Sophos Entegrasyon Rehberi

Bu rehber, bir **Sophos Firewall** ile Useroam Cloud arasındaki entegrasyonun tamamını anlatır: RADIUS kimlik doğrulama, web kimlik doğrulama, captive portal şablonu, firewall kuralları ve 5651 syslog yönlendirmesi.

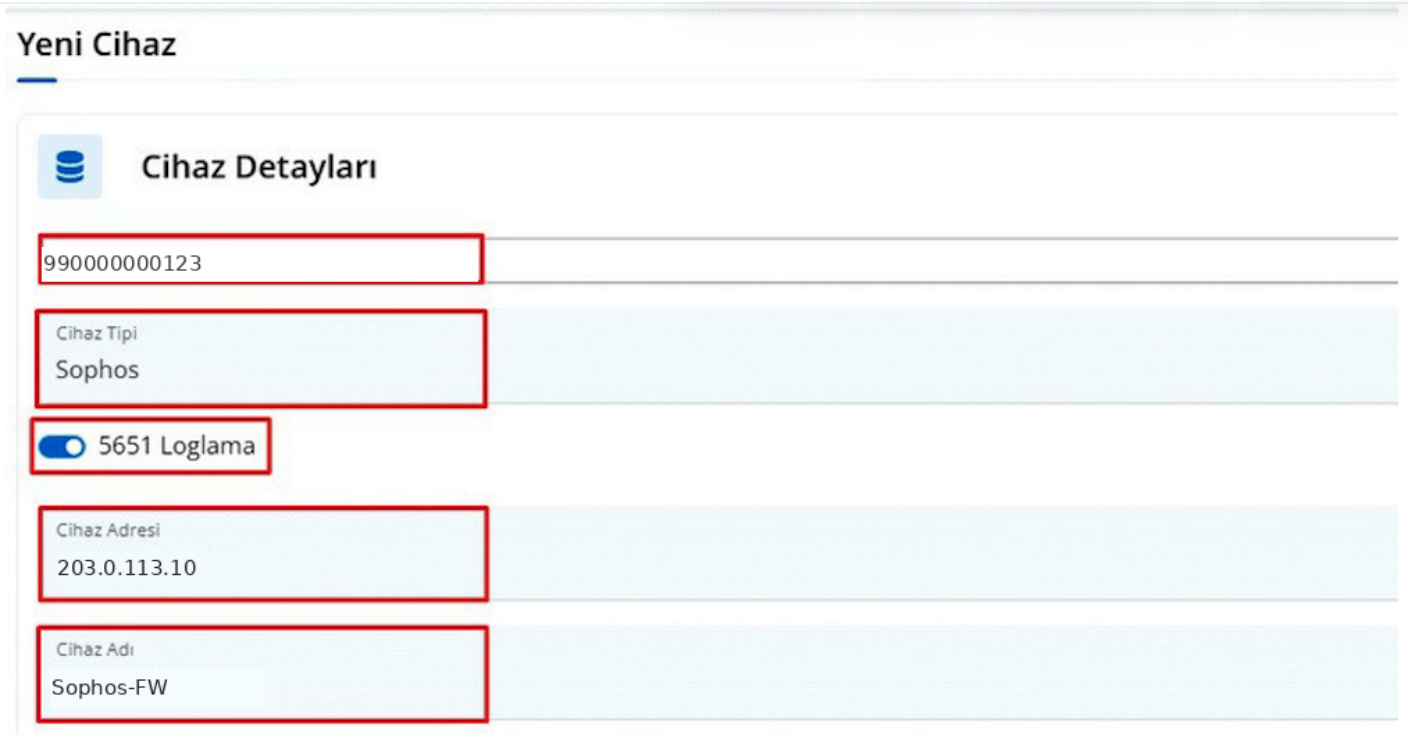
> **Başlamadan önce:** Sophos web arayüzüne yönetici erişimi ve firewall'un WAN IP adresi gerekir. Useroam kullanıcıları API üzerinden de yönetecekse, ardından **Sophos API Bağlantısı** sayfasındaki adımları tamamlayın.

1 - Useroam Panele Cihaz Ekleme

panel.useroam.com adresinden panelinize giriş yapıp **Yeni Cihaz** ekleyiniz. Sistem, lisansınızı otomatik olarak seçecektir.

- **Cihaz tipi:** Sophos seçiniz.
- **Cihaz adresi:** Firewall'un WAN IP adresini seçiniz. Eğer birden fazla WAN IP adresiniz varsa, Sophos cihazı bu isteği varsayılan olarak ilk WAN bacağından gönderir.

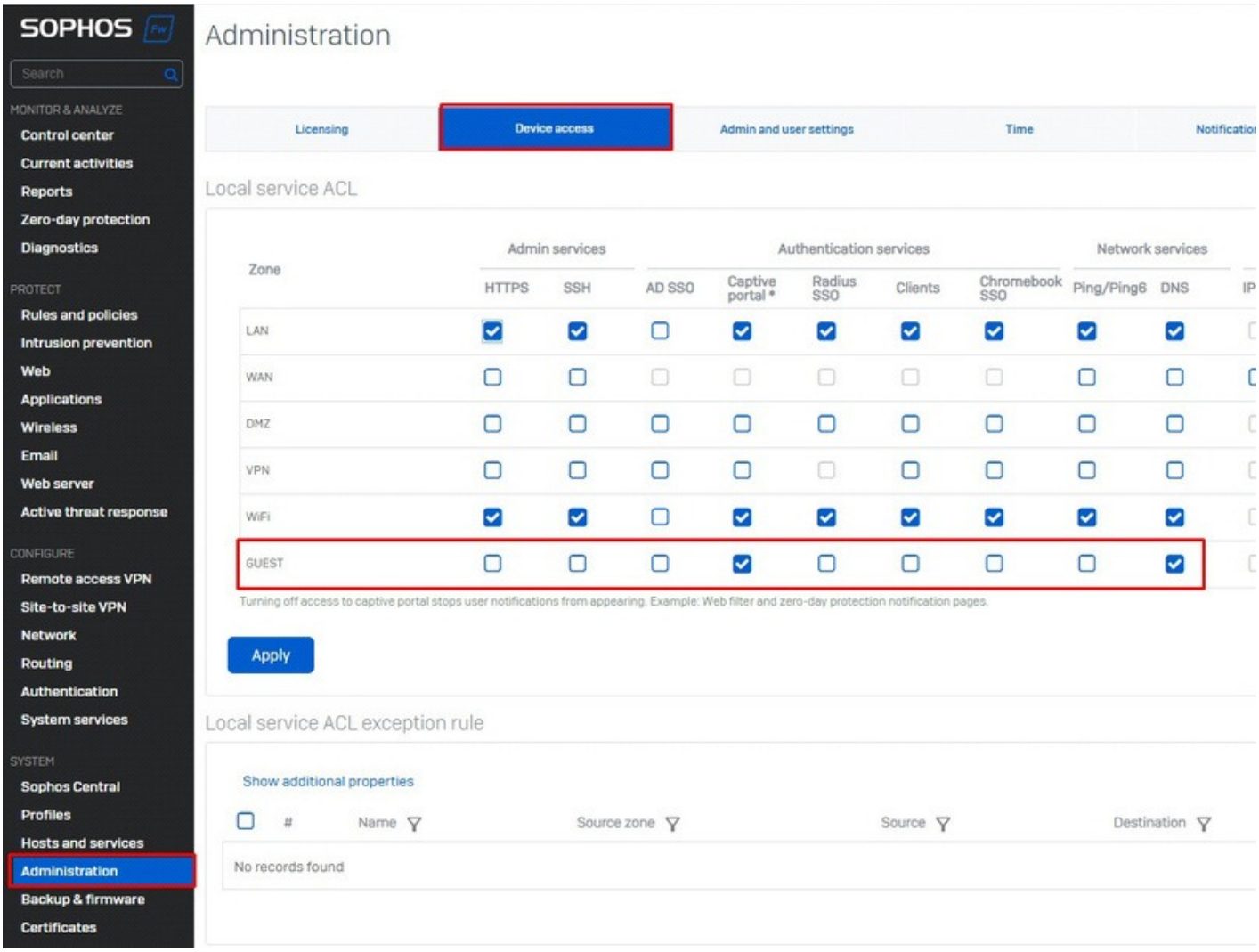
`Not: Farklı bir WAN bacağından gönderim yapmak isterseniz, bir SNAT kuralı oluşturarak ilgili trafiği istediğiniz WAN bacağına yönlendirebilirsiniz.`



2- Cihaz Erişim Ayarları (Device Access)

Sonra **Administration > Device Access** menüsüne gidiniz. Burada Useroam'u kullanacağınız Zone'da sadece **Captive Portal** ve **DNS** seçeneklerini işaretleyerek aktif hale getiriniz.

