Kurulum Rehberleri

- Useroam Cloud Sophos Entegrasyon Rehberi
- Useroam Cloud Fortigate Entegrasyon Rehberi
- Useroam Cloud Palo Alto Entegrasyon Rehberi
- Useroam Cloud Mikrotik Entegrasyon Rehberi
- Useroam Cloud Ruijie Entegrasyon Rehberi

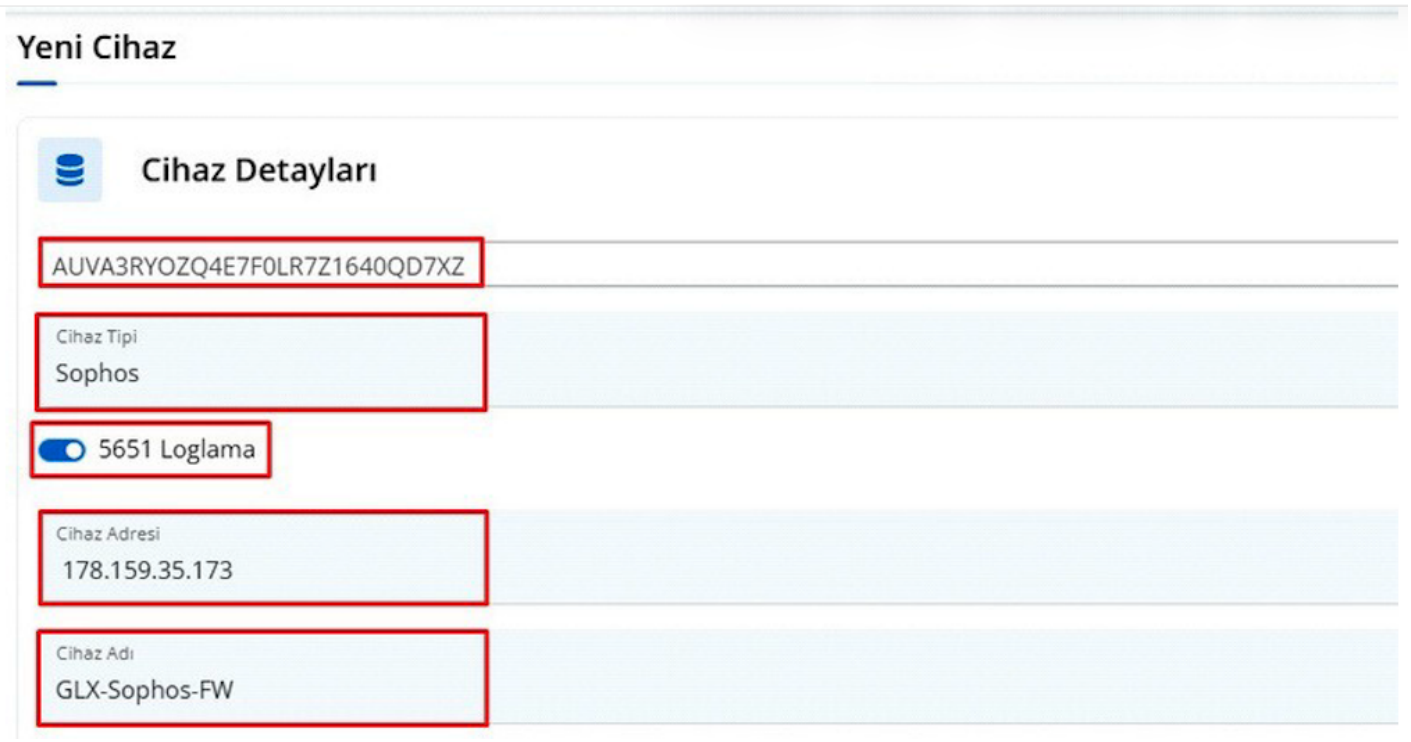
Useroam Cloud Sophos Entegrasyon Rehberi

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.

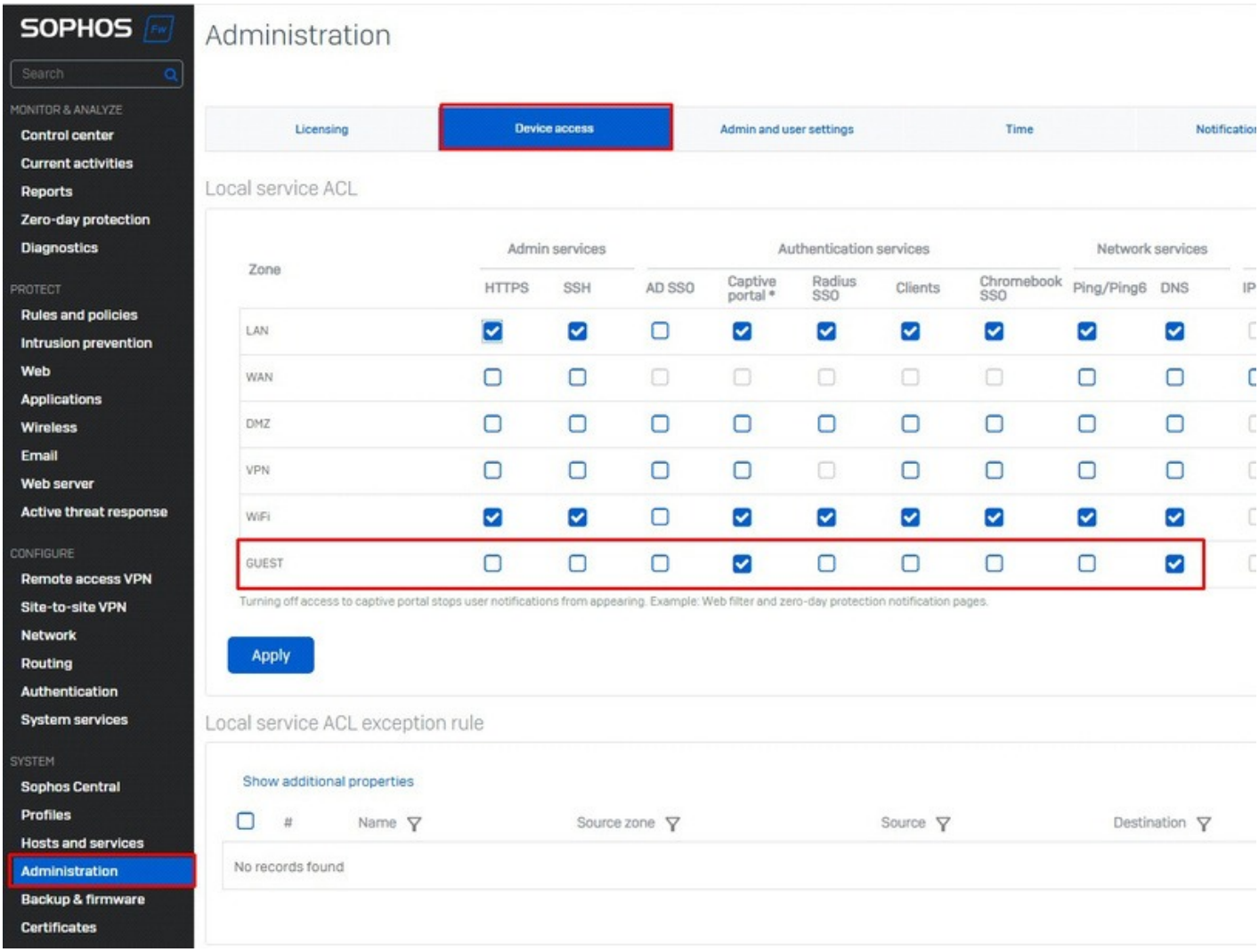
`Not: Farklı bir WAN bacağından gönderim yapmak isterseniz, bir SNAT kuralı oluşturarak ilgili trafiği istediğiniz WAN bacağına yönlendirebilirsiniz.`



2- Cihaz Eri?im Ayarlar? (Device Access)

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

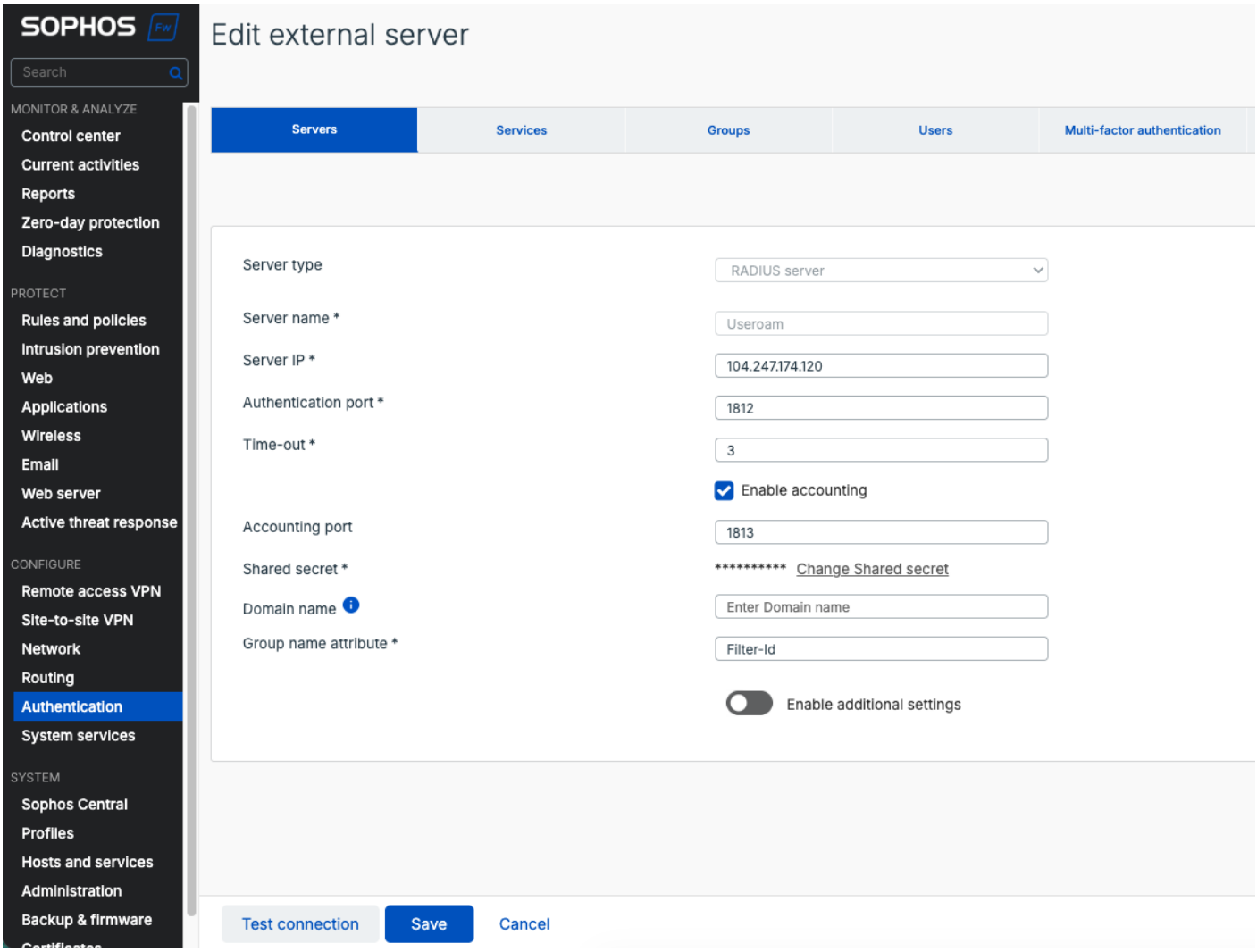
Dikkat: Radius SSO gibi farklı kimlik doğrulama mekanizmalarını aktif hale getirmeniz durumunda, yönlendirme sorunları veya Captive Portal sayfasının yavaş açılması gibi problemler yaşanabilir.



3 - Radius Sunucu Ekleme

Authentication > Servers menüsünden yeni bir Radius sunucu ekleyiniz. [cite: 189, 190] 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.

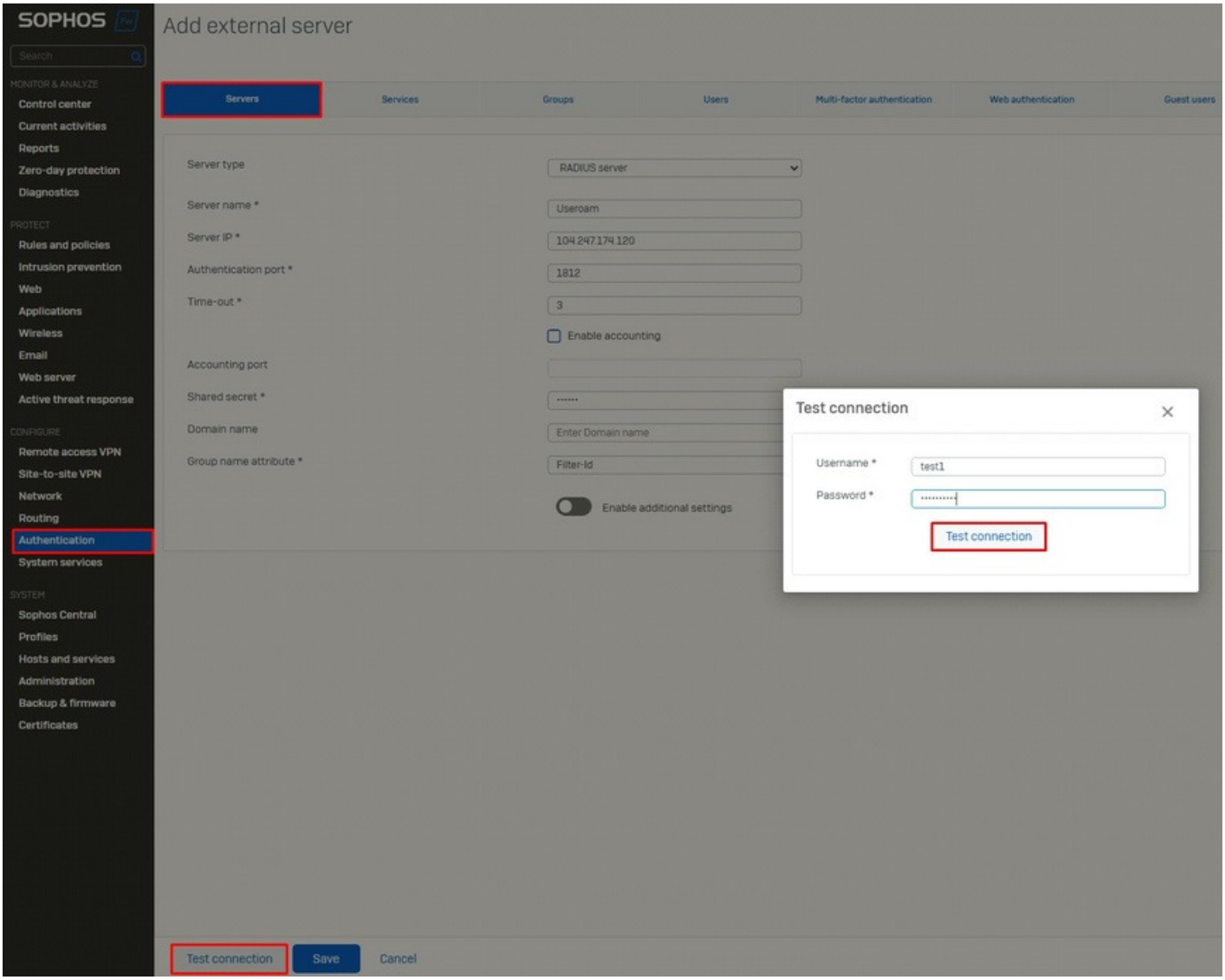


4 - Ba?lant? Testi (?ste?e Ba?l?)

Bu noktada bir test yapmak isterseniz:

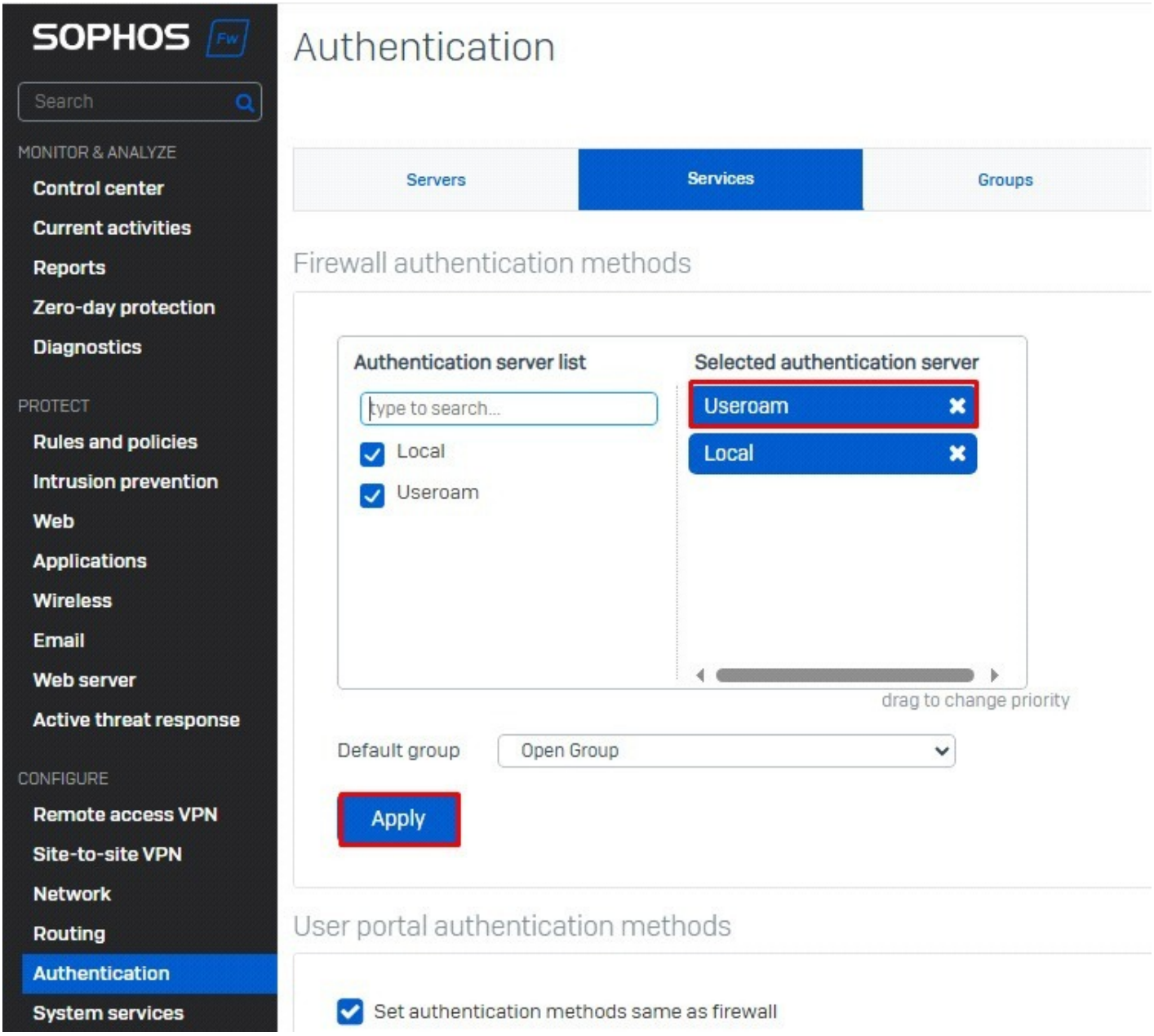
Useroam Cloud panelinden **Kullanıcı Yönetimi > Yeni Kullanıcı** adımlarıyla yeni kullanıcı oluşturabilir; Firewall'da Radius Sunucu ayarının içinden **Test Connection** ile bağlantıyı kontrol

edebilirsiniz.



5 - Kimlik Do?rulama Önceli?i (Authentication Methods)

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

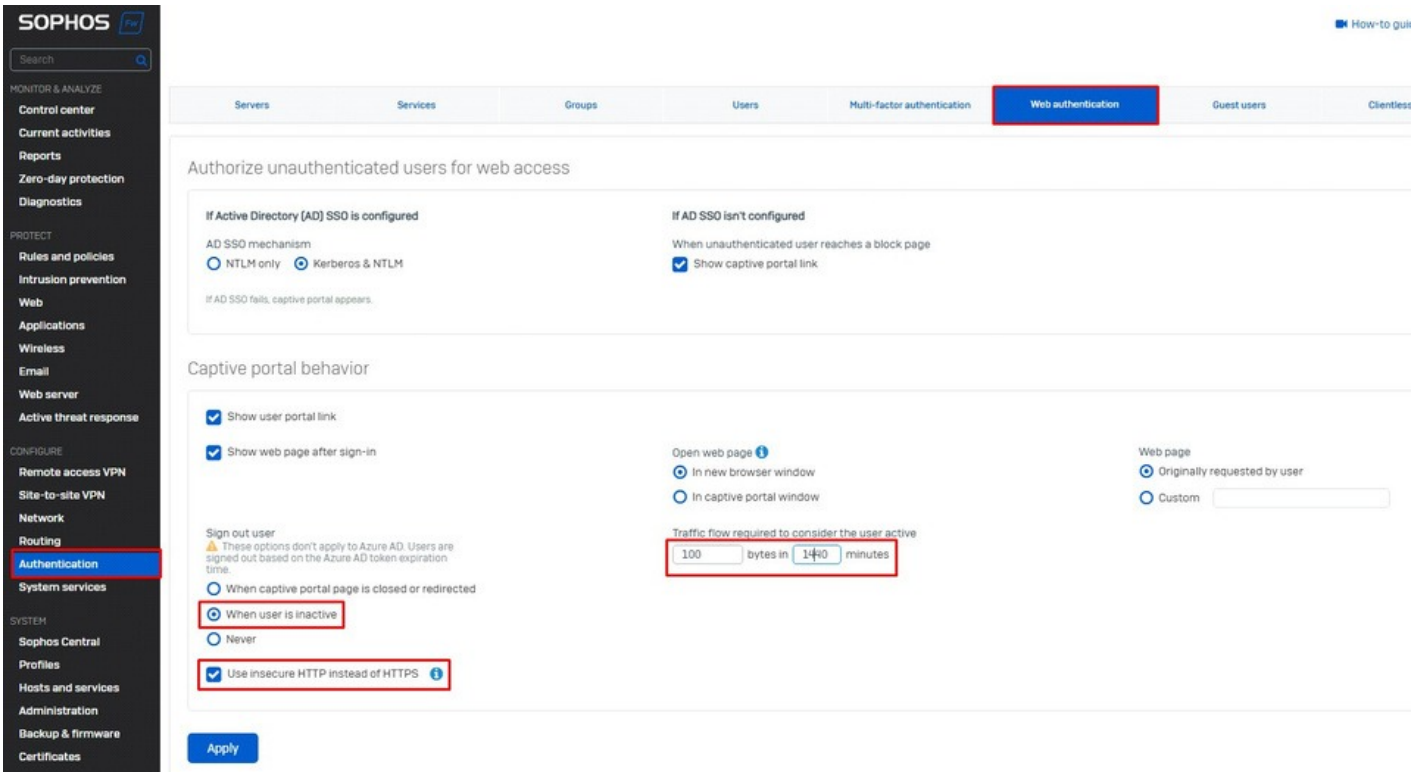


6 - Web Kimlik Do?rulama Ayarlar?

