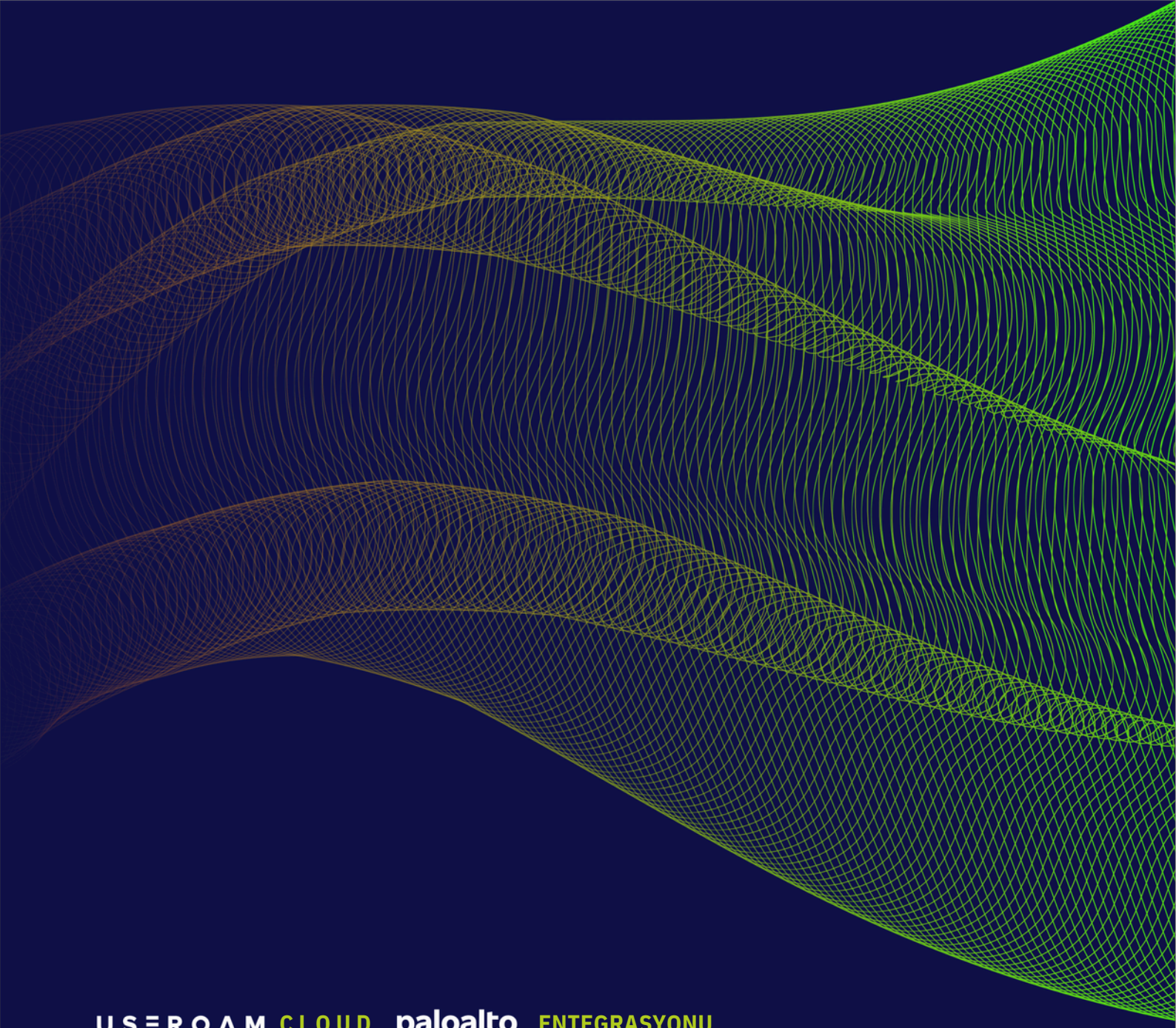


USEROAM CLOUD paloalto ENTEGRASYONU

USEROAM
HOTSPOT&REPORTING

Kullanıcı deneyimini iyileştirmek ve sizlere daha iyi bir hizmet sunabilmek için Useroam Cloud sunucu altyapımızı yeniledik.

Bu kılavuz, Palo Alto güvenlik duvarınıza ait sunucu değişikliği işlemini nasıl gerçekleştireceğinize dair detaylı talimatları içermektedir.

