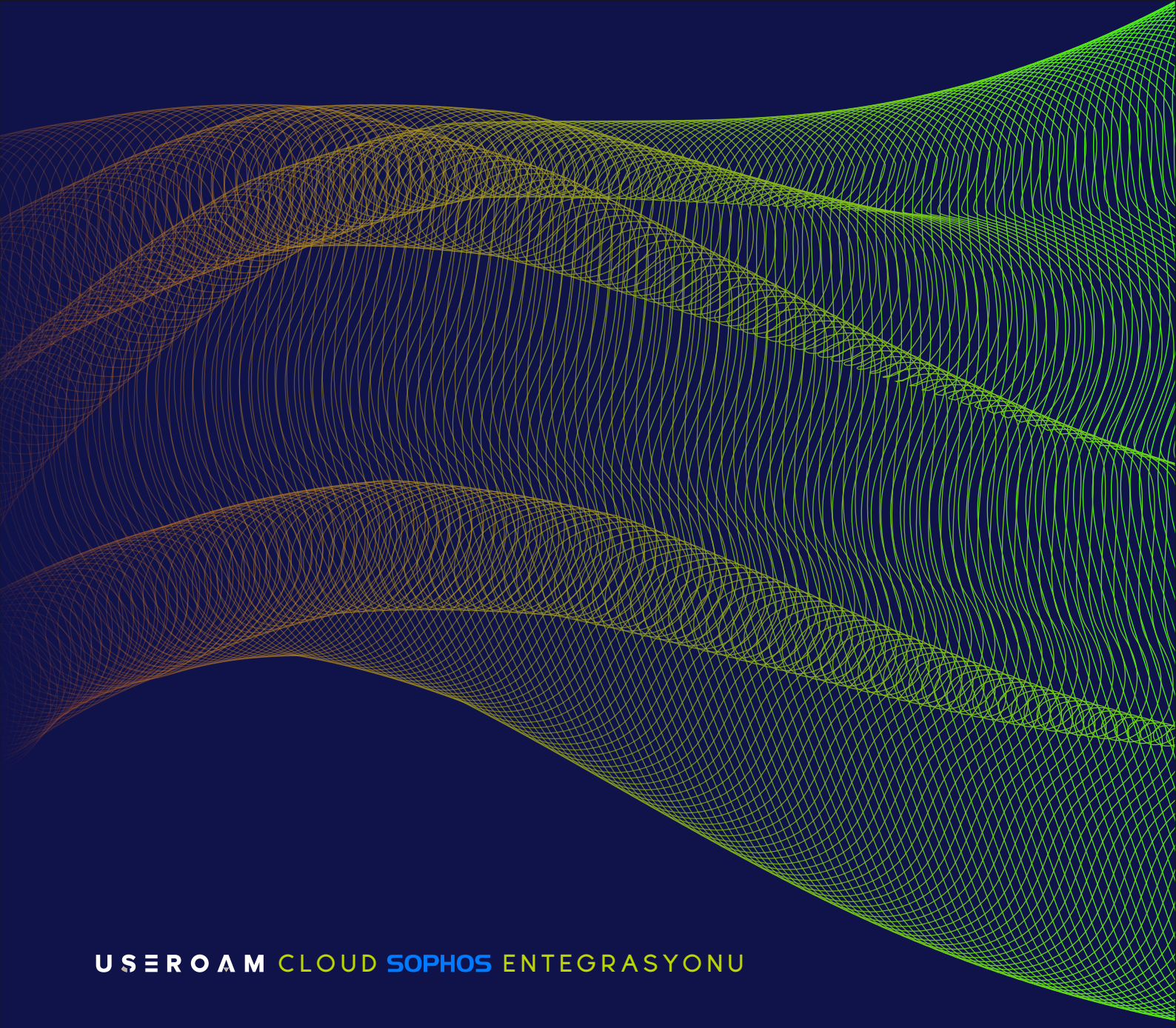


USEROAM CLOUD SOPHOS ENTEGRASYONU

USEROAM
HOTSPOT&REPORTING

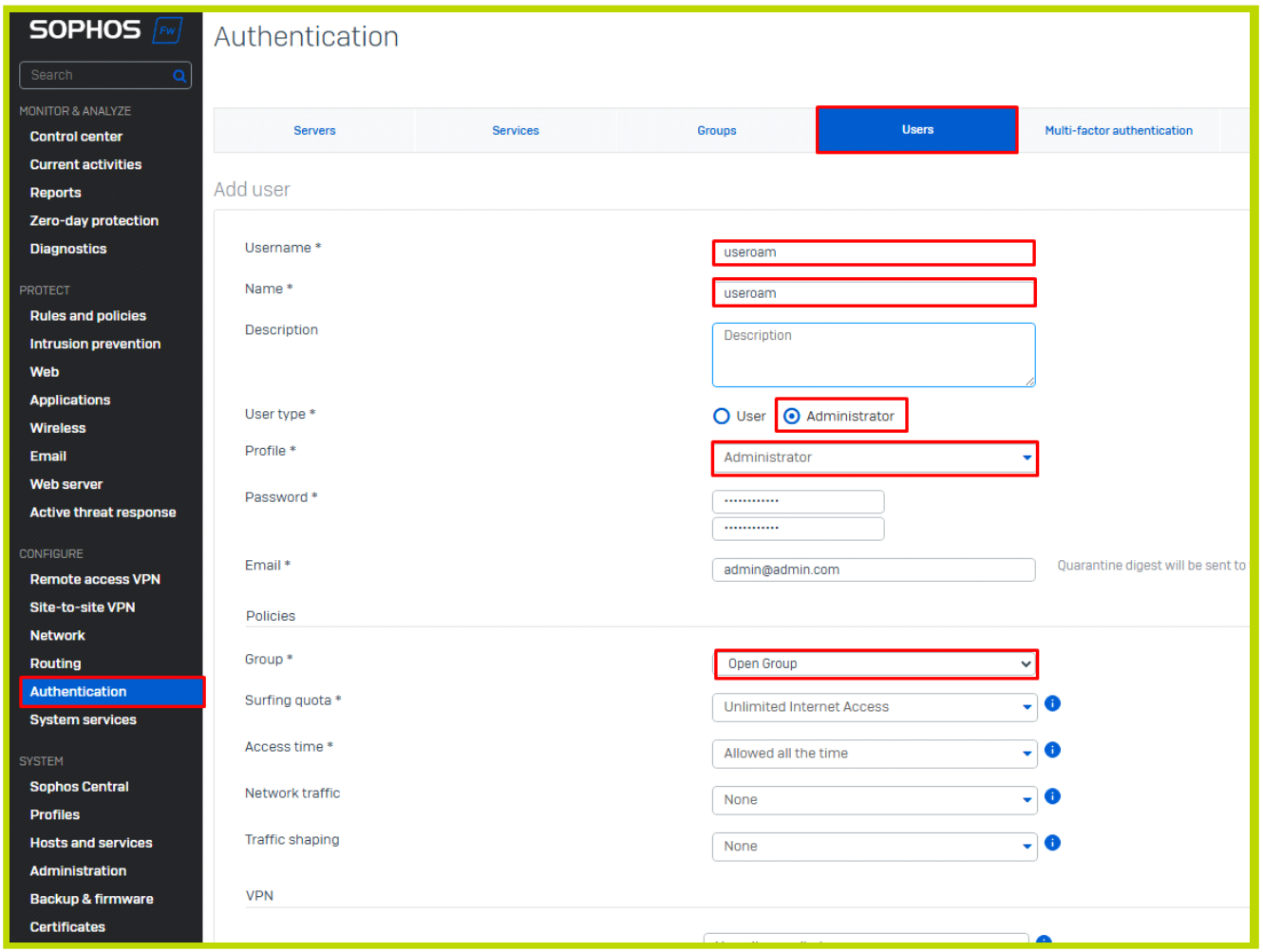
GLOX

Useroam Cloud'a hoş geldiniz!

Bu rehber Useroam Cloud ile Sophos güvenlik duvarınızın entegrasyon sürecini hızlı ve sorunsuz bir şekilde tamamlamanıza yardımcı olmak için detaylı talimatları içermektedir.

