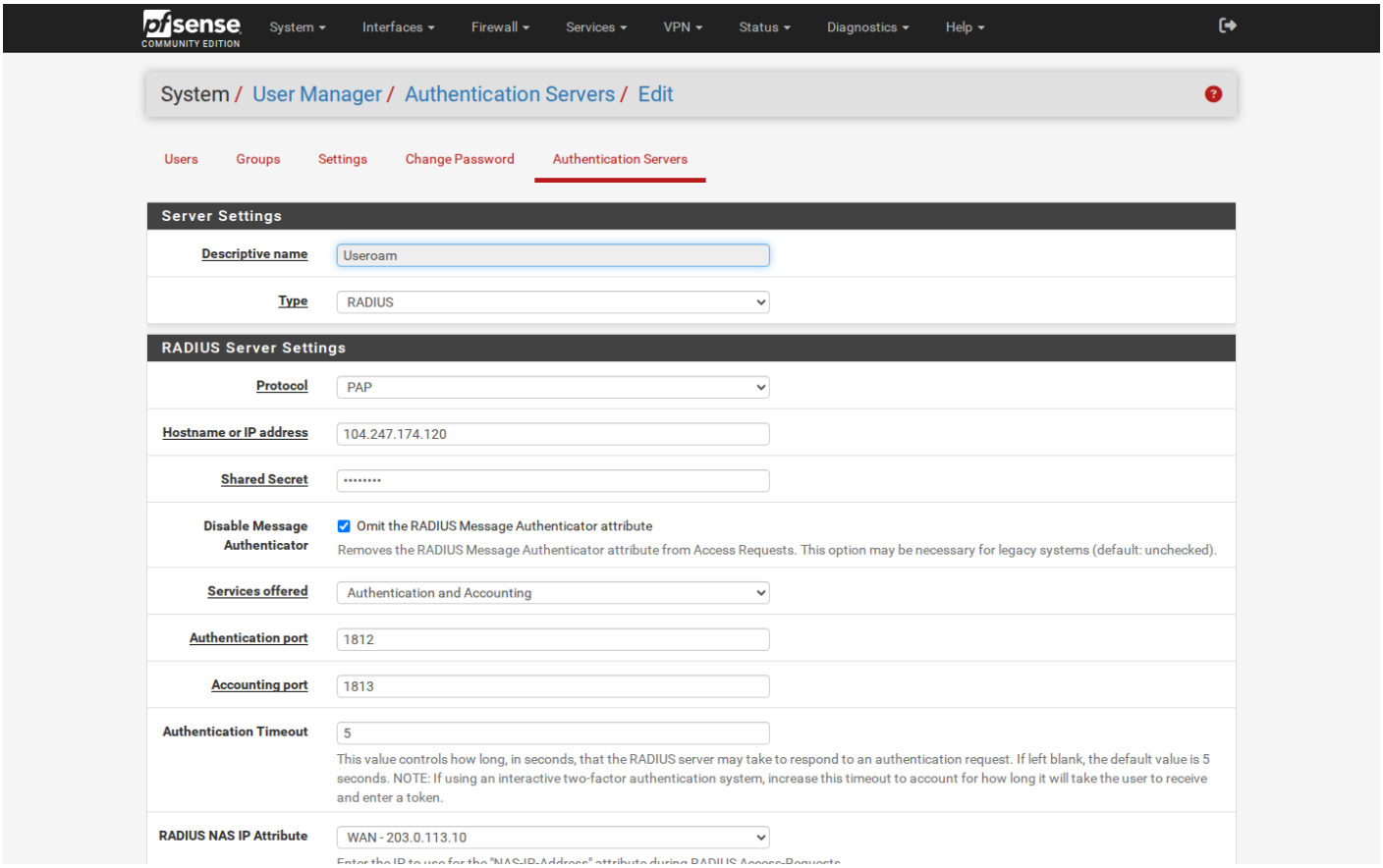


3 - RADIUS Sunucusunu Tanımlama

pfSense'te **System > User Manager > Authentication Servers** sayfasına gidip **Add** düğmesine basın.



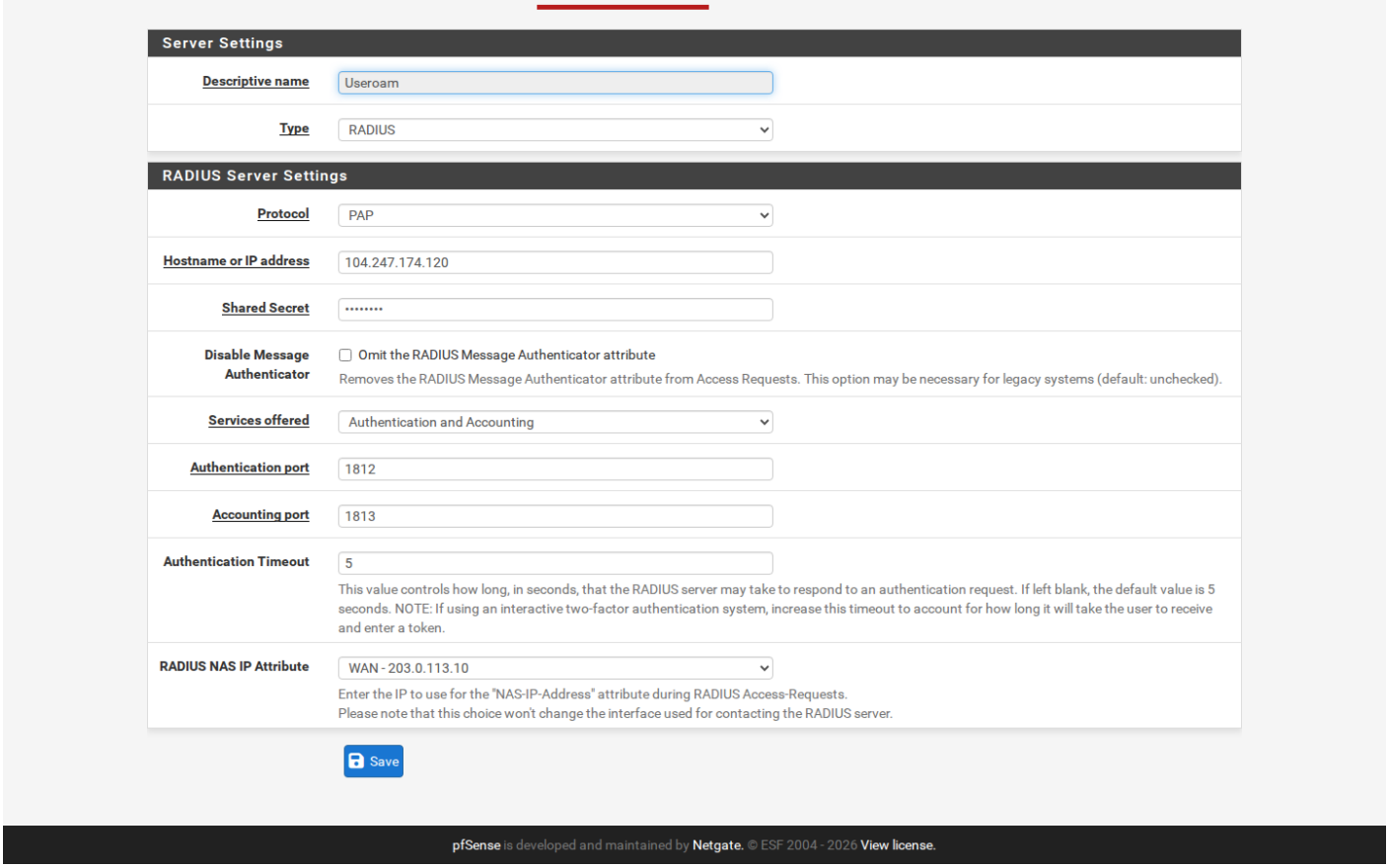
- **Descriptive name:** `Useroam`
- **Type:** `RADIUS`