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

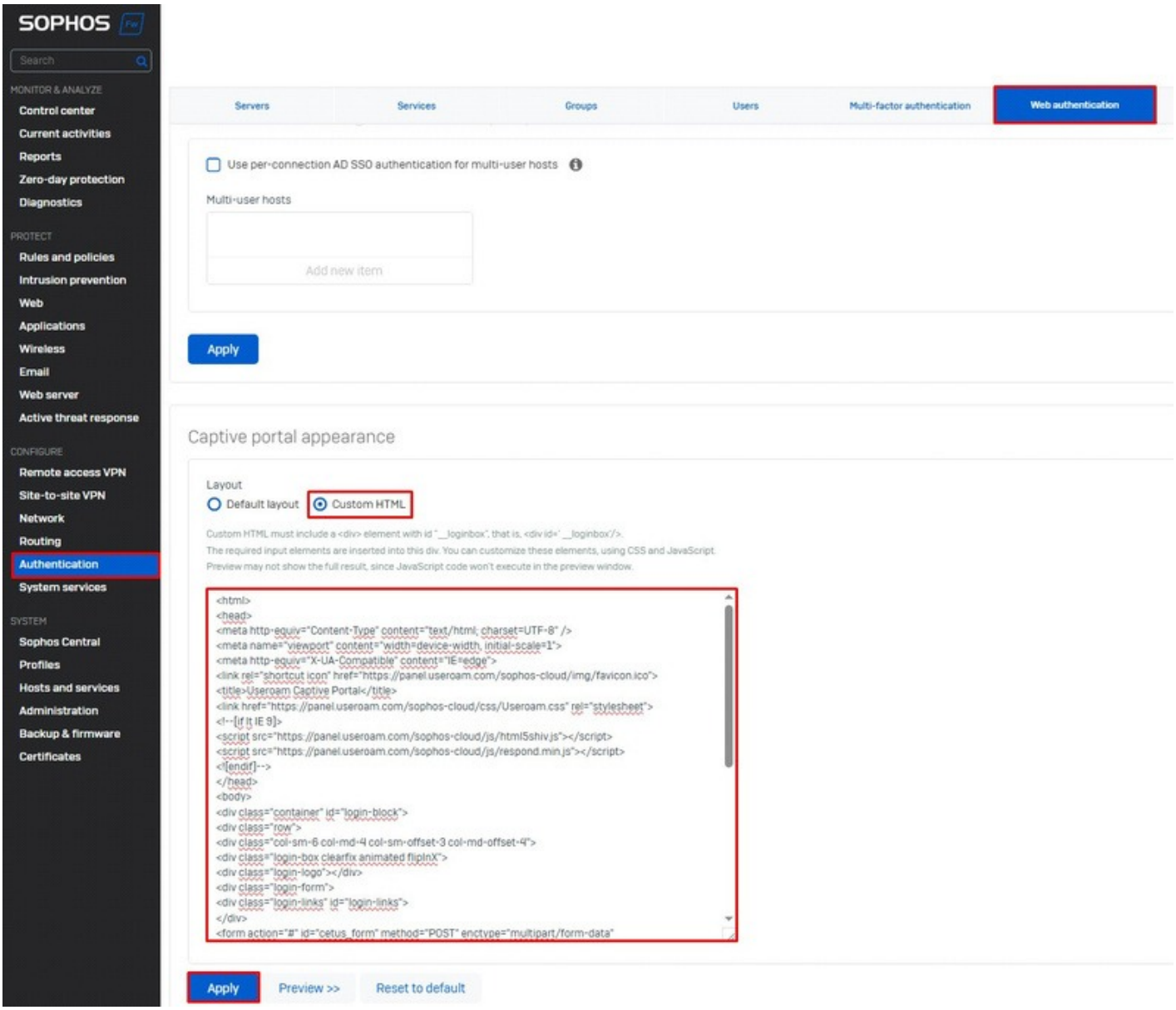
Yan taraftaki *Traffic flow* kısmında ise 100 bytes için **1440 dk** (24 saate denk gelmektedir) olarak ayarlayınız; böylece bağlı her cihaz, 24 saat içinde en az 100 bytes veri yaptığı sürece oturumu Firewall'dan düşmeyecektir. İsterseniz bu süreyi kısaltabilirsiniz.

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

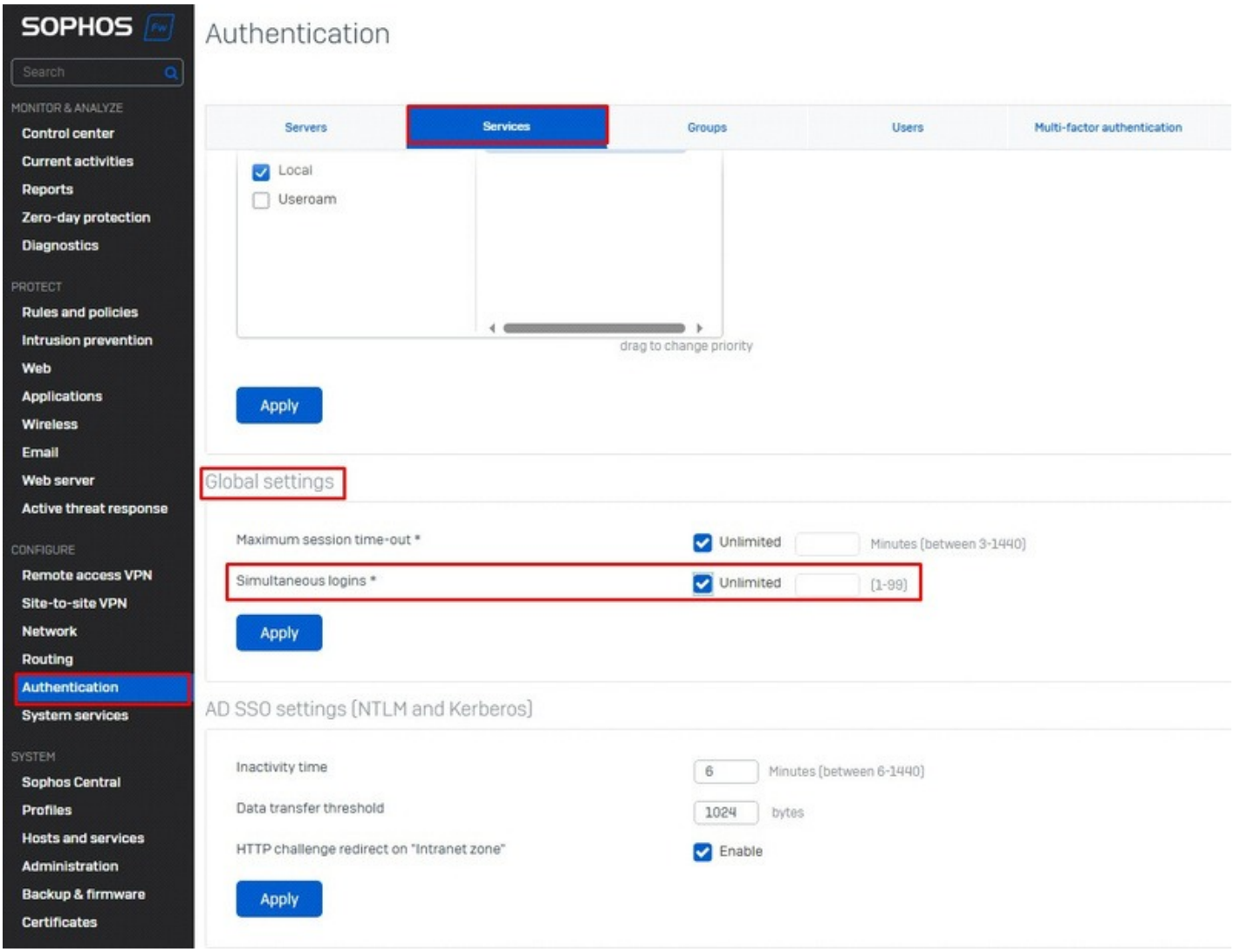


7 - Captive Portal Tasar?m?n?n Entegrasyonu (Custom HTML)

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 Kurallar?n?n Olu?turulmas?

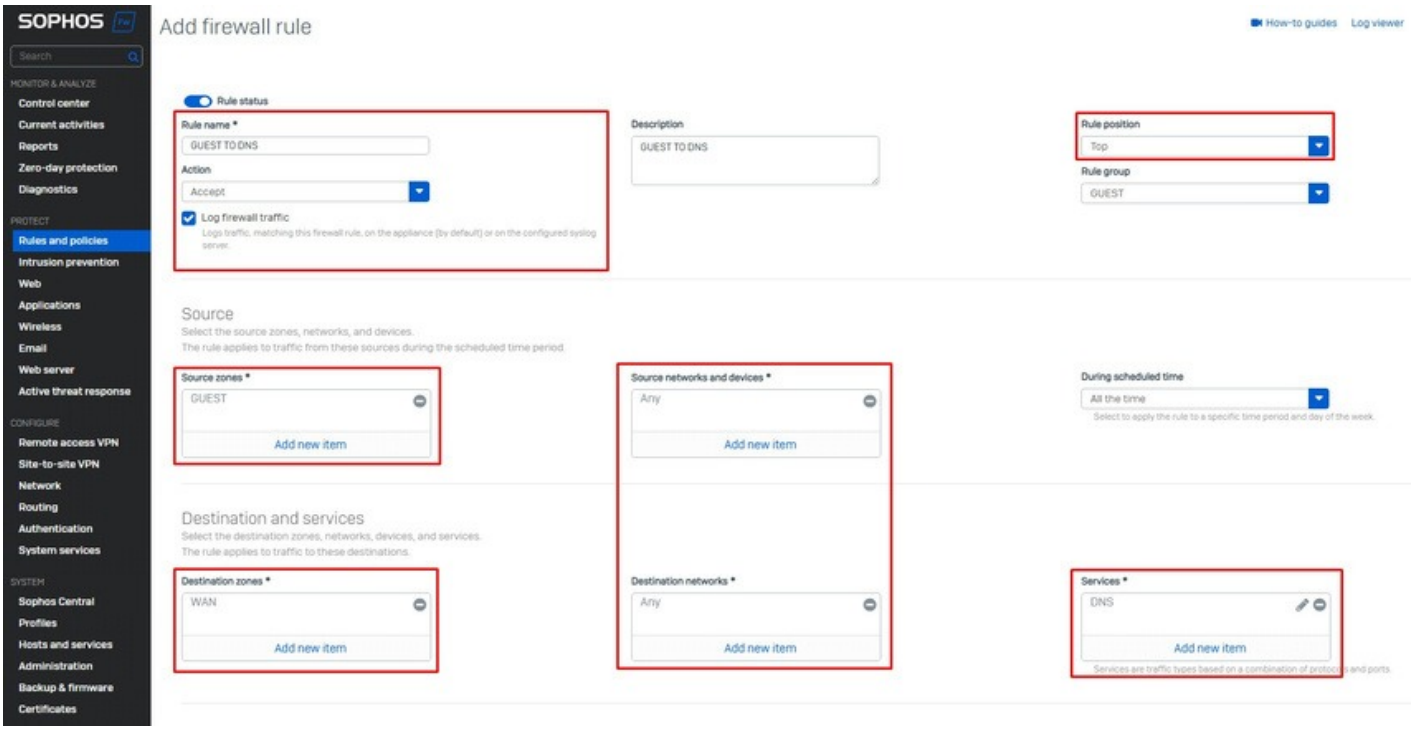
Kuralları oluşturmak için önce Sophos Firewall altında **Protect > Rules and Policies** menüsünden **Add Firewall Rule** sayfasına geliniz.

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.

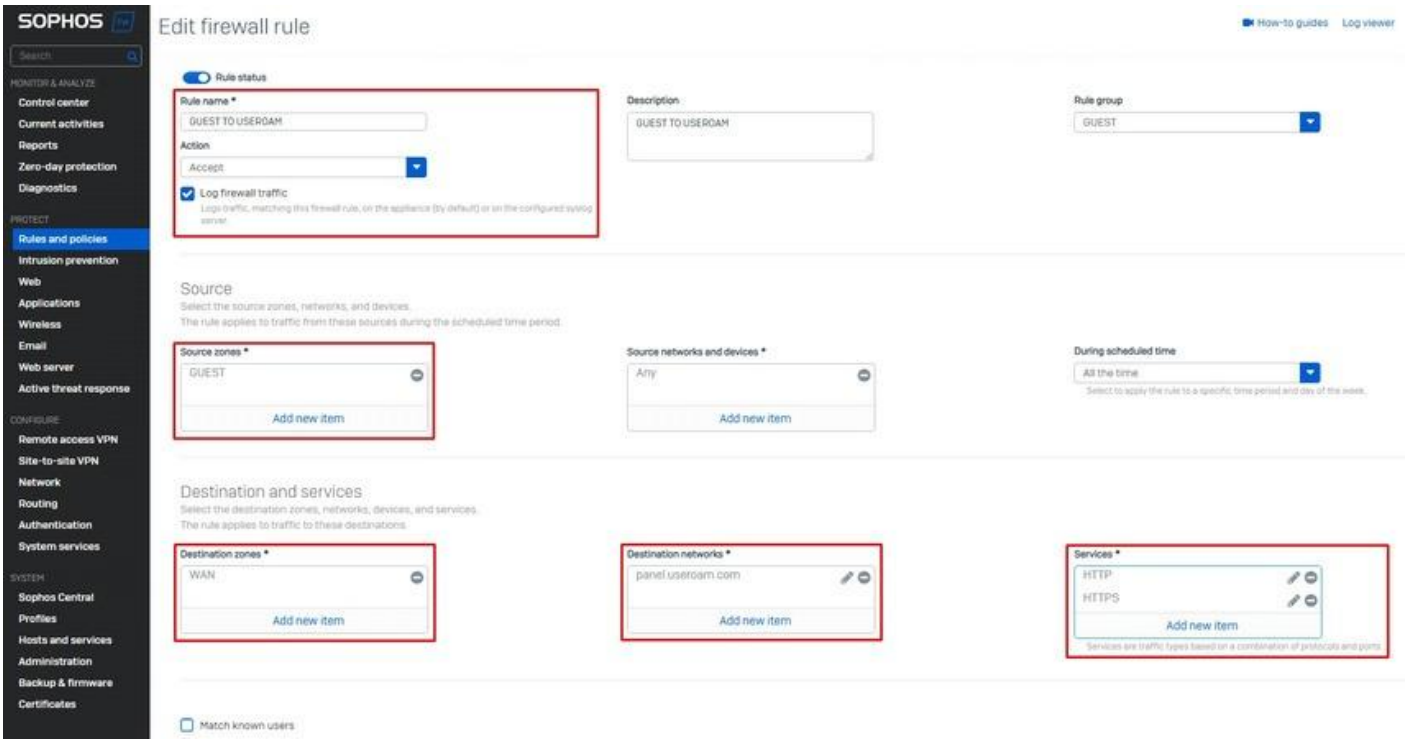
Bu kuralın misafirlerin internet çıkışı kuralının üstünde olması gerekiyor.



KURAL 2: Guest to Useroam

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

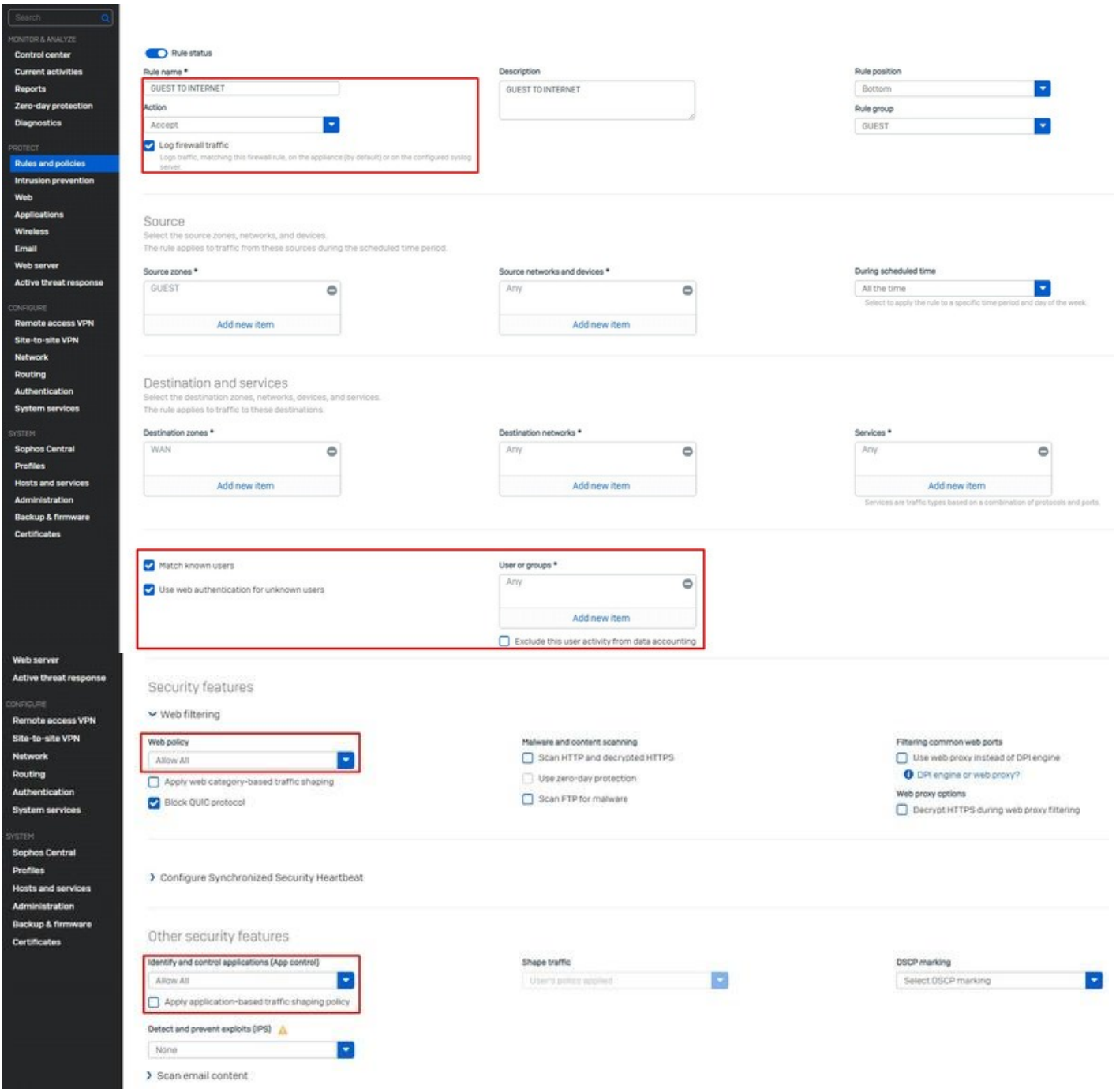
Bunun için Services kısmında **HTTP/HTTPS** seçmeniz yeterli olacaktır.



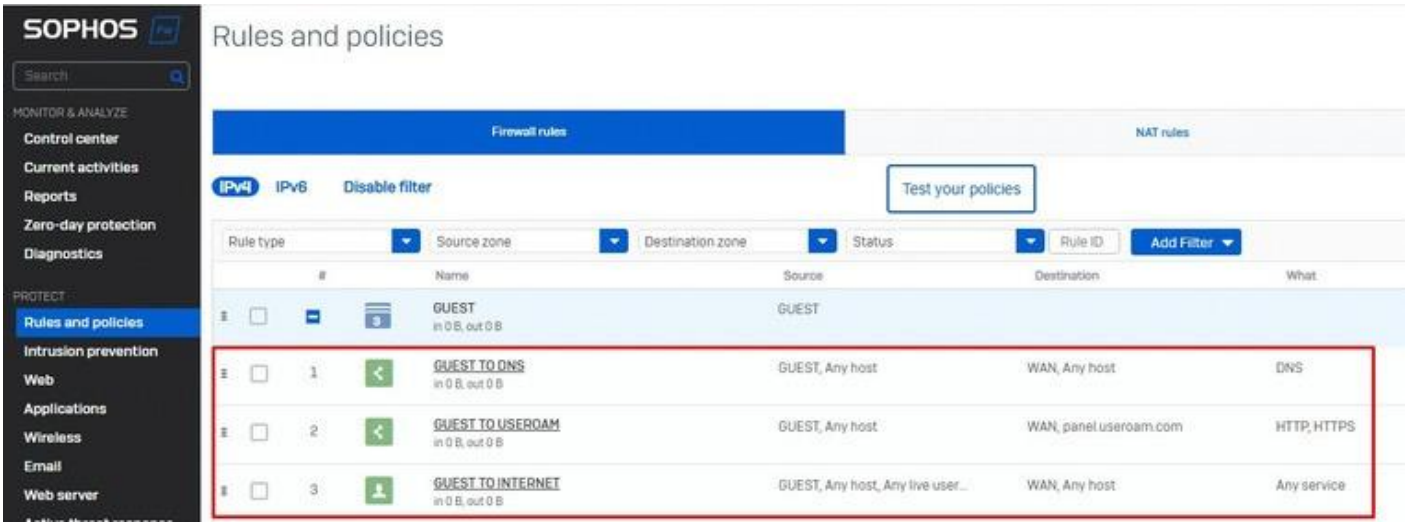
KURAL 3: Guest to Internet

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.



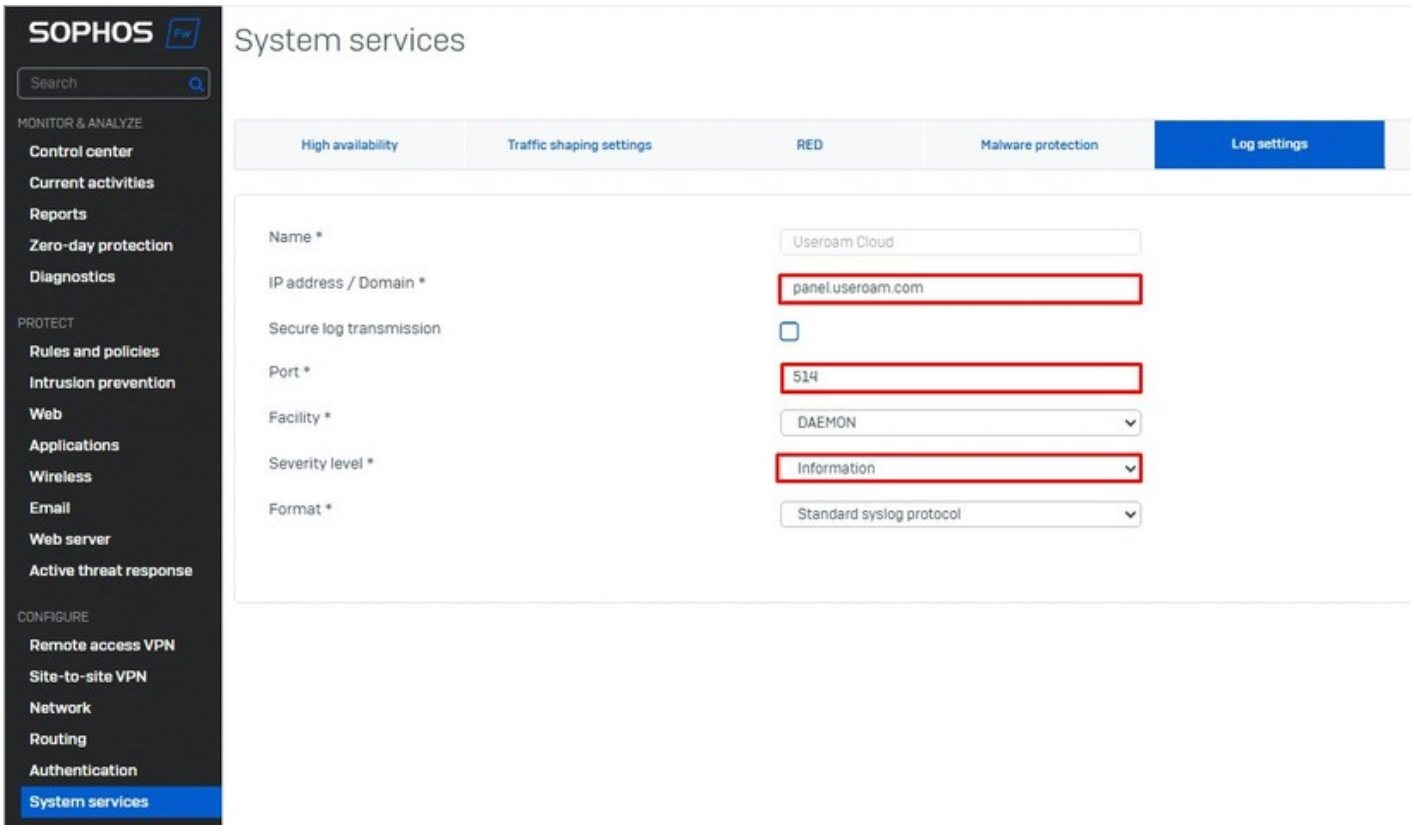
*İşlemler sonucunda **Protect > Rules and Policies** menüsü sıralaması görseldeki gibi görünmelidir. [cite: 566]*



Loglar?n Useroam Cihaz?na Yönlendirilmesi

1 - Syslog Server Tan?mlama

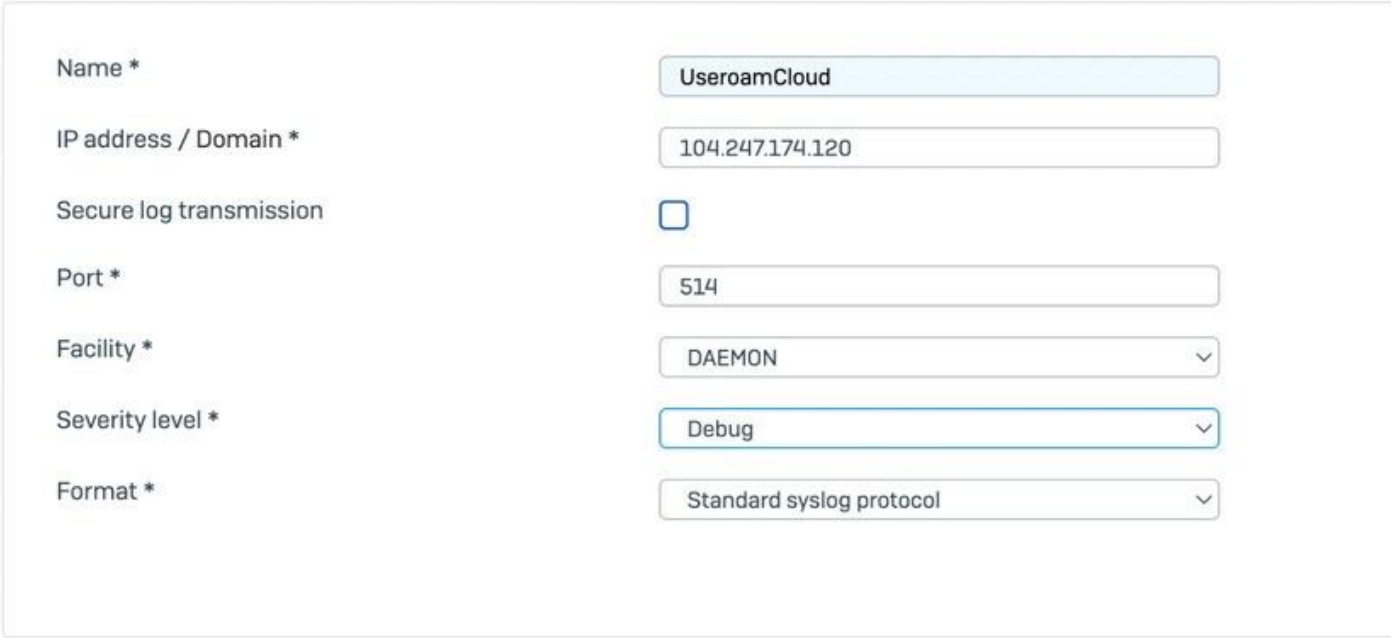
Öncelikle **System Services > Log Settings** menüsüne gelerek yeni bir Syslog server tanımlayınız.