Dikkat: Radius SSO gibi farklı kimlik doğrulama mekanizmalarını aktif hale getirmeniz durumunda, yönlendirme sorunları veya Captive Portal sayfasının yavaş açılması gibi problemler yaşanabilir.

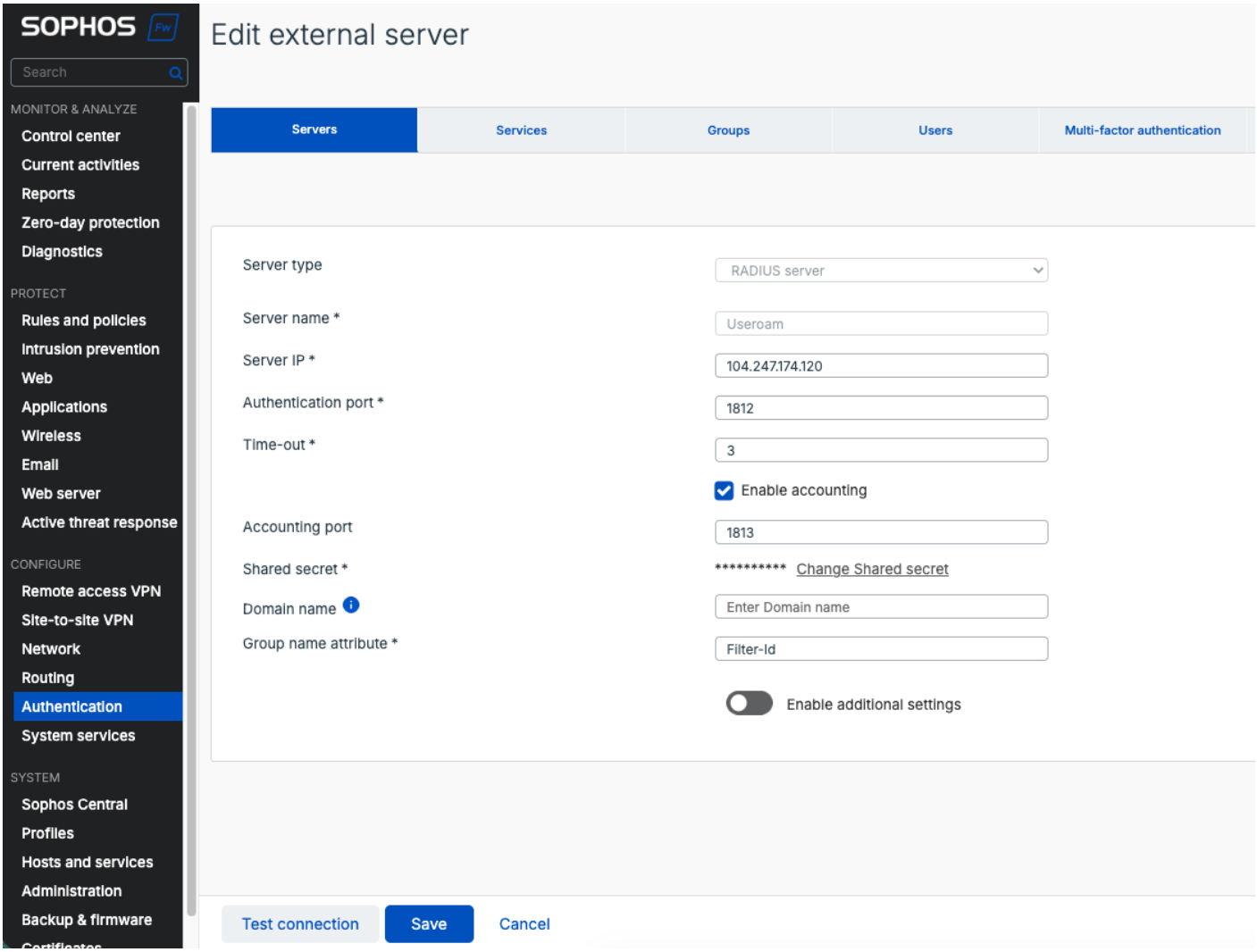


3 - Radius Sunucu Ekleme

Authentication > Servers menüsünden yeni bir Radius sunucu ekleyiniz. Server IP kısmına, **panel.useroam.com** adresini pingleyerek çıkan IP adresini yazınız.

Ardından, **Useroam > Sistem Ayarları > Cihaz Ayarları** altında bulunan **Cihaz Şifresi** kısmının karşısında yazan kodu da **Shared Secret** kısmına giriniz.