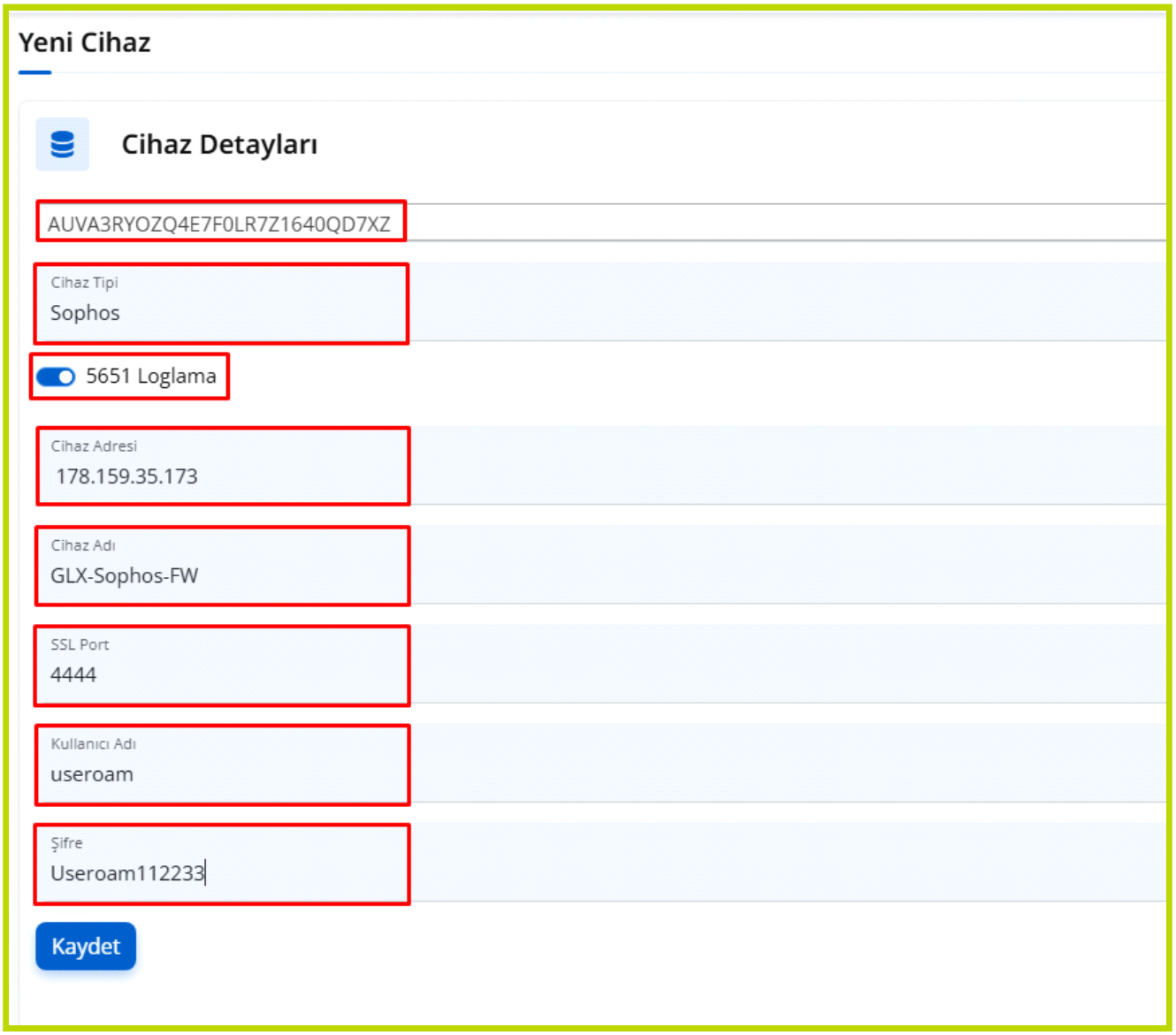
Aşağıda verilen adımları takip ederek entegrasyon sürecinizi kolayca tamamlayabilirsiniz.

1 İlk olarak Sophos Firewall'da **Authentication > Users** menüsünden yeni bir yetkili kullanıcı oluşturup firewall tarafındaki iletişimi kurmasını sağlayınız.
User type olarak ***Administrator***; **Profile** olarak ***Administrator*** seçiniz. Ardından **Group** kısmında sınırsız erişimi olan herhangi bir grup seçerek kullanıcınızı oluşturunuz.



2

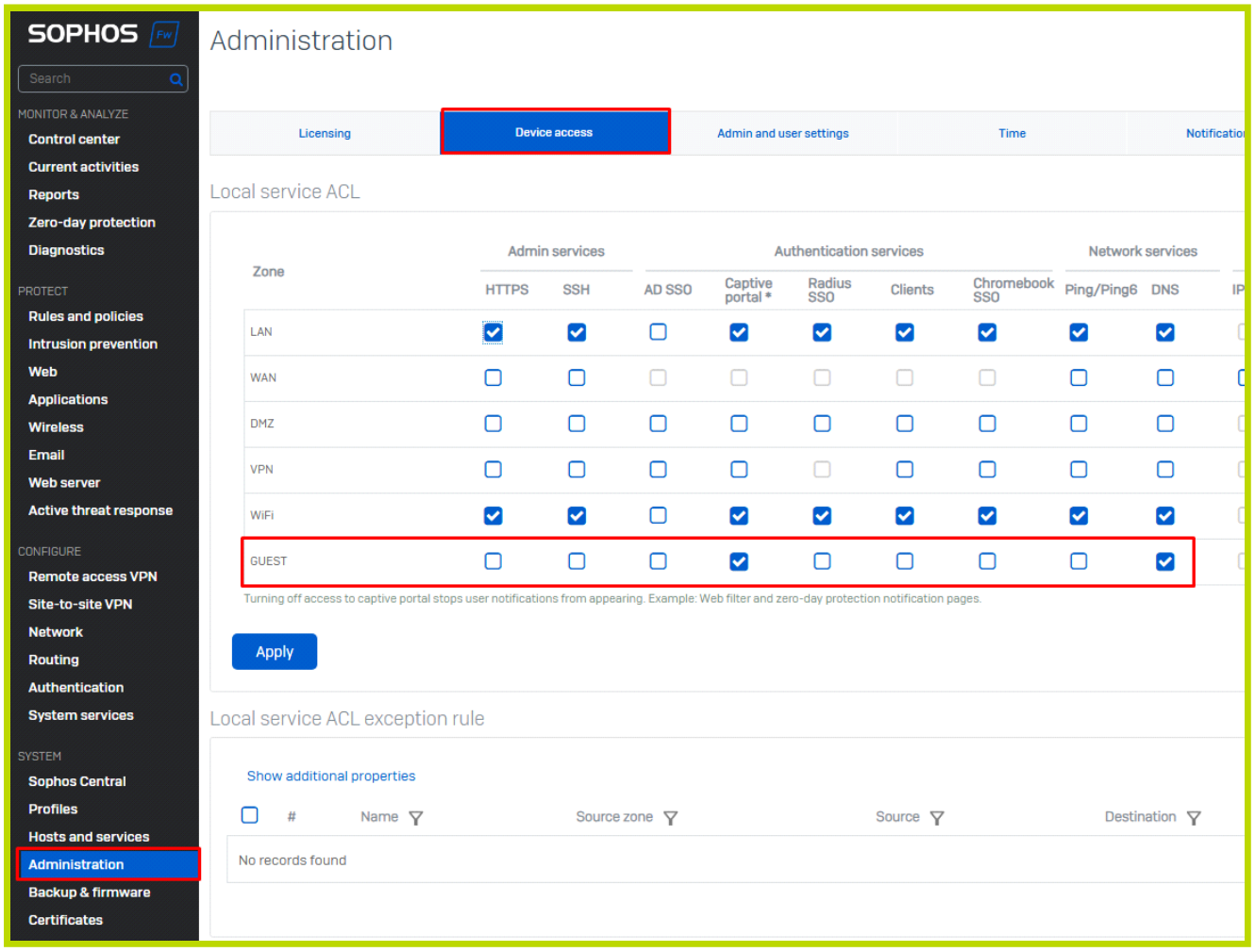
Ardından **panel.useroam.com** adresinden panelinize giriş yapıp Yeni Cihaz ekleyiniz.
Sistem, lisansınızı otomatik olarak seçecektir.
Cihaz tipinden **Sophos**'u seçiniz.
Cihaz adresi olarak **Firewall'un WAN IP adresini** seçiniz. Eğer birden fazla WAN IP adresiniz varsa, Sophos cihazı bu isteği varsayılan olarak **ilk WAN** bacağından gönderir.
Farklı bir WAN bacağından gönderim yapmak isterseniz, bir **SNAT kuralı** oluşturarak ilgili trafiği istediğiniz WAN bacağına yönlendirebilirsiniz.