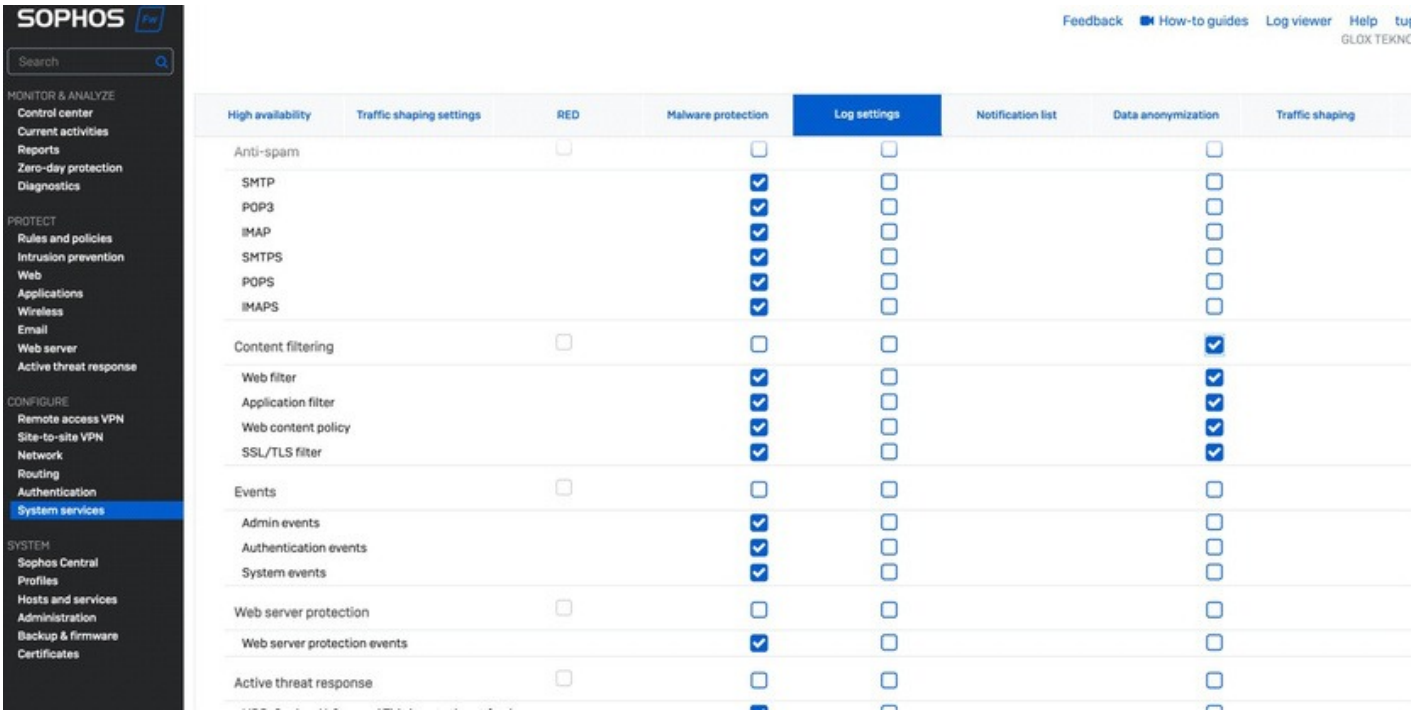
2 - Syslog Detaylar?n? Girme ve Ba?latma

Yeni eklenen syslog server için aşağıdaki bilgileri doldurunuz: [cite: 644]

- **Name:** Useroam Cloud [cite: 646]
- **IP address / Domain:** 104.247.174.120 [cite: 647]
- **Port:** 514 [cite: 654]
- **Facility:** DAEMON [cite: 655]
- **Severity level:** Debug [cite: 656]
- **Format:** Standard syslog protocol [cite: 657]



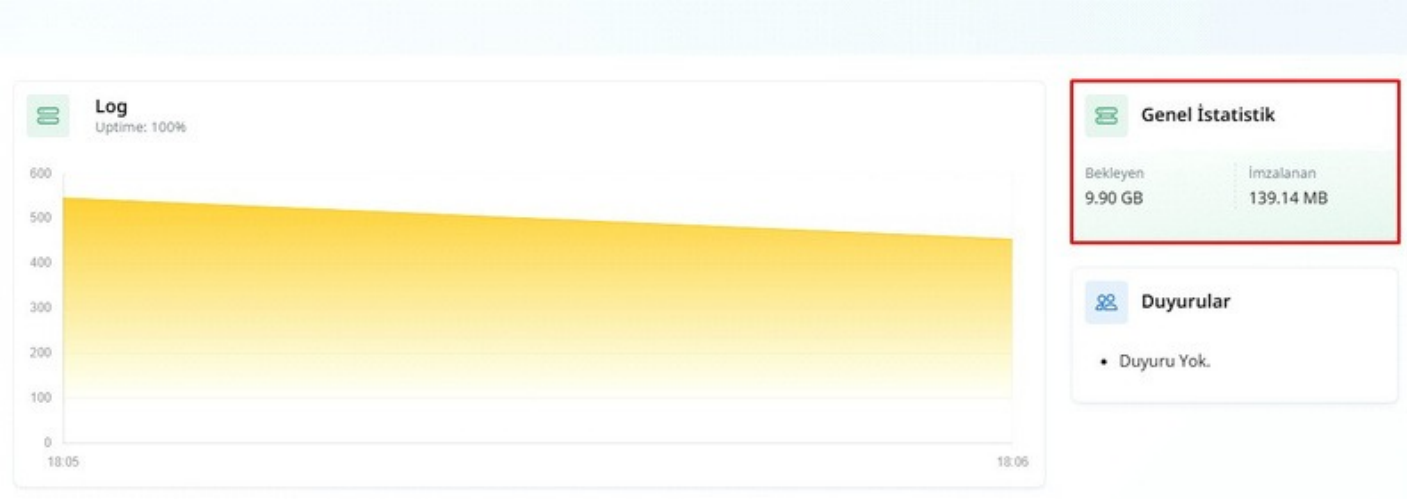
Daha sonra yeni eklenen syslog server satırında sadece **Content Filtering** alanlarını seçerek loglamayı Useroam'a doğru başlatınız.



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.



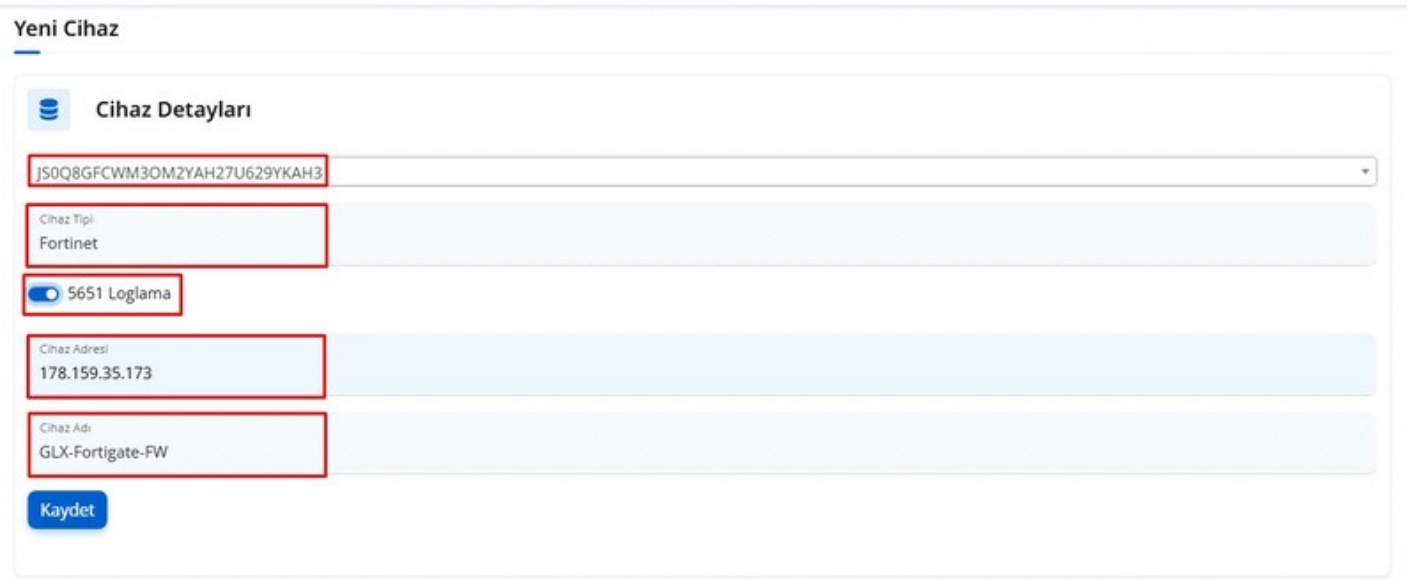
Useroam Cloud Fortigate Entegrasyon Rehberi

1 - Useroam Panele Cihaz Ekleme

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

- **Cihaz tipi:** Fortinet seçiniz.
- **Cihaz adresi:** Firewall'un WAN IP adresini seçiniz. Eğer birden fazla WAN IP adresiniz varsa, Firewall cihazı genelde 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.`



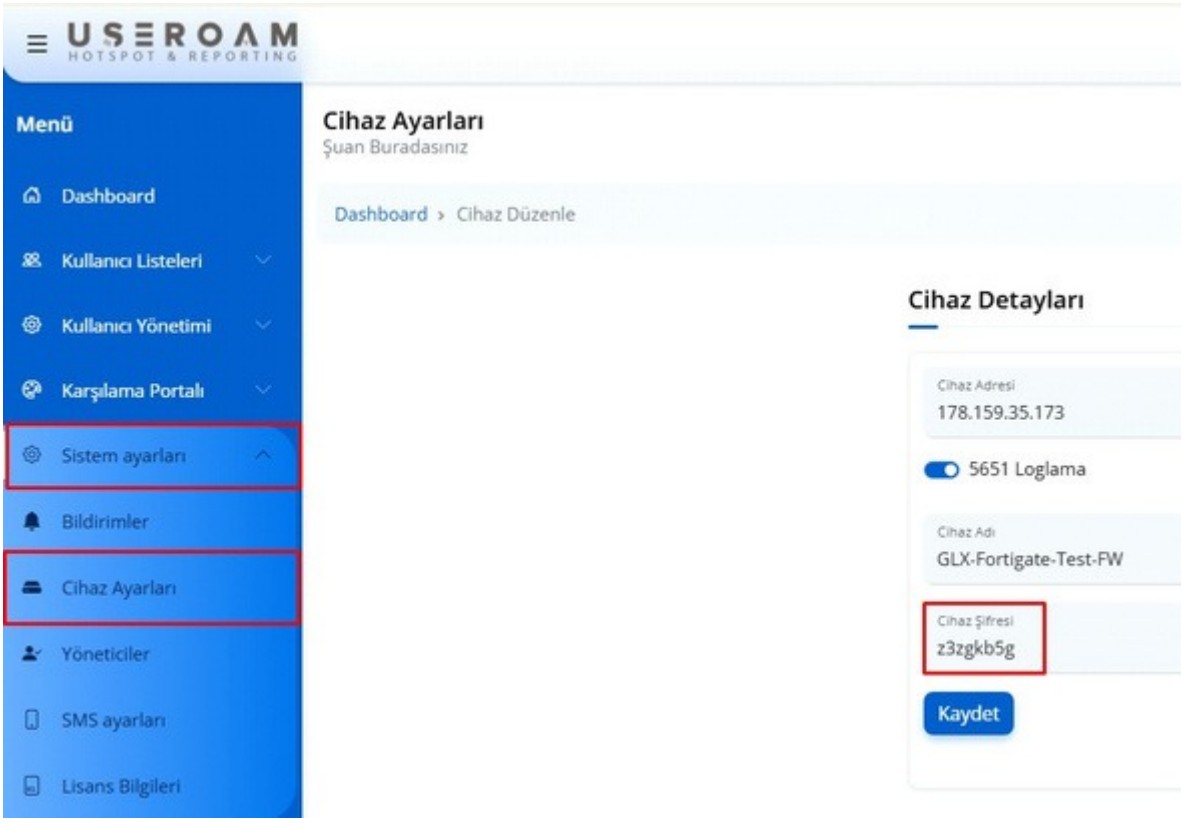
2 - Radius Sunucu Ekleme

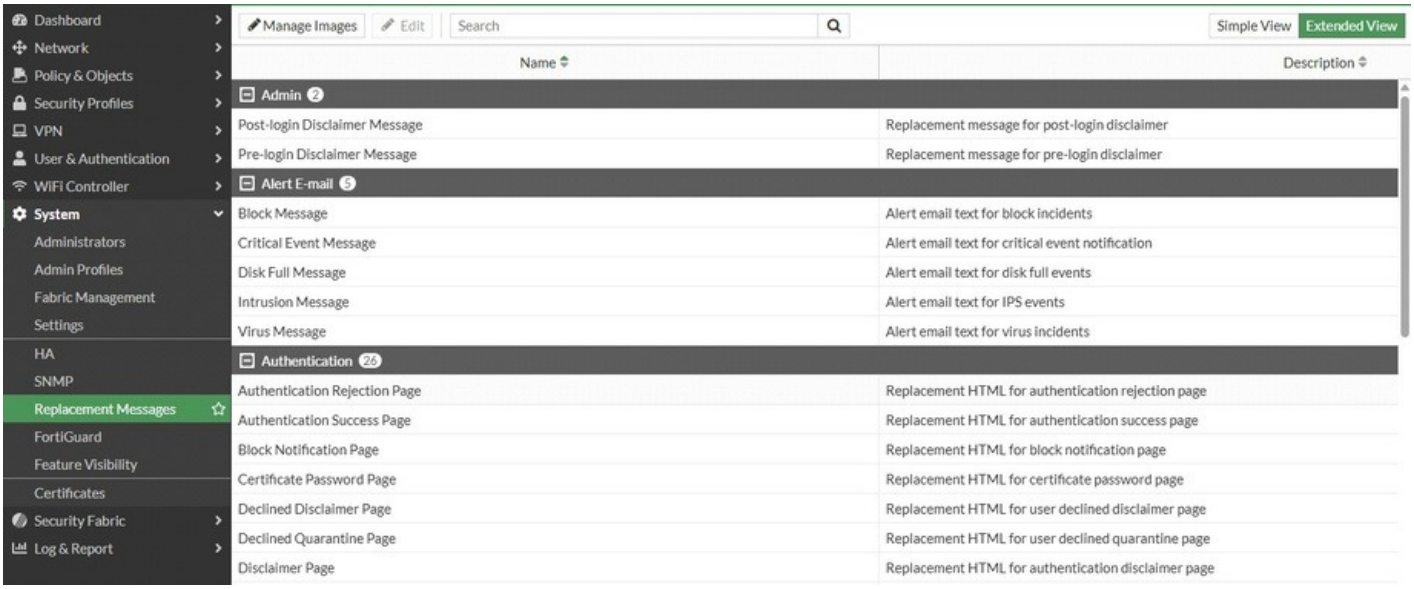
Ardından Firewall cihazınızın **User & Authentication > RADIUS SERVERS** menüsünden **Create New** butonu ile Useroam Cloud sunucusunu tanımlayınız.

- **Authentication method:** Specify / PAP
- **Primary Server/IP/Name:** `panel.useroam.com` ya da IP adresi olarak: `104.247.174.120`

- **Secret:** Useroam Cloud'da cihazı ekledikten sonra otomatik üretilen **Sistem Ayarları / Cihaz Ayarları / Cihaz Şifresini** alıp bu alana kopyalayınız.

```
Test Connectivity: Firewall'unuzun Useroam Cloud ile Radius testini yapabilirsiniz.
```



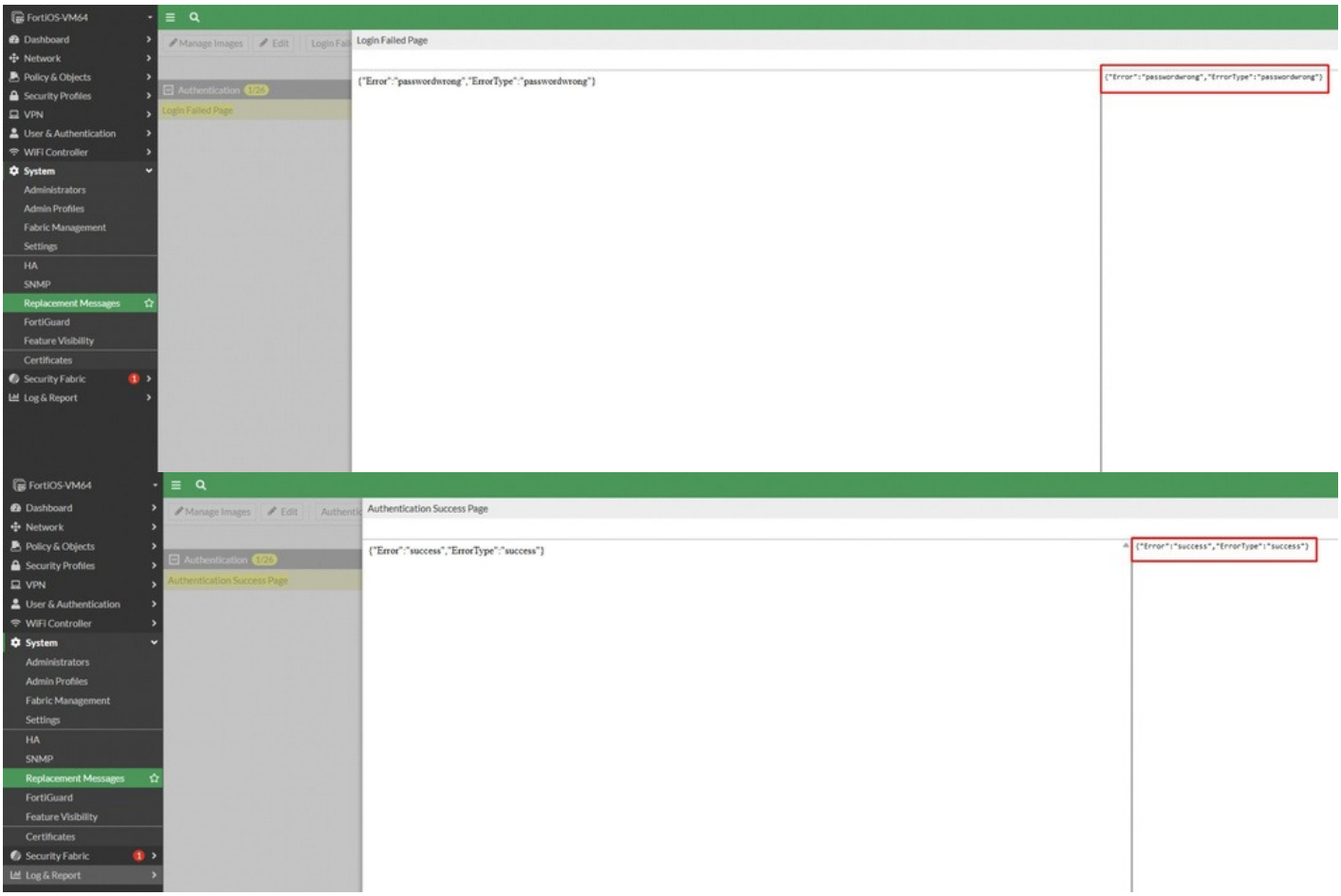


3 - Kar??lama Ekran? Mesajlar? (Replacement Messages)

System > Replacement Messages menüsünde bulunan 3 alanın kodlarını değiştirmek için önce sağ üst köşeden **Extended View** moduna geçiniz.

3A - Login Failed Page Ayar?

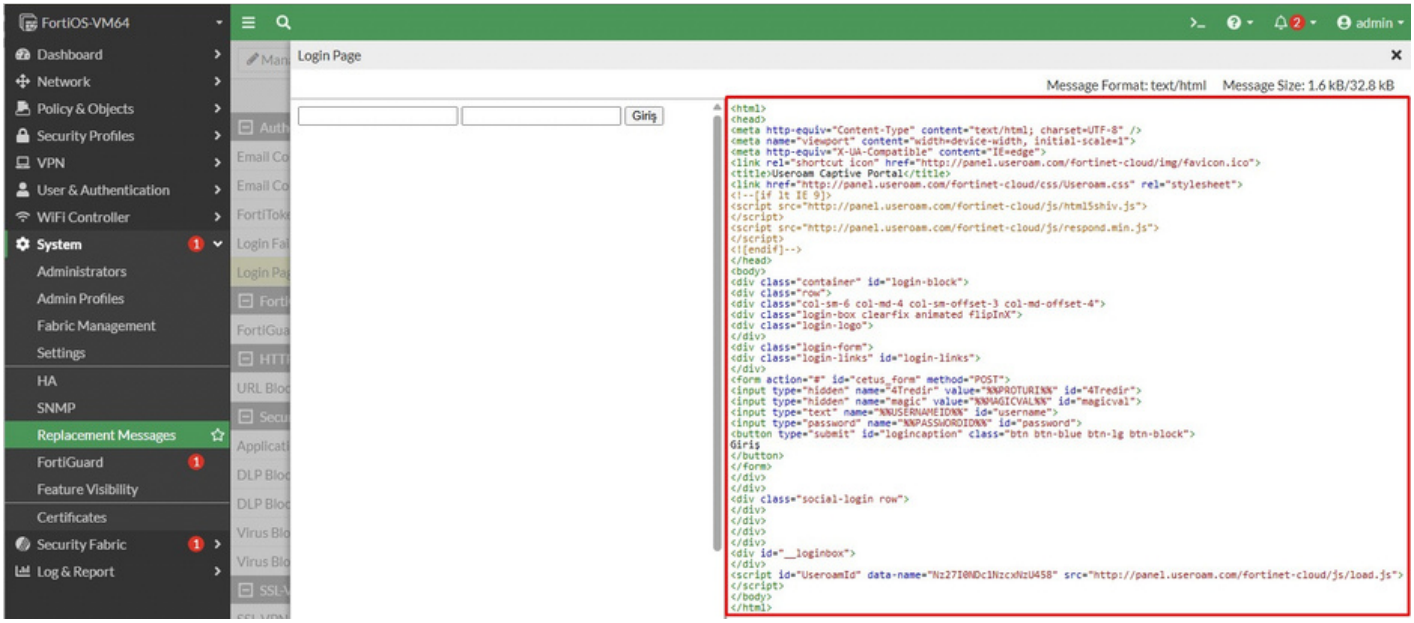
Login Failed Page'i aratın, karşınıza gelen ekranda sağ taraftaki kod kısmını temizleyerek, `{"Error":"passwordwrong", "ErrorType":"passwordwrong"}` kodunu içine yapıştırarak, kaydediniz.



3B - Authentication Success Page & Login Page Ayar?