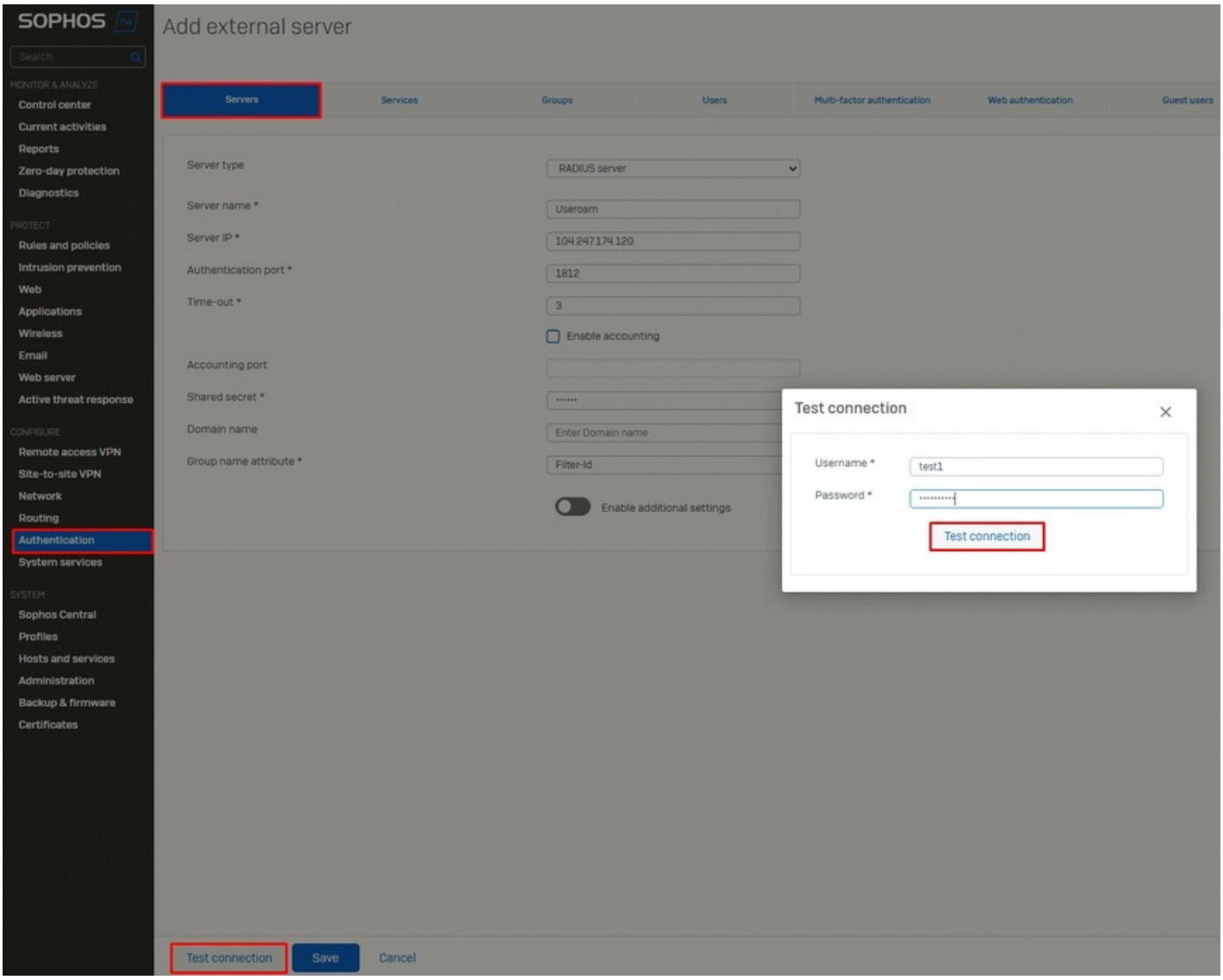




4 - Bağlantı Testi (İsteğe Bağlı)

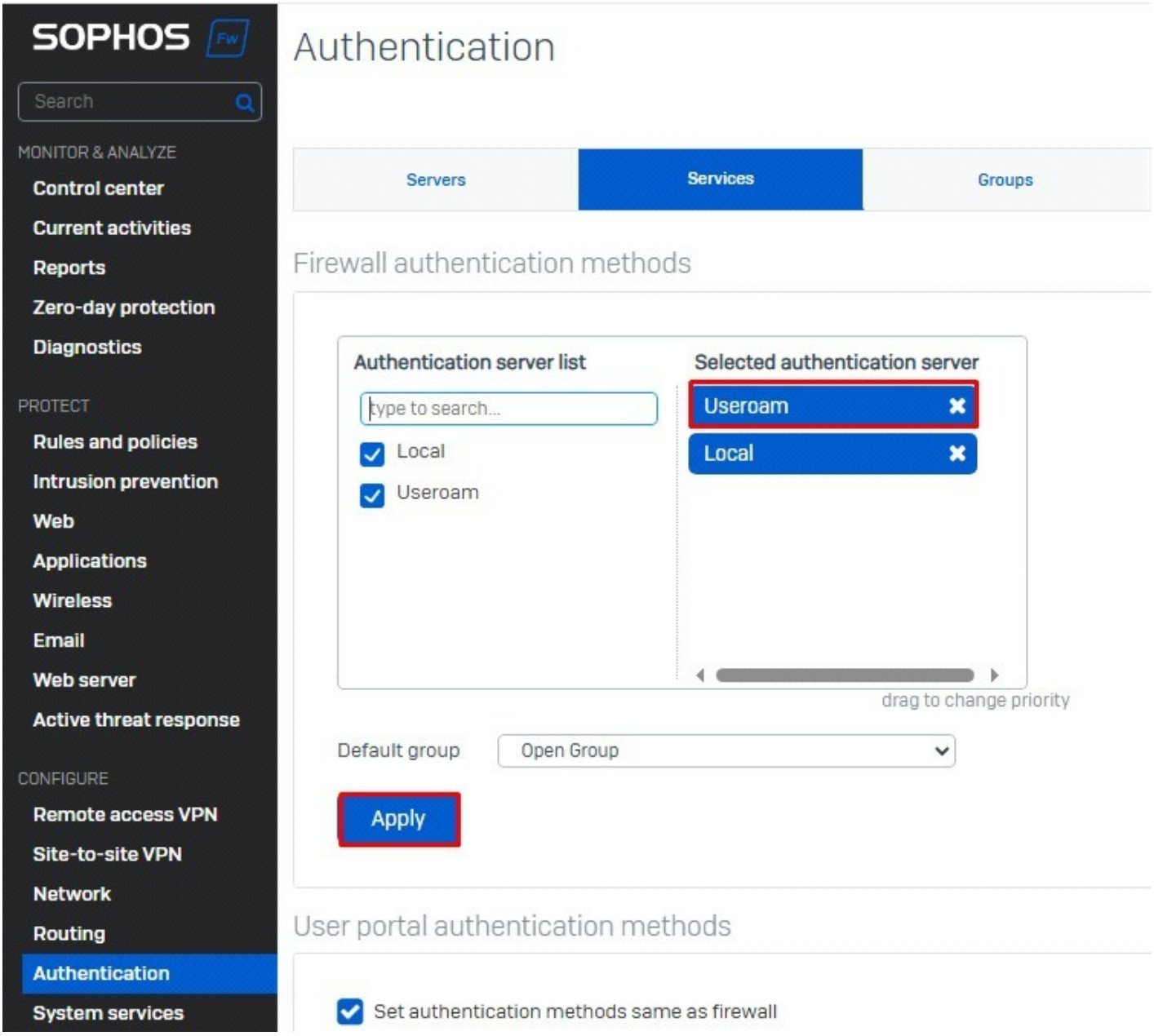
Bu noktada bir test yapmak isterseniz:

Useroam Cloud panelinden **Kullanıcı Yönetimi > Yeni Kullanıcı** adımlarıyla yeni kullanıcı oluşturabilir; Firewall'da Radius Sunucu ayarının içinden **Test Connection** ile bağlantıyı kontrol edebilirsiniz.



5 - Kimlik Doğrulama Önceliği (Authentication Methods)

Sonra **Authentication > Services** menüsünden Useroam'u *Firewall Authentication Methods* kısmında en üste çekip, **Apply** butonuna basarak ayarları kaydediniz.