RADIUS Server Settings bölümünü şöyle doldurun:

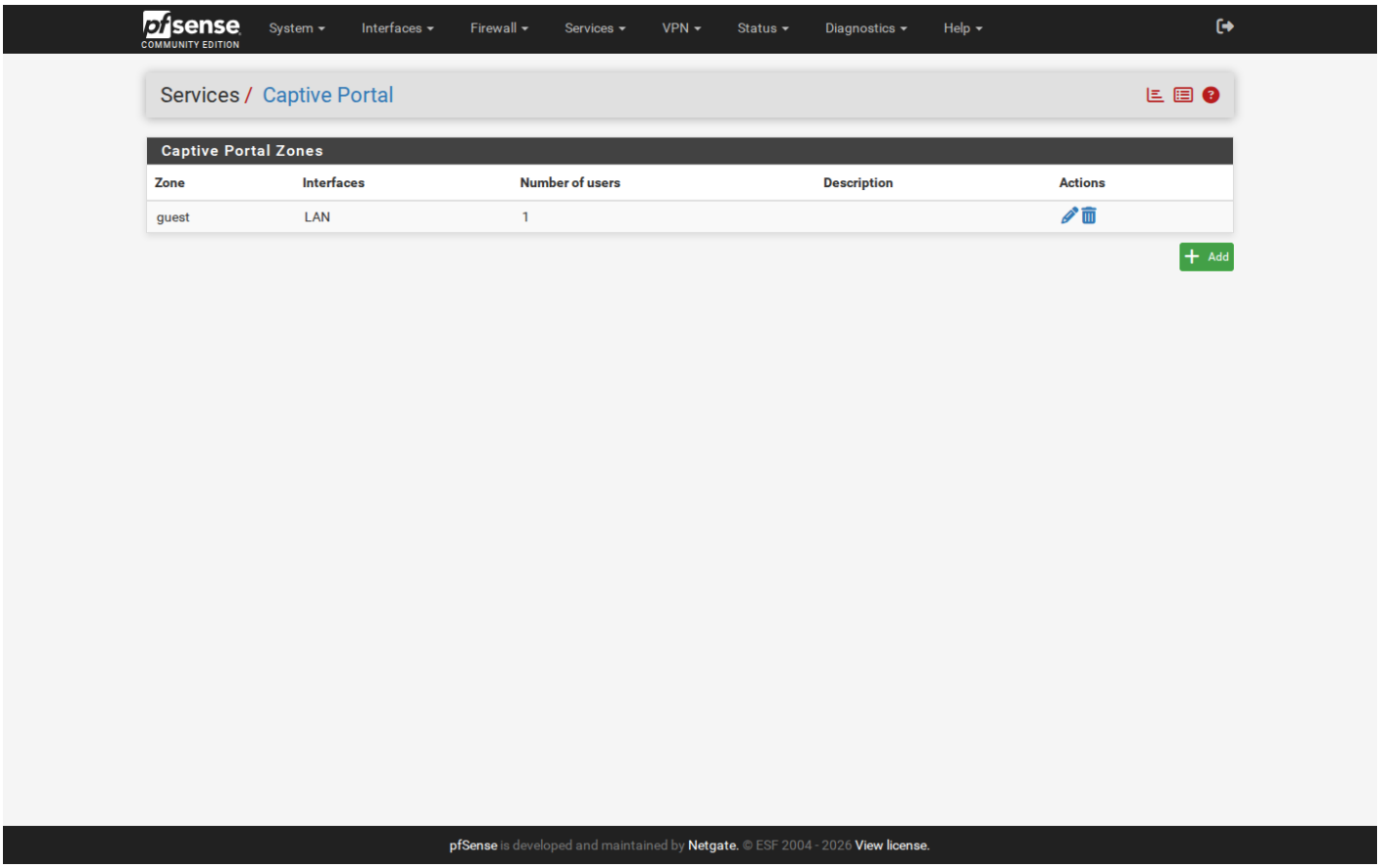
- **Protocol:** `PAP`
- **Hostname or IP address:** `104.247.174.120`
- **Shared Secret:** 2. adımda paneldeki karttan aldığınız değer.
- **Disable Message Authenticator:** işaretsiz bırakın.
- **Services offered:** `Authentication and Accounting`
- **Authentication port:** `1812`, **Accounting port:** `1813`
- **Authentication Timeout:** `5`
- **RADIUS NAS IP Attribute:** internete çıkan arayüz (genellikle `WAN`).

Save düğmesine basın.

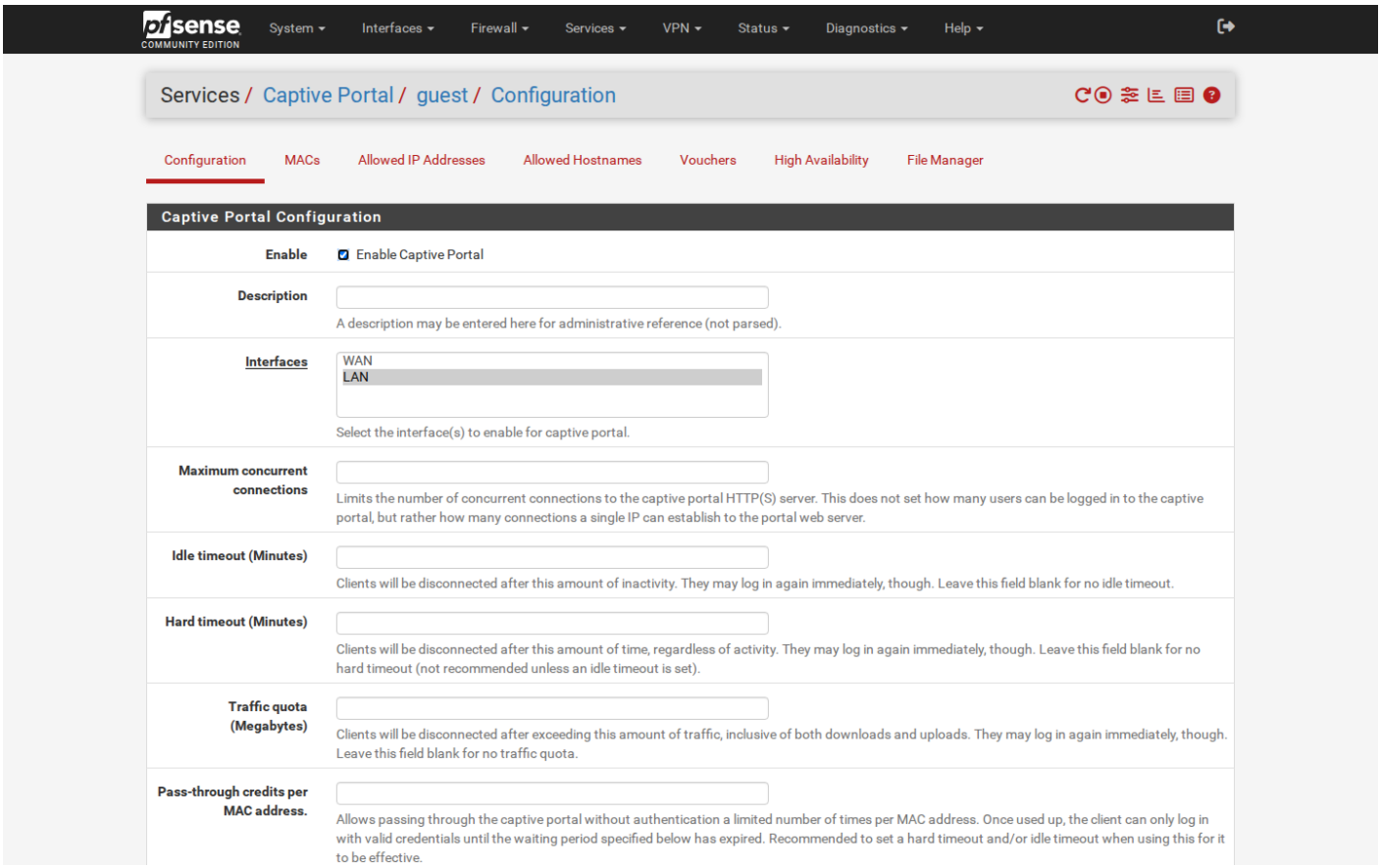


4 - Captive Portal Bölgesi (Zone) Oluşturma

Services > Captive Portal sayfasında **Add** ile yeni bir bölge ekleyin (ör. `guest`). Ardından bölgenin düzenleme simgesine basın.