3

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

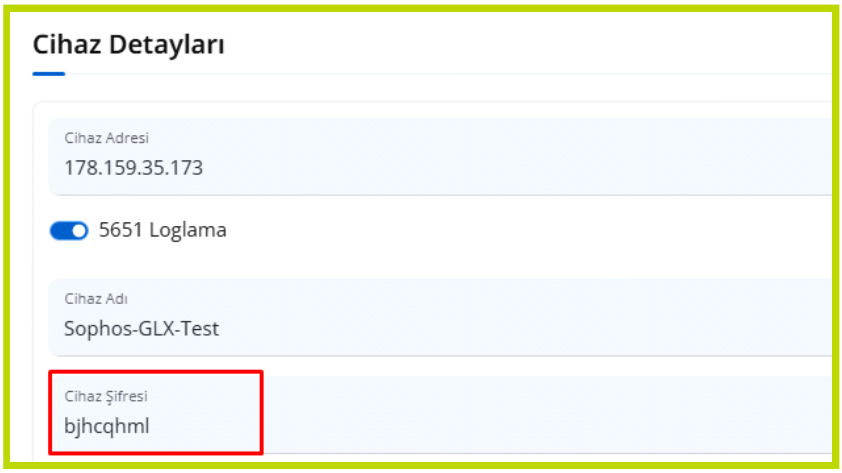
Dikkat: Radius SSO gibi farklı kimlik doğrulama mekanizmalarını aktif hale getirmeniz durumunda, yönlendirme sorunları veya Captive Portal sayfasının yavaş açılması gibi problemler yaşanabilir.