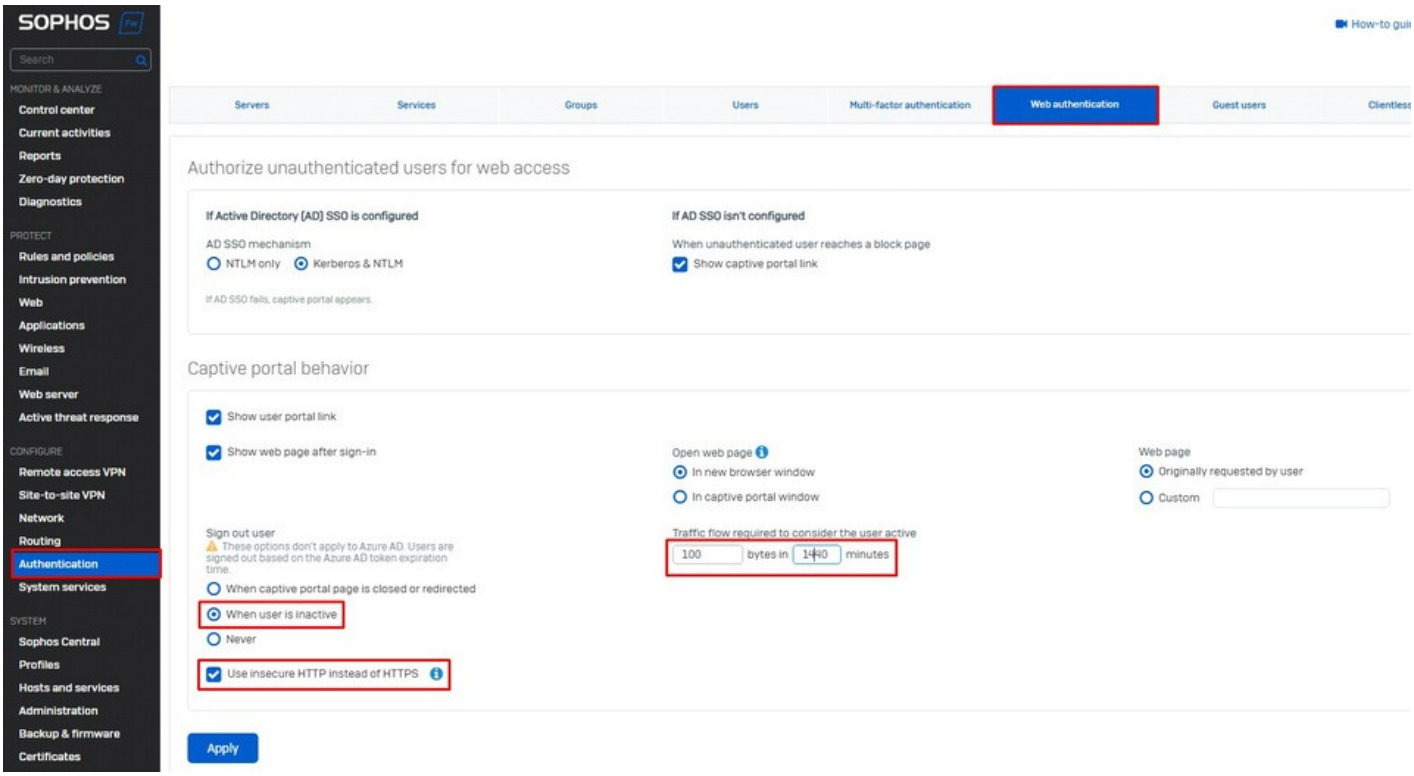


6 - Web Kimlik Doğrulama Ayarları

Ardından **Authentication > Web Authentication** menüsüne geçiniz. Burada *Sign Out User* kısmına gelerek, **When User is Inactive** seçeneğini işaretleyiniz.

Yan taraftaki *Traffic flow* kısmında ise 100 bytes için **1440 dk** (24 saate denk gelmektedir) olarak ayarlayınız; böylece bağlı her cihaz, 24 saat içinde en az 100 bytes veri yaptığı sürece oturumu Firewall'dan düşmeyecektir. İsterseniz bu süreyi kısaltabilirsiniz.

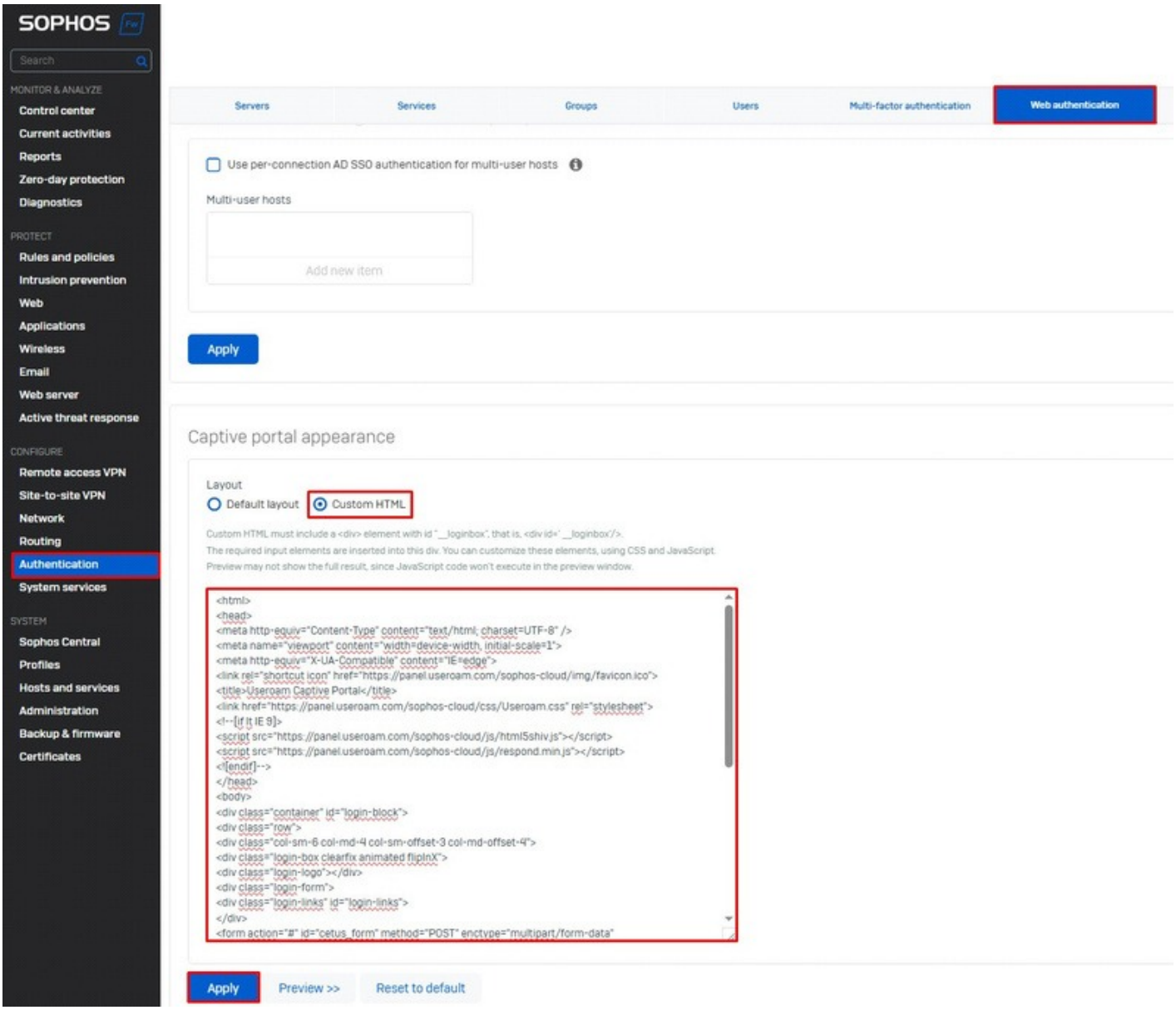
Son olarak **"Use insecure HTTP instead of HTTPS"** kutucuğunu seçerek ayarları kaydediniz.



