Ruijie Entegrasyon Rehberi

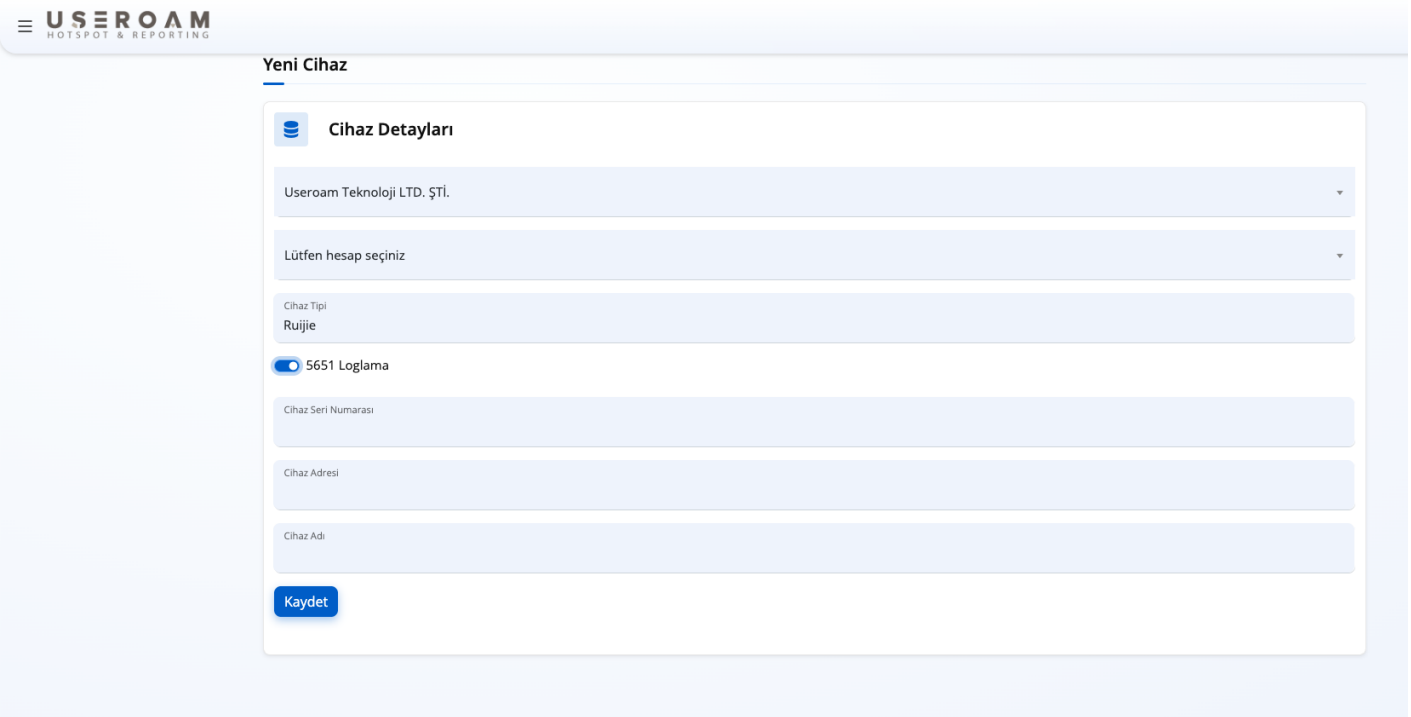
Bu rehber, bir **Ruijie / Reyee gateway** ile Useroam Cloud arasındaki entegrasyonun tamamını anlatır: captive portal kimlik doğrulaması (WiFiDog external portal) ve yasal 5651 syslog yönlendirmesi.

> **Başlamadan önce:** Ruijie web arayüzüne yönetici erişimi, gateway'in aktif WAN IP adresi ve cihaz etiketinde yazan donanım seri numarası gerekir.