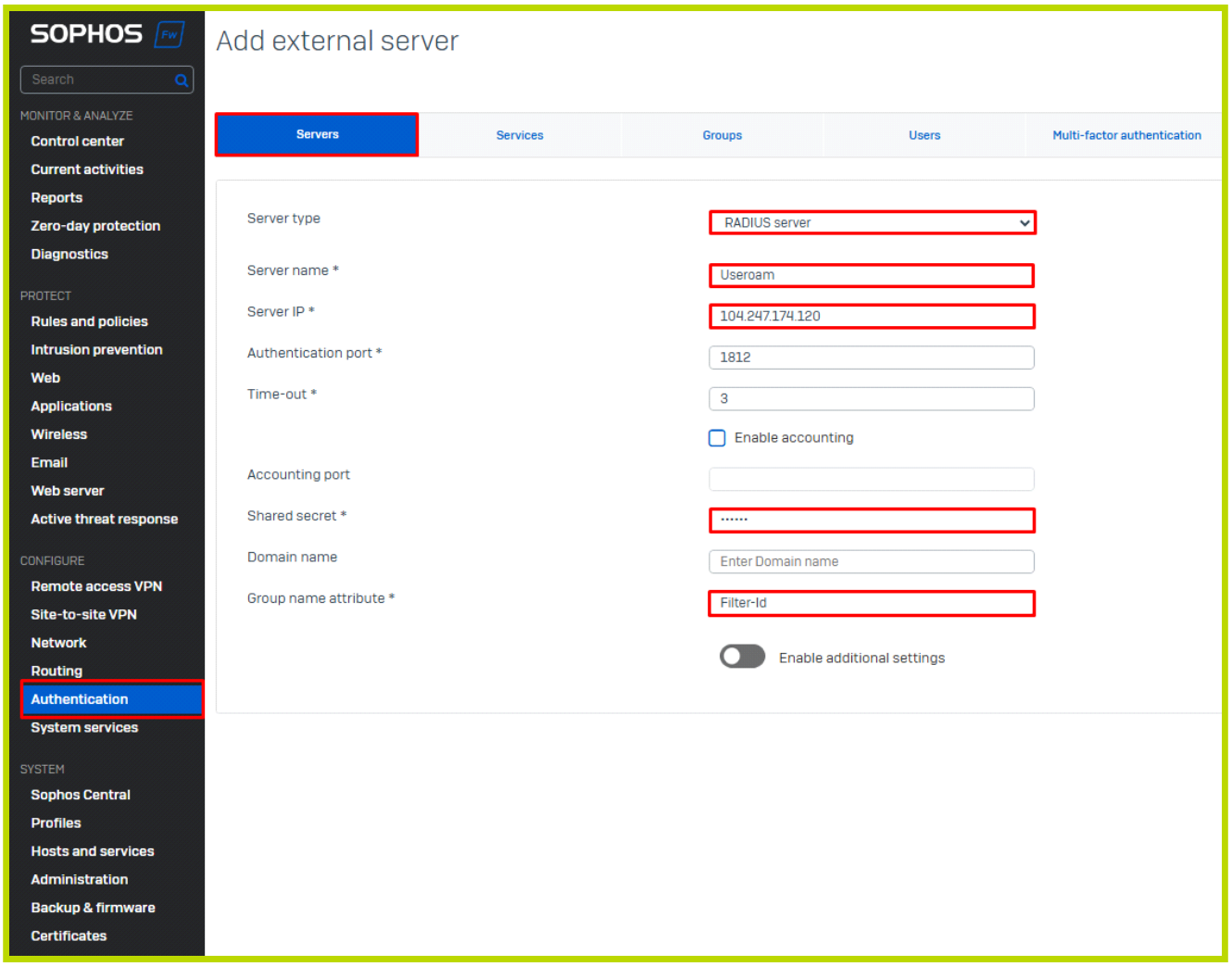


4

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

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

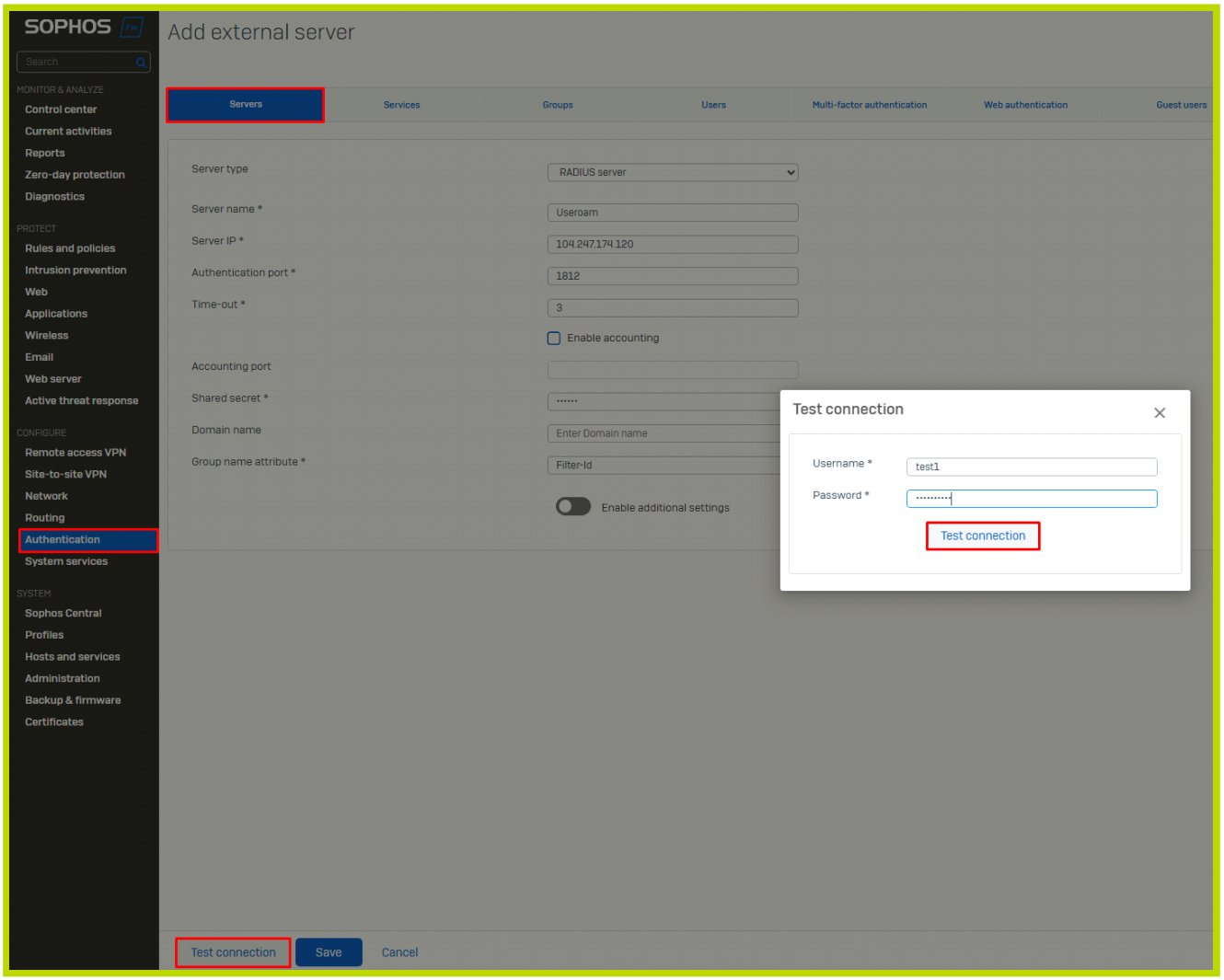




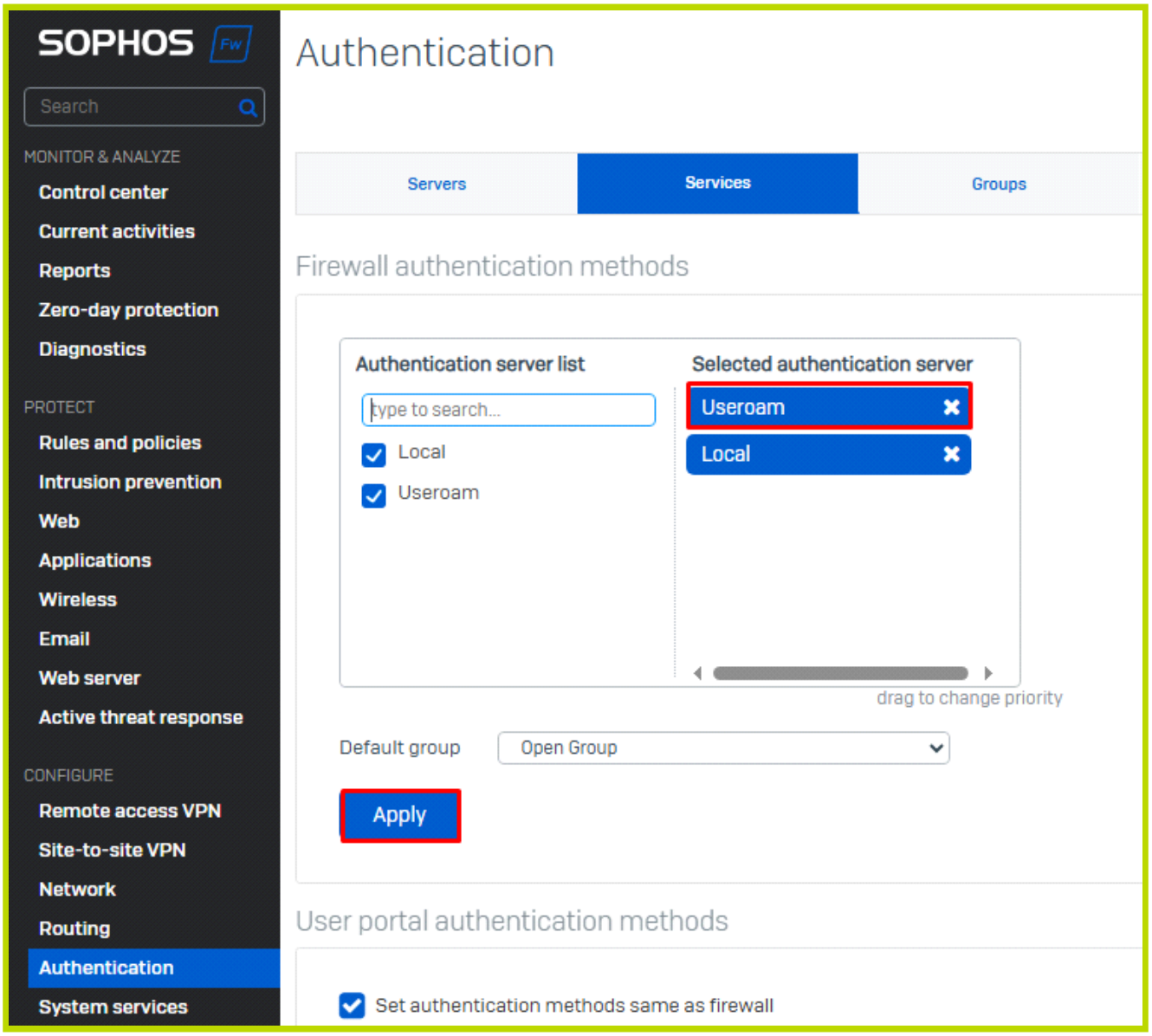
Bu noktada bir test yapmak isterseniz,

5 **Useroam Cloud** panelinden **Kullanıcı Yönetimi> Yeni Kullanıcı** adımlarıyla yeni kullanıcı oluşturabilir;

Firewall'da Radius Sunucu ayarının içinden Test Connection ile bağlantıyı kontrol edebilirsiniz.

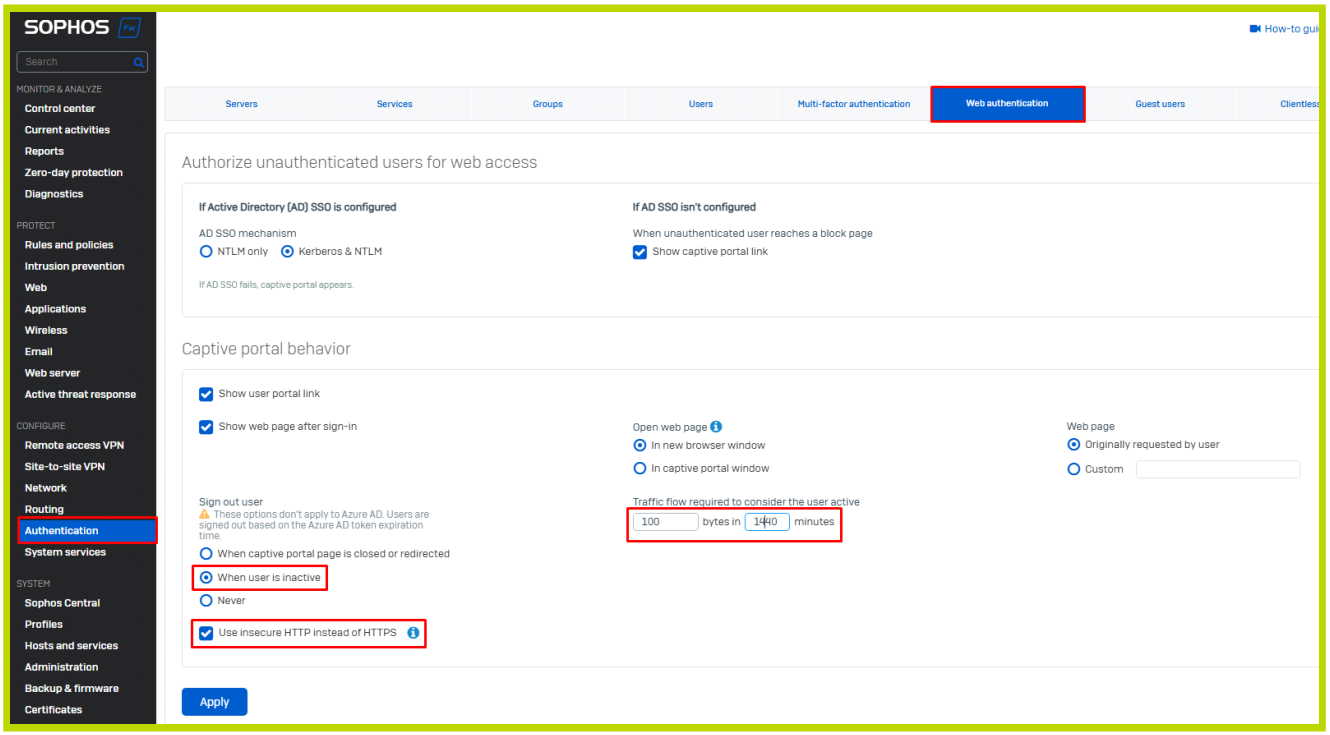


6 Sonra **Authentication> Services** menüsünden **Useroam**'u **Firewall Authentication Methods** kısmında üste çekip, **Apply** butonuna basarak, ayarları kaydediniz.