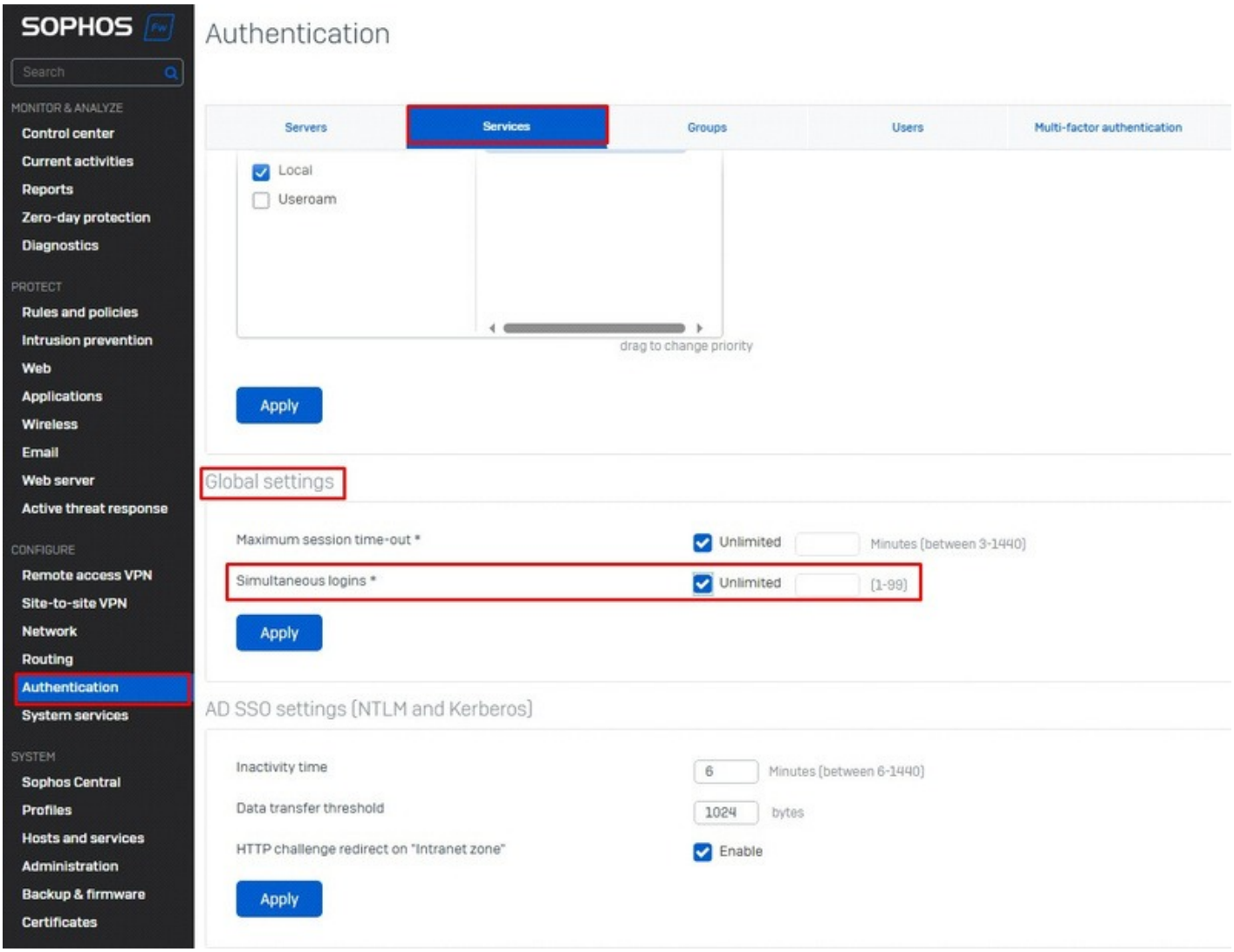
7 - Captive Portal Tasarımının Entegrasyonu (Custom HTML)

Useroam > Sistem Ayarları > Template kısmından `<html>` kod satırı ile başlayan bölümün hepsini alarak, Sophos Firewall'daki **Authentication > Web Authentication > Captive portal appearance > Custom HTML** kısmına yapıştırınız ve kaydediniz.





Eşzamanlı Oturum Sınırlandırması: Bir hesabın birden fazla cihazda kullanılmasını sınırlandırmak istiyorsanız, Sophos Firewall altında **Configure > Authentication > Services > Global Settings** menüsünden düzenlemeyi yapabilirsiniz.
Sistem varsayılan olarak limitsiz cihaz ayarı ile gelmektedir.



Firewall Kurallarının Oluşturulması

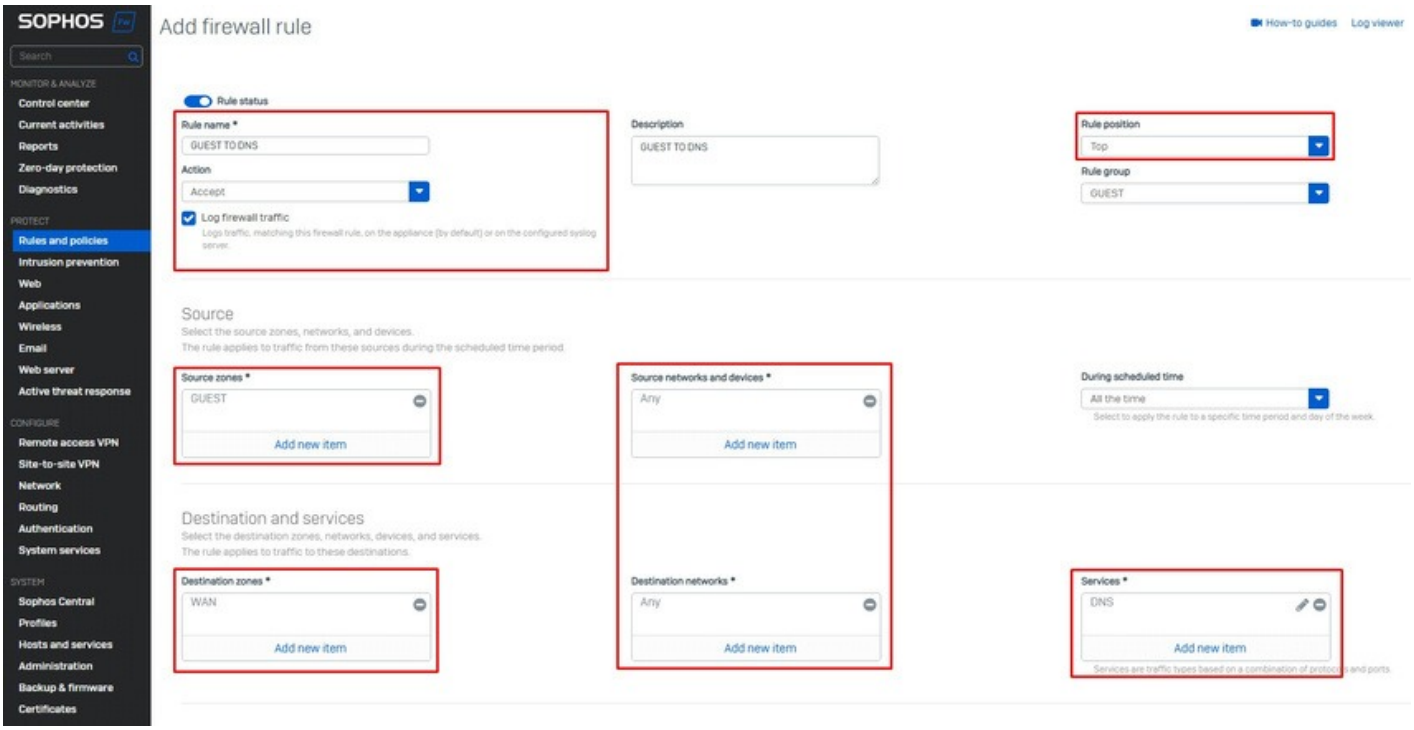
Kuralları oluşturmak için önce Sophos Firewall altında **Protect > Rules and Policies** menüsünden **Add Firewall Rule** sayfasına geliniz.

KURAL 1: Guest to DNS

Tüm cihazlar, bağlandıkları ağda internet erişimi olup olmadığını anlamak için cihaza özel alan adına bir DNS sorgusu atar (Örn: `captive.apple.com`).

Bu sorgu sonucu gelince cihaz internet olduğunu anlayıp trafik akışını başlatır. Aksi takdirde hotspot yönlendirmesi yapılmayacaktır.