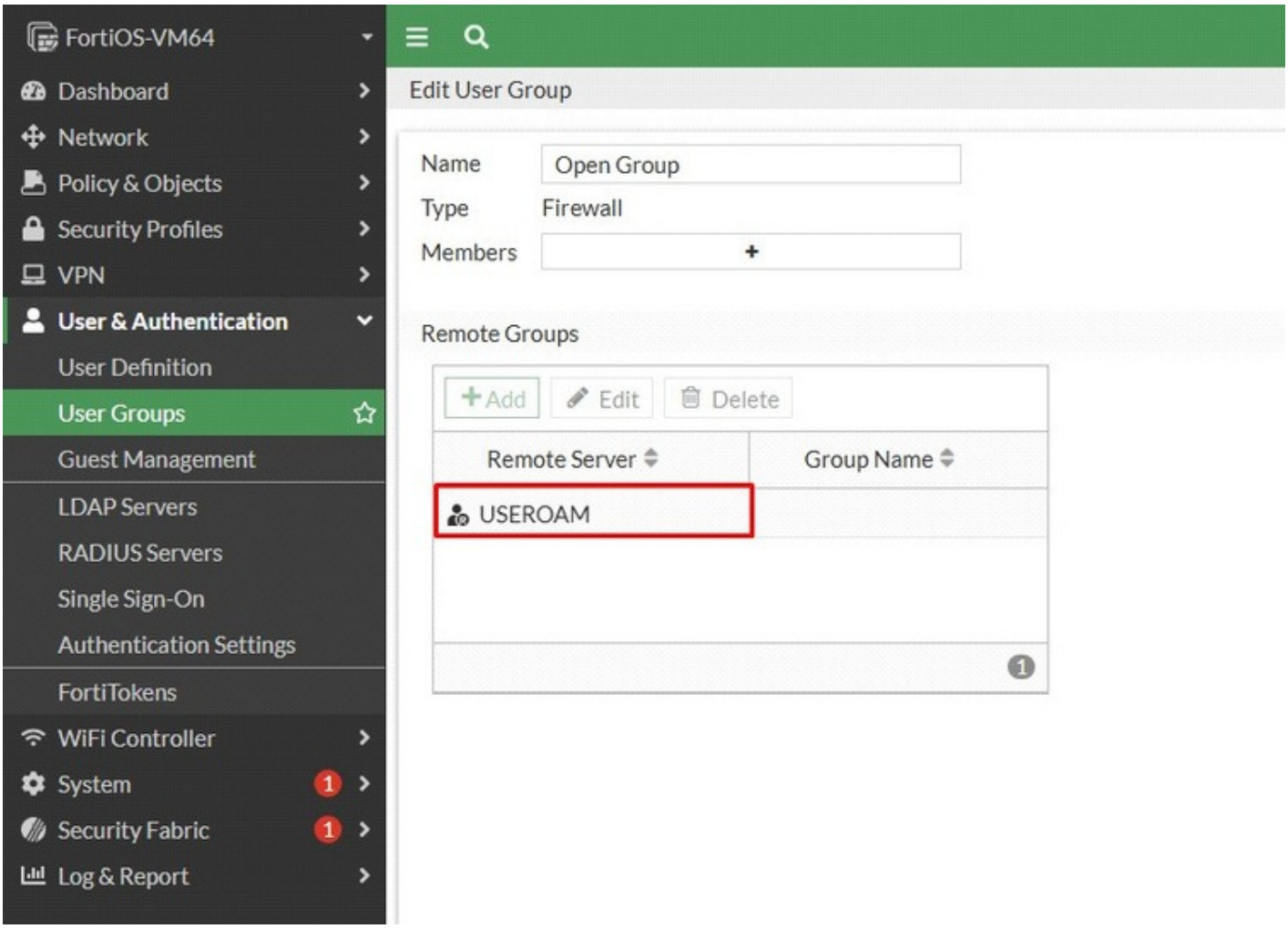
Authentication Success Page'i aratın, karşınıza gelen ekranda sağ taraftaki kod kısmını temizleyerek, `{"Error":"success", "ErrorType":"success"}` kodunu içine yapıştırarak, kaydediniz.

Son olarak **Login Page** kısmına Useroam Cloud panelinden (**Sistem Ayarları / Cihaz Ayarları**) kopyaladığınız kodun hepsini yapıştırınız.



4 - Kullan?c? Grubu Olu?turma (User Groups)

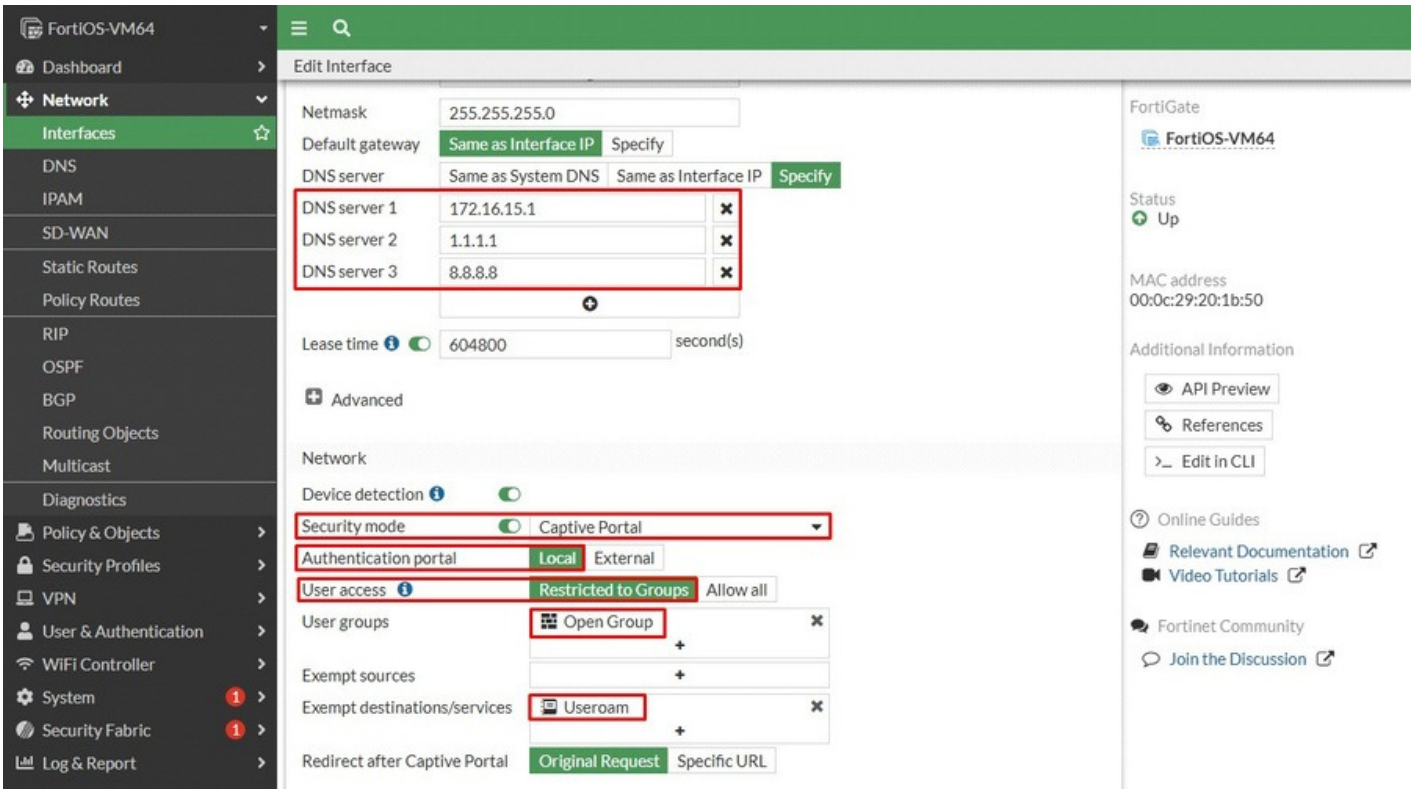
User & Authentication > User Groups menüsünden kendinize Useroam Cloud için bir grup oluşturunuz.



5 - Arayüz Ayarlar? (Interface Config)

Firewall'da **Interface** menüsünden ilgili Portunuzu düzenleyiniz.

- **DNS Server:** Bu kısımda, önce bu Interface'in Firewall'un Gateway IP'sini giriniz. Aden DNS sunucularını tanımlayınız.
- **Security Mode:** Captive Portal özelliğini açınız.
- **User Access:** Restricted to Groups
- **User Groups:** Bir önceki adımda oluşturduğunuz grubu (Örn: *Open Group*) seçiniz.
- **Exempt destinations/services:** `panel.useroam.com` fqdn objesini oluşturup seçiniz.

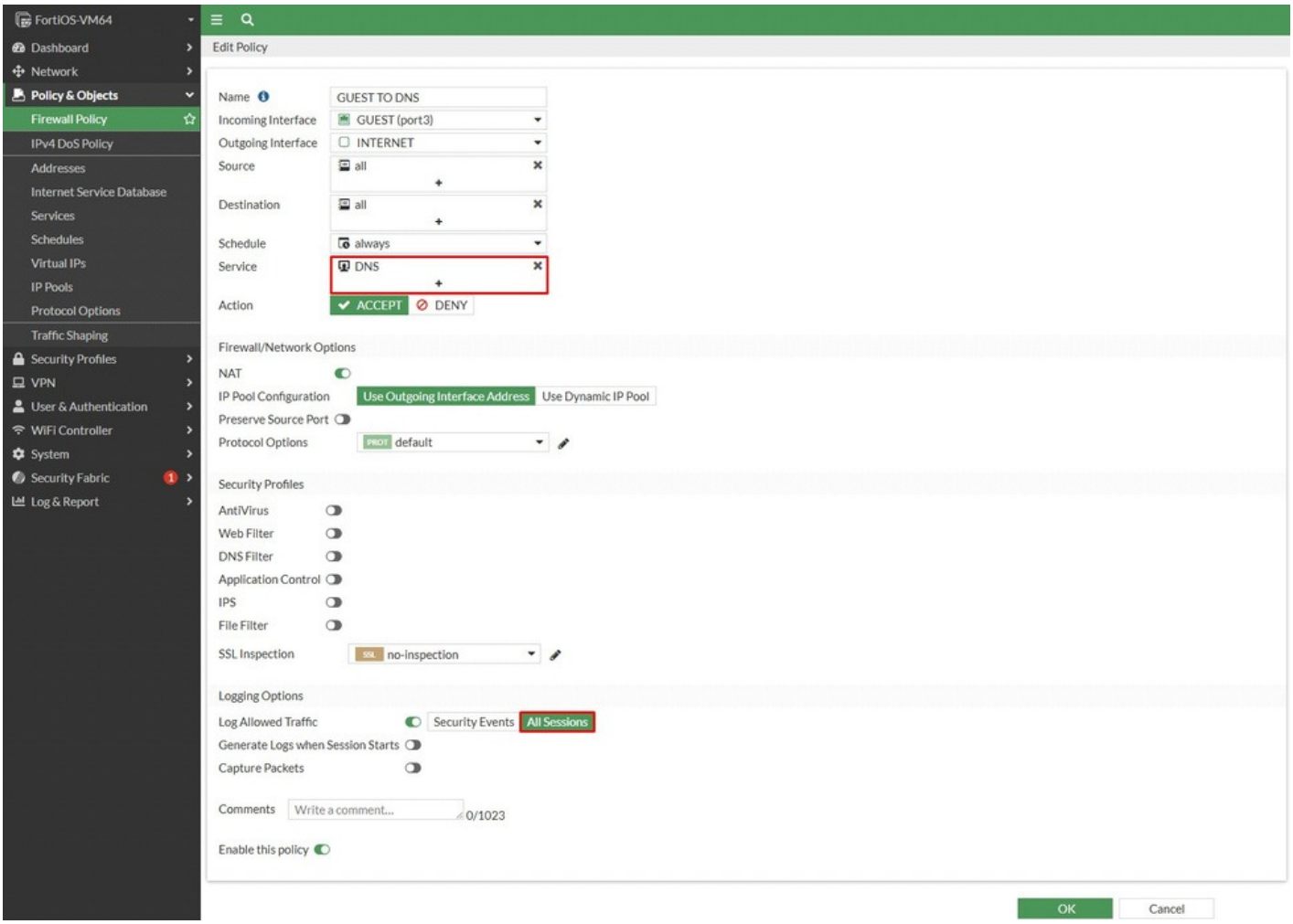


Firewall Kurallar?n?n Olu?turulmas?

Kuralları oluşturmak için önce FortiGate Firewall altında **Policy & Objects > Firewall Policy** menüsüne geliniz.

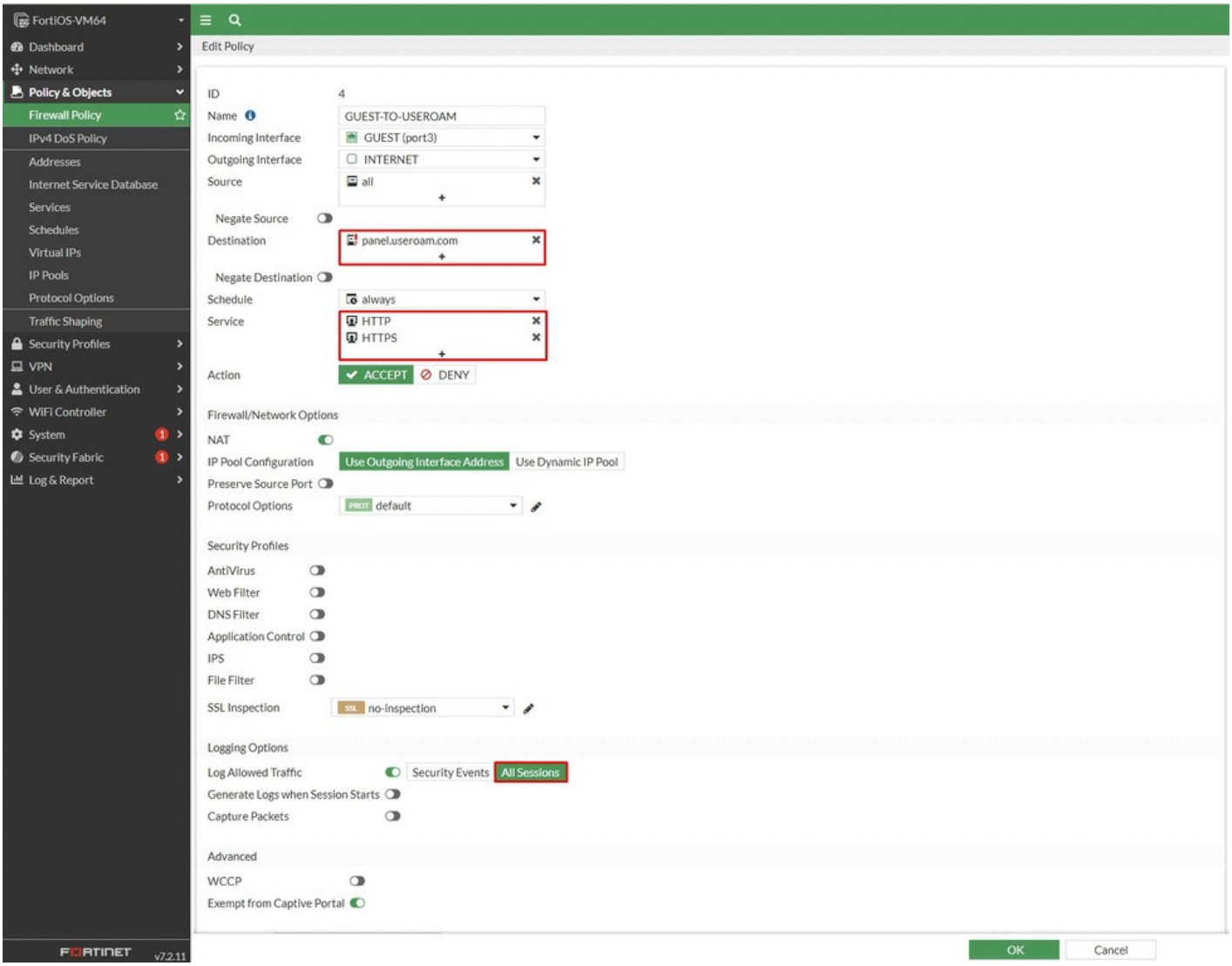
KURAL 1: Guest to DNS

Önce DNS kuralınızı oluşturunuz. Bunun için sadece **DNS** servisinin seçili olması yeterli olacaktır.



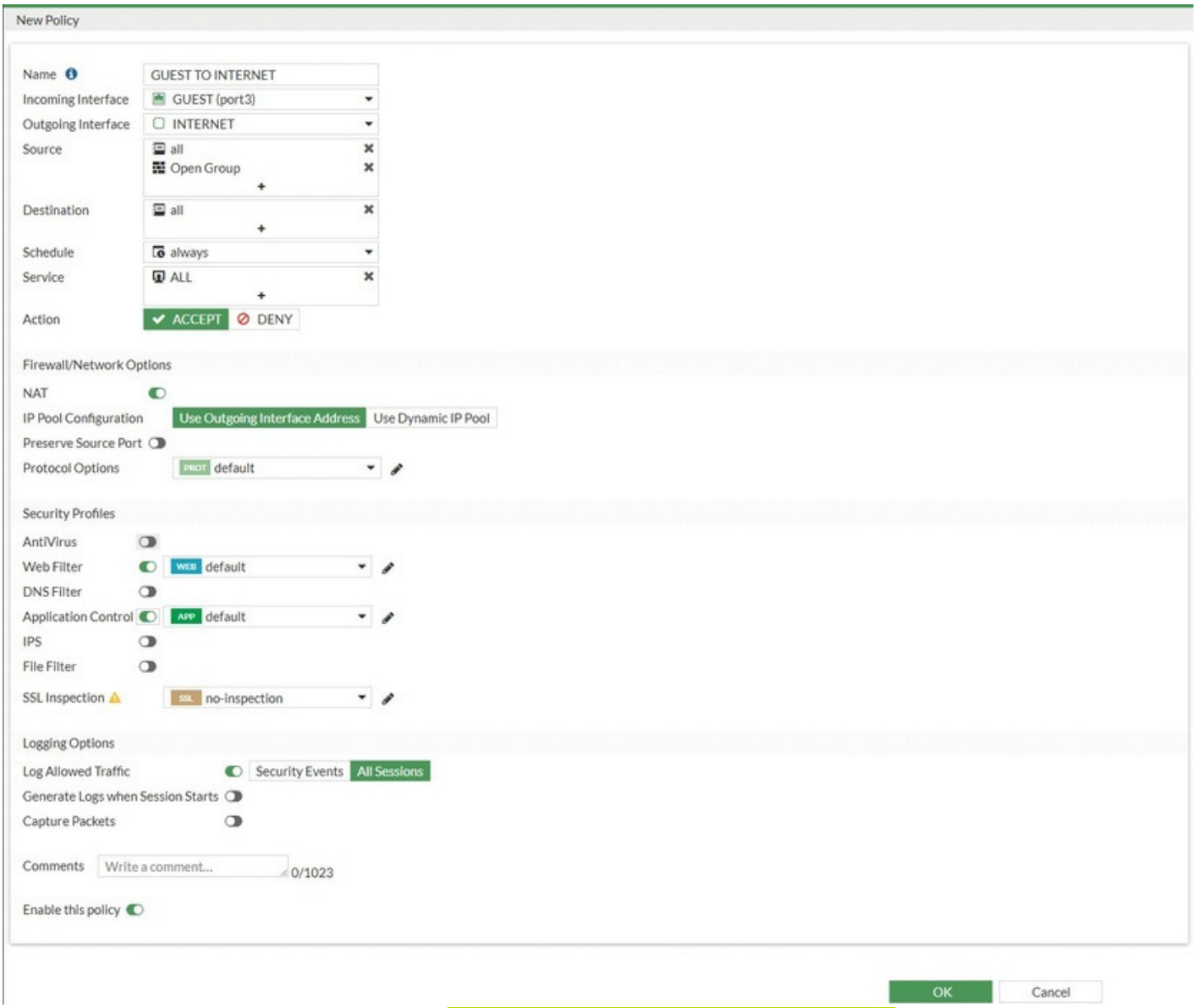
KURAL 2: Guest to Useroam

Bu kural ile Useroam'u aktifleştireceğiniz Zone'daki kullanıcıların **panel.useroam.com** paneline erişmesi sağlanacak. Service kısmından **HTTP/HTTPS** servislerini seçmeniz gerekmektedir.

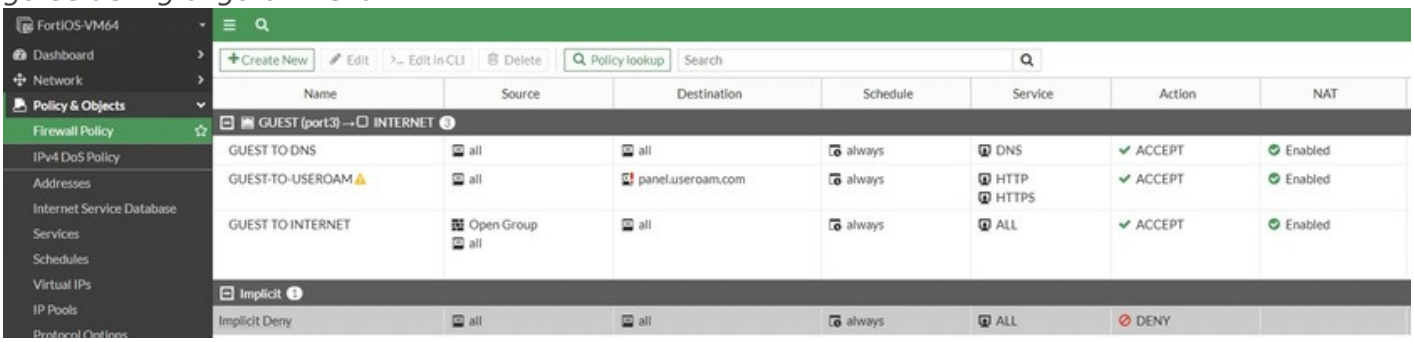


KURAL 3: Guest to Internet

Bu kural ile genel internet çıkış kuralınızı oluşturacaksınız. Source kısmına oluşturduğunuz **User Group (Open Group)** objesini, Service kısmına ise **ALL** servisini ekleyerek kuralı tanımlayınız.

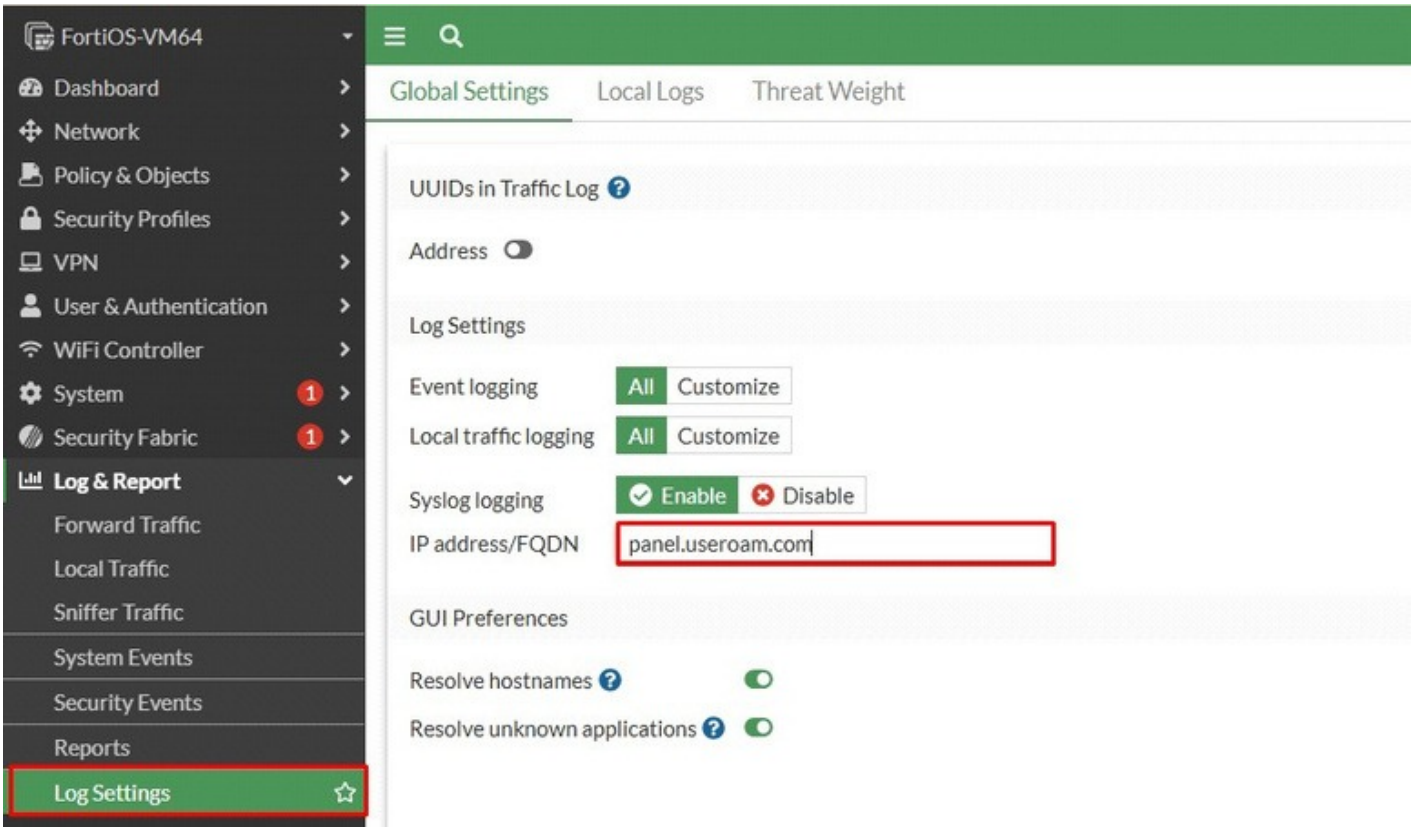


*Üç kuralı da oluşturmanızın ardından **Policy & Objects > Firewall Policy** menüsü sıralaması görseldeki gibi görünmelidir.*



Loglar?n Useroam Cihaz?na Yönlendirilmesi

Log & Report > Log Settings altından **Syslog logging** kısmını **Enable** konumuna getiriniz. Ardından IP Address/FQDN kısmına sunucu bilgilerini **panel.useroam.com** olarak giriniz.



Dikkat: Eğer bu kısımda halihazırda farklı bir IP tanımlı ise, ikinci Syslog sunucunuzu komut satırı (CLI) üzerinden yapmanız gerekiyor.
Firewall üzerinden `syslogd2`'nin içinde başka bir konfigürasyon olup olmadığını kontrol ettikten sonra aşağıdaki örnek komut bloğunu kullanabilirsiniz:

```
config log syslogd2 setting
set status enable
set server "panel.useroam.com"
set port 514
set format default
end
```

Önemli - Entegrasyon Tamamland?