1 - Useroam Panele Cihaz Ekleme

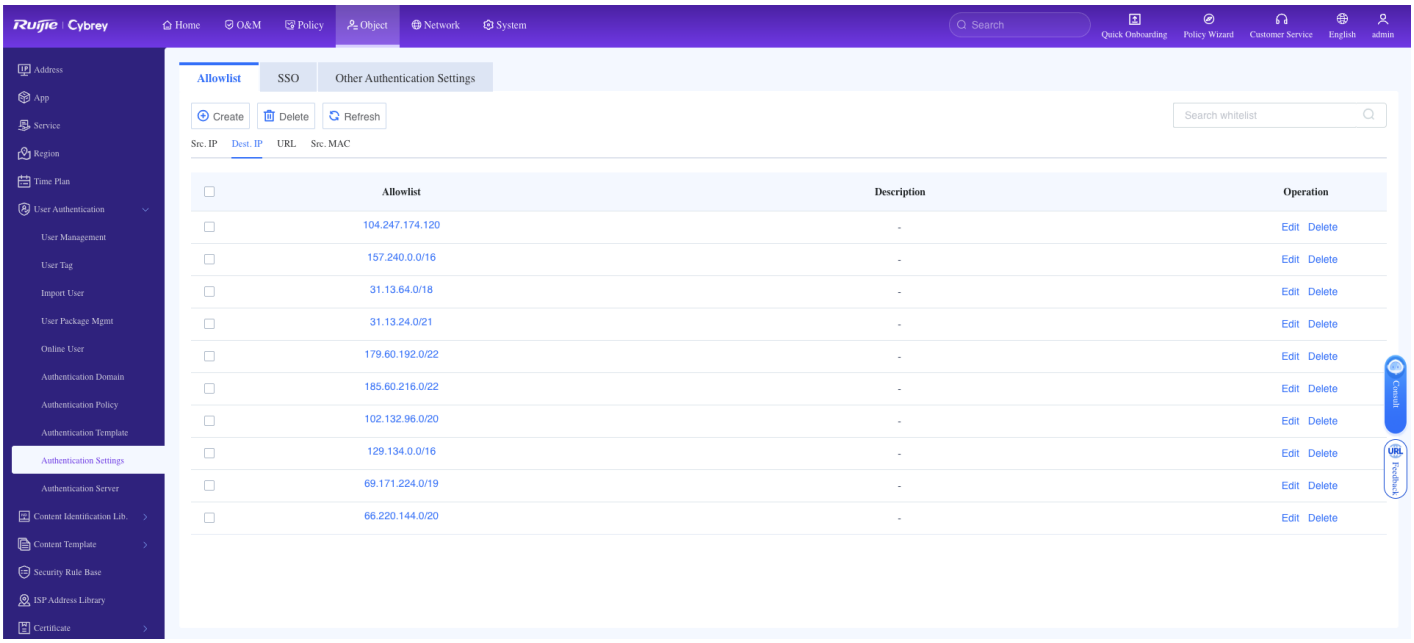
İlk olarak **panel.useroam.com** adresinden panelinize giriş yapıp **Yeni Cihaz** ekleyiniz.

- **Cihaz Tipi:** Ruijie seçiniz.
- **5651 Loglama:** 5651 Loglama kutucuğunu aktif ediniz.
- **Cihaz Seri Numarası:** **[KRİTİK ADIM]** Cihazınızın altındaki etikette veya arayüzde yer alan orijinal donanım seri numarasını bu alana eksiksiz giriniz. Ruijie entegrasyonunun sorunsuz çalışması için seri numarası doğruluğu zorunludur.
- **Cihaz Adresi:** Cihazın dış dünyaya açılan aktif WAN IP adresini giriniz.