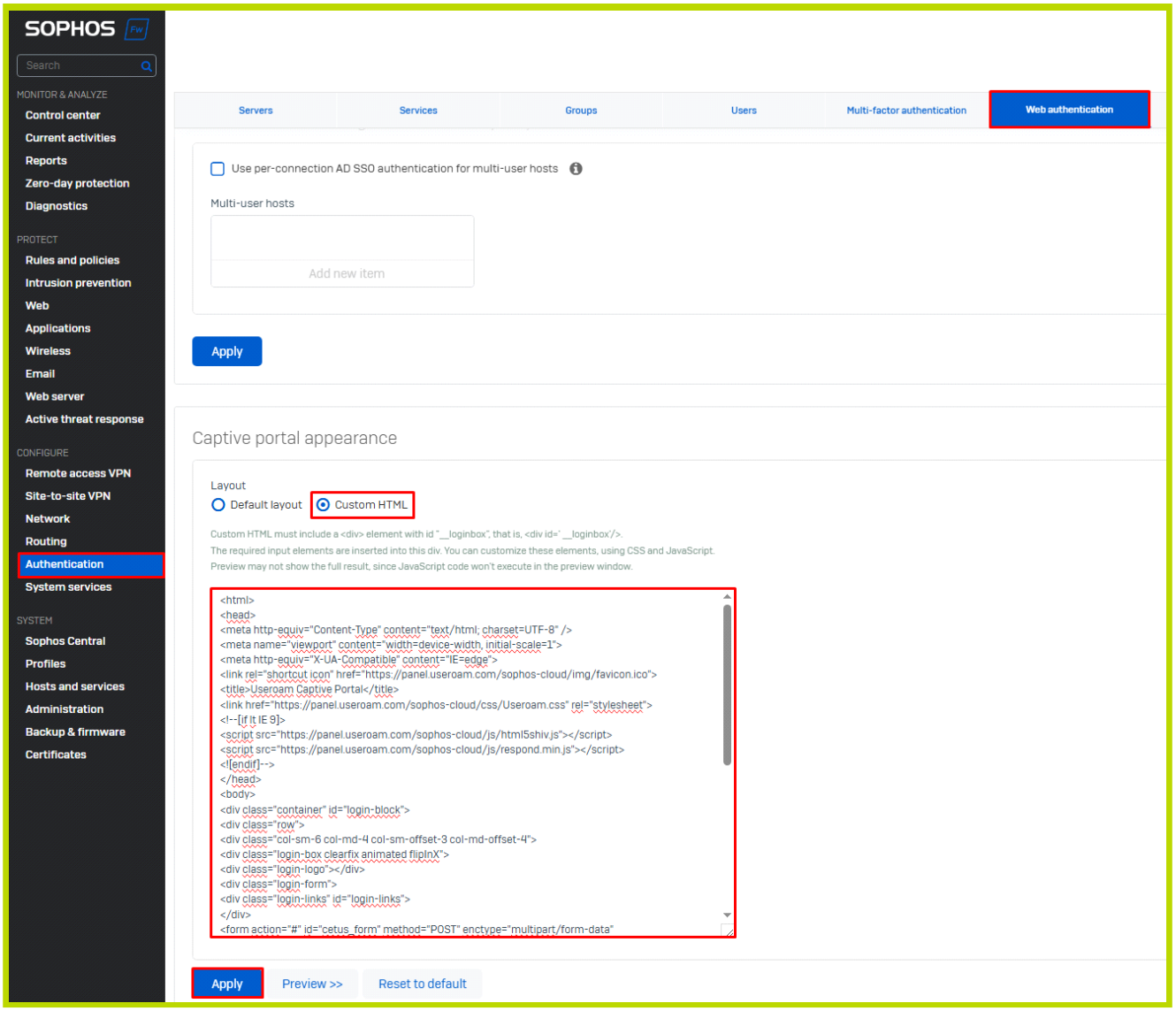


7 Ardından **Authentication > Web Authentication** menüsüne geçiniz. Burada **Sign Out User** kısmına gelerek, **When User is Inactive** seçeneğini işaretleyiniz. Yan taraftaki **Traffic flow** kısmında ise **100bytes** için **1440 dk** olarak ayarlayınız - *bu süre 24 saate denk gelmektedir; böylece bağlı her cihaz, 24 saat içinde en az 100 bytes veri yaptığı sürece oturumu Firewall dan düşmeyecektir. İsterseniz bu süreyi kısaltabilirsiniz.*

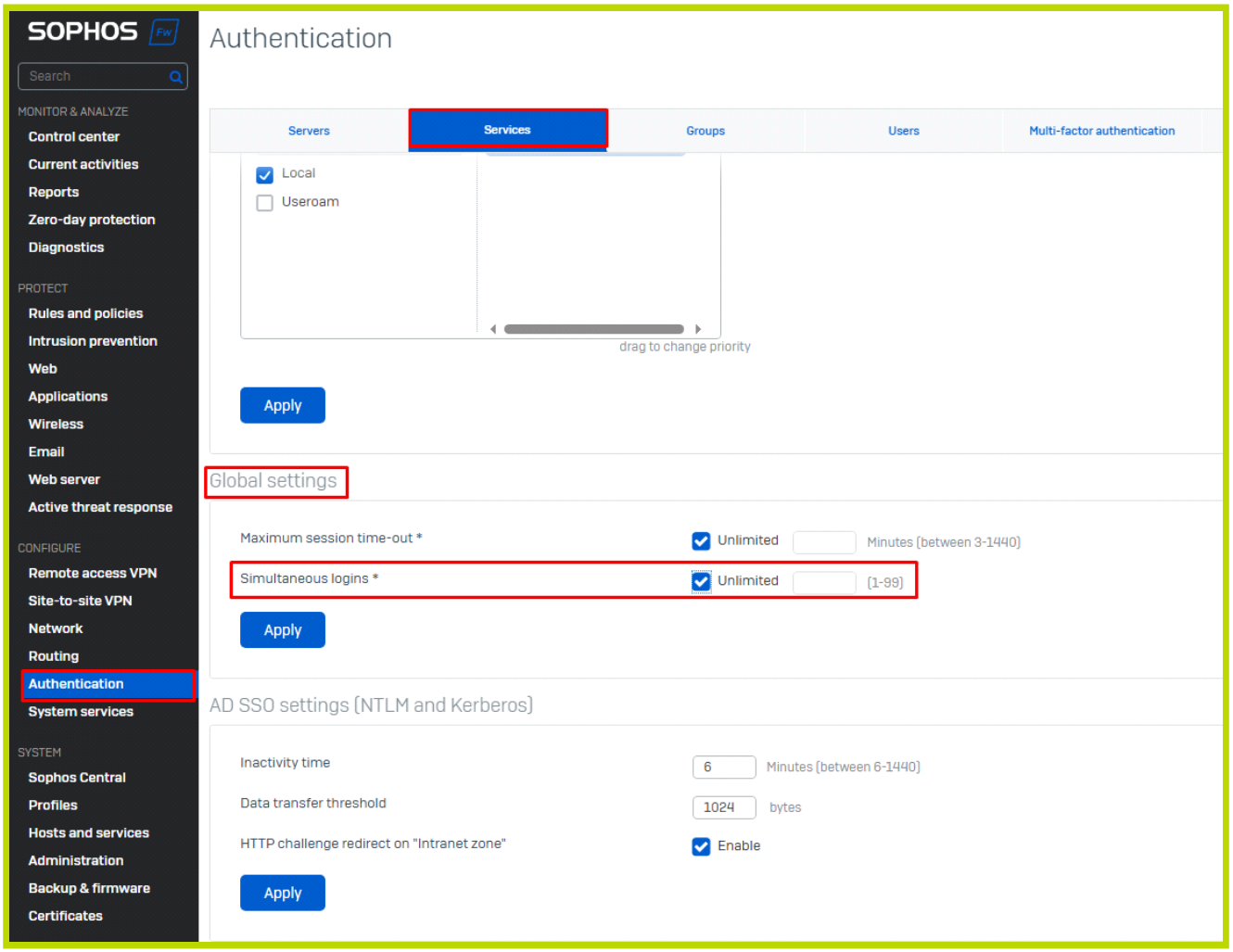
Son olarak **"Use insecure HTTP instead of HTTPS"** kutucuğunu seçerek ayarları kaydediniz



8 **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.