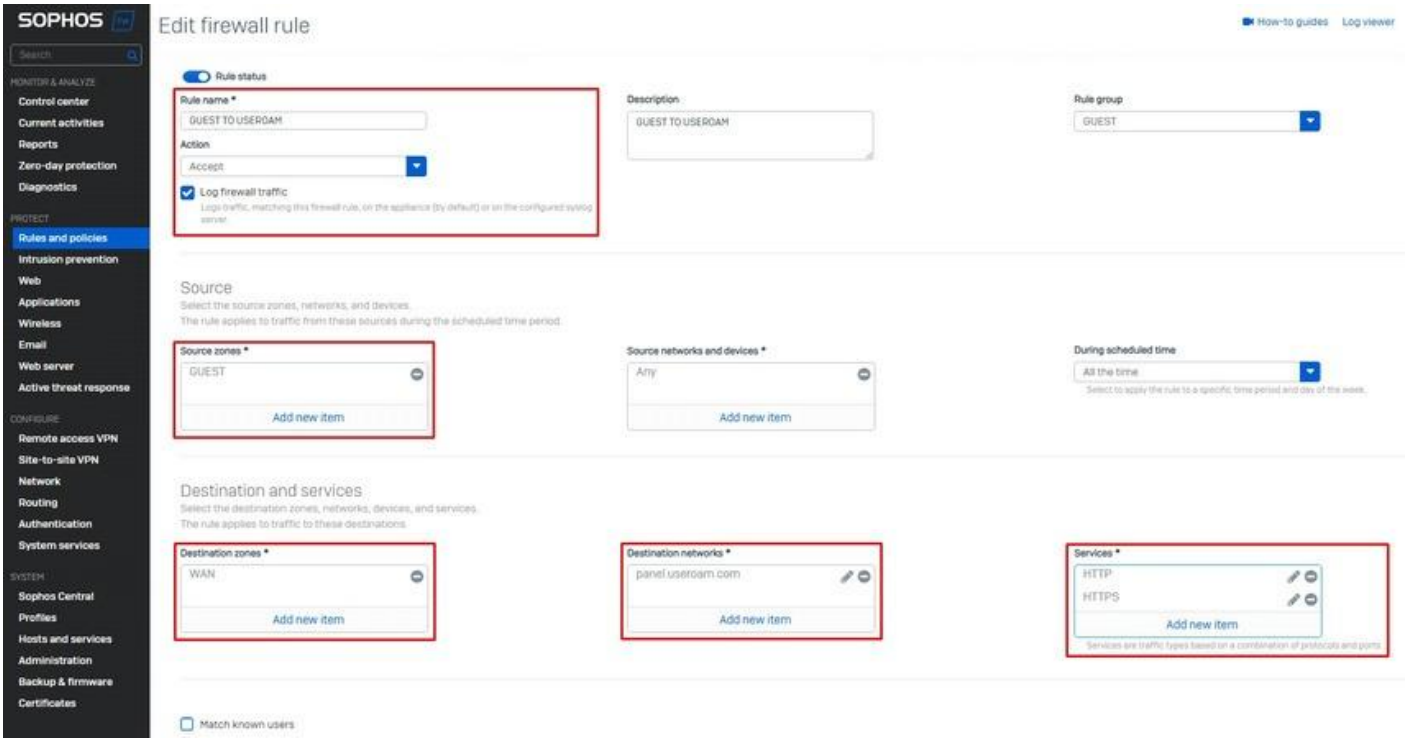
Bu kuralın misafirlerin internet çıkışı kuralının üstünde olması gerekiyor.



KURAL 2: Guest to Useroam

Bu kural ile misafir ağınızdaki cihazların `*.useroam.com`'a erişmesini sağlayacaksınız.

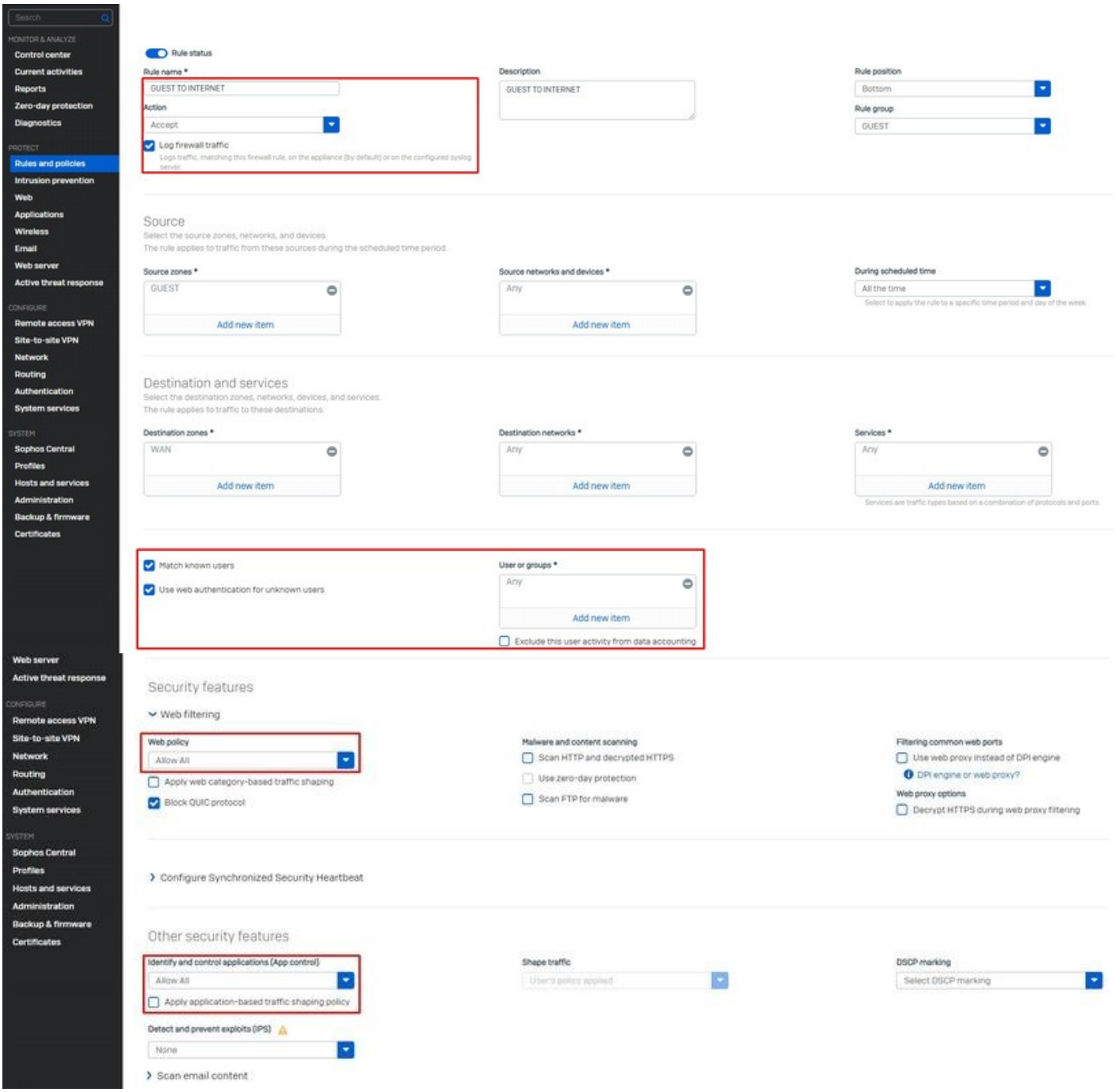
Bunun için Services kısmında **HTTP/HTTPS** seçmeniz yeterli olacaktır.