- **Enable:** `Enable Captive Portal` işaretli.
- **Interfaces:** misafir ağının bağlı olduğu arayüz (ör. `LAN` ya da misafir VLAN'ı).
- **Idle timeout, Hard timeout, Traffic quota:** boş bırakın. Bu sınırlar Useroam panelindeki gruptan gelir (13. adım).



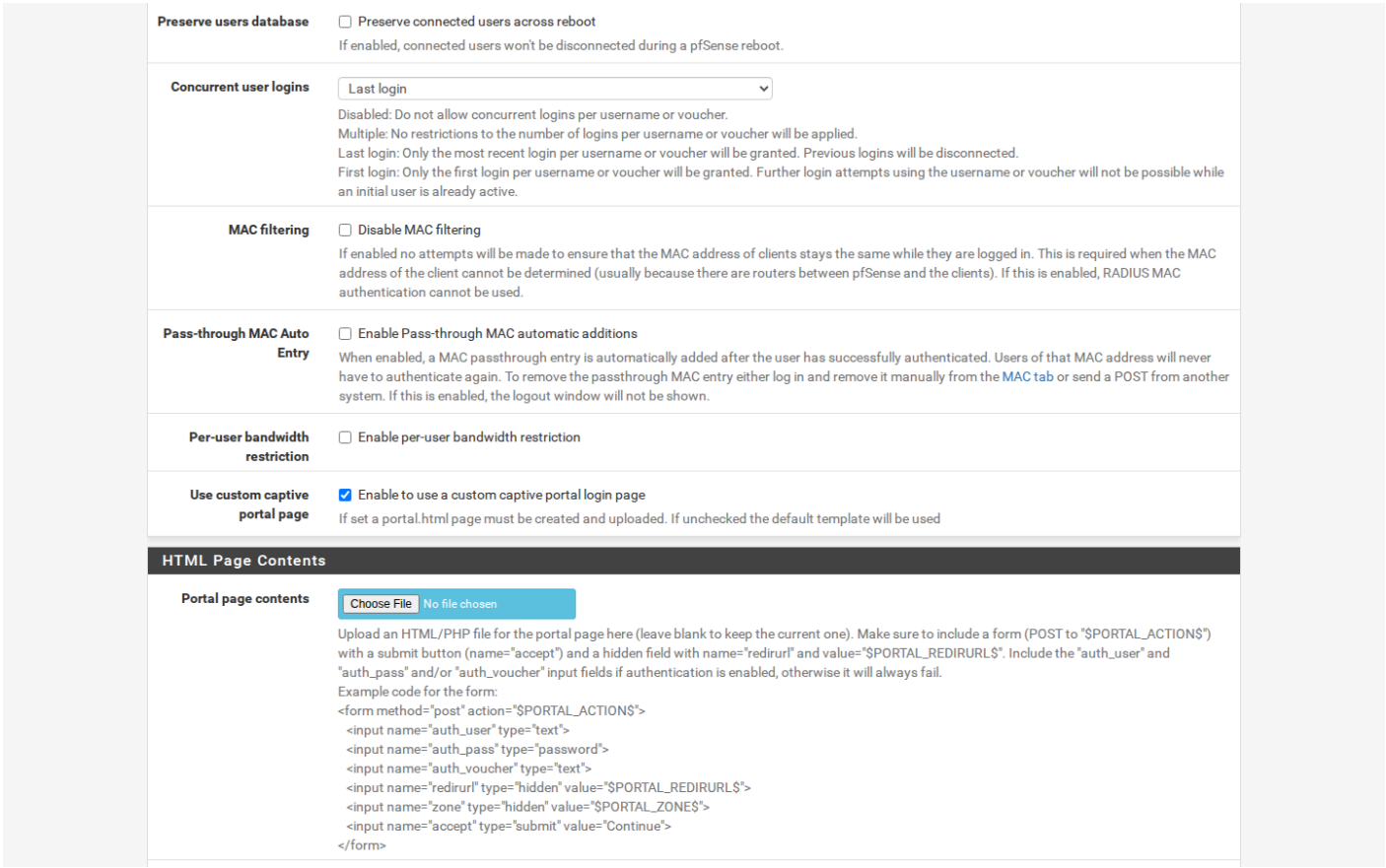
> Misafir arayüzünde **DHCP sunucusu açık** olmalı ve **DNS Resolver/Forwarder** çalışmalıdır; aksi halde misafir portalı göremez.

5 - Aynı Numaranın Cihaz Sayısı

Aynı bölge sayfasında **Concurrent user logins** ayarı, bir numaranın aynı anda kaç cihazda açık kalacağını belirler. pfSense bu sınırı RADIUS'tan almaz; burada seçilir.

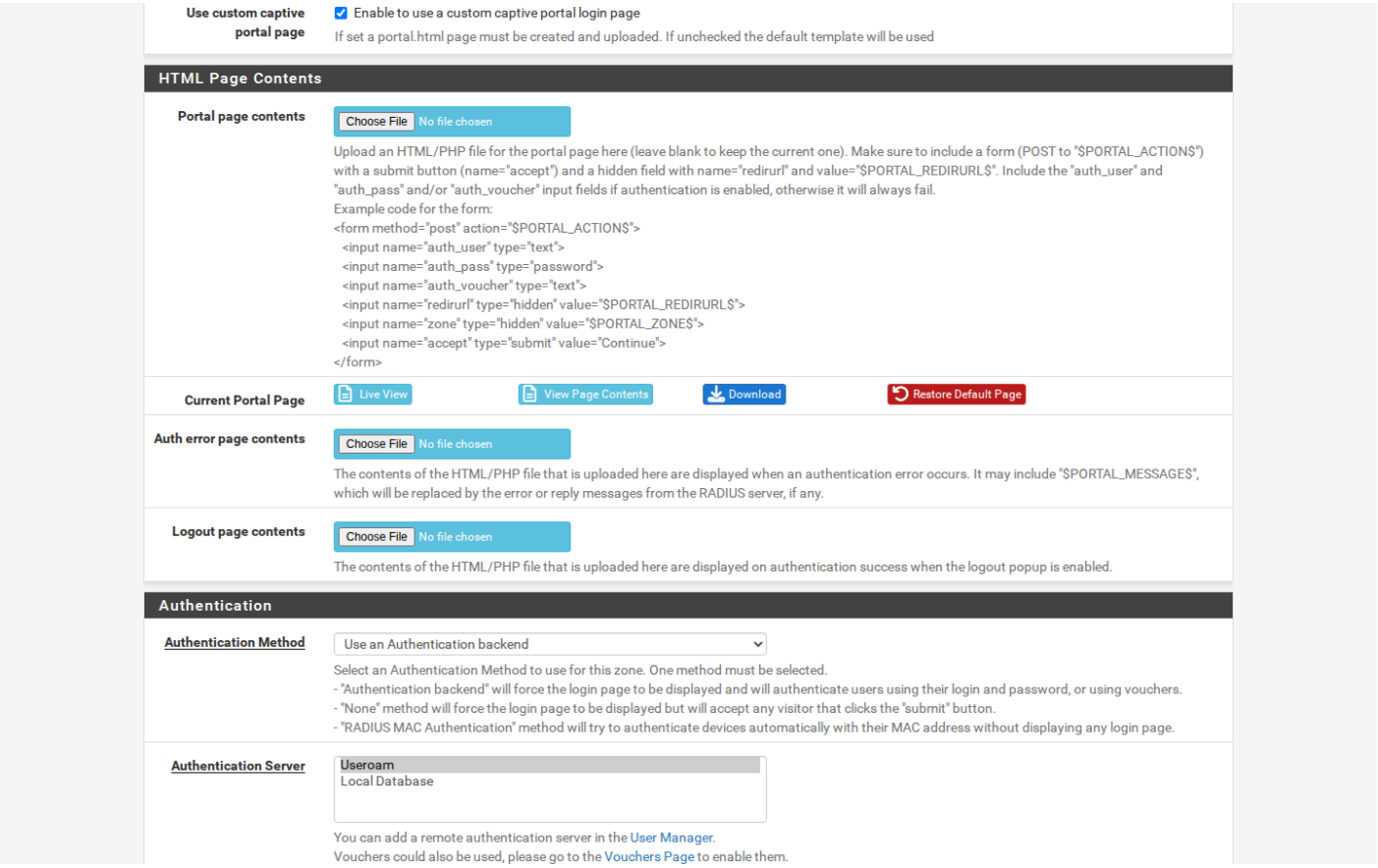
- **Multiple:** sınır yok, aynı numara birden çok cihazda açık kalabilir.
- **Last login (önerilen):** numara başka bir cihazda girince önceki cihazın oturumu kapanır (tek cihaz).
- **First login:** ilk giren cihaz açık kalır, diğer cihazlar giremez.