Dikkat: 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.

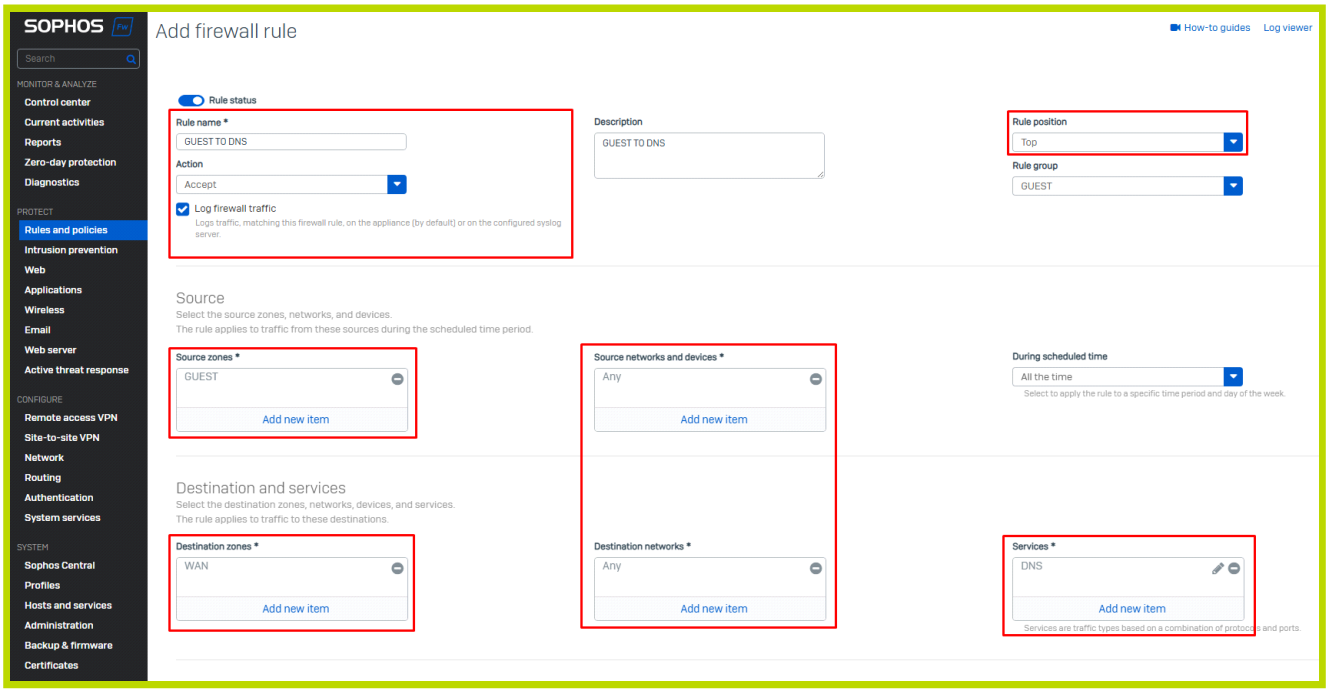


FIREWALL KURALLARININ OLUŞTURULMASI

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

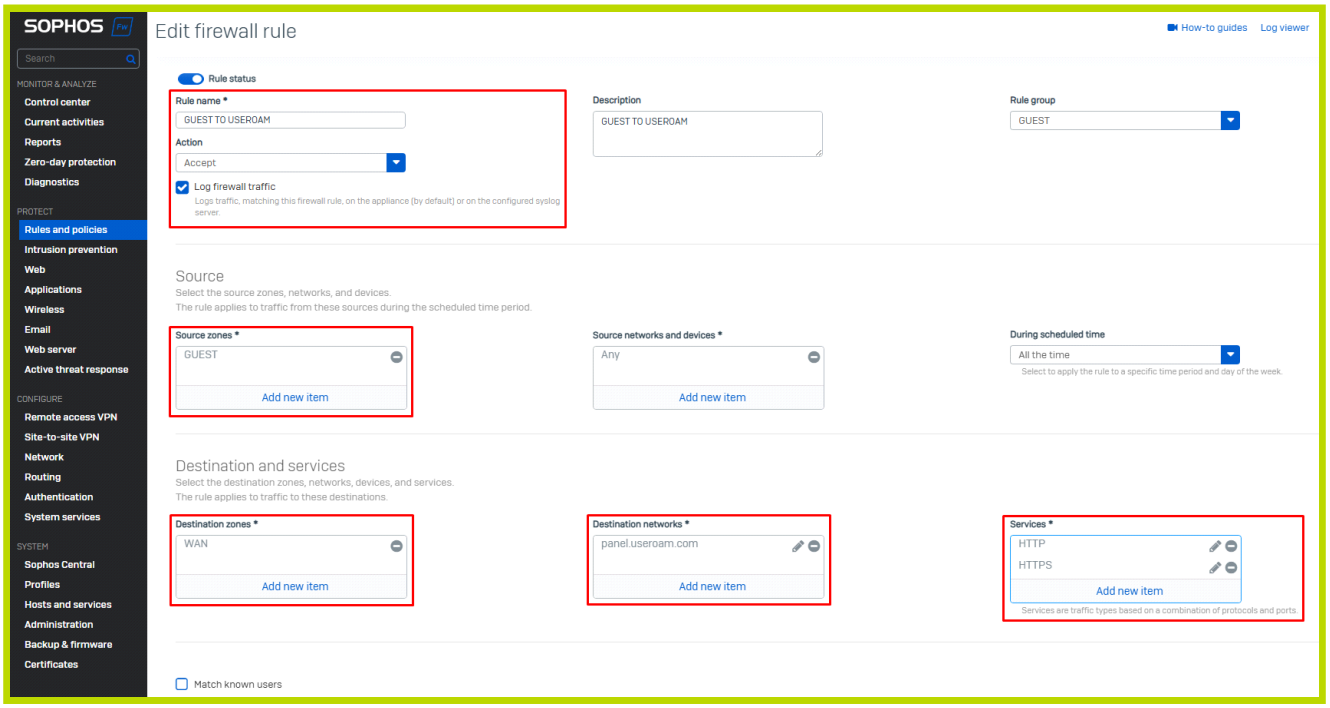
KURAL 1.

Guest to DNS: *Tüm cihazlar, bağlandıkları ağda internet erişimi olup olmadığını anlamak için cihaza özel alan adına bir DNS sorgusu atar. Örneğin captive.apple.com; bu sorgu sonucu gelince, cihaz, ağda internet olduğunu anlayıp, trafik akışını başlatır. Aksi takdirde, hotspot yönlendirmesi de yapılmayacaktır. Bu kuralın misafirlerin internet çıkışı kuralının üstünde olması gerekiyor.*