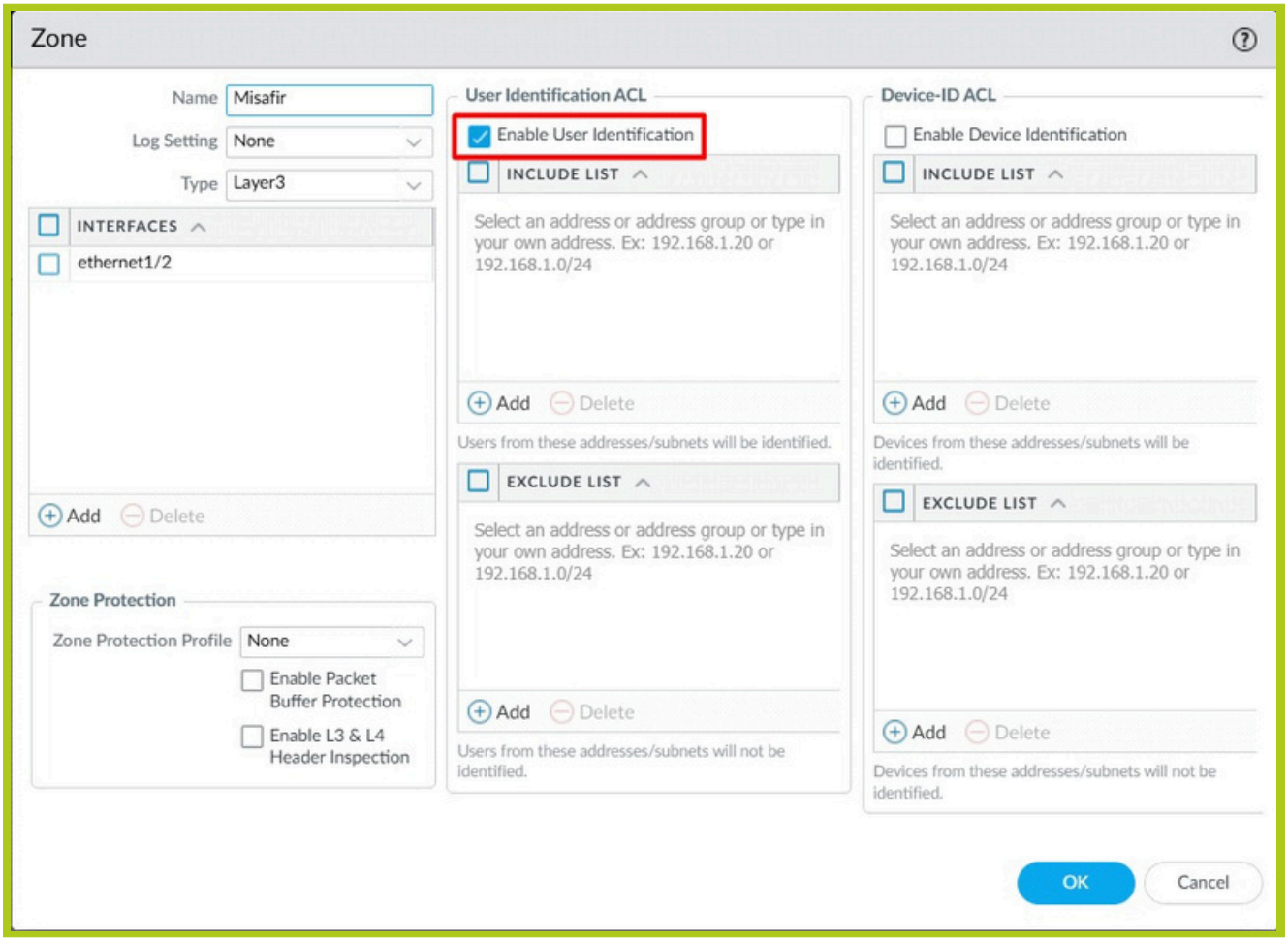
Aşağıda verilen adımları takip ederek sunucu değişikliği işlemini kolayca tamamlayabilirsiniz.

1 Panele güvenlik duvarının 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. **5651 Loglama** kutucuğunu aktif ediniz.

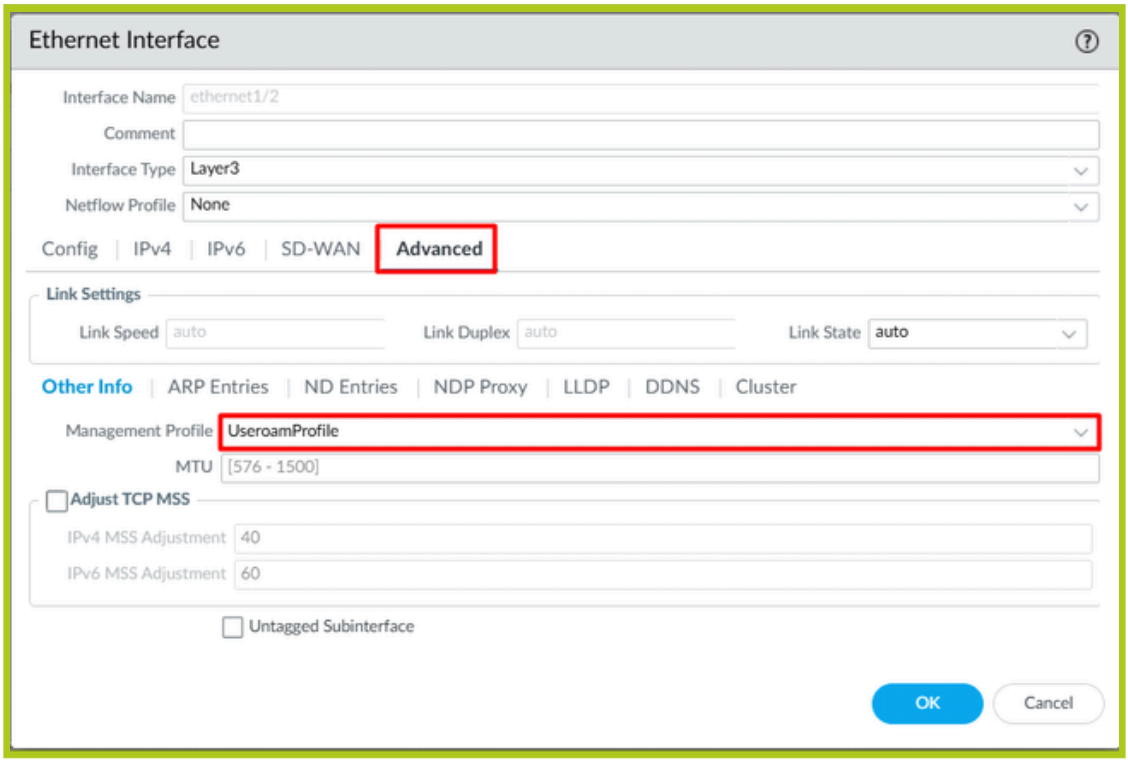
2 Zone Ayarları