MAC filtering ve **Pass-through MAC Auto Entry** işaretsiz kalsın. **Use custom captive portal page** kutusunu **işaretleyin**.



6 - Useroam Portal Sayfasını Yükleme

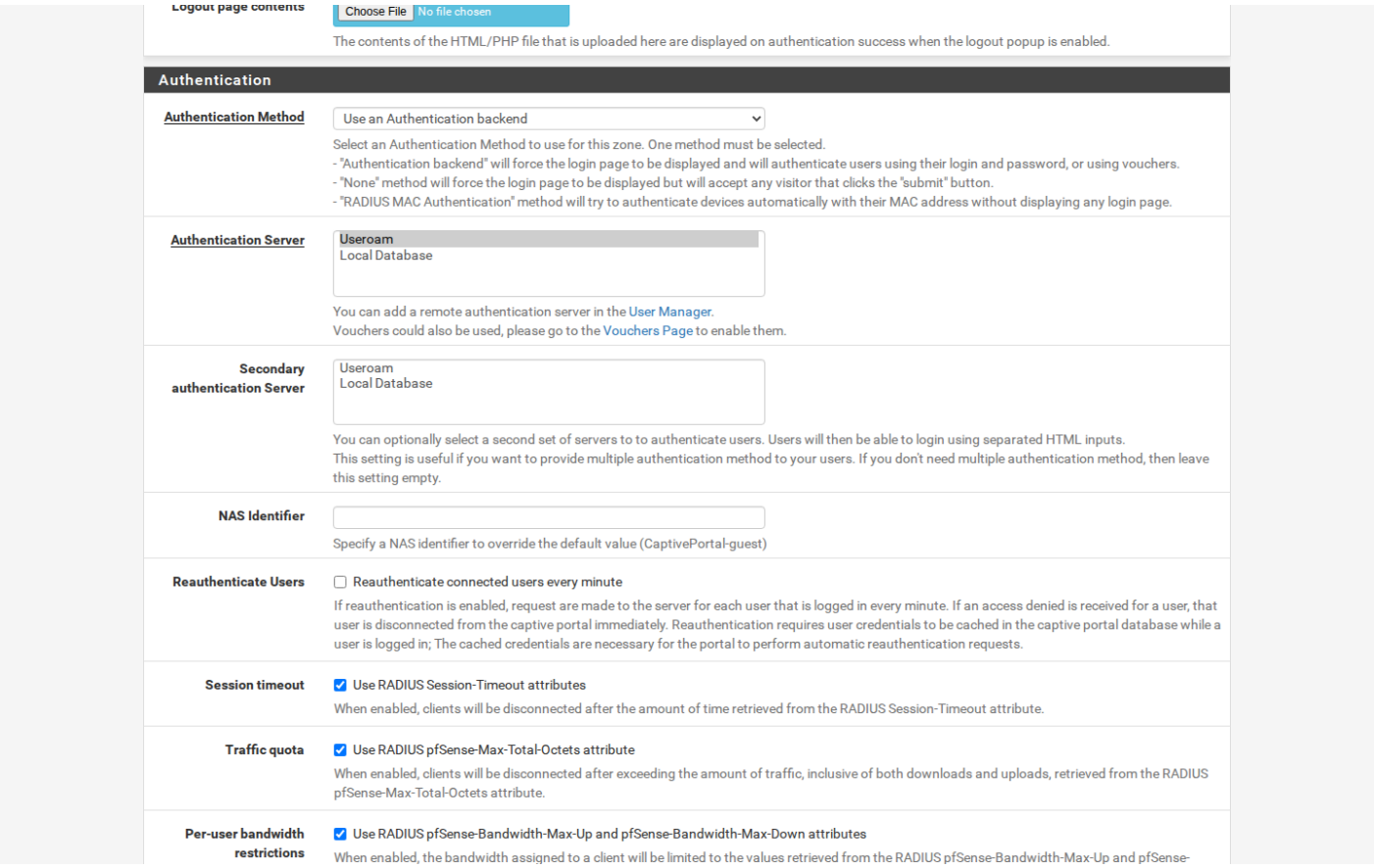
HTML Page Contents bölümünde **Portal page contents** alanındaki **Choose File** düğmesiyle 2. adımda indirdiğiniz `portal.html` dosyasını seçin. Auth error ve Logout sayfalarını boş bırakın.



7 - Kimlik Doğrulama Ayarları

Authentication bölümünde:

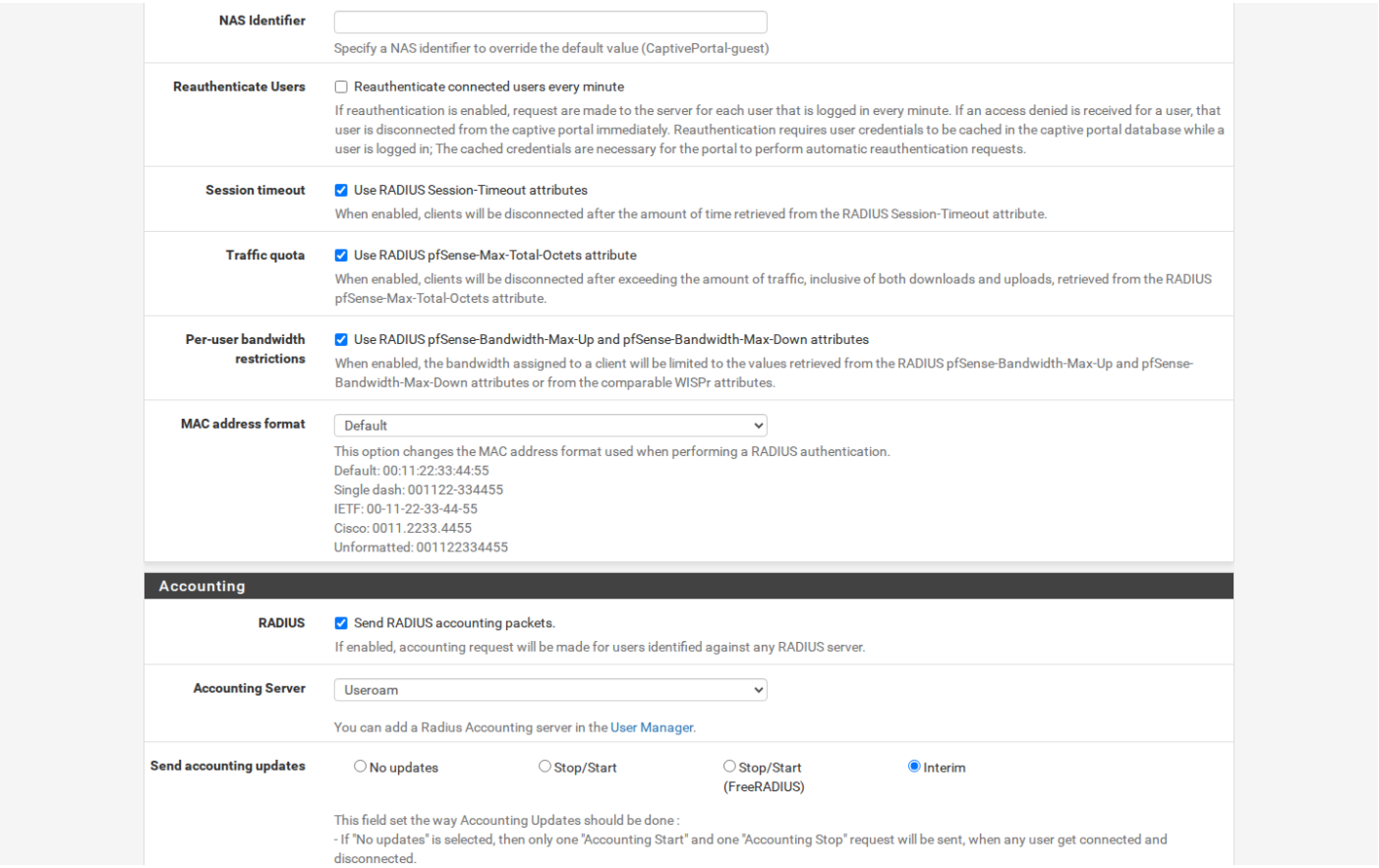
- **Authentication Method:** `Use an Authentication backend`
- **Authentication Server:** 3. adımda eklediğiniz `Useroam`
- **Secondary authentication Server:** boş bırakın (hiçbiri seçili olmasın).
- **NAS Identifier:** boş bırakın.



8 - RADIUS Seçenekleri (Hız, Kota, Süre)

> **[KRİTİK ADIM]** Aşağıdaki üç kutu işaretli değilse pfSense, Useroam'un gönderdiği hız, kota ve süre değerlerini **yok sayar**; misafir sınırsız kalır.

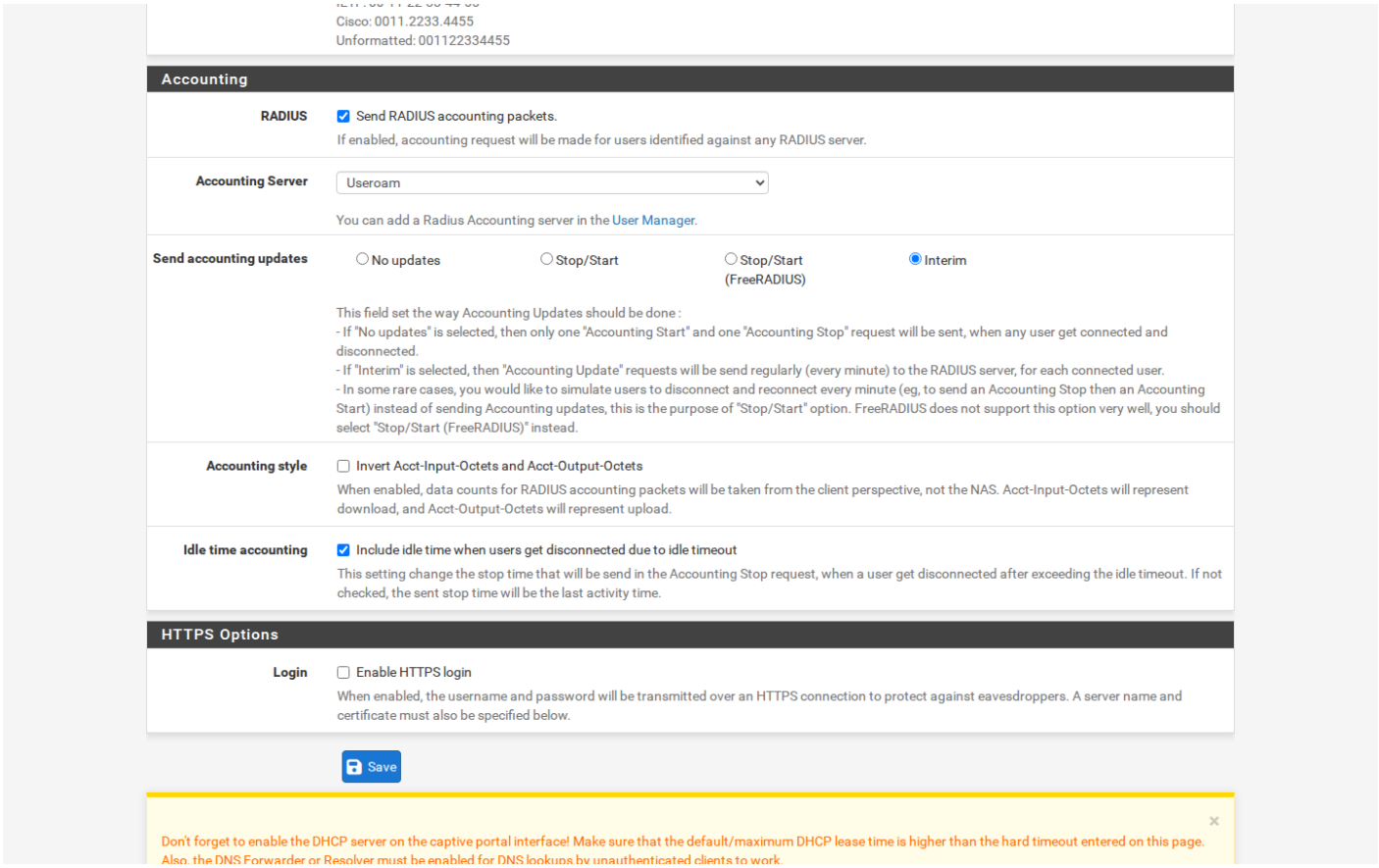
- **Reauthenticate Users:** işaretsiz bırakın.
- **Session timeout:** `Use RADIUS Session-Timeout attributes` işaretli. Grubun geçerlilik süresi ve günlük bitiş saati bununla uygulanır.
- **Traffic quota:** `Use RADIUS pfSense-Max-Total-Octets attribute` işaretli.
- **Per-user bandwidth restrictions:** `Use RADIUS pfSense-Bandwidth-Max-Up and pfSense-Bandwidth-Max-Down attributes` işaretli.
- **MAC address format:** `Default`



9 - Accounting (Oturum Kaydı)