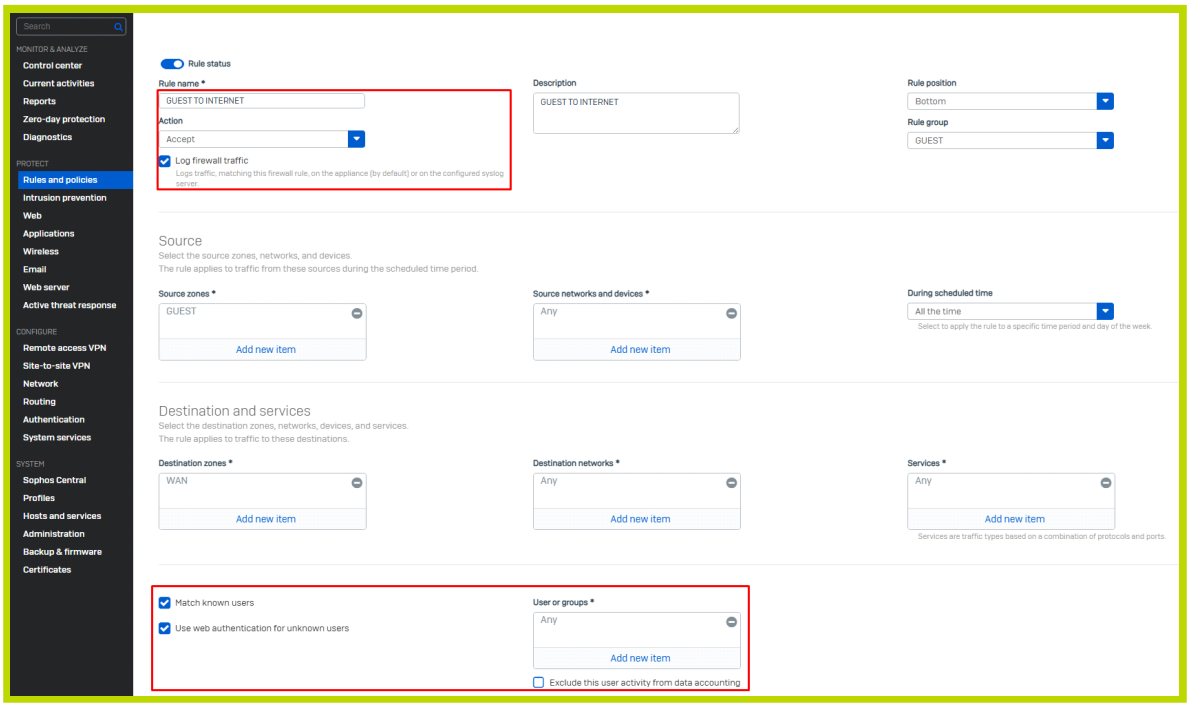
KURAL 2.

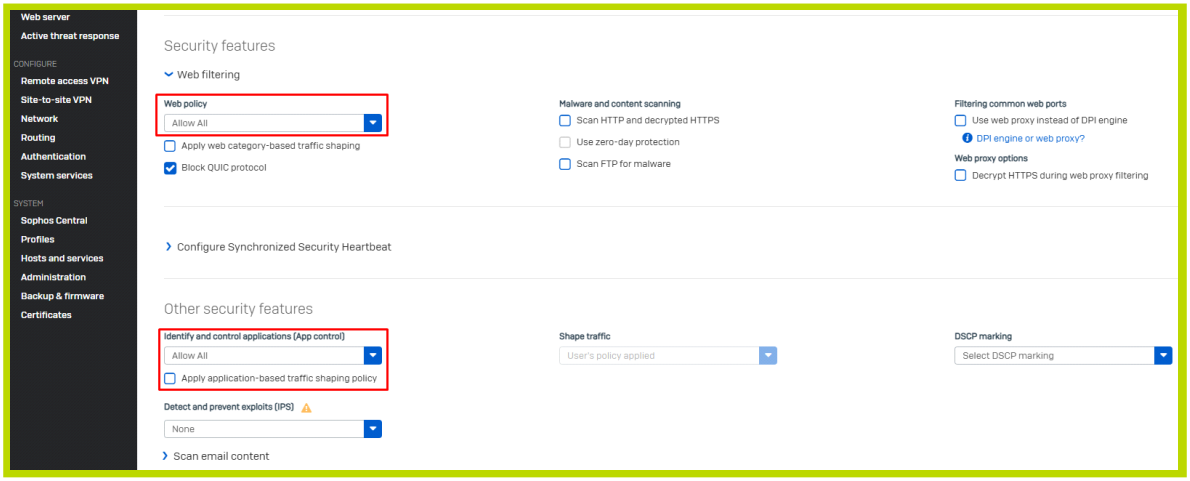
Guest to Useroam: Bu kural ile misafir ağınızdaki cihazların **panel.useroam.com**'a erişmesini sağlayacaksınız. Bunun için **Services** kısmında **HTTP/HTTPS** seçmeniz yeterli olacaktır.



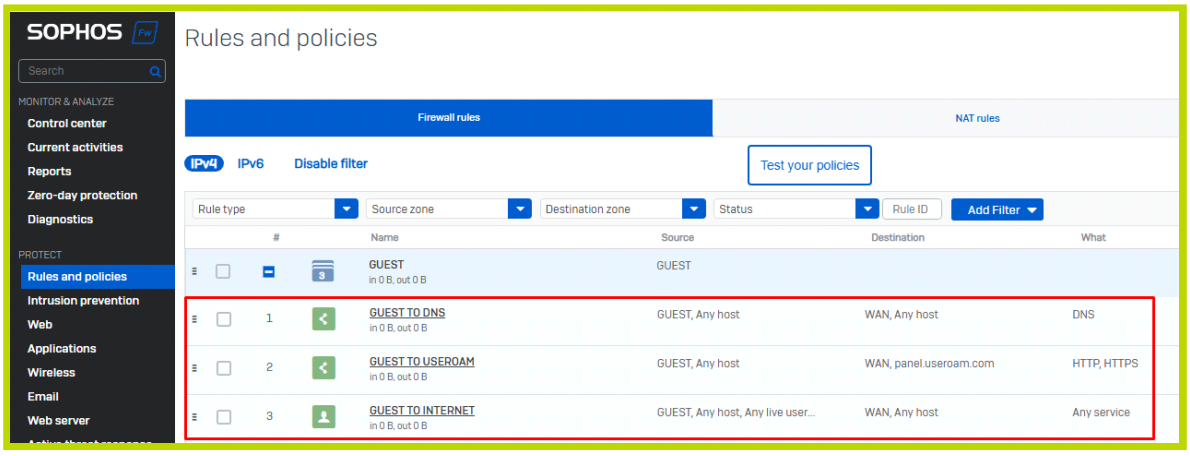
KURAL 3.

Guest to Internet: Bu kuralda cihazlarınızın internet erişimi sağlanacak. **Log Firewall** kutucuğunu seçiniz. **Match Known Users** ve **Use Web Authentication For Unknown Users** kutucuklarını da tanımsız kullanıcılara Hotspot ekranı gelmesi için seçiniz. **Web Policy** ve **Identify And Control Applications (App Control)** kısımlarında **Allow All** ya da herhangi bir politika seçiniz.





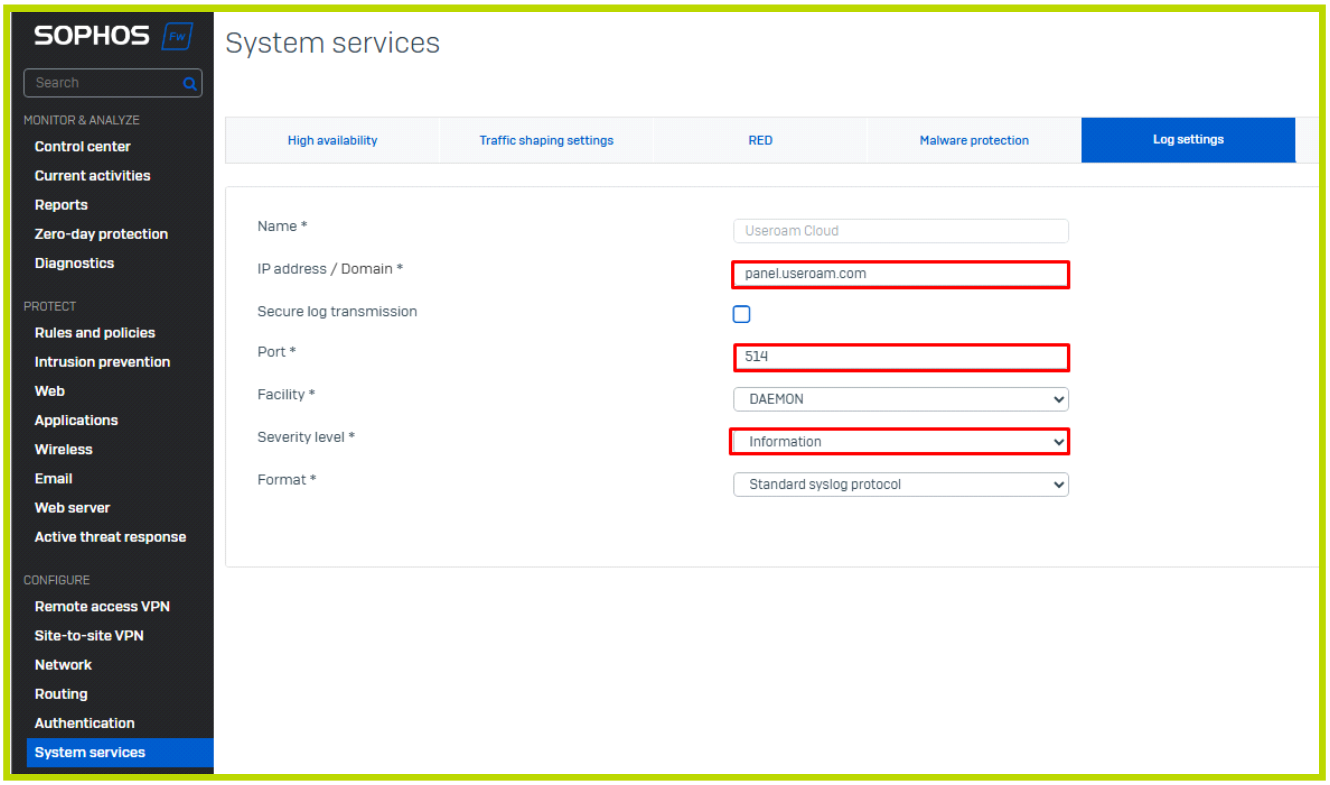
İşlemler sonucunda **Protect> Rules and Policies** menüsü aşağıdaki şekilde görünecektir.