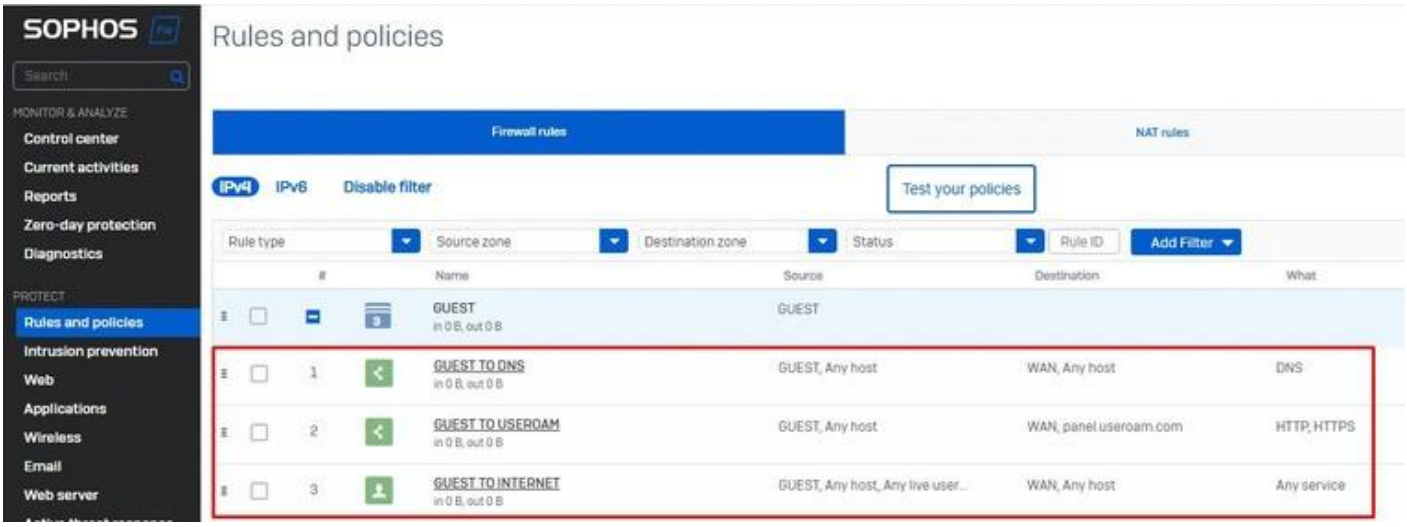
KURAL 3: Guest to Internet

Bu kuralda cihazlarınızın internet erişimi sağlanacak.

Log Firewall kutucuğunu seçiniz. Tanımsız kullanıcılara Hotspot ekranı gelmesi için **Match Known Users** ve **Use Web Authentication For Unknown Users** kutucuklarını da seçiniz. Web Policy ve Identify And Control Applications (App Control) kısımlarında *Allow All* ya da herhangi bir politika seçiniz.



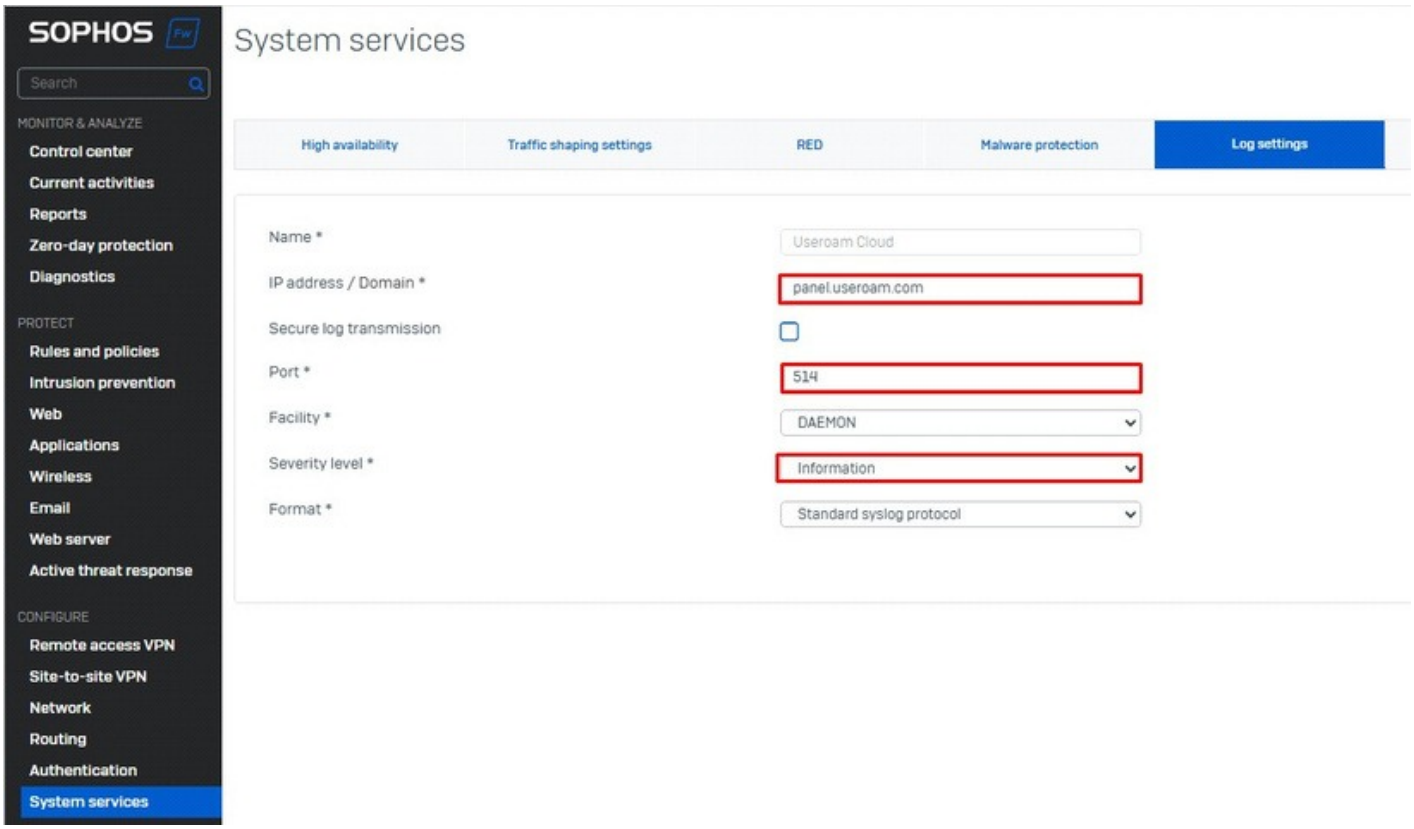
*İşlemler sonucunda **Protect > Rules and Policies** menüsü sıralaması görseldeki gibi görünmelidir.*



Logların Useroam Cihazına Yönlendirilmesi

1 - Syslog Server Tanımlama

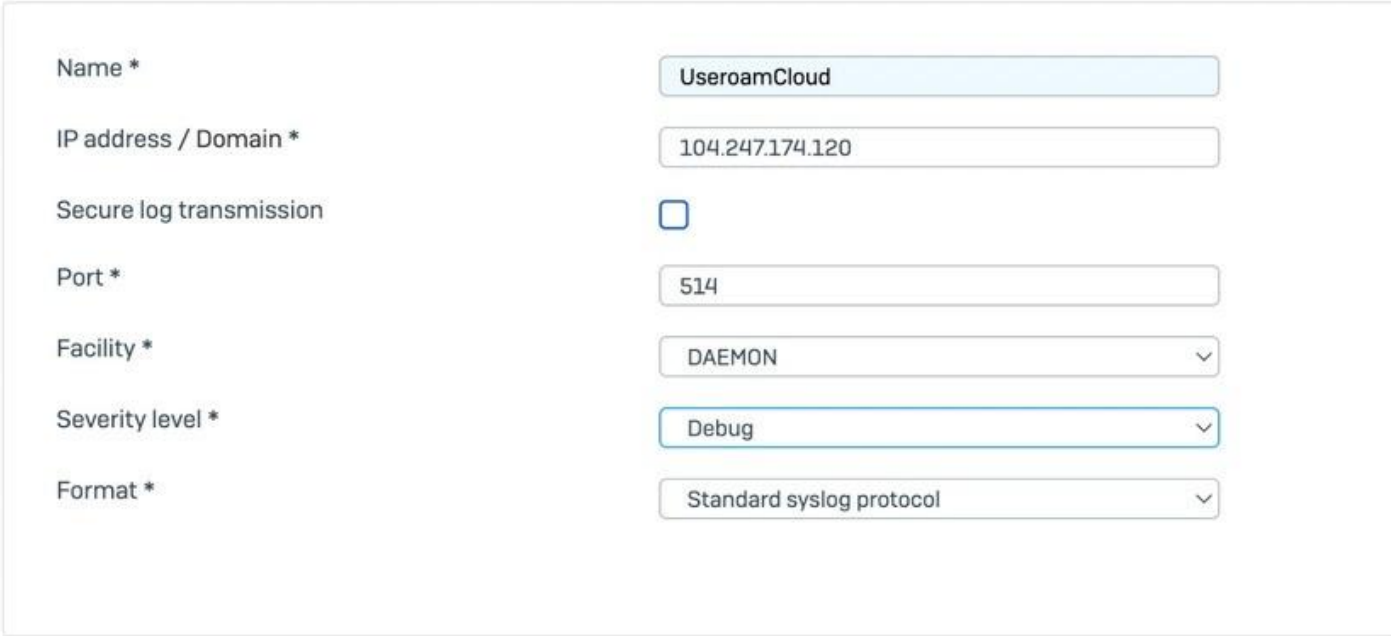
Öncelikle **System Services > Log Settings** menüsüne gelerek yeni bir Syslog server tanımlayınız.