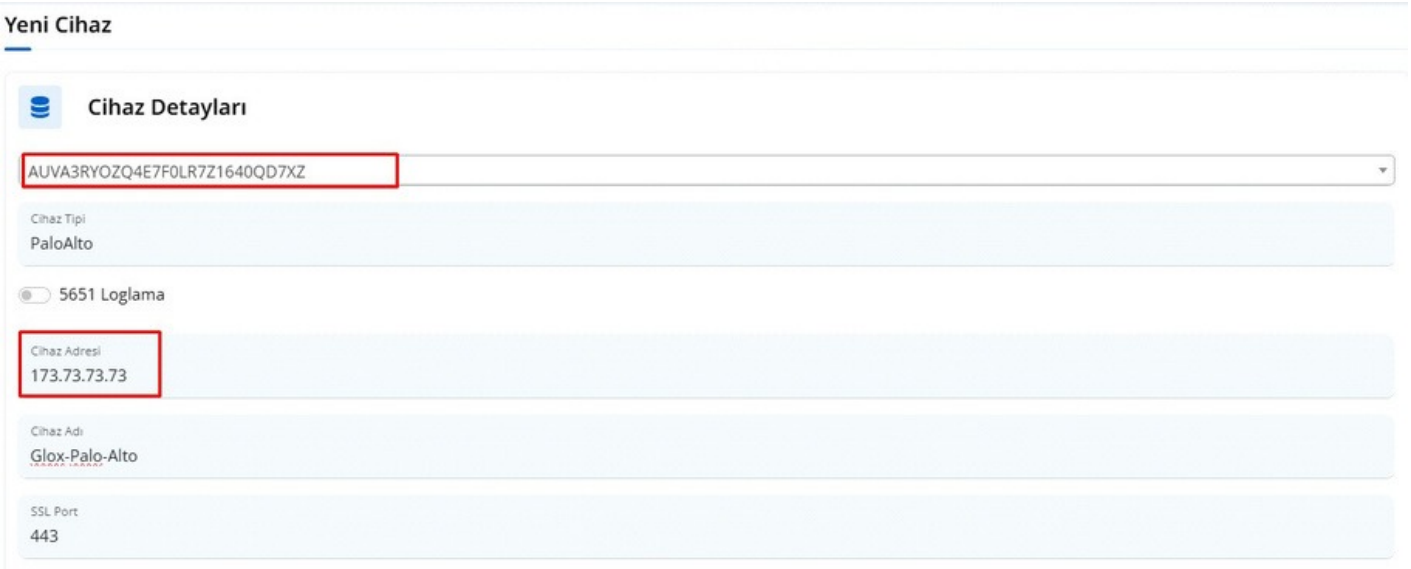
Hepsi bu kadar. FortiGate entegrasyon işleminiz başarıyla tamamlandı. İşlem sırasında herhangi bir sorun yaşarsanız **destek@useroamteknoloji.com** adresinden destek ekibiyle iletişime geçebilirsiniz.

Useroam Cloud Palo Alto Entegrasyon Rehberi

1 - Panele Güvenlik Duvar?n?n Eklenmesi

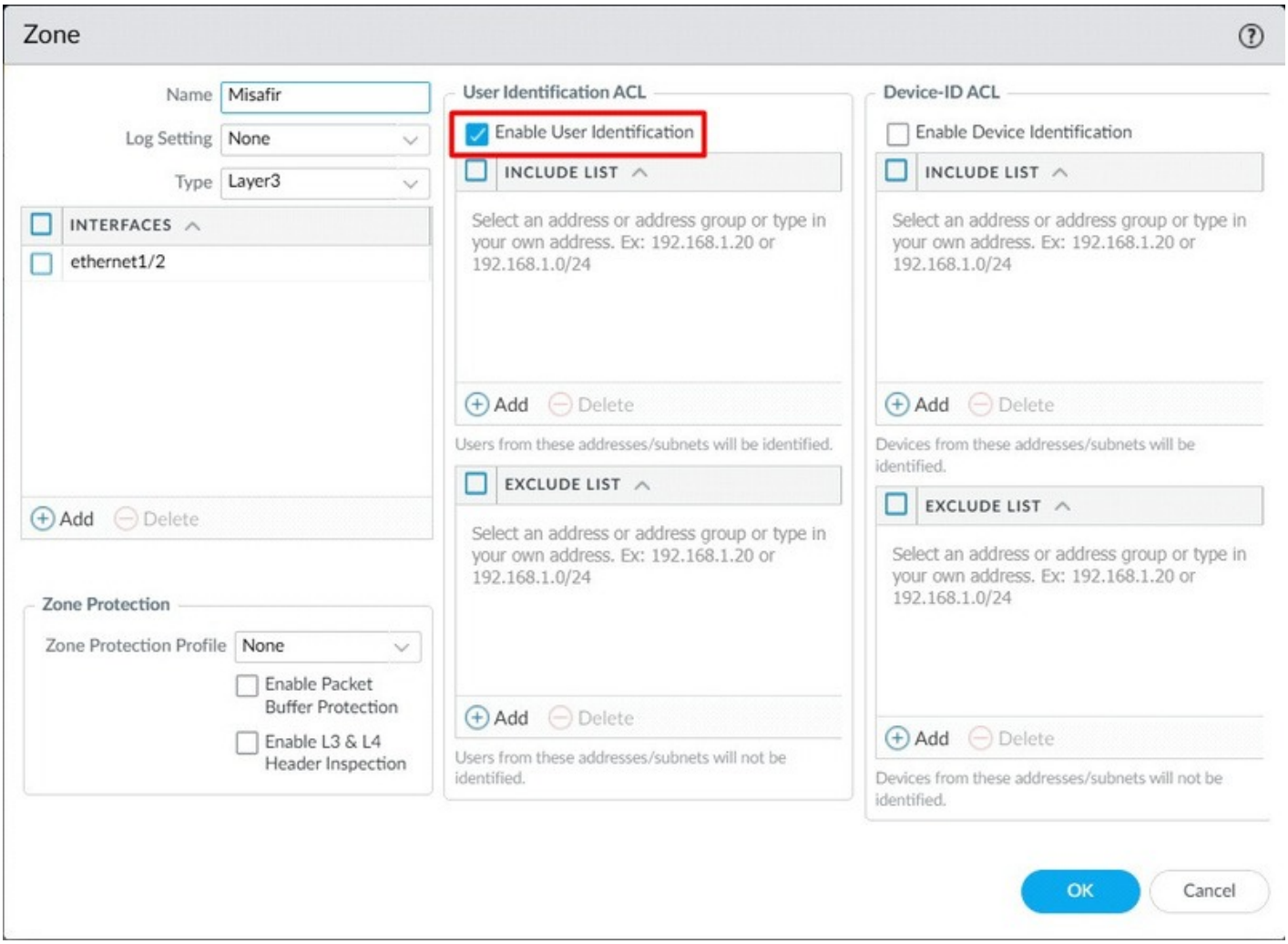
İlk olarak **panel.useroam.com** panelinize giriş yapıp **"Yeni Cihaz"** ekleyiniz. Cihaz Adresi kısmına firewall üzerinden hangi IP adresi ile iletişim kuracaksanız, ilgili dış bacak IP adresini giriniz.

- **Cihaz tipi:** PaloAlto seçiniz.
- **5651 Loglama:** 5651 Loglama kutucuğunu aktif ediniz.



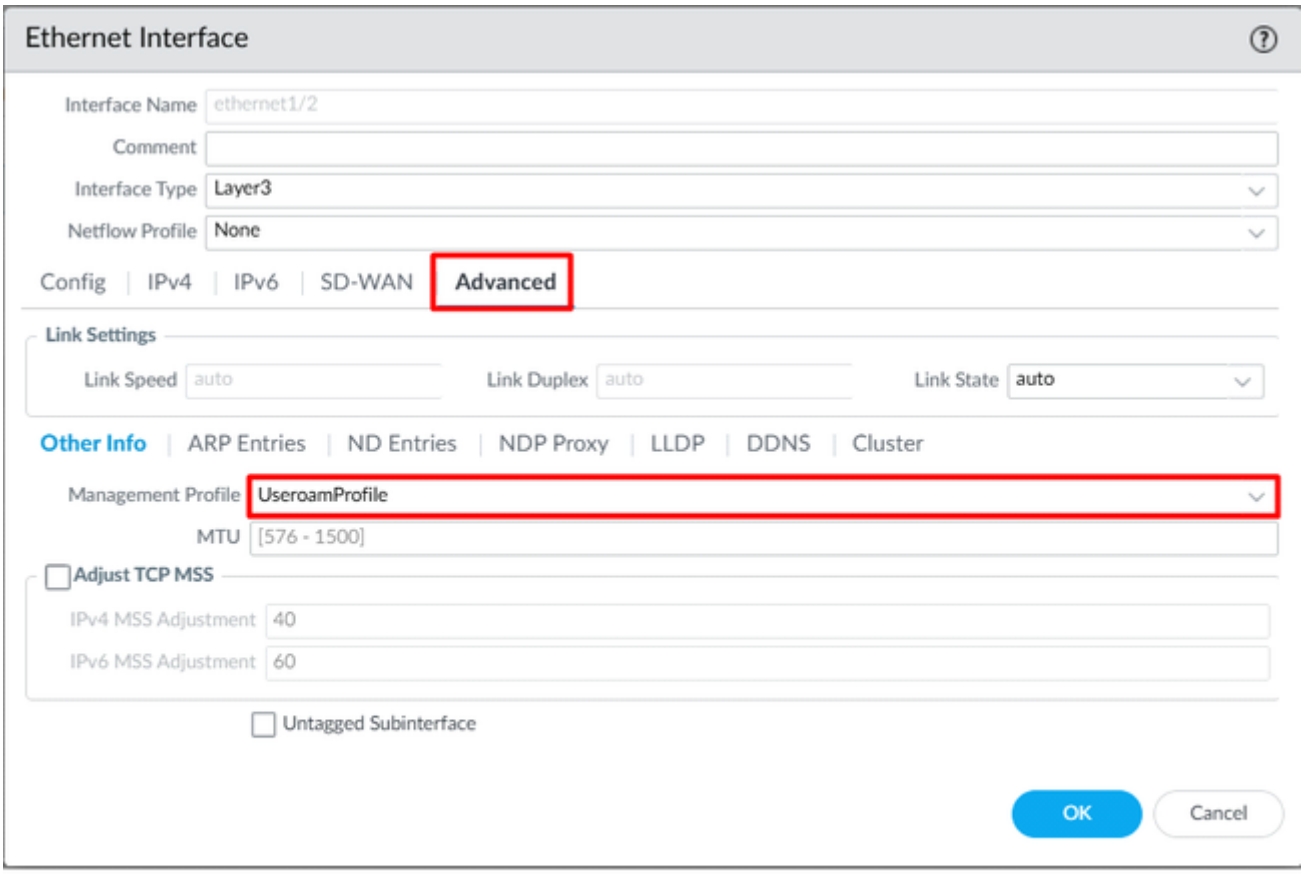
2 - Zone Ayarlar?

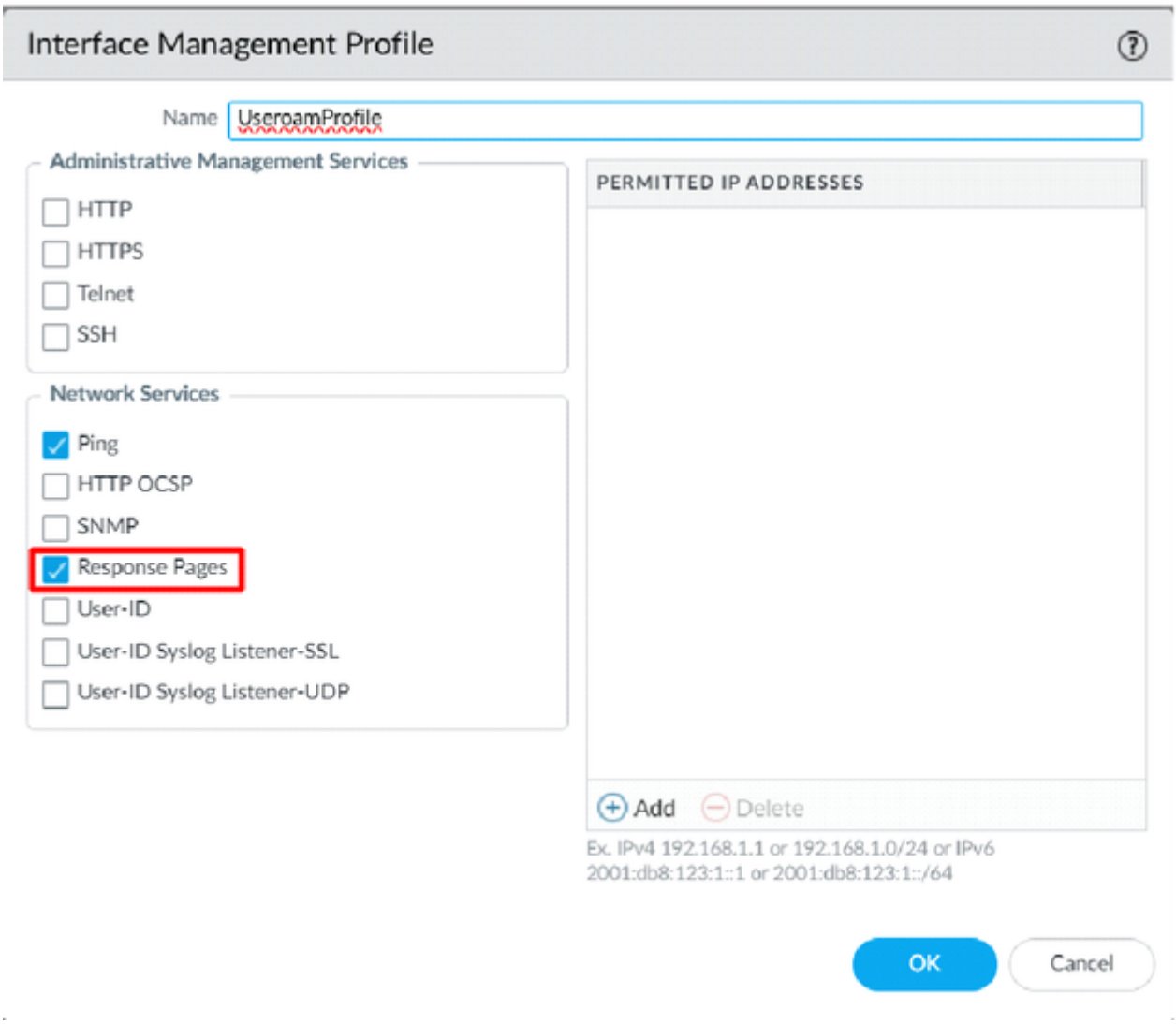
Useroam'u aktif edeceğimiz interface için **Network / Zone** menüsünden yeni bir zone oluşturup, **"Enable User Identification"** kutucuğunu seçiyoruz.



3 - Interface ve Profil Ayarlar?

Firewall üzerinden Useroam'u aktif edeceğimiz interface'de (arayüz) **Advanced** Kısmından yeni bir Profil oluşturuyoruz. Bunu yaparken **Response Pages** kutucuğunu seçiyoruz.

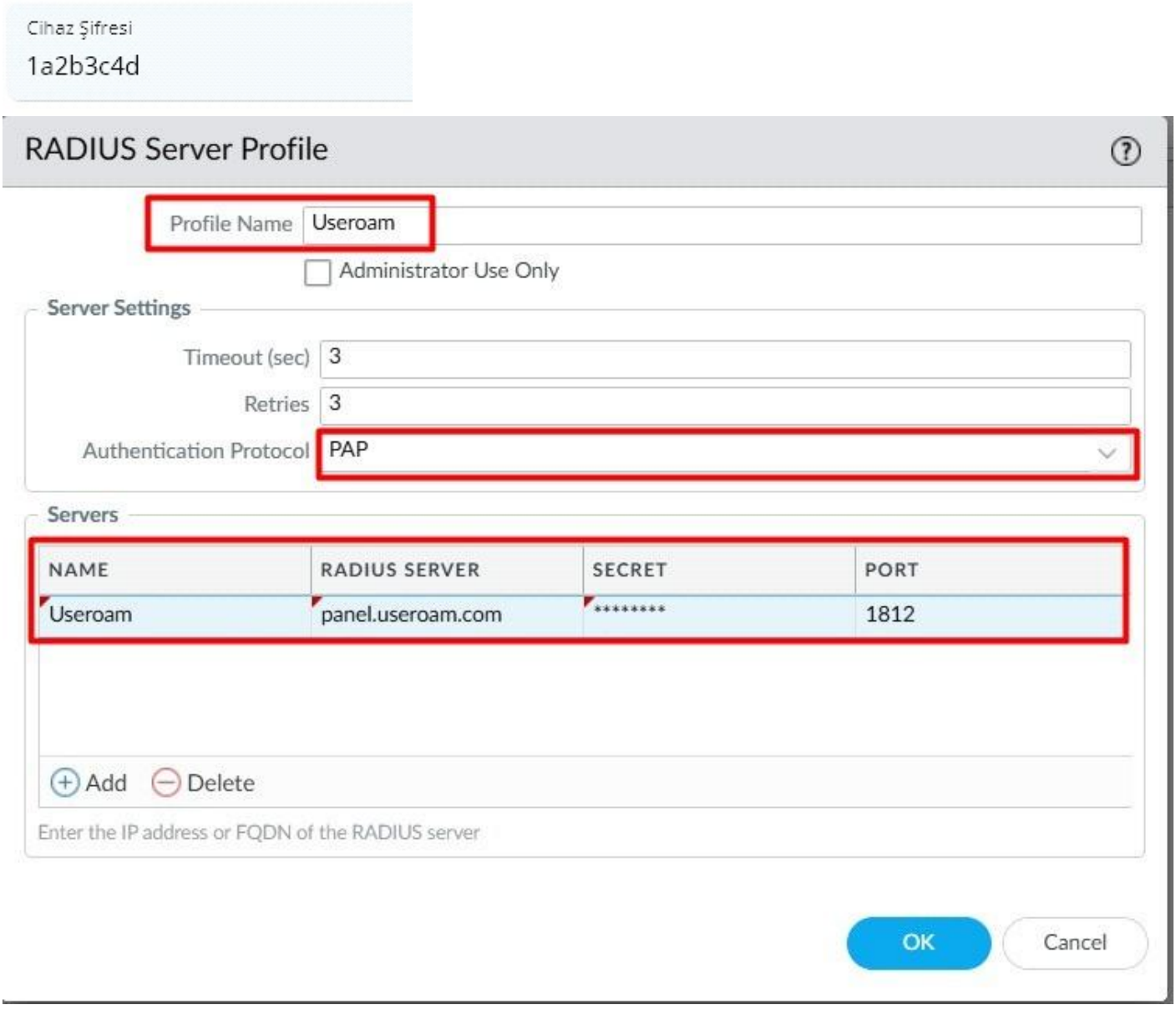

Ethernet Interface
Interface Name
ethernet1/2
Comment
Interface Type
Layer3
Netflow Profile
None
Config
IPv4
IPv6
SD-WAN
Advanced
Link Settings
Link Speed
auto
Link Duplex
auto
Link State
auto
Other Info
ARP Entries
ND Entries
NDP Proxy
LLDP
DDNS
Cluster
Management Profile
UseroamProfile
MTU
[576 - 1500]
Adjust TCP MSS
IPv4 MSS Adjustment
40
IPv6 MSS Adjustment
60
Untagged Subinterface
OK
Cancel


Interface Management Profile
Name
UseroamProfile
Administrative Management Services
HTTP
HTTPS
Telnet
SSH
Network Services
Ping
HTTP OCSP
SNMP
Response Pages
User-ID
User-ID Syslog Listener-SSL
User-ID Syslog Listener-UDP
PERMITTED IP ADDRESSES
Add
Delete
Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64
OK
Cancel

4 - Radius Ayarlar?

İlgili ayarları **Device > Server Profiles > Radius** menüsünden şu şekilde uyguluyoruz:

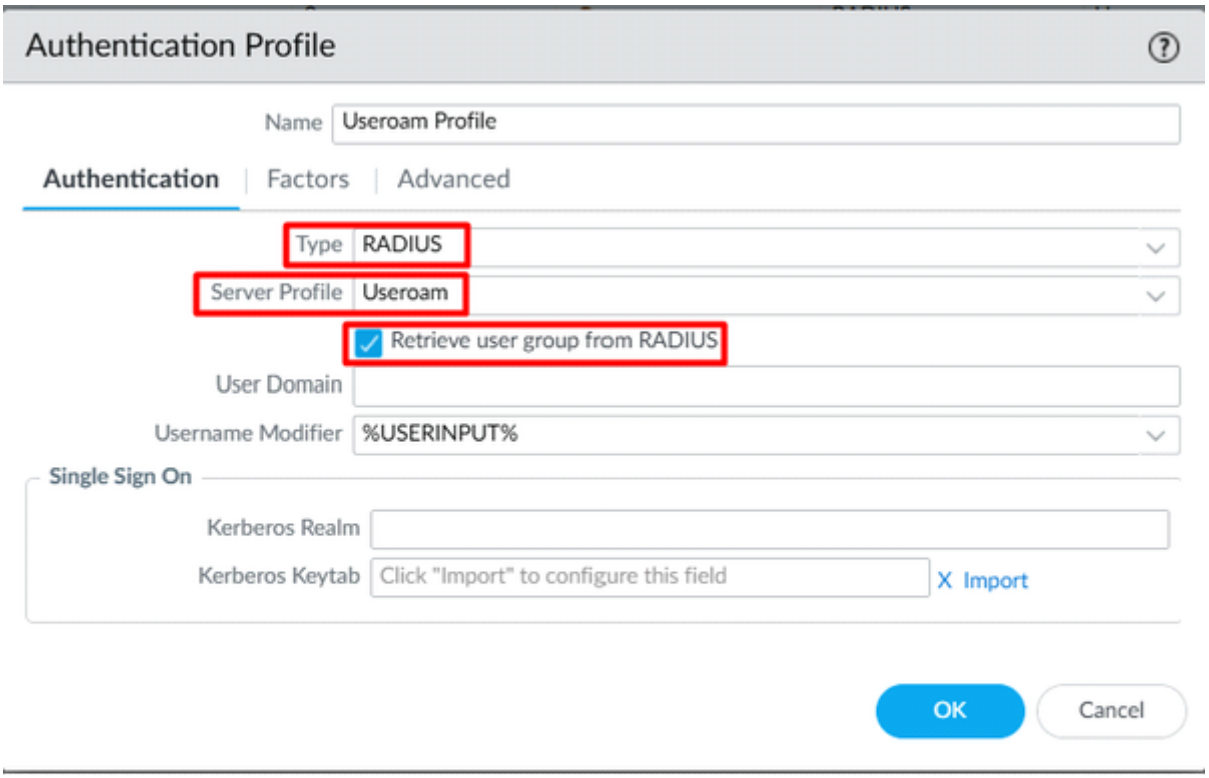
- **Authentication Protocol:** PAP
- **Radius Server / FQDN:** panel.useroam.com
- **Secret:** panel.useroam.com'da Sistem Ayarları / Cihaz Detaylarından almış olduğunuz cihaz şifresi

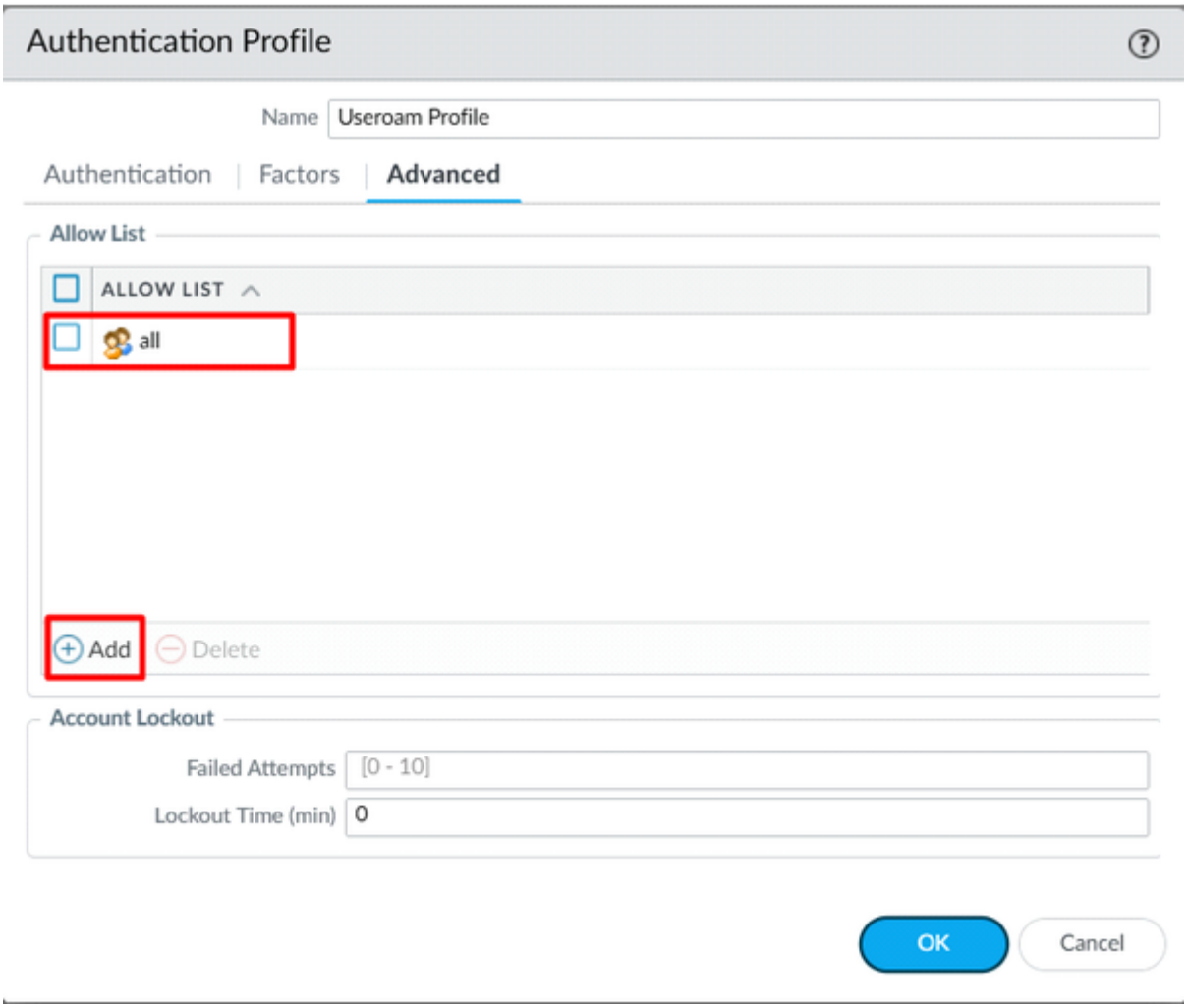


5 - Authentication Profile Ayar?