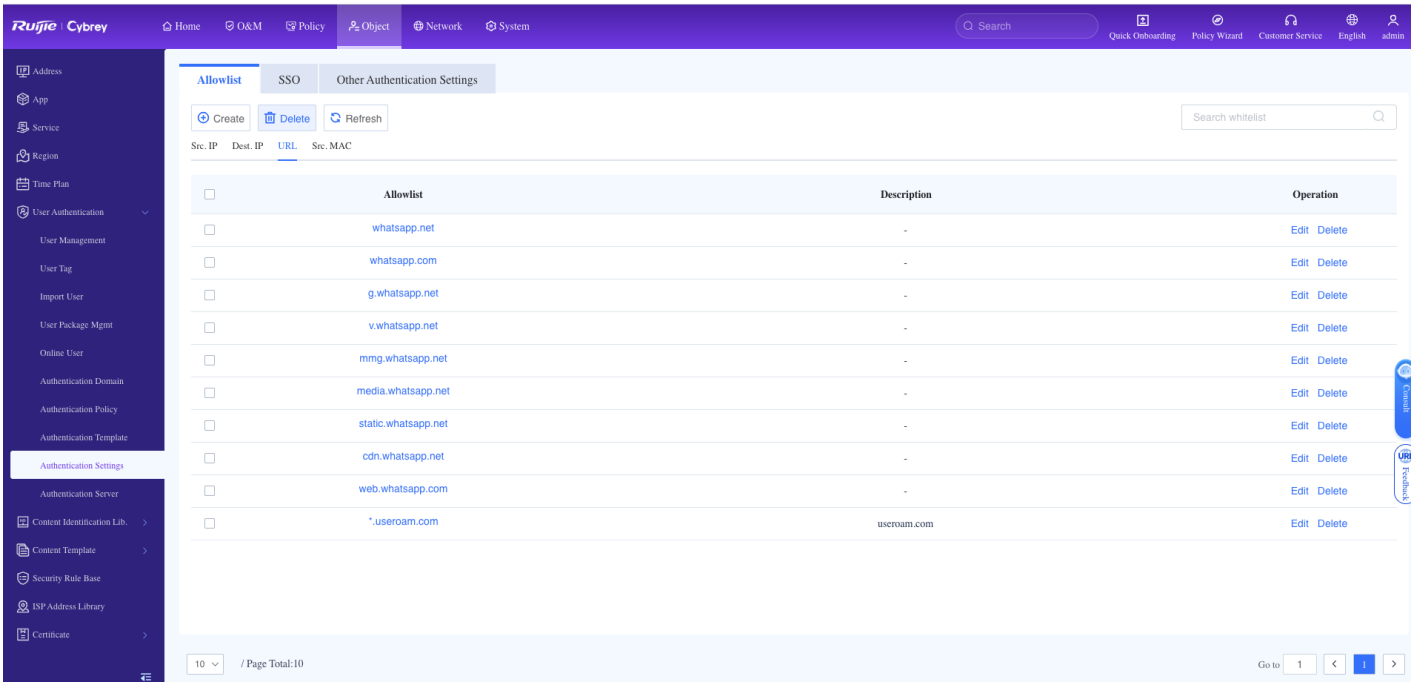
2 - Güvenli IP İzin Listesi Ayarları (Allowlist Dest. IP)

Ruijie cihazınızın yönetim arayüzünde üst menüden **Object > User Authentication > Authentication Settings** yolunu takip ediniz. **Allowlist** sekmesi altında **Dest. IP** seçeneğini işaretleyerek Useroam Cloud sunucu IP adresini (`104.247.174.120`) ve hotspot servis ağlarını izinli olarak ekleyiniz.