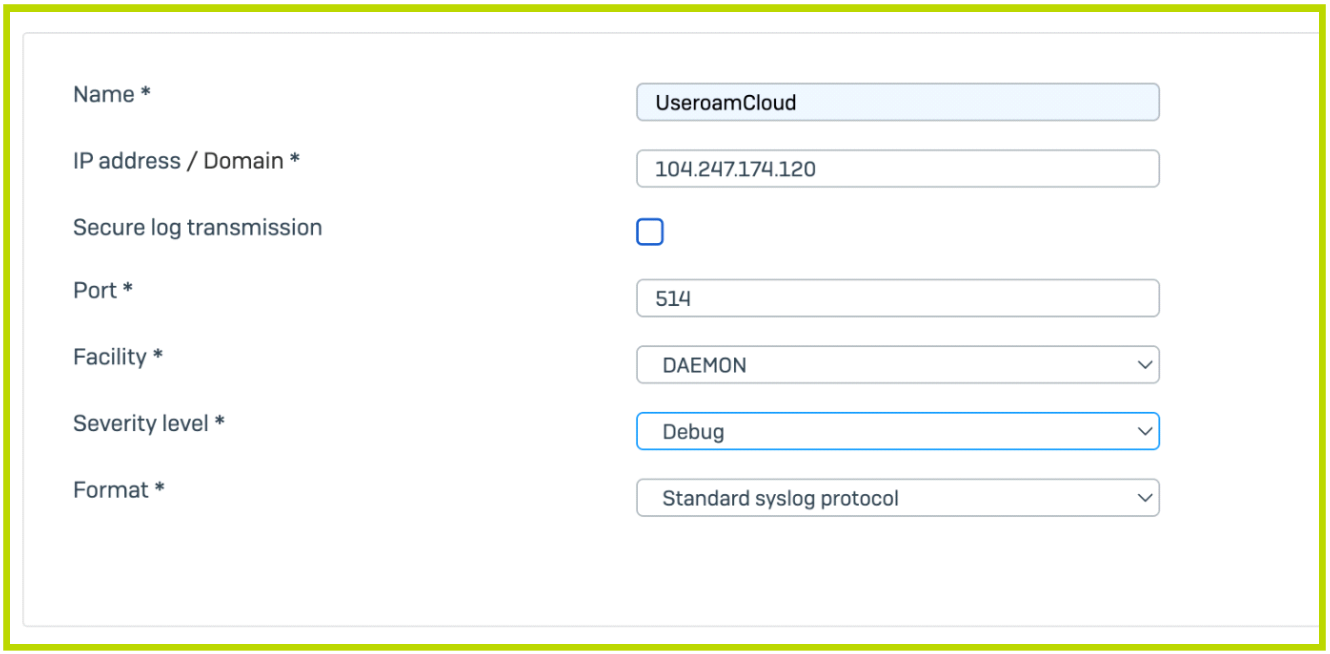
LOGLARIN USEROAM CİHAZINA YÖNLENDİRİLMESİ

I.

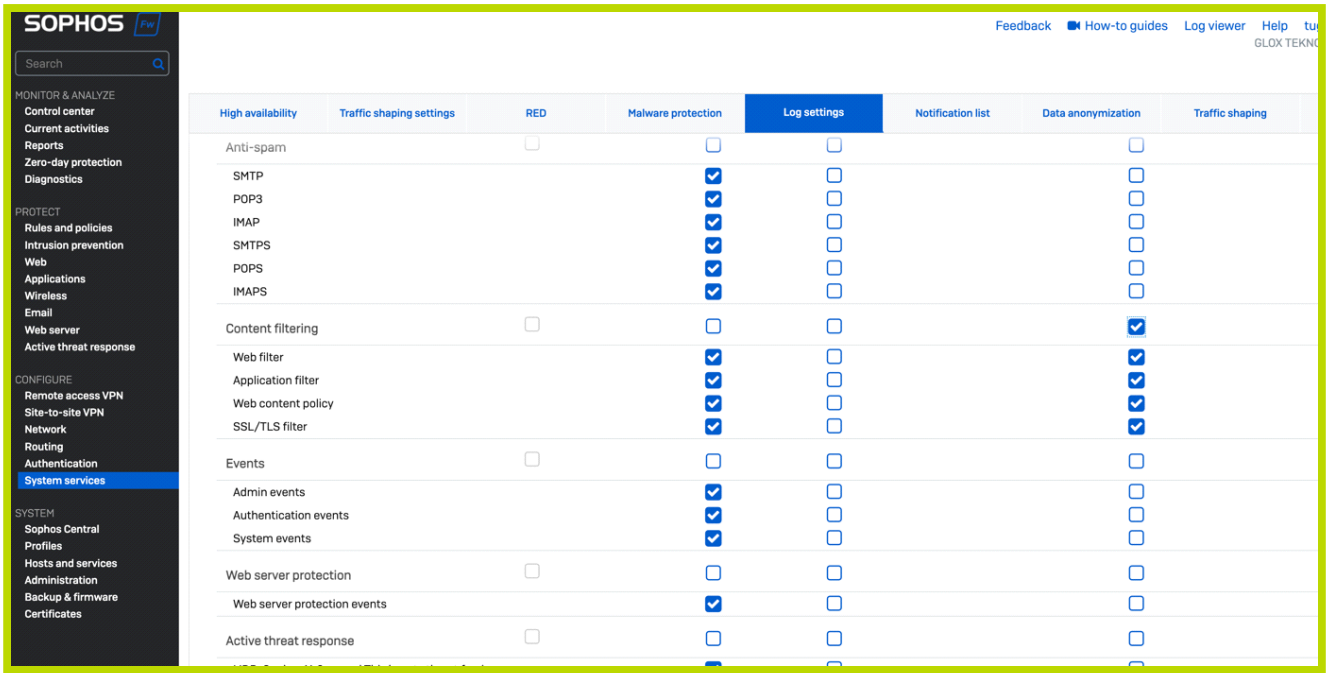
Öncelikle **System Services> Log Settings** menüsüne gelerek yeni bir **Syslog server** tanımlayınız.



2.
Ardından loglarınızı göndermek için yeni bir **syslog server** eklenerek aşağıdaki bilgiler girilir.



Daha sonra yeni eklenen syslog server sadece **Content Filtering** alanları seçilerek loglama Useroam'a doğru başlatılır.



3.
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.

Hepsi bu kadar.
Entegrasyon işleminiz tamamlandı.İşlem sırasında bir sorun yaşarsanız destek@glox.com.tr adresinden bizimle iletişime geçebilirsiniz.