Device > Authentication Profile menüsünden yeni profilimizi tanımlıyoruz.

- **Type:** RADIUS
- **Server Profile:** Oluşturmuş olduğumuz Radius Server Profilini seçiyoruz.
- **Retrieve user group from RADIUS:** Bu kutucuğu işaretleyerek seçili olduğundan emin oluyoruz.
- **Advanced:** Advanced kısmında ise Allow List'e **all** nesnesini ekliyoruz.



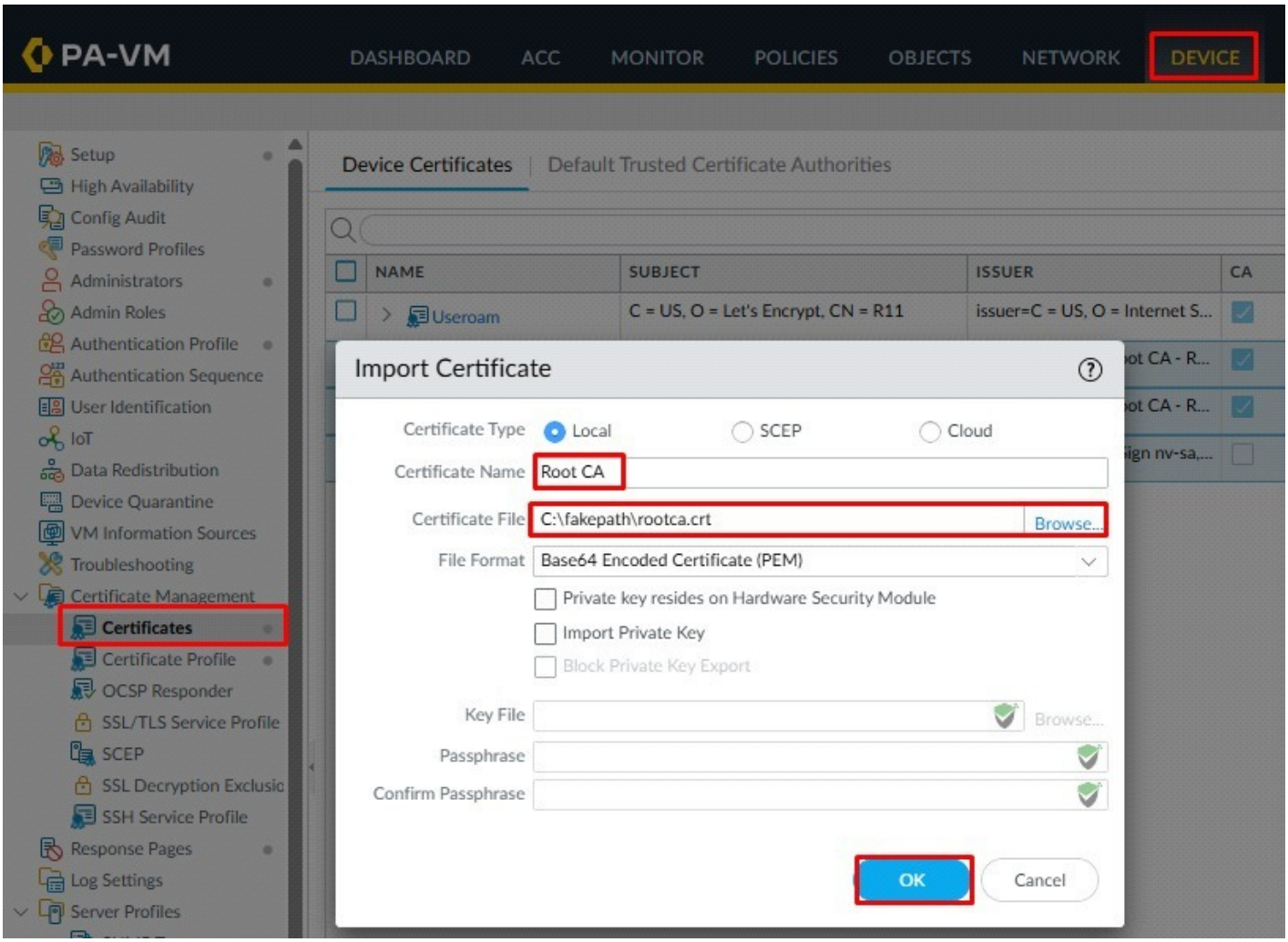


6 - Sertifika Ayarlar?n?n Yap?lmas?

Cihazımıza tanımlanacak sertifikalar yüklenmeden önce, ilgili Root CA veya Intermediate gibi kök sertifikaların sisteme eklenmiş olması gerekir. Bu işlem, mevcut sertifikanın güven zincirinin (trust chain) eksiksiz şekilde oluşturulmasını sağlar ve bağlanacak istemci cihazlarda SSL/TLS hatalarının önüne geçer.

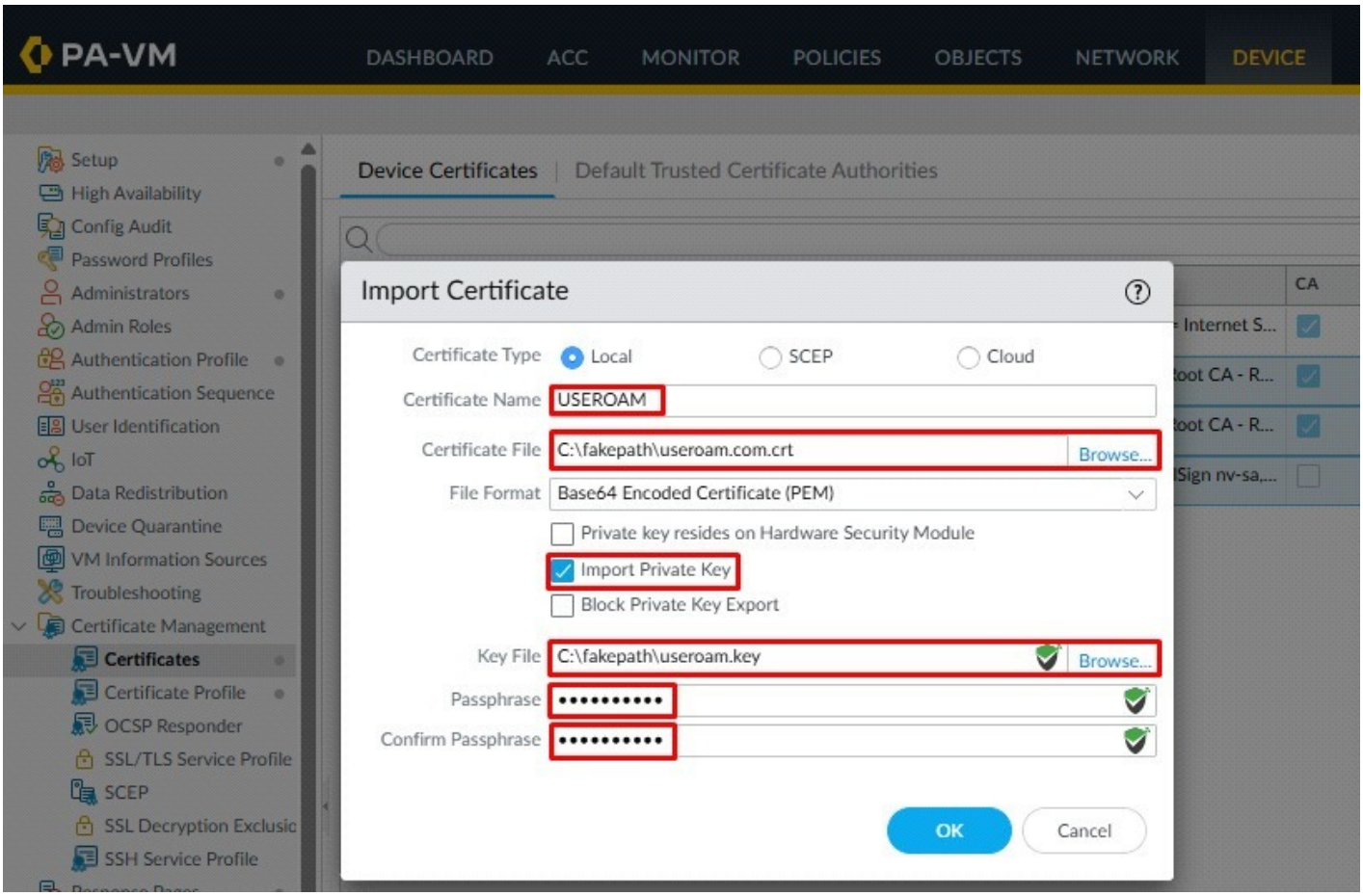
6A - Root CA Import ??lemi

İlk adım olarak, Root CA veya CA sertifikasını import ediniz.



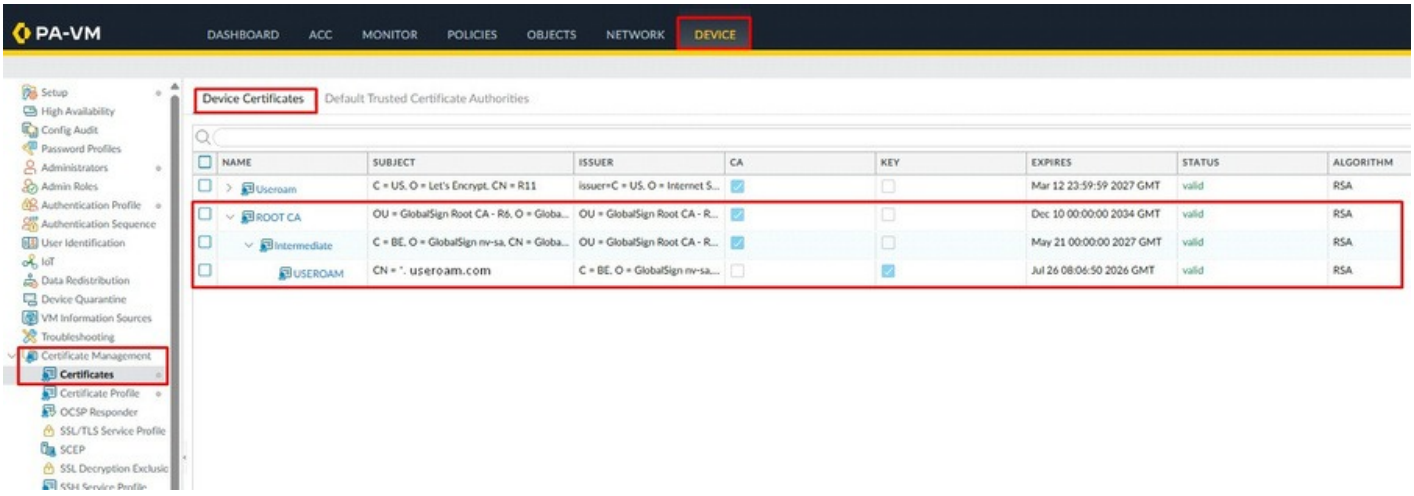
6B - Sertifika ve Anahtar Dosyas?n?n Yüklenmesi

Sonraki adımda; sertifika dosyasını, anahtar dosyası (key) ve şifreyle birlikte güvenlik duvarına yükleyiniz.



6C - Katmanl? Sertifika Zinciri Kontrolü

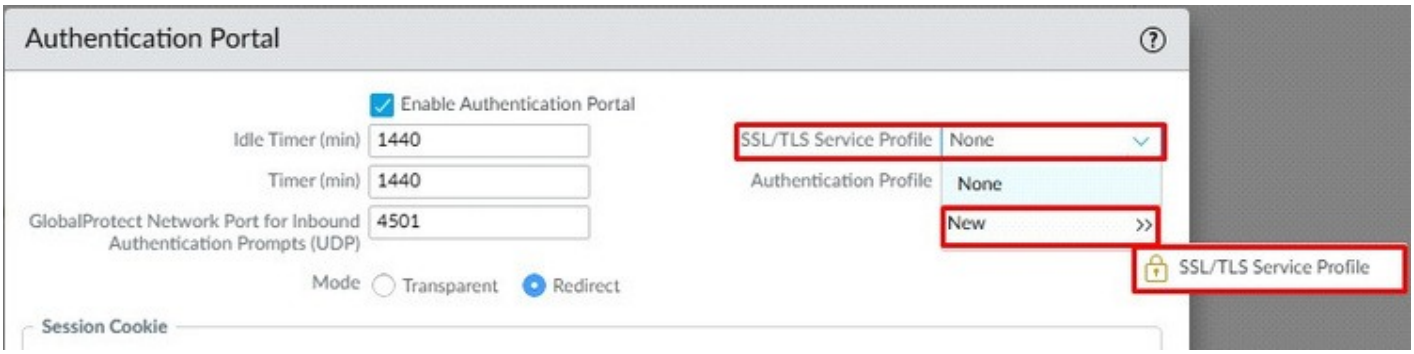
Yükleme işlemi tamamlandığında, karşımıza çıkan görüntü; katmanlı bir yapı şeklinde, birbirine bağlı bir sertifika zinciri şeklinde olmalıdır.



7 - Authentication Portal Ayarlar?

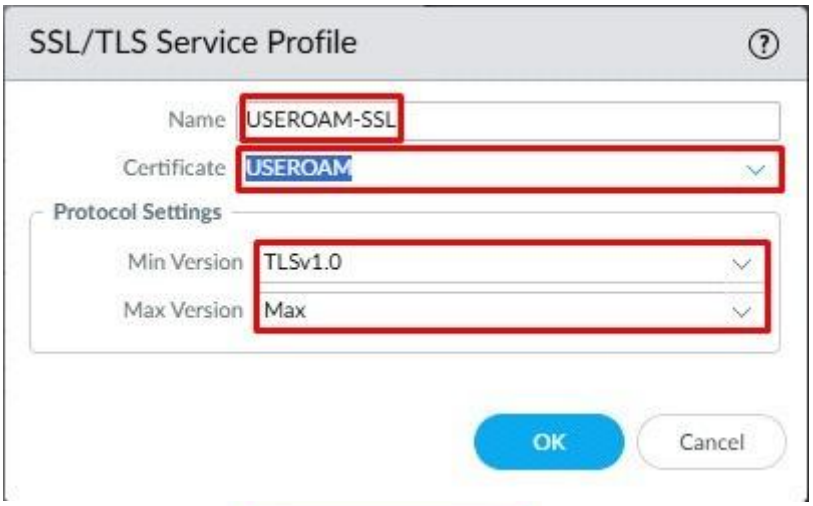
Ardından **Device > User Identification > Authentication Portal** menüsünden Settings kısmını açınız.

- Enable Authentication Portal: Bu seçeneği işaretleyerek hotspotu aktif hale getiriniz.
- Idle Timer ve Timer: Her iki alan için de maksimum değer olan 1440 dakika (24 saat) girilir. Bu, bir kullanıcının hotspot ekranını günde yalnızca bir kez görmesini sağlar. Biz bir kullanıcının önüne hotspot ekranının 24 saatte bir gelmesini istediğimiz için bu değeri giriyoruz. Daha kısa oturum süreleri tercih ediyorsanız, bu değeri ihtiyacınıza göre güncelleyebilirsiniz.
- SSL/TLS Service Prole: Bu alandan, daha önce oluşturulan SSL prolini seçiniz. Ancak burada şuna dikkat etmeniz gerekmektedir: Palo Alto'nun bazı sürümlerinde, önceden oluşturulmuş proller bu alanda görünmeyebilir. Bu durumda, “New” seçeneği ile bu ekrandan yeni bir SSL/TLS proli oluşturularak işlem tamamlanmalıdır.
- Eğer sisteminizde seçim yapılabiliyorsa, önceden oluşturulmuş prol kullanılabilir



Yeni bir profill oluşturmanız gerekiyorsaa şağıdaki adımları izleyiniz.

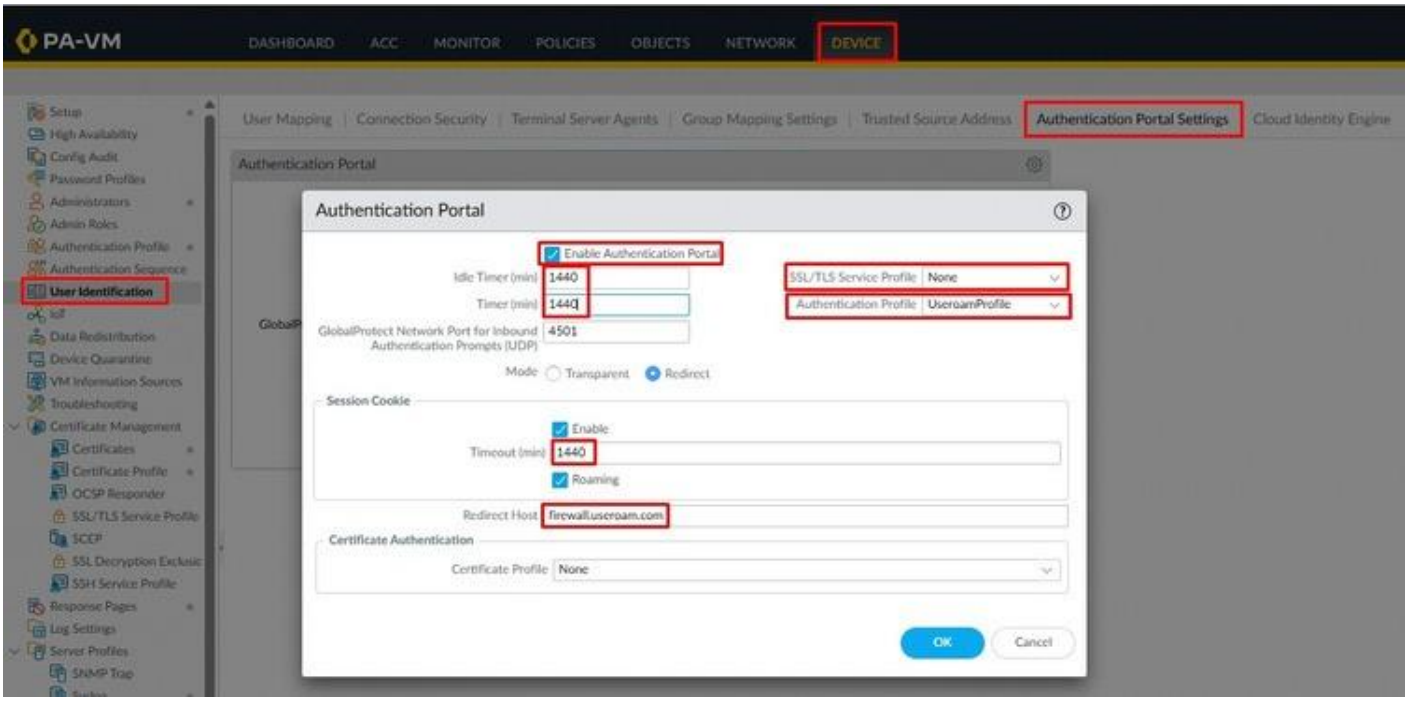
- Profile bir isim vererek, kullanılacak SSL sertikasını seçiniz.
- Protocol Settings bölümünden, çalışması istenen minimum ve maksimum SSL/TLS versiyon değerlerini seçiniz.
- Ayarlar tamamlandıktan sonra OK butonuna tıklanarak prol kaydediniz.



Authentication Prole : Oluşturulan Useroam prolini seçerek devam ediniz.

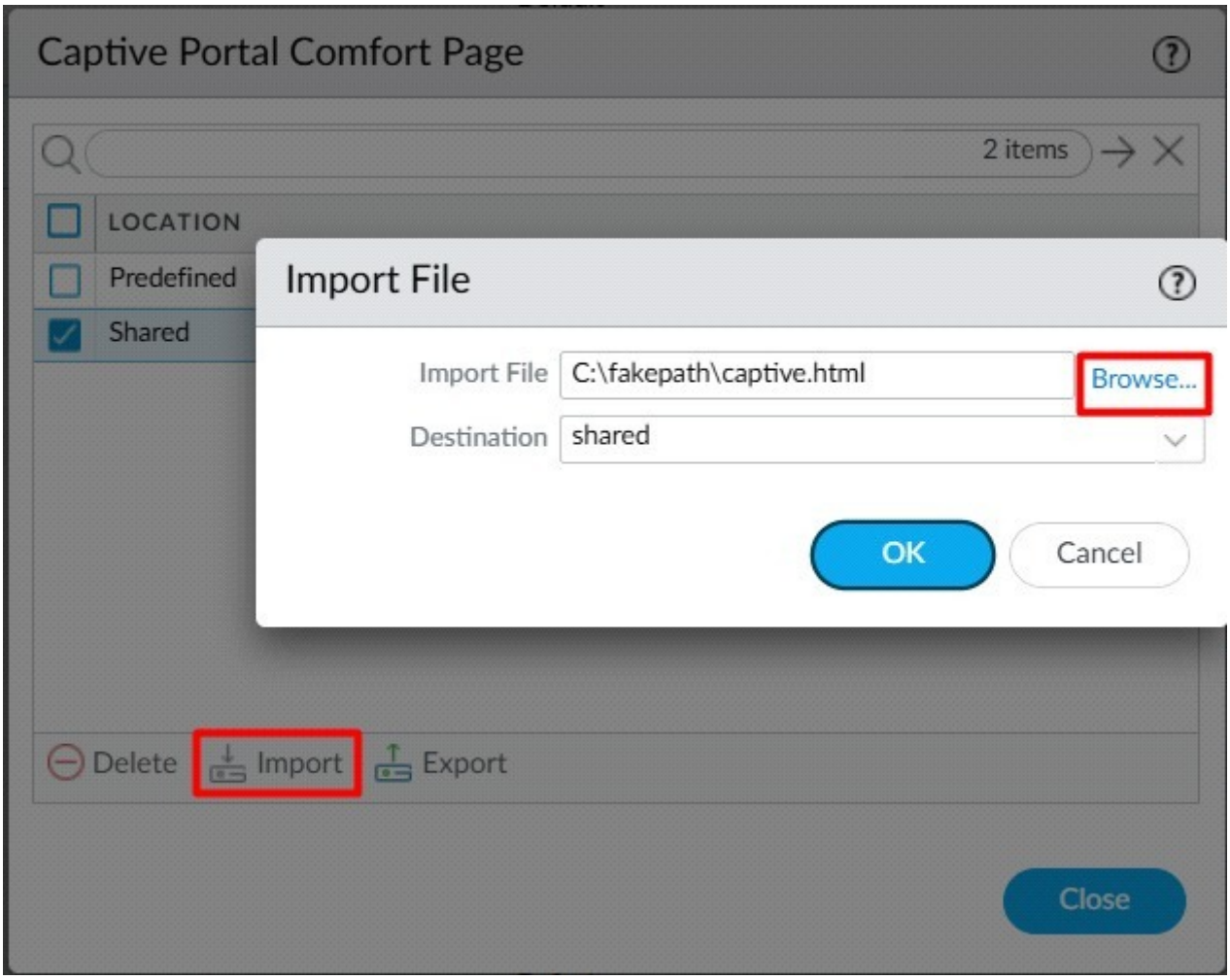
Session Cookie / Timeout : Bu alanda da daha önce belirlediğimiz gibi 1440 dakika (24 saat)d eğerini girerek oturum süresini tanımlayınız.

Redirect Host : Buraya sertika üzerinden yönlendirme yapılacağı için subdomaini giriniz.