3 - Güvenli Alan Adı İzin Listesi Ayarları (Allowlist URL)

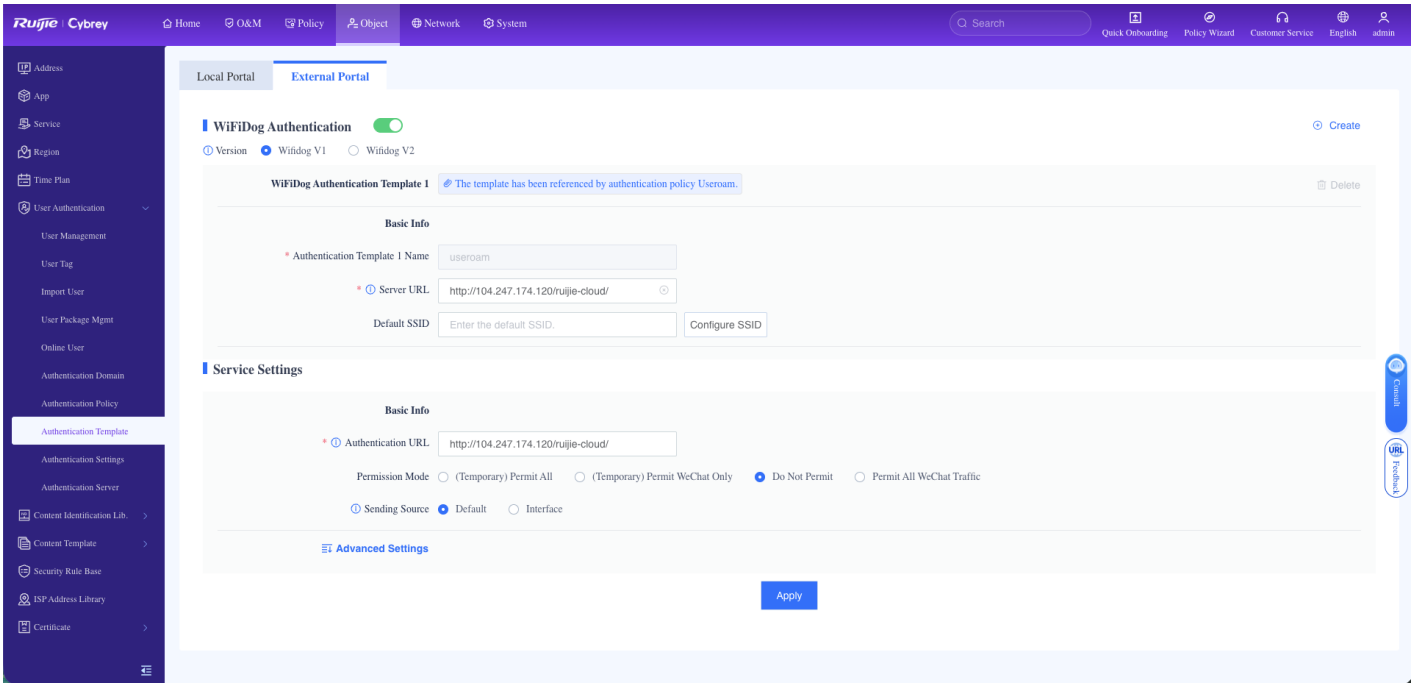
Aynı menü altındaki **URL** sekmesine geçiş yapınız. Kullanıcıların kimlik doğrulaması yapmadan önce erişebilmesi gereken `*.useroam.com` adresini izin listesine ekleyiniz. Ayrıca, mobil cihazların arka planda hotspot ağını doğrulayabilmesi için gerekli olan mesajlaşma ve işletim sistemi captive alan adı (Örn: WhatsApp ağları vb.) URL kurallarını tanımlayınız.