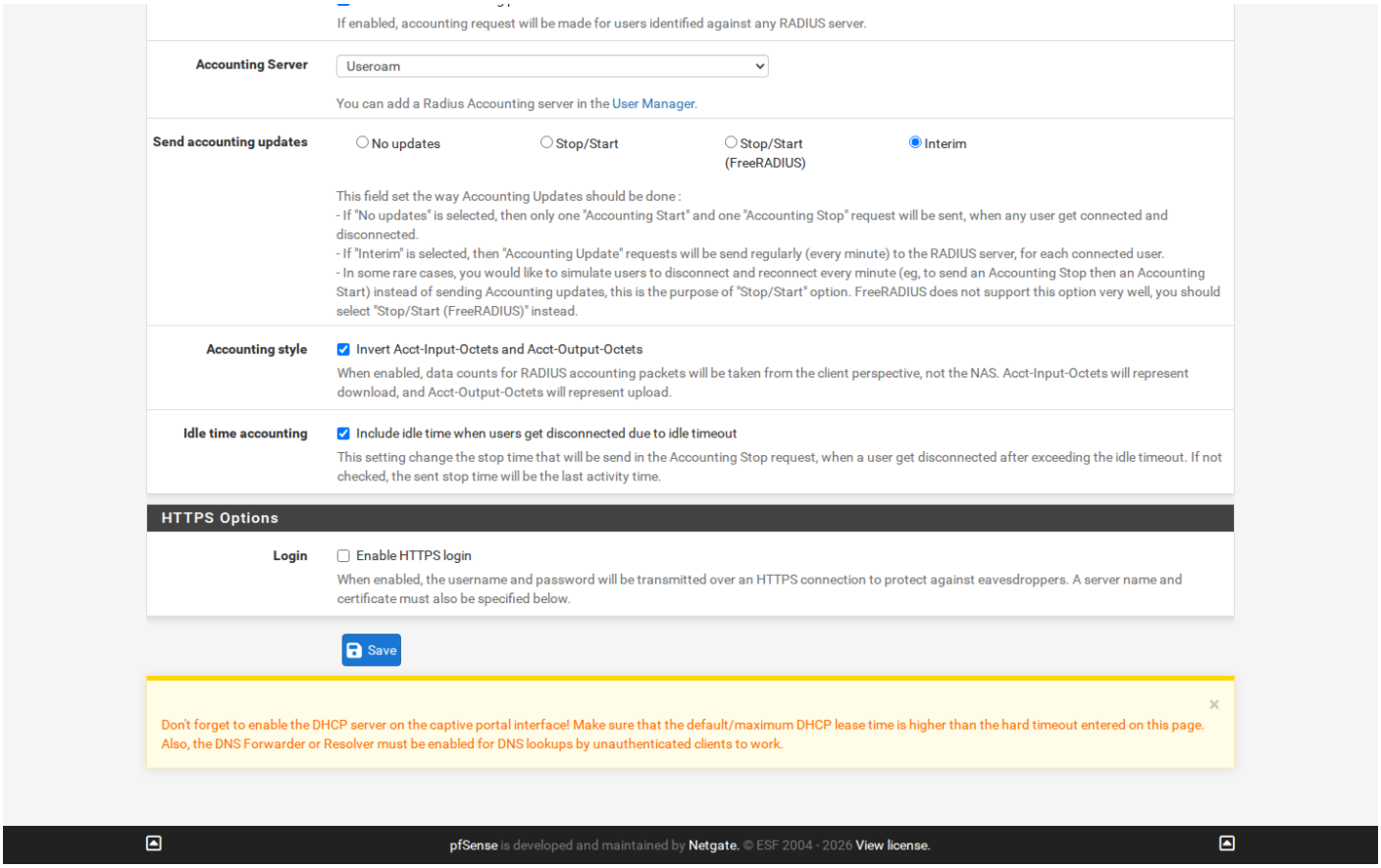
Accounting bölümünde:

- **RADIUS:** `Send RADIUS accounting packets` işaretli.
- **Accounting Server:** `Useroam`
- **Send accounting updates:** `Interim`. Useroam ara kayıt sıklığını 5 dakika olarak bildirir.
- **Accounting style:** işaretsiz bırakın (varsayılan).



10 - HTTPS Seçenekleri ve Kaydetme

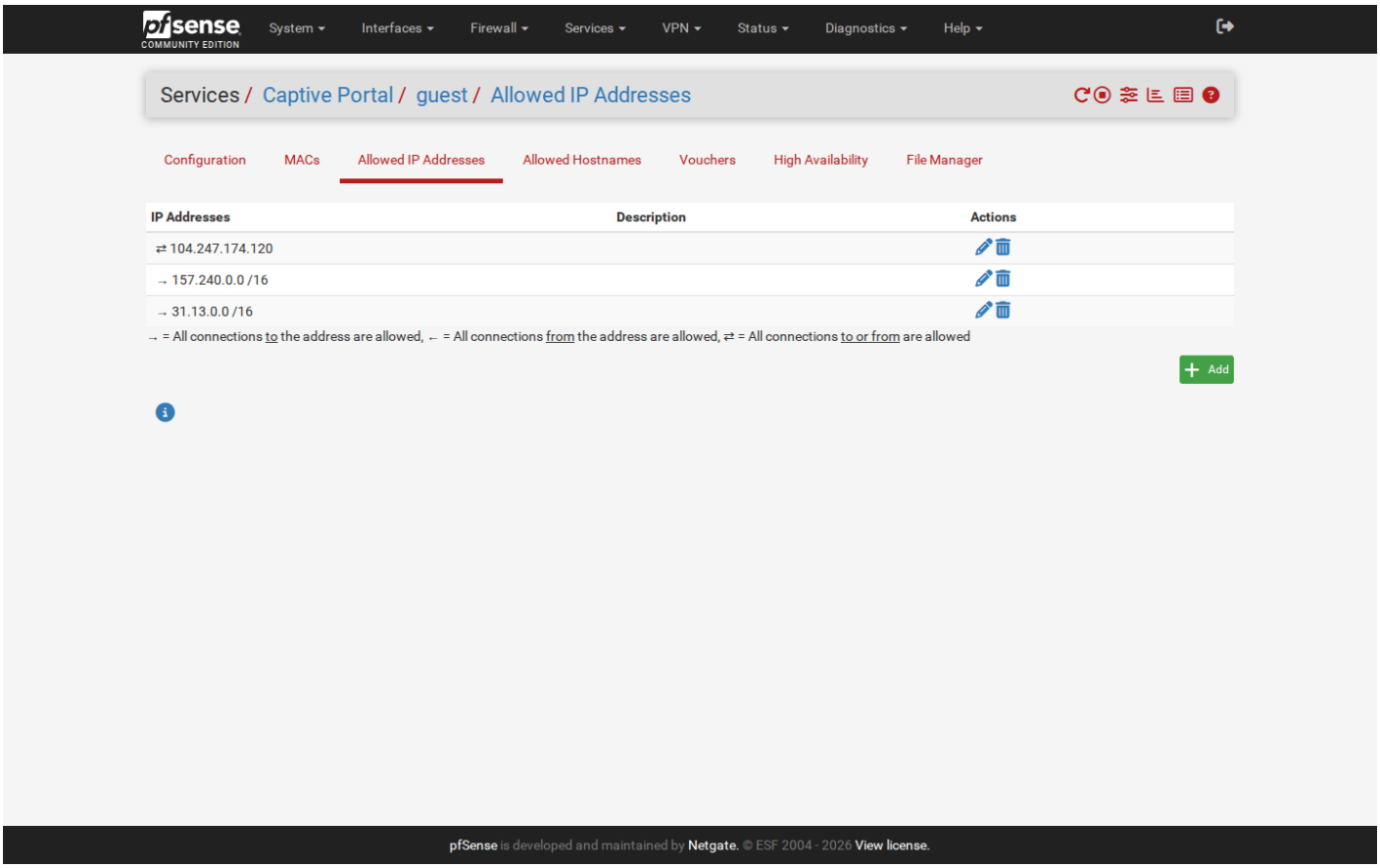
HTTPS Options bölümünde **Enable HTTPS login** işaretsiz kalsın. Sayfanın altındaki **Save** düğmesine basın.



11 - Giriş Öncesi İzinler (Allowed IP Addresses)

Misafir giriş yapmadan önce Useroam karşılama sayfasına erişebilmelidir. Bölgenin **Allowed IP Addresses** sekmesinde **Add** ile şunları ekleyin:

- `104.247.174.120` (Useroam). **Direction:** `Both` ya da `To`.
- WhatsApp ile giriş kullanılacaksa: `157.240.0.0/16` ve `31.13.0.0/16` (Direction: `To`).

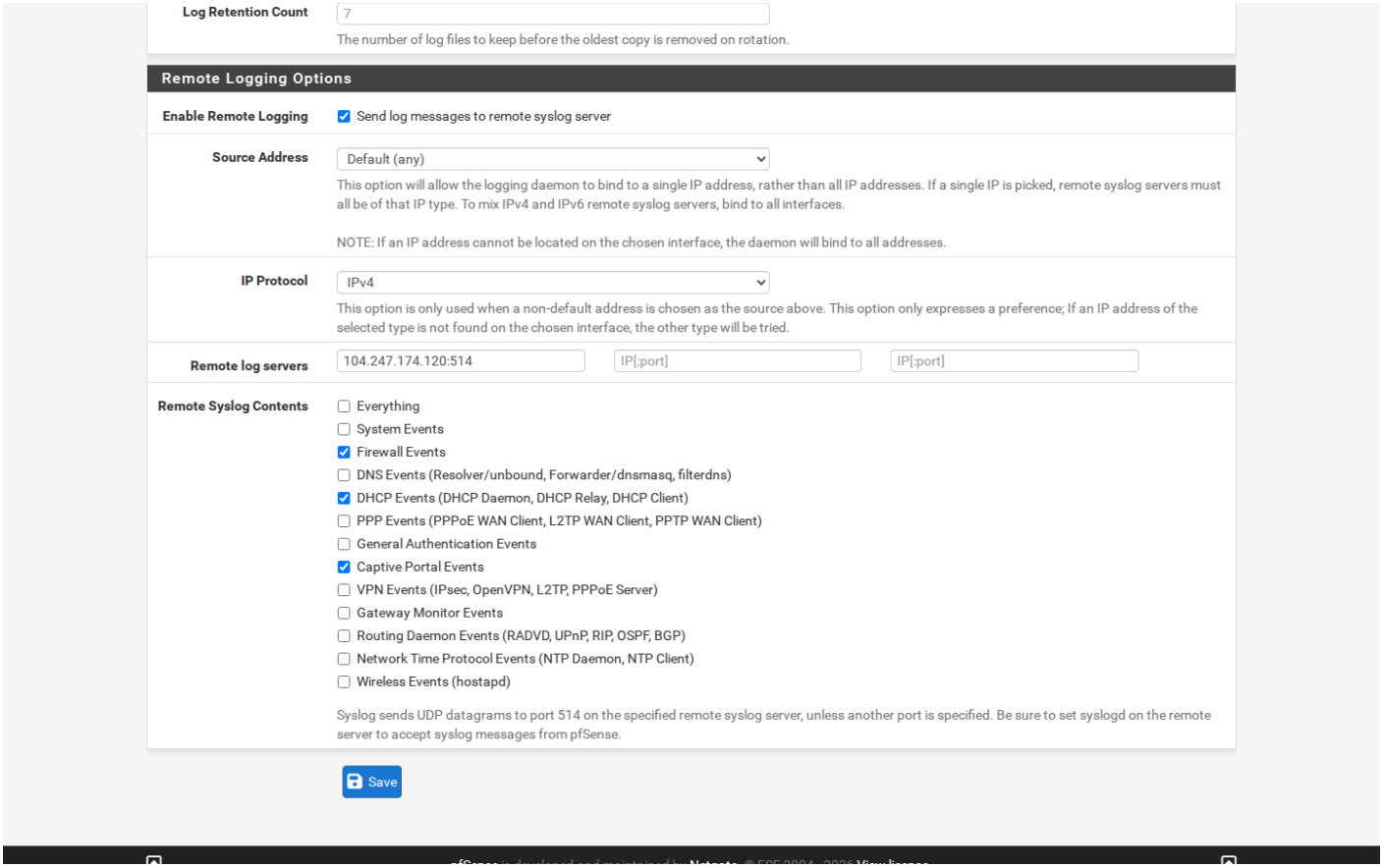


12 - 5651 Log Gönderimi

Status > System Logs > Settings sayfasında **Remote Logging Options** bölümüne inin:

- **Enable Remote Logging:** işaretli.
- **Remote log servers:** `104.247.174.120:514`
- **Remote Syslog Contents:** `Firewall Events`, `DHCP Events` ve `Captive Portal Events` işaretli.

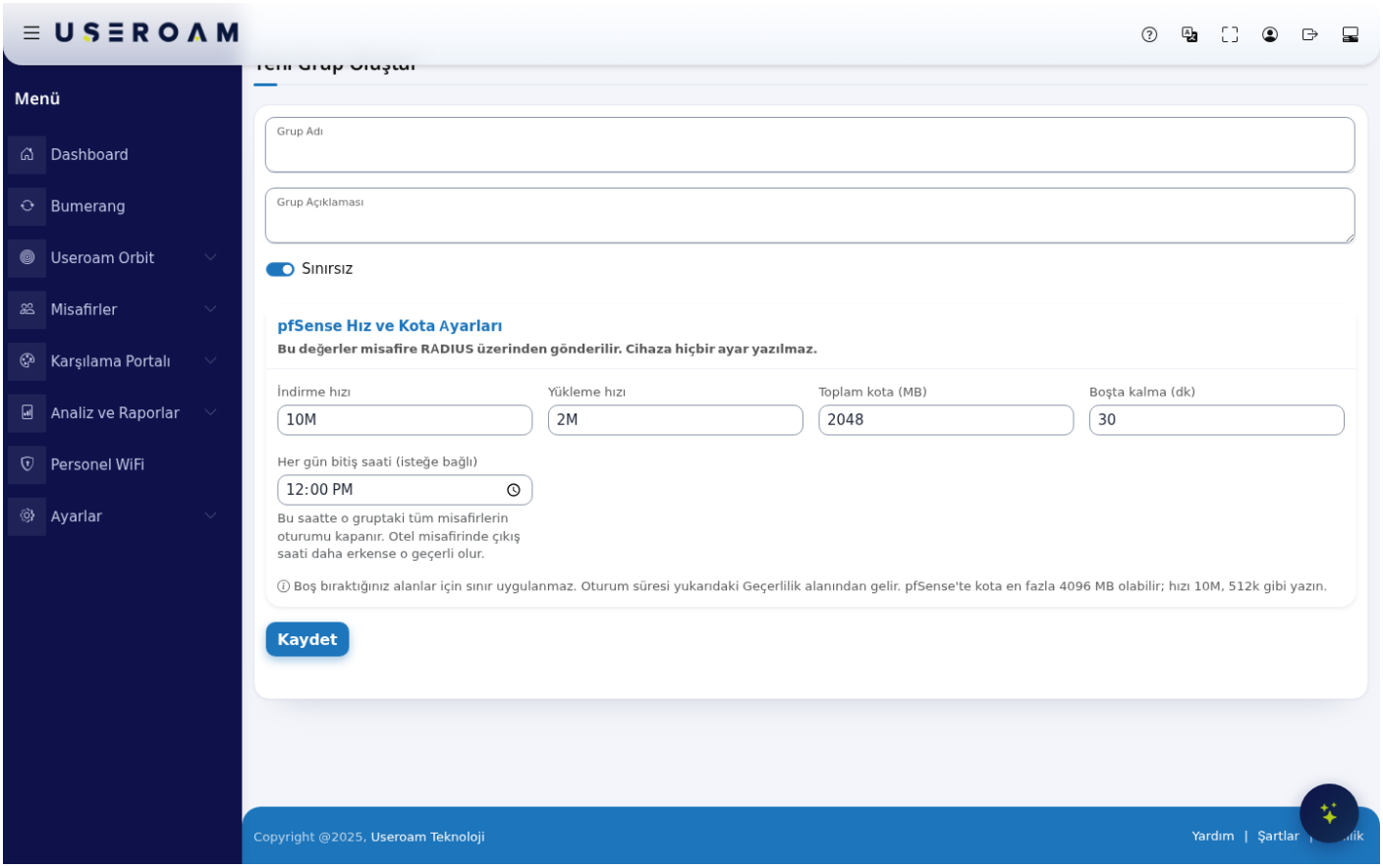
Ayrıca **Firewall > Rules** altında misafir arayüzündeki izin kuralını açıp **Log packets that are handled by this rule** seçeneğini işaretleyin. **Save** ve **Apply Changes**.