8 - Captive Portal Tasar?m?n?n Yüklenmesi (Comfort Page)

panel.useroam.com'dan Sistem Ayarları / Cihaz Detayları'nda bulunan `<html>` olarak başlayan kod satırının hepsini kopyalayıp, not defteri veya benzeri bir uygulamaya yapıştırıp, ilgili kodu **"captive.html"** gibi bir isimle, html formatında olacak şekilde kaydediniz. Sonrasında firewall'da **Device > Response Pages > Captive Portal Comfort Page** üzerinden oluşturduğumuz dokümanı yüklüyoruz.

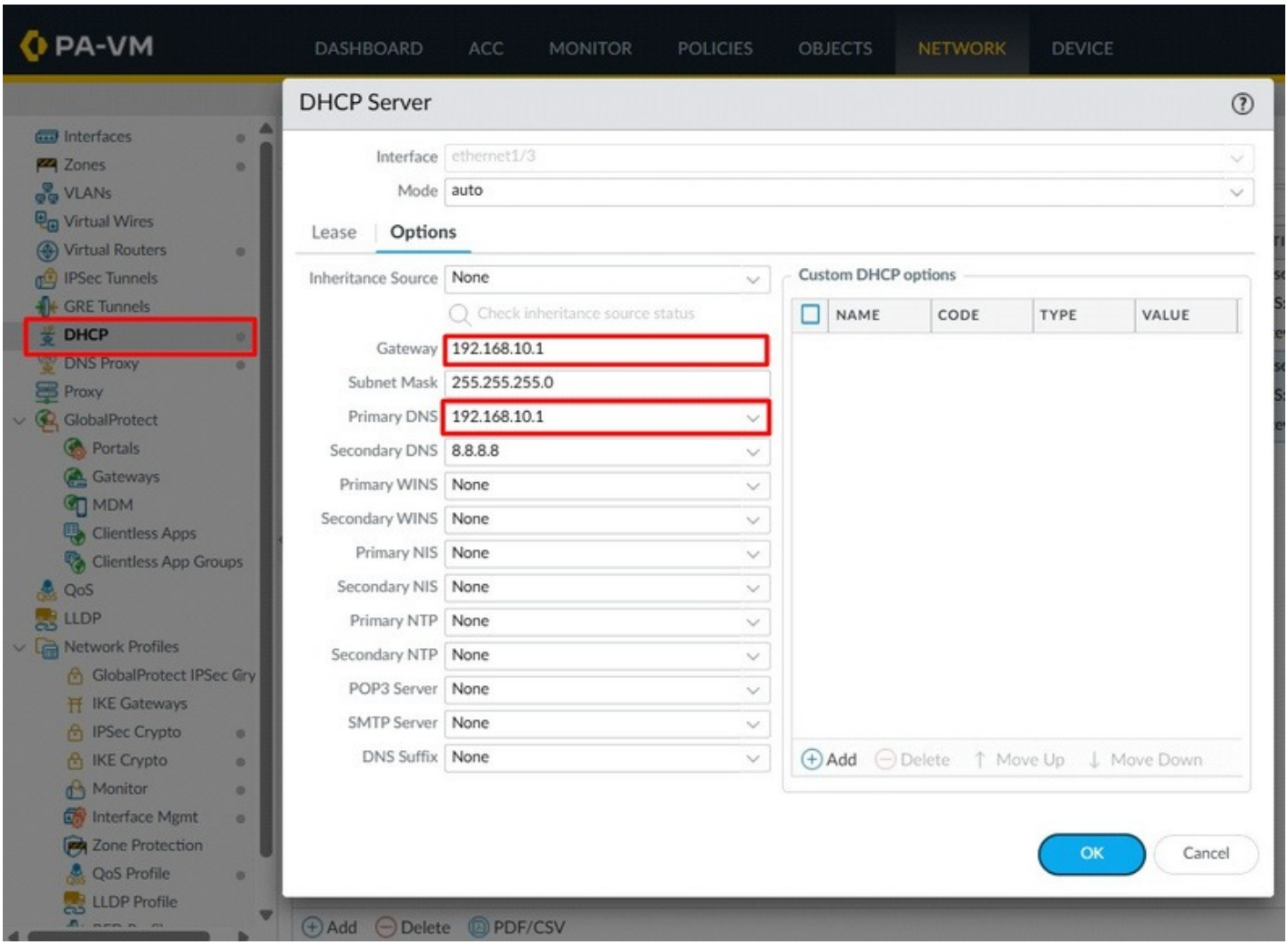


9 - DHCP Ayarlar?

İç ağdan yapılacak DNS sorgularının sorunsuz şekilde işlenebilmesi için, eğer ayrı bir DNS sunucusu bulunmuyorsa, DHCP ve DNS Proxy kısmının güncellenmesi gerekmektedir. **Network > DHCP > Options** menüsüne gidilir.

- **Primary DNS:** Primary DNS alanına, firewall cihazının kendi bacak IP adresi yazılır.
- **Secondary DNS:** Global bir DNS sunucusu tanımlanabilir (Örnek: `8.8.8.8` - Google DNS).

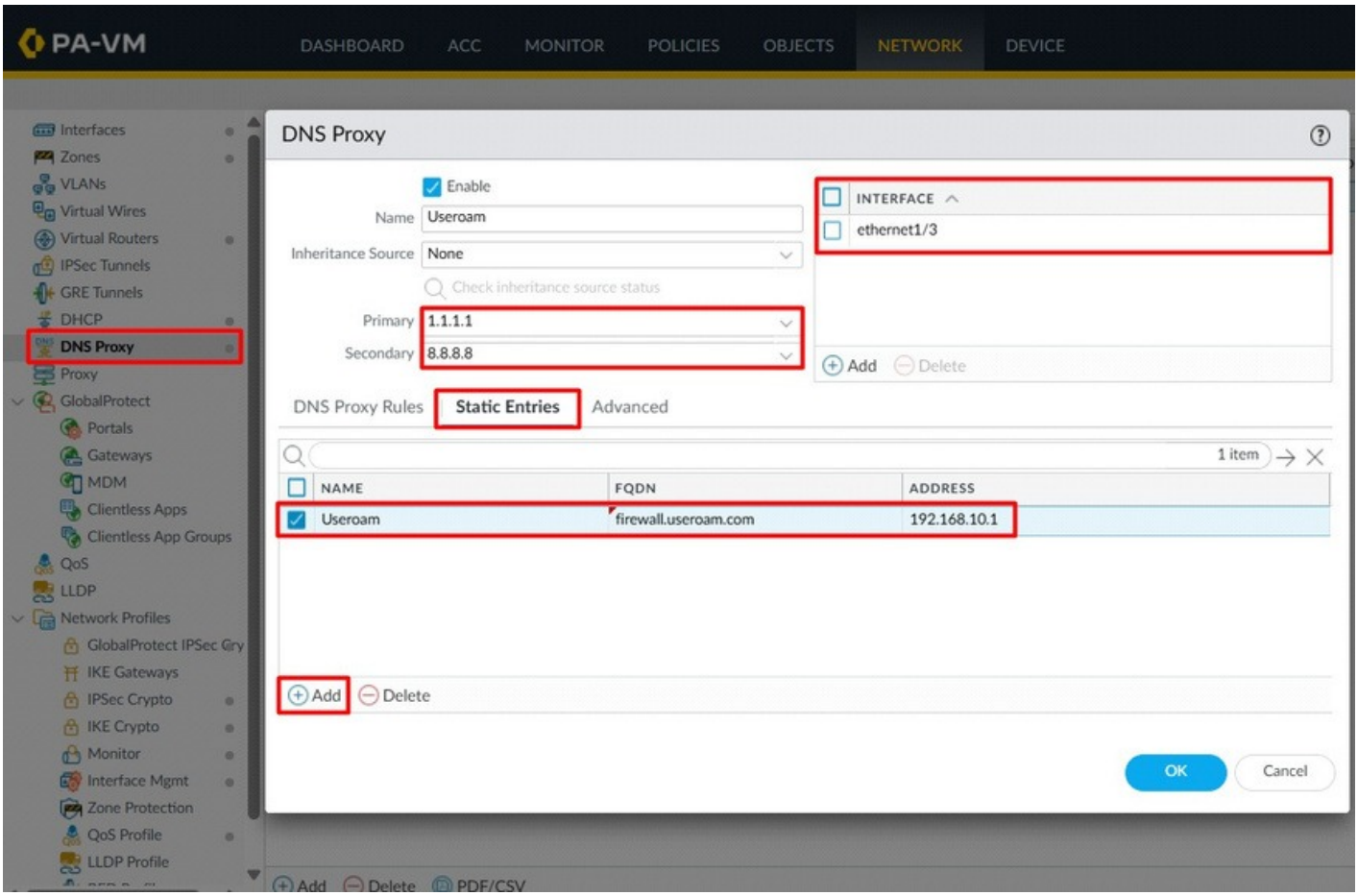
`Not: Mevcutta içeride bir DNS sunucunuz varsa alan adı yönlendirmesi için gerekli kaydı iç DNS ağınızda da (Static Entries kısmında) tanımlayarak 11. adımdan devam edebilirsiniz.`



10 - DNS Proxy Ayarlar?

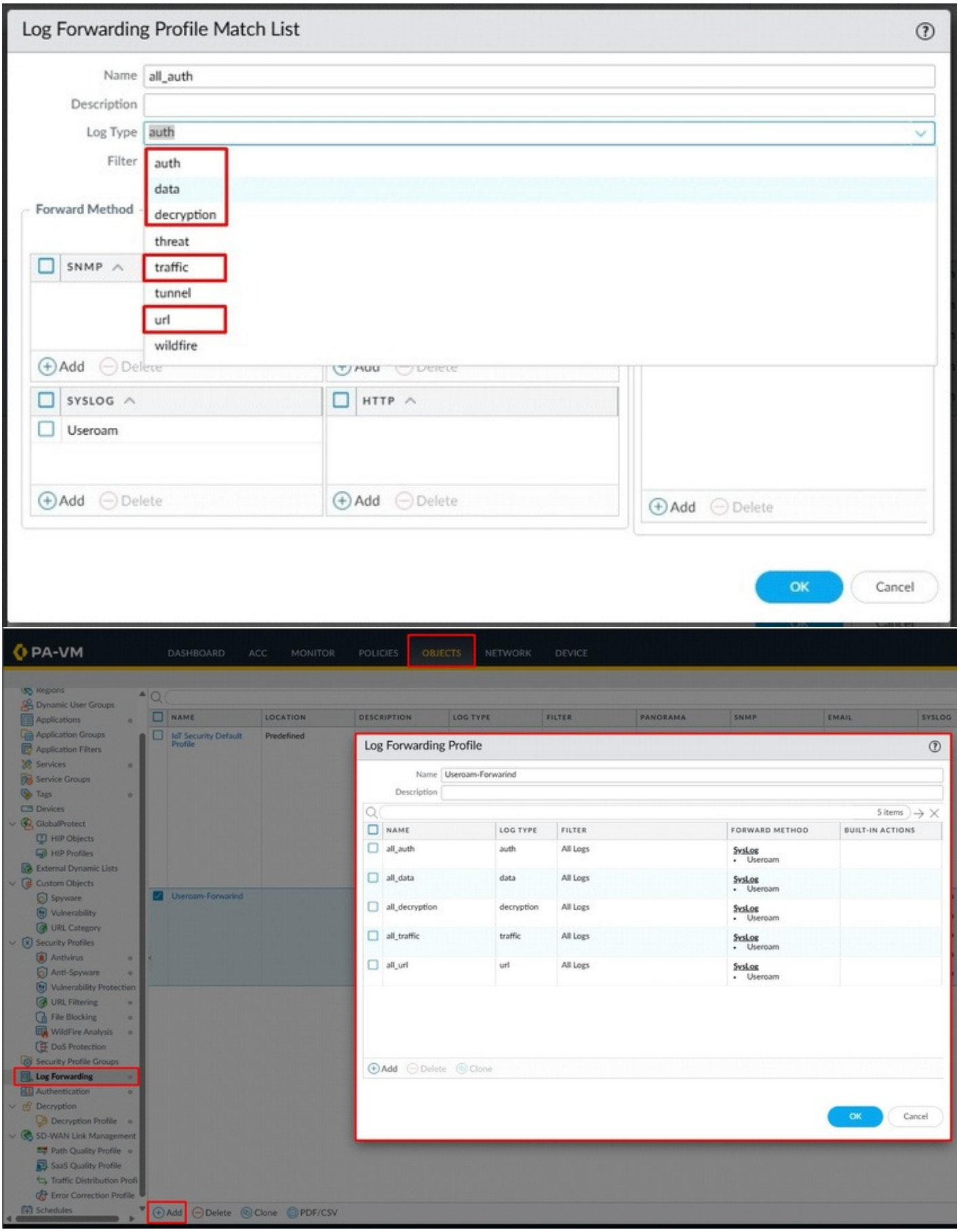
Ardından DNS sorgularının doğru şekilde çözümlenebilmesi için **Network > DNS Proxy** menüsünden yeni bir proxy tanımlanır.

- **Interface:** Bu kısımda Useroam'un aktif olacağı interface veya arayüzleri seçiniz.
- **Primary / Secondary DNS:** Global DNS sunucularını giriniz.
- **Static Entries:** Burada Add butonuna tıklanarak yeni bir kayıt oluşturunuz. **Bu aşamada, yönlendirme yapılacak IP'nin, firewall cihazının Management Interface'inin gateway IP adresi olması önemlidir.**



11 - Loglar?n Useroam'a Yönlendirilmesi (Log Forwarding)

OBJECTS > Log Forwarding kısmından Add ile yeni profil eklemesi yapınız. **5 farklı log tipi (auth, data, decryption, traffic, url) için ayrı ayrı profil oluşturulmalıdır.** Her eklemede Syslog kısmında Useroam profilini seçmeniz gerekmektedir.

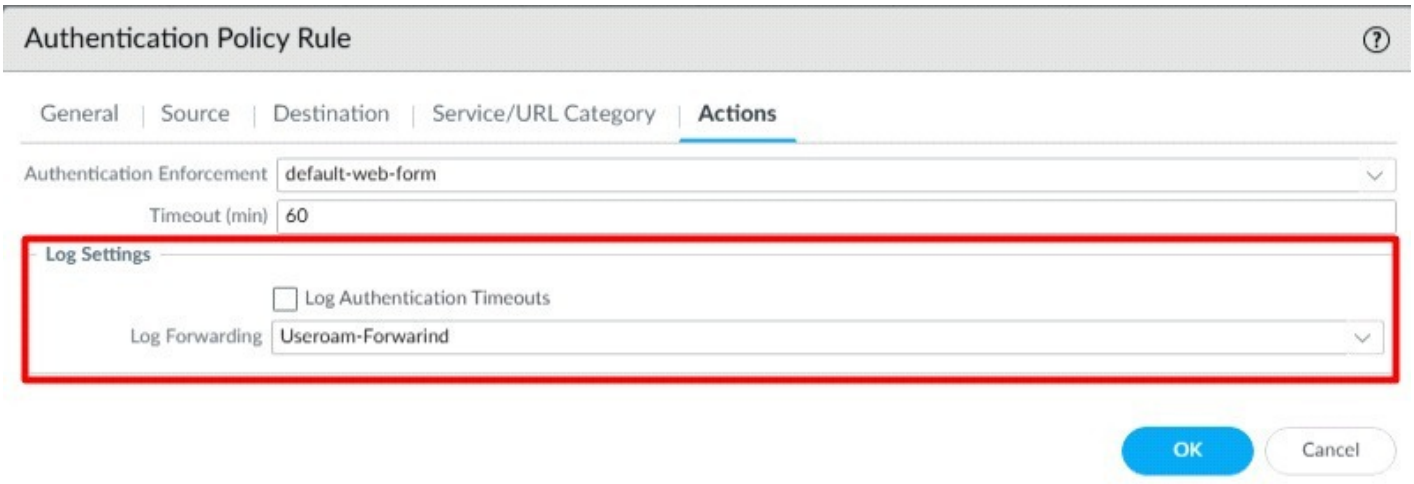


Firewall Kurallar?n?n Olu?turulmas?

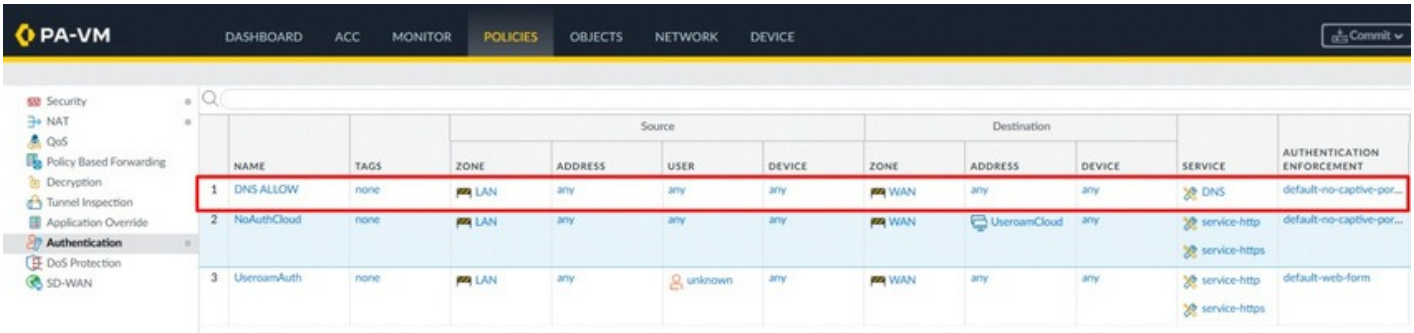
Palo Alto Firewall entegrasyonunda iki grup kural oluşturulması gerekmektedir. Kurallar ilk oluşturulurken Palo Alto'nun trafiği öğrenmesi gerekeceğinden Service kısmını öncelikle **Any** olarak kullanıp, sonrasında **application-default** olarak değiştirebilirsiniz.

12A - KURAL SET? 1: Authentication Kurallar?

Policies > Authentication menüsüne gelerek aşağıdaki üç kuralı tanımlayınız. **Tüm kurallarda Log Forwarding alanında Useroam seçili olmalıdır.**

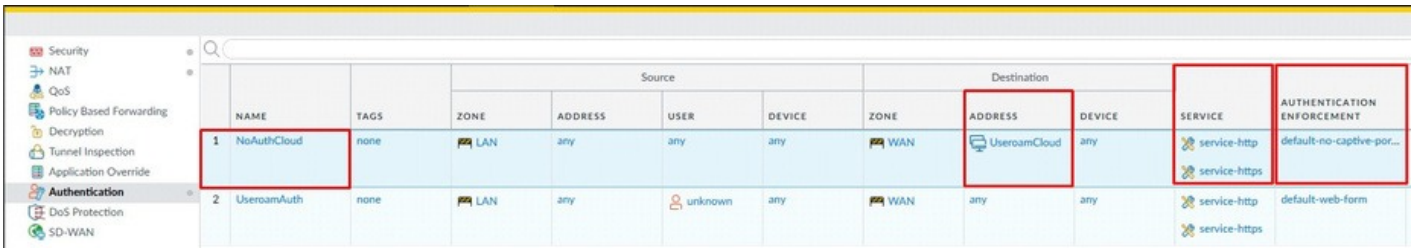


- **KURAL 1 (DNS İzni):** DNS sorgularının authentication aşamasından sorunsuz geçebilmesi için oluşturulur. WAN yönüne doğru tüm DNS sorgularına Authentication Enforcement alanında **default-no-captive-portal** seçilerek izin verilir.
- **KURAL 2 (Useroam Cloud İzni):** Bu kural sayesinde Useroam Cloud'a sorunsuz erişim sağlanacaktır. Destination Address alanında oluşturduğunuz **UseroamCloud (panel.useroam.com)** fqdn adres nesnesini seçiniz.
- **KURAL 3 (Captive Yönlendirme):** Captive portalda henüz oturum açmamış veya ağa ilk defa giren kullanıcıların HTTP ve HTTPS trafiklerinde **default-web-form** yani captive portal ekranına yönlenmesini sağlayan ana kuraldır.



12B - KURAL SET? 2: Security Kurallar?

Policies > Security menüsüne geliniz. **Her kuralda Log Settings kısmında "Log at Session End" seçili olmalı ve Log Forwarding'te Useroam atanmalıdır.**



- **KURAL 1 (WAN DNS İzni):** Tüm cihazların Captive Portal'a takılmadan WAN üzerinden DNS sorguları gerçekleştirebilmesini sağlar. Cihazın kendi global captive alan adına erişip (Örn: `captive.apple.com`) internetin varlığını anlaması ve arkasından hotspot ekranını tetiklemesi için gereklidir.
- **KURAL 2 (Useroam Erişim İzni):** Captive Portal Zone'undaki cihazların `panel.useroam.com` adresine güvenlik duvarı üzerinden sorunsuz şekilde erişebilmesi için tanımlanır.
- **KURAL 3 (İnternet Çıkış İzni):** Misafir ağınızın internete çıkışını sağlayan son kuraldır. Bu kuralda Source kısmında **Source User** değeri mutlaka **known-user** olarak seçilmelidir.

Ek Teknik Bilgi (Giriş Yapmış Kullanıcıyı Düşürmek): Oturum açmış aktif bir misafir kullanıcının oturumunu sonlandırmak veya önbelleğini temizlemek için Palo Alto CLI arabirimine giriş yapılarak sırasıyla aşağıdaki komutlar çalıştırılır.
Giriş yapmış tüm aktif kullanıcıların listesini ve IP adreslerini görmek için:
`show user ip-user-mapping all`
Listeden alınan ilgili IP adresini ağdan düşürmek için aşağıdaki kodlar tetiklenir:

`clear user-cache ip <ip-adresi>`
`debug user-id reset captive-portal ip-address <ip-adresi>`

Önemli - Entegrasyon Tamamland?

Hepsi bu kadar! Palo Alto entegrasyon ve sunucu değişiklik işleminiz başarıyla tamamlandı. İşlem sırasında herhangi bir teknik sorunla karşılaşırsanız **destek@useroamteknoloji.com** adresinden destek ekibiyle iletişime geçebilirsiniz.

Useroam Cloud Mikrotik Entegrasyon Rehberi

1 - Useroam Panele Cihaz Ekleme

İlk olarak **panel.useroam.com** adresinden panelinize giriş yapıp **Yeni Cihaz** ekleyiniz. Cihaz Adresi kısmına, firewall üzerinden hangi dış bacak IP adresi ile iletişim kuracaksanız onu tanımlayınız.

- **Cihaz tipi:** MikroTik seçiniz.
- **5651 Loglama:** 5651 Loglama kutucuğunu aktif ediniz.

2 - Bridge ve Port Yap?land?rmas?

Bridge > Bridge ekranından `BR-MISAFIR` isimli yeni bir sanal köprü oluşturunuz. Ardından **Bridge > Ports** ekranına gelerek misafir ağına ayıracağınız fiziksel portları (Örn: `ether4` ve `ether5`) bu bridge'e dahil ediniz.

Layer-2 İzolasyon (Horizon): Misafir ağındaki istemcilerin kablolu veya kablosuz olarak birbirini doğrudan görmesini engellemek için, portları eklerken **Horizon** değerini `1` olarak tanımlayınız.

Alternatif CLI Komutları:

```
/interface bridge add name=BR-MISAFIR comment="Misafir bridge"
/interface bridge port add bridge=BR-MISAFIR interface=ether4 horizon=1
/interface bridge port add bridge=BR-MISAFIR interface=ether5 horizon=1
```

3 - Misafir A? IP ve DHCP Sunucu Kurulumu

IP > Addresses menüsünden oluşturduğunuz `BR-MISAFIR` arayüzüne misafir ağ geçidi IP'sini (Örn: `192.168.3.1/24`) tanımlayınız.

Ardından **IP > Pool** altından misafir cihazların alacağı IP aralığını belirleyip, **IP > DHCP Server** menüsünden misafir IP dağıtım servisini aktif ediniz.

Alternatif CLI Komutları:

```
/ip address add address=192.168.3.1/24 interface=BR-MISAFIR comment="Guest GW"
/ip pool add name=POOL-MISAFIR ranges=192.168.3.50-192.168.3.250
```

```
/ip dhcp-server add name=DHCP-MISAFIR interface=BR-MISAFIR address-pool=POOL-MISAFIR disabled=no
/ip dhcp-server network add address=192.168.3.0/24 gateway=192.168.3.1 dns-server=192.168.3.1
```

4 - Hotspot ve RADIUS / Useroam Entegrasyonu

IP > Hotspot menüsünde `BR-MISAFIR` üzerinde Hotspot servisini sihirbaz yardımıyla kurunuz. Yerel ağ geçidi adresini `192.168.3.1` olarak seçerek ilerleyiniz.

Hotspot kurulumu bittikten sonra, ana menüdeki **Radius** sekmesine gelerek yeni bir servis ekleyiniz. Sunucu IP alanına Useroam Cloud RADIUS IP adresi olan **`104.247.174.120`** giriniz. Hotspot Server Profile ayarları içerisinden **Use RADIUS** seçeneğini aktif (yes) konumuna getiriniz.

Alternatif CLI Komutları:

```
/radius add service=hotspot address=104.247.174.120 secret="RADIUS_SECRET" authentication-port=1812 accounting-port=1813 require-message-auth=no
/ip hotspot profile set HS-PROFILE-MISAFIR use-radius=yes radius-accounting=yes
```

5 - Walled Garden ?zin Kurallar?