4 - External Portal & WiFiDog Kimlik Doğrulama Şablonu

Sol taraftaki menüden **Authentication Template** sekmesine giderek **External Portal** tabını açınız. **WiFiDog Authentication** özelliğini aktif konuma getirdikten sonra şablonu oluşturunuz:

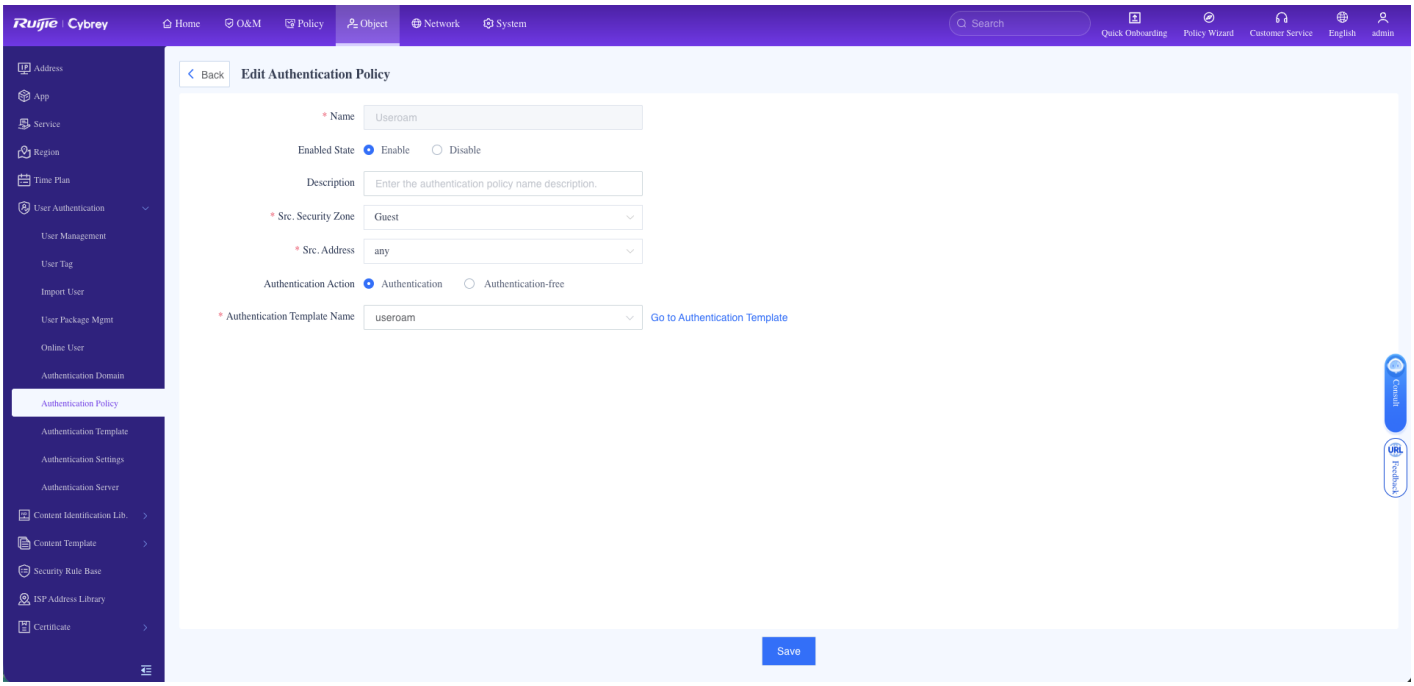
- **Version:** Wifidog V1 seçiniz.
- **Authentication Template Name:** useroam
- **Server URL:** `http://104.247.174.120/ruijie-cloud/`
- **Permission Mode:** Do Not Permit seçiniz.
- **Sending Source:** Default olarak bırakınız.



5 - Kimlik Doğrulama Politikası (Edit Authentication Policy)

Son aşama olarak sol menüden **Authentication Policy** alanına gelerek yeni bir kural ekleyiniz veya mevcut misafir politikanızı düzenleyiniz:

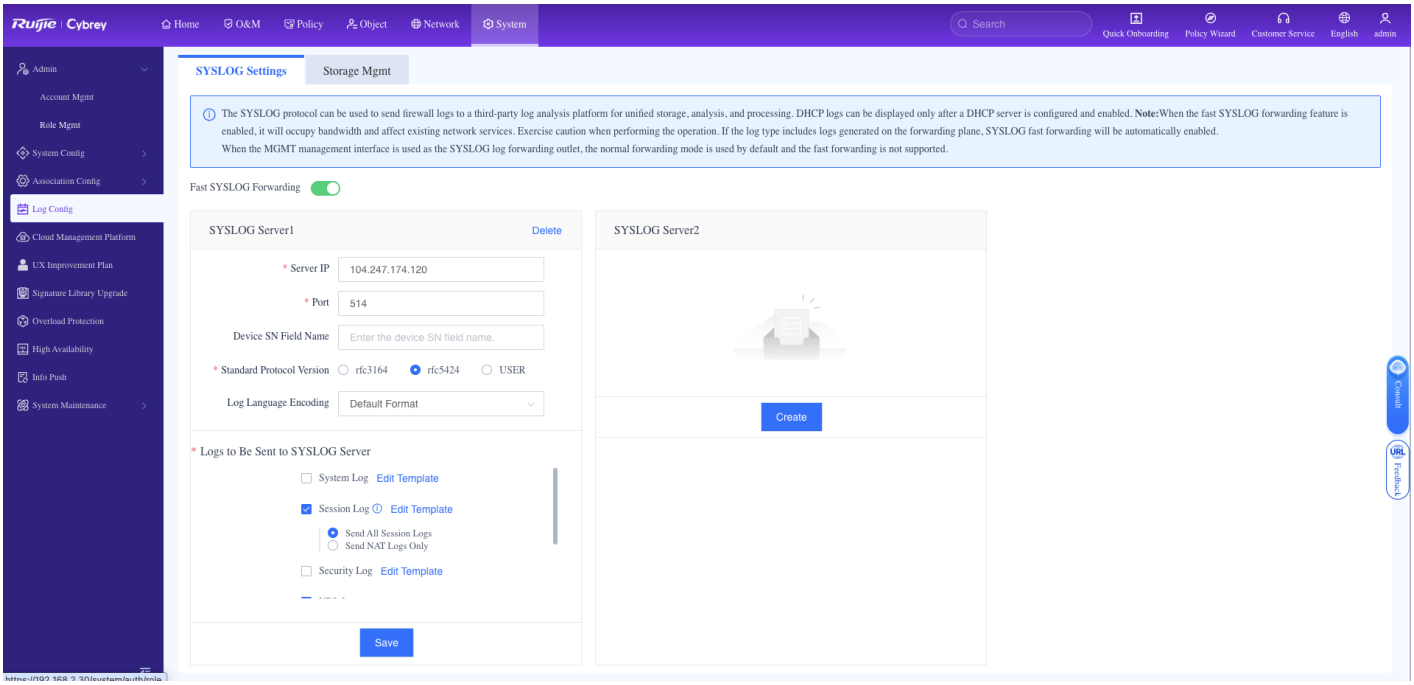
- **Name:** useroam
- **Enabled State:** Enable konumuna getiriniz.
- **Src. Security Zone:** Misafir ağınızın bağlı olduğu zone'u seçiniz (Örn: `Guest`).
- **Src. Address:** any
- **Authentication Action:** Authentication seçeneğini işaretleyiniz.
- **Authentication Template Name:** Bir önceki adımda oluşturduğunuz `useroam` şablonunu seçerek kaydediniz.



6 - Logların Useroam'a Yönlendirilmesi (Syslog Config)