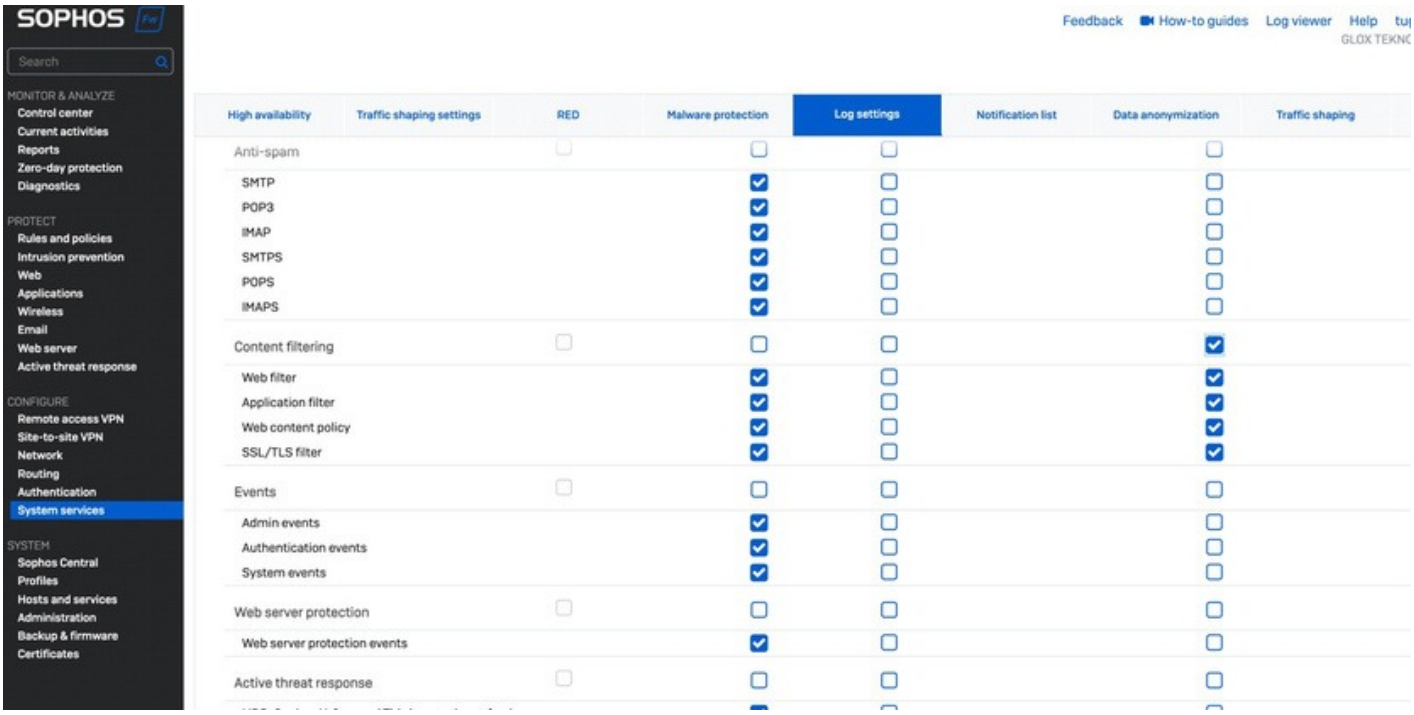
2 - Syslog Detaylarını Girme ve Başlatma

Yeni eklenen syslog server için aşağıdaki bilgileri doldurunuz:

- **Name:** Useroam Cloud
- **IP address / Domain:** 104.247.174.120
- **Port:** 514
- **Facility:** DAEMON
- **Severity level:** Debug
- **Format:** Standard syslog protocol



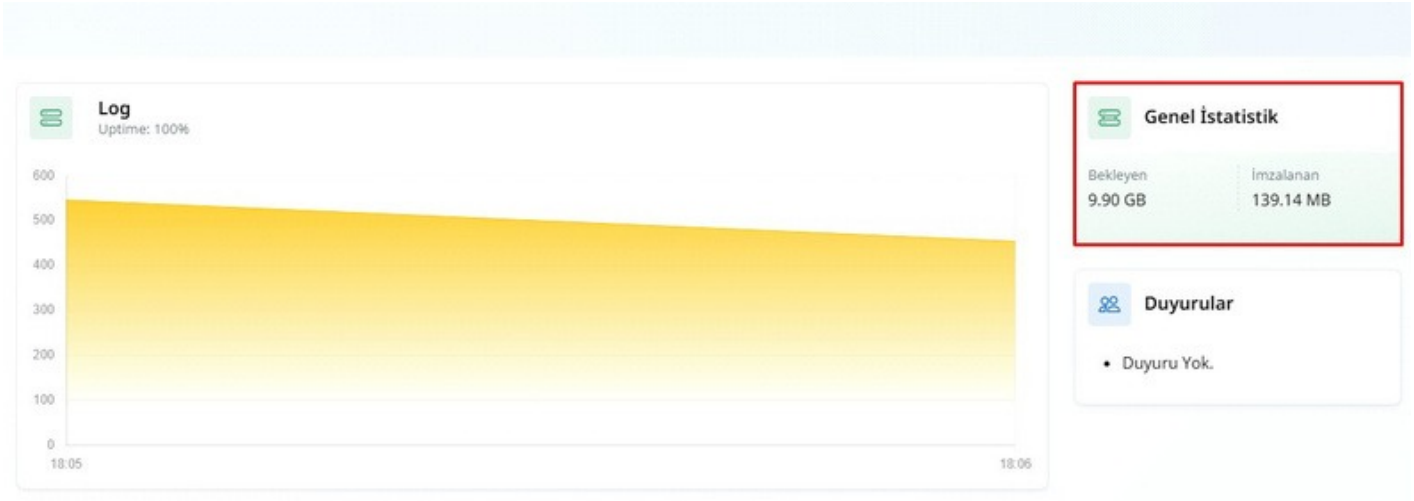
Daha sonra yeni eklenen syslog server satırında sadece **Content Filtering** alanlarını seçerek loglamayı Useroam'a doğru başlatınız.



3 - Log Paket Kontrolü

Bu işlem sonrasında Firewall'dan paketlerinizin gelip gelmediğini anlamak için Useroam paneline dönünüz.

Sağ üst köşedeki **Genel İstatistik** kısmını kontrol edip, **İmzalama Bekleyen** alanın altındaki kısmı kontrol ediniz.



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 #10
tugay tarafından 6 Temmuz 2026 08:25:14 oluşturuldu
tugay tarafından 13 Ekim 2026 12:43:17 güncellendi