13 - Gruplarda Hız, Kota ve Bitiş Saati

Useroam panelinde **Gruplar** ekranında pfSense cihazına ait bir grup açtığınızda **pfSense Hız ve Kota Ayarları** kartı görünür. Boş bıraktığınız alan için sınır uygulanmaz.

- **İndirme hızı / Yükleme hızı:** `10M`, `512k` gibi yazın.
- **Toplam kota (MB):** indirme ve yükleme toplamı. pfSense'te en fazla 4096 MB olabilir.
- **Boşta kalma (dk):** bu kadar süre trafik olmazsa oturum kapanır.
- **Her gün bitiş saati:** bu saatte o gruptaki tüm misafirlerin oturumu kapanır (ör. `12:00`). Otel misafirinde çıkış saati daha erkense o geçerli olur.
- **Geçerlilik:** grubun üstündeki süre alanı oturumun en uzun süresidir.

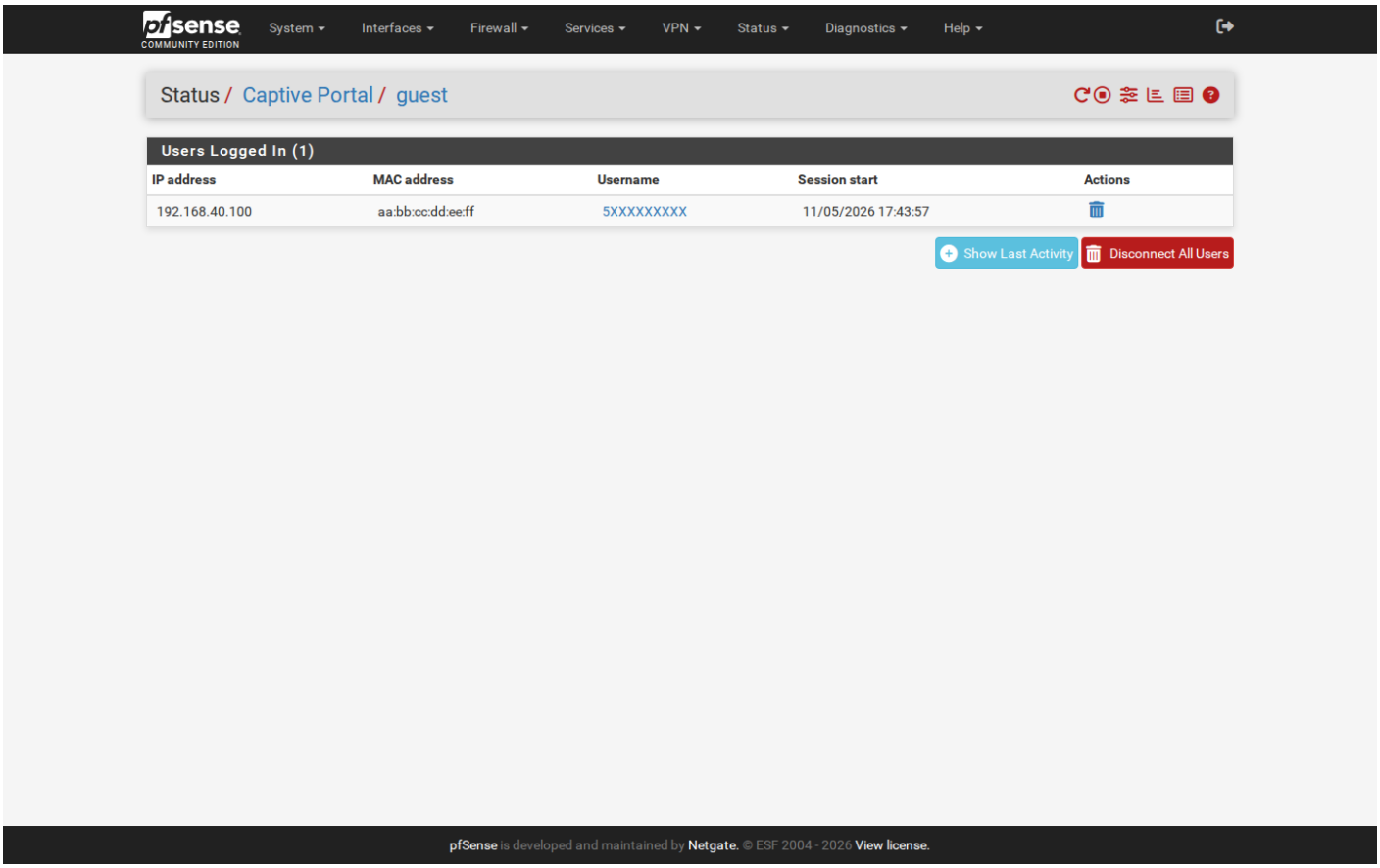


> Grup değişiklikleri misafirin **bir sonraki girişinde** uygulanır. pfSense dışarıdan anında bağlantı kesme komutu almadığı için otel hız paketi satışı pfSense'te henüz desteklenmez.

14 - Test

Misafir ağına daha önce bağlanmamış bir telefonla bağlanın ve tarayıcıda `http://neverssl.com` adresini açın. Useroam karşılama sayfası açılmalı; SMS ya da WhatsApp ile giriş yaptıktan sonra internete çıkmalısınız. Cihaz panele yeni eklendiyse portalın açılması 5 dakikayı bulabilir.

Bağlı misafirleri **Status > Captive Portal** sayfasında görebilirsiniz.



Sorun Giderme

Belirti	Kontrol edin
Portal açılmıyor, sayfa beyaz ya da zaman aşımı	11. adımda 104.247.174.120 izni; misafir arayüzünde DHCP ve DNS; cihaz yeni eklendiyse 5 dakika bekleyin.
Portal açılıyor ama giriş "şifre hatalı" diyor	Shared Secret paneldekiyle aynı mı; panelde yazdığınız Cihaz Adresi pfSense'in gerçekten internete çıktığı IP mi.
Hız ya da kota uygulanmıyor	8. adımdaki üç kutu işaretli mi; grupta değer var mı; misafir değişiklikten sonra yeniden girdi mi.
Oturum bitiş saatinde kapanmıyor	Session timeout kutusu işaretli mi; pfSense saat ve saat dilimi doğru mu (System > General Setup).
Aynı numara birden çok cihazda açık kalıyor	5. adımda Concurrent user logins: Last login.
Panelde 5651 logu görünmüyor	12. adımdaki Remote Logging ve misafir kuralındaki Log seçeneği.

Revizyon #2
tugay tarafından 5 Kasım 2026 14:56:38 oluşturuldu
tugay tarafından 5 Kasım 2026 14:56:58 güncellendi