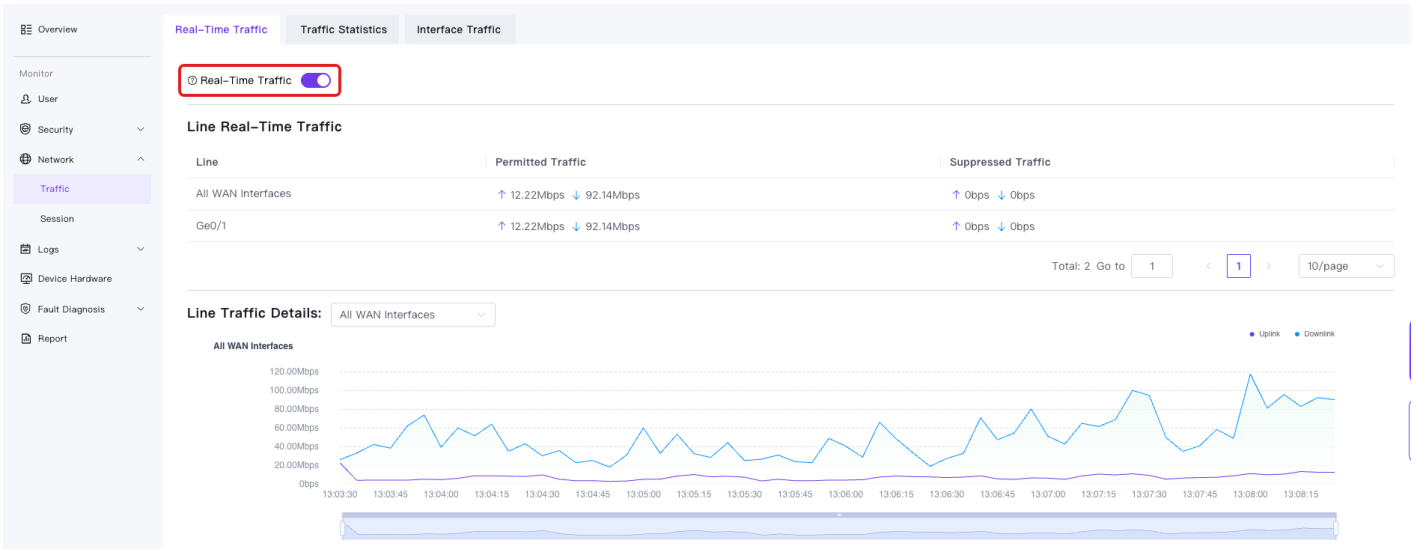
Kullanıcıların internet trafiğinin ve hotspot oturum hareketlerinin 5651 sayılı kanun kapsamında yasal olarak imzalanabilmesi için logların Useroam Cloud sunucusuna aktarılması gerekmektedir. Bu işlem için Ruijie yönetim arayüzünde **Advanced > Syslog** menüsüne gidiniz ve **Add** butonu ile yeni bir syslog sunucusu tanımlayınız:

- **Syslog Server Status:** Enable konumuna getirerek aktifleştiriniz.
- **Server IP:** Sunucu IP adresi alanına Useroam Cloud IP adresi olan `104.247.174.120` giriniz.
- **Server Port:** `514` (Varsayılan syslog portu).



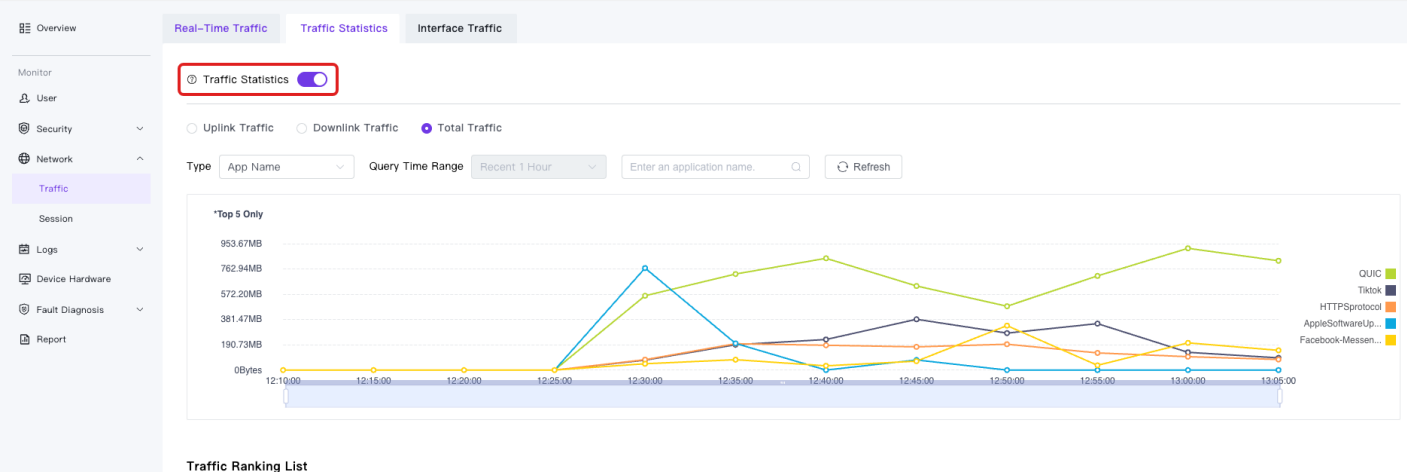
7 - Trafik Raporlamasını Açın (Real-Time Traffic)

Ruijie yönetim arayüzünde **Monitor > Network > Traffic** menüsüne gidiniz. **Real-Time Traffic** sekmesinde **Real-Time Traffic** anahtarını açık konuma getiriniz.



8 - Trafik Raporlamasını Açın (Traffic Statistics)

Aynı sayfada **Traffic Statistics** sekmesine geçiniz ve **Traffic Statistics** anahtarını açık konuma getiriniz.



Neden gerekli? Bu iki anahtar açık olmadan cihaz, misafirlerin indirme ve yükleme trafiğini Useroam'a bildiremez; panelde **Aktif Misafirler** ekranında trafik 0 görünür.

Önemli - Entegrasyon Tamamlandı

Hepsi bu kadar! Ruijie / Reyee Gateway cihazınız üzerinde Useroam Cloud Hotspot ve yasal 5651 Syslog entegrasyon süreçlerinin tamamı başarıyla tamamlanmıştır. Cihaz seri numarası veya WAN IP adresi değişikliklerinde entegrasyonun aksamaması için Useroam panelini güncellemeyi unutmayınız. Süreç esnasında destek almak için **destek@useroamteknoloji.com** adresi üzerinden teknik ekibimizle iletişime geçebilirsiniz.

WhatsApp ile Giriş: Firewall İzin Listesi (Walled Garden)

Misafir henüz internete çıkmadan (captive portal / giriş öncesi aşamada) **WhatsApp ile Giriş** akışının çalışabilmesi için, firewall veya walled-garden yapılandırmasında aşağıdaki adreslere **izin verilmesi zorunludur**. Bu izinler tanımlanmadan WhatsApp giriş ekranı açılmaz ve teslim (delivered) onayına dayalı otomatik giriş çalışmaz.

İzin verilecek alan adları (FQDN)

- `*.wa.me`
- `*.whatsapp.com`
- `*.whatsapp.net`
- `g.whatsapp.net`

- `mmg.whatsapp.net`
- `fbsbx.com`
- `*.useroam.com`

İzin verilecek IP adresleri

- `157.240.0.0`: Meta / Facebook ağ bloğu
- `31.13.0.0`: Meta / Facebook ağ bloğu
- `104.247.174.120`: Useroam panel

Not: `157.240.0.0` ve `31.13.0.0` tipik olarak `/16` ağ bloklarıdır (Meta altyapısı); firewall'da blok olarak (`157.240.0.0/16`, `31.13.0.0/16`) tanımlanması önerilir. `104.247.174.120` Useroam panel IP'sidir (`/32`). FQDN tabanlı filtreleme destekleniyorsa alan adı listesi, desteklenmiyorsa IP blokları kullanılmalıdır.

Revizyon #7
tugay tarafından 6 Temmuz 2026 13:31:40 oluşturuldu
tugay tarafından 13 Ekim 2026 12:43:21 güncellendi