Oturum açmamış misafir kullanıcıların karşılama ekranına ve Useroam paneline kesintisiz ulaşabilmesi için Hotspot altındaki Walled Garden listesine gerekli izinleri ekleyiniz.

Alternatif CLI Komutları:

```
/ip hotspot walled-garden add dst-host=panel.useroam.com action=allow
/ip hotspot walled-garden ip add dst-address=104.247.174.120 protocol=tcp dst-port=80 action=accept
/ip hotspot walled-garden ip add dst-address=104.247.174.120 protocol=tcp dst-port=443 action=accept
```

6 - Firewall Güvenlik S?k?la?t?rma (Hardening) Kurallar?

IP > Firewall > Filter Rules menüsüne giderek misafir ağından MikroTik cihazının yönetim portlarına (Winbox, SSH, Webfig, API) erişimi kapatınız. Ayrıca misafir ağından şirket iç ağlarına (LAN) veya kamera ağlarına erişimi engellemek için izolasyon kurallarını tanımlayınız.

Alternatif CLI Komutları:

```
/ip firewall filter add chain=input src-address=192.168.3.0/24 protocol=tcp dst-port=22,80,443,8291,8728,8729 action=drop comment="Guest -> Router mgmt DROP"
/ip firewall filter add chain=forward src-address=192.168.3.0/24 dst-address=192.168.2.0/24
```

```
action=drop comment="Guest -> LAN DROP"
/ip firewall filter add chain=forward src-address=192.168.3.0/24 dst-address=192.168.88.0/24
action=drop comment="Guest -> CAMERA DROP"
```

7 - DNS Görünürlü?ü ve Bypass Engelleme (DNS Visibility)

Kullanıcıların harici DNS sunucuları (DoH, DoT, QUIC) kullanarak 5651 loglama sistemini ve DNS visibility politikalarını aşmasını (bypass) engellemek amacıyla, tüm DNS isteklerini MikroTik üzerinden geçmeye zorlayınız.

Alternatif CLI Komutları:

```
/ip dns set allow-remote-requests=yes servers=1.1.1.3,1.0.0.3
/ip firewall nat add chain=dstnat src-address=192.168.3.0/24 protocol=udp dst-port=53
action=redirect to-ports=53 comment="Force Guest DNS UDP"
/ip firewall nat add chain=dstnat src-address=192.168.3.0/24 protocol=tcp dst-port=53
action=redirect to-ports=53 comment="Force Guest DNS TCP"
/ip firewall filter add chain=forward src-address=192.168.3.0/24 protocol=tcp dst-port=853
action=drop comment="Block Guest DoT TCP"
/ip firewall filter add chain=forward src-address=192.168.3.0/24 protocol=udp dst-port=853
action=drop comment="Block Guest DoT UDP"
/ip firewall filter add chain=forward src-address=192.168.3.0/24 protocol=udp dst-port=443
action=drop comment="Block Guest QUIC"
```

8 - Syslog ile Loglar? Useroam'a Yönlendirme

System > Logging ve **Logging Actions** menüleri altından; hotspot, account, dhcp ve firewall süreçlerine ait tüm log akışını yasal 5651 imzalamasının yapılabilmesi amacıyla Useroam syslog sunucusuna yönlendiriniz.

Alternatif CLI Komutları:

```
/system logging action set remote remote=104.247.174.120 remote-port=514 remote-protocol=udp
/system logging add topics=hotspot action=remote
/system logging add topics=hotspot,account action=remote
/system logging add topics=dhcp action=remote
/system logging add topics=firewall action=remote
```

9 - Kontrol ve Do?rulama Ad?mlar?

Sistem kurulumunu tamamladıktan sonra terminal üzerinden aşağıdaki komutları çalıştırarak servislerin, RADIUS iletişiminin ve aktif kullanıcı oturumlarının durumunu doğrulayabilirsiniz:

`/ip hotspot active print`
`/ip hotspot host print`
`/radius print detail`
`/ip hotspot profile print detail`
`/ip firewall filter print`
`/ip firewall nat print`
`/ip dns cache print`
`/log print where topics~"hotspot|radius|account|dns|firewall"`

Önemli - Entegrasyon Tamamland?

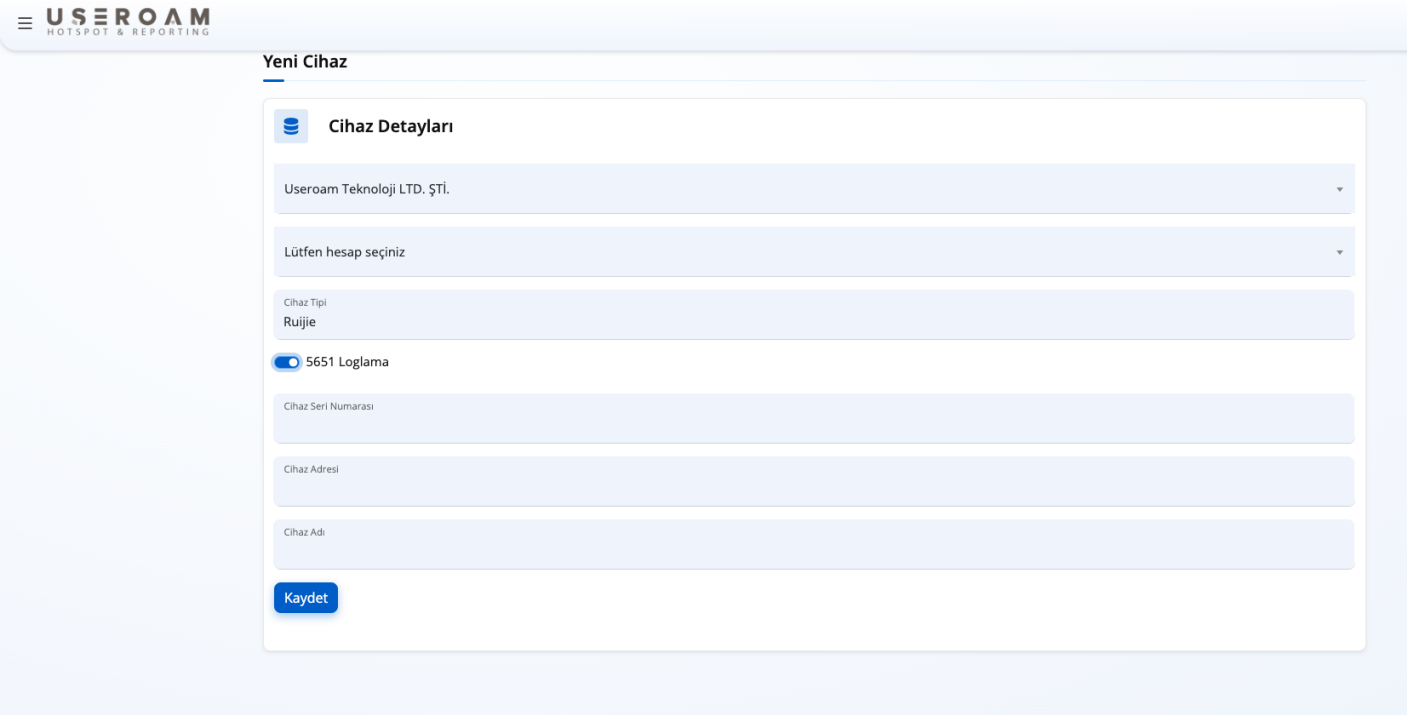
Hepsi bu kadar! MikroTik mevcut cihaz üzerinde misafir ağı, Hotspot ve Useroam entegrasyon işlemleriniz başarıyla tamamlandı. Süreç esnasında herhangi bir teknik aksaklık yaşarsanız **destek@useroamteknoloji.com** adresi üzerinden teknik destek ekibimizle iletişime geçebilirsiniz.

Useroam Cloud Ruijie Entegrasyon Rehberi

1 - Useroam Panele Cihaz Ekleme

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

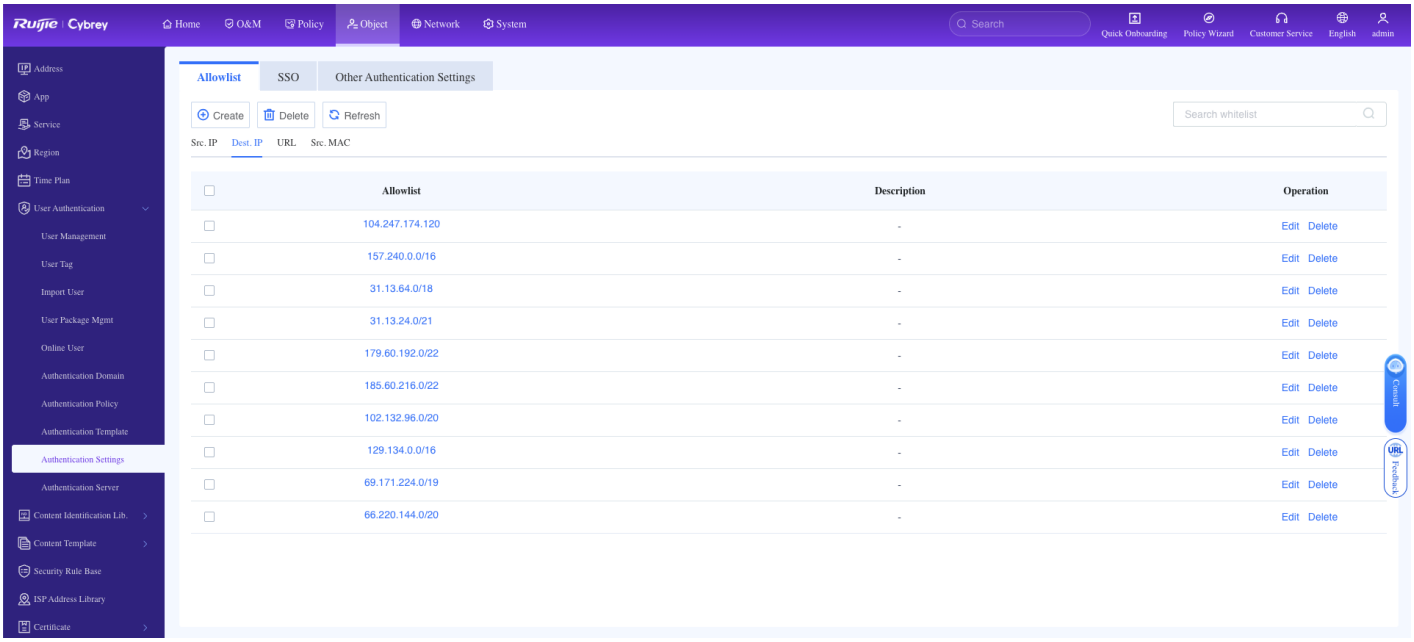
- **Cihaz Tipi:** Ruijie seçiniz.
- **5651 Loglama:** 5651 Loglama kutucuğunu aktif ediniz.
- **Cihaz Seri Numarası:** **[KRİTİK ADIM]** Cihazınızın altındaki etikette veya arayüzde yer alan orijinal donanım seri numarasını bu alana eksiksiz giriniz. Ruijie entegrasyonunun sorunsuz çalışması için seri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



2 - Güvenli IP ?zin Listesi Ayarlar? (Allowlist Dest. IP)

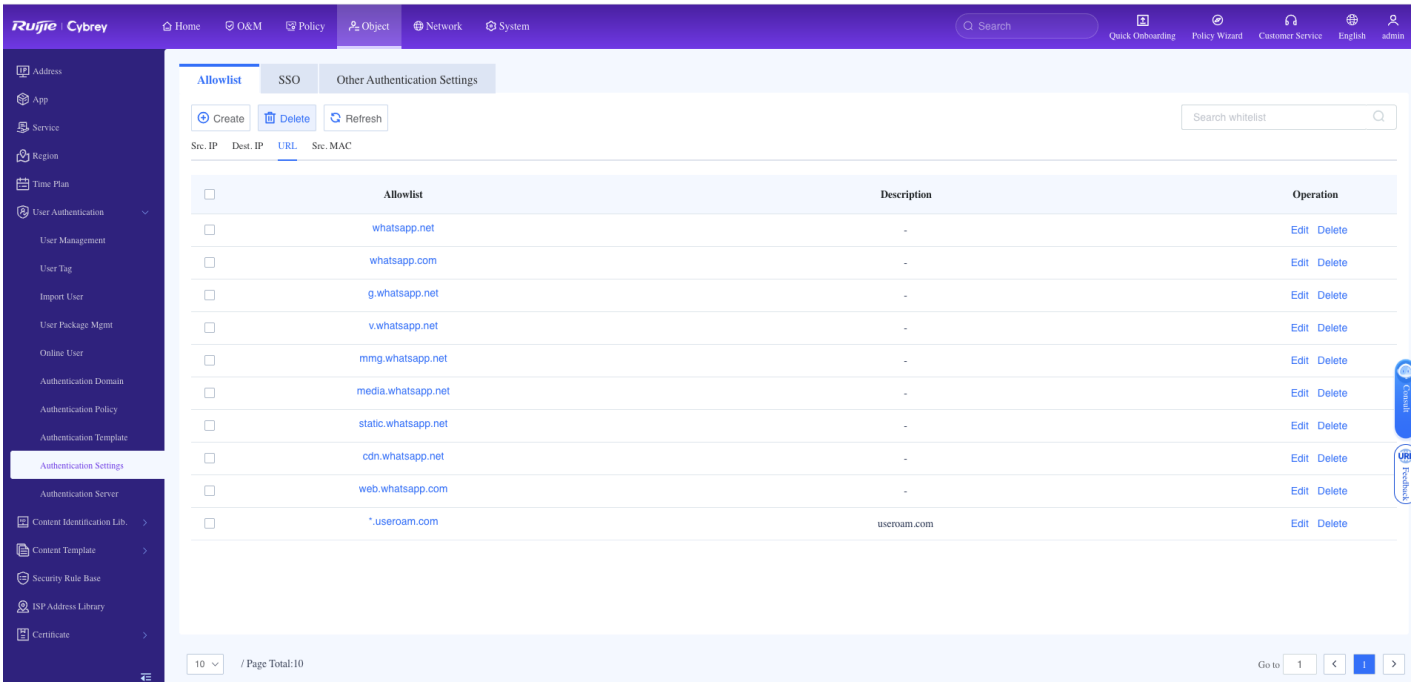
Ruijie cihazınızın yönetim arayüzünde üst menüden **Object > User Authentication > Authentication Settings** yolunu takip ediniz. **Allowlist** sekmesi altında **Dest. IP** seçeneğini işaretleyerek Useroam Cloud sunucu IP adresini (`104.247.174.120`) ve hotspot servis ağlarını izinli

olarak ekleyiniz.



3 - Güvenli Alan Ad? ?zin Listesi Ayarlar? (Allowlist URL)

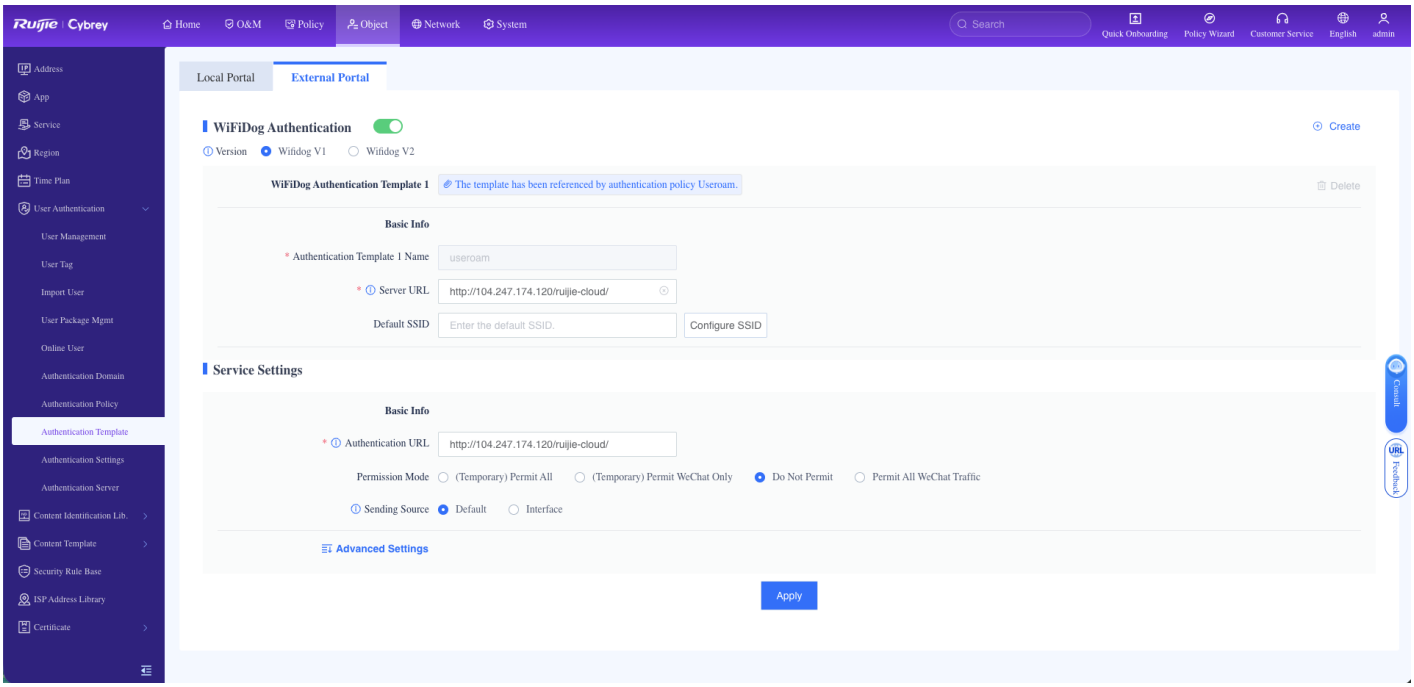
Aynı menü altındaki **URL** sekmesine geçiş yapınız. Kullanıcıların kimlik doğrulaması yapmadan önce erişebilmesi gereken `*.useroam.com` adresini izin listesine ekleyiniz. Ayrıca, mobil cihazların arka planda hotspot ağını doğrulayabilmesi için gerekli olan mesajlaşma ve işletim sistemi captive alan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



4 - External Portal & WiFiDog Kimlik Do?rulama ?ablonu

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

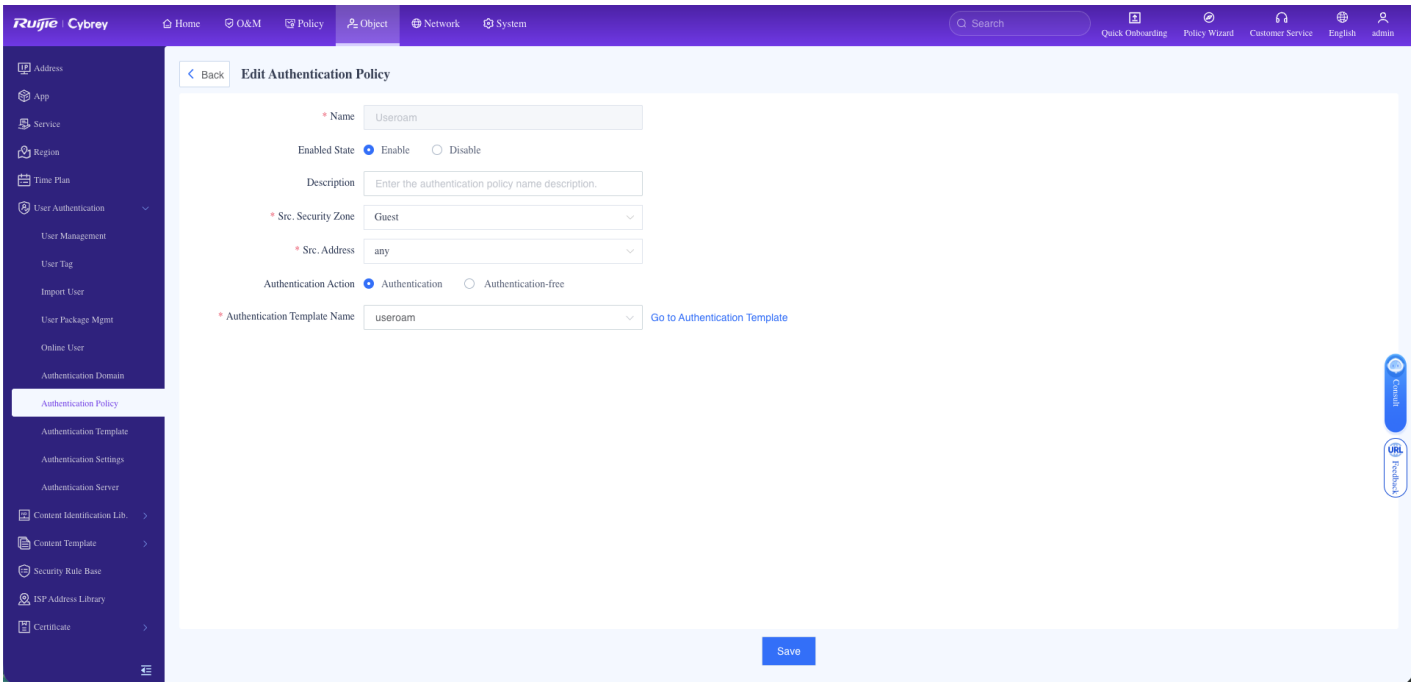
- **Version:** Wifidog V1 seçiniz.
- **Authentication Template Name:** useroam
- **Server URL:** `http://104.247.174.120/ruijie-cloud/`
- **Permission Mode:** Do Not Permit seçiniz.
- **Sending Source:** Default olarak bırakınız.



5 - Kimlik Do?rulama Politikas? (Edit Authentication Policy)

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

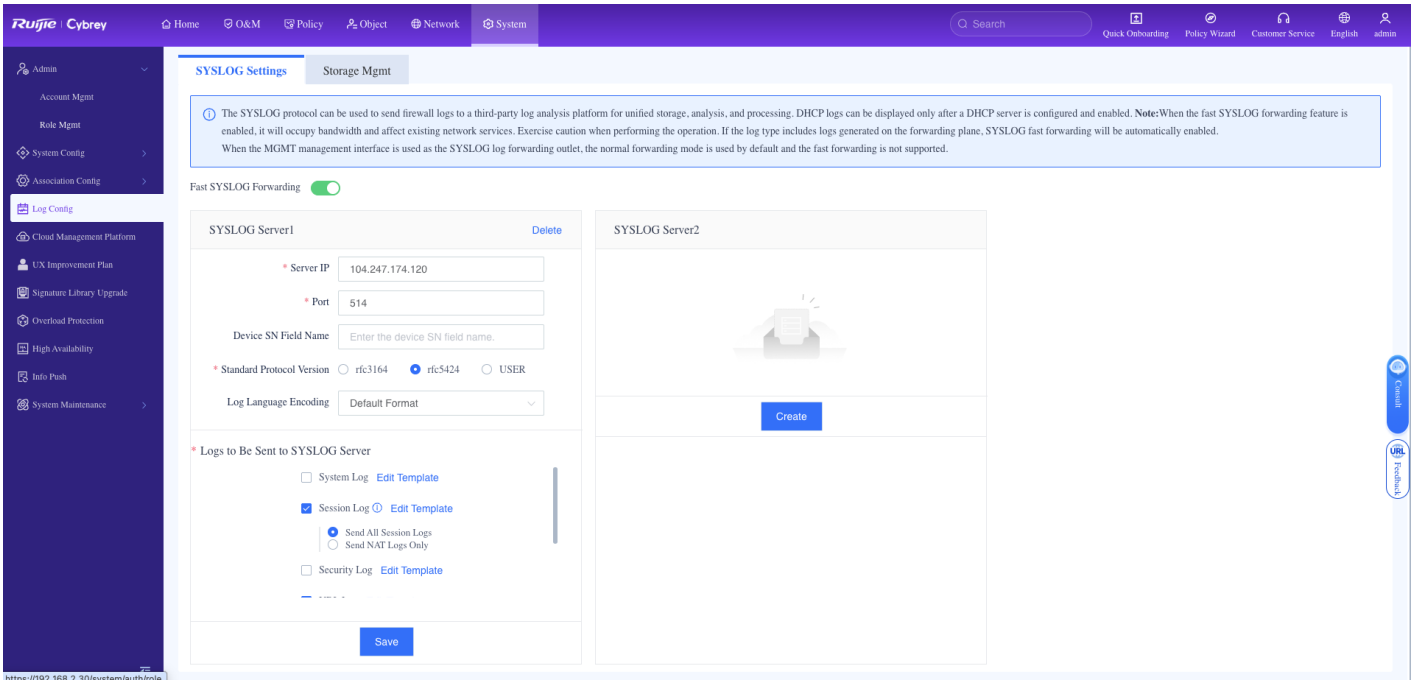
- **Name:** useroam
- **Enabled State:** Enable konumuna getiriniz.
- **Src. Security Zone:** Misafir ağınızın bağlı olduğu zone'u seçiniz (Örn: `Guest`).
- **Src. Address:** any
- **Authentication Action:** Authentication seçeneğini işaretleyiniz.
- **Authentication Template Name:** Bir önceki adımda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



6 - Loglar?n 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).



Önemli - Entegrasyon Tamamland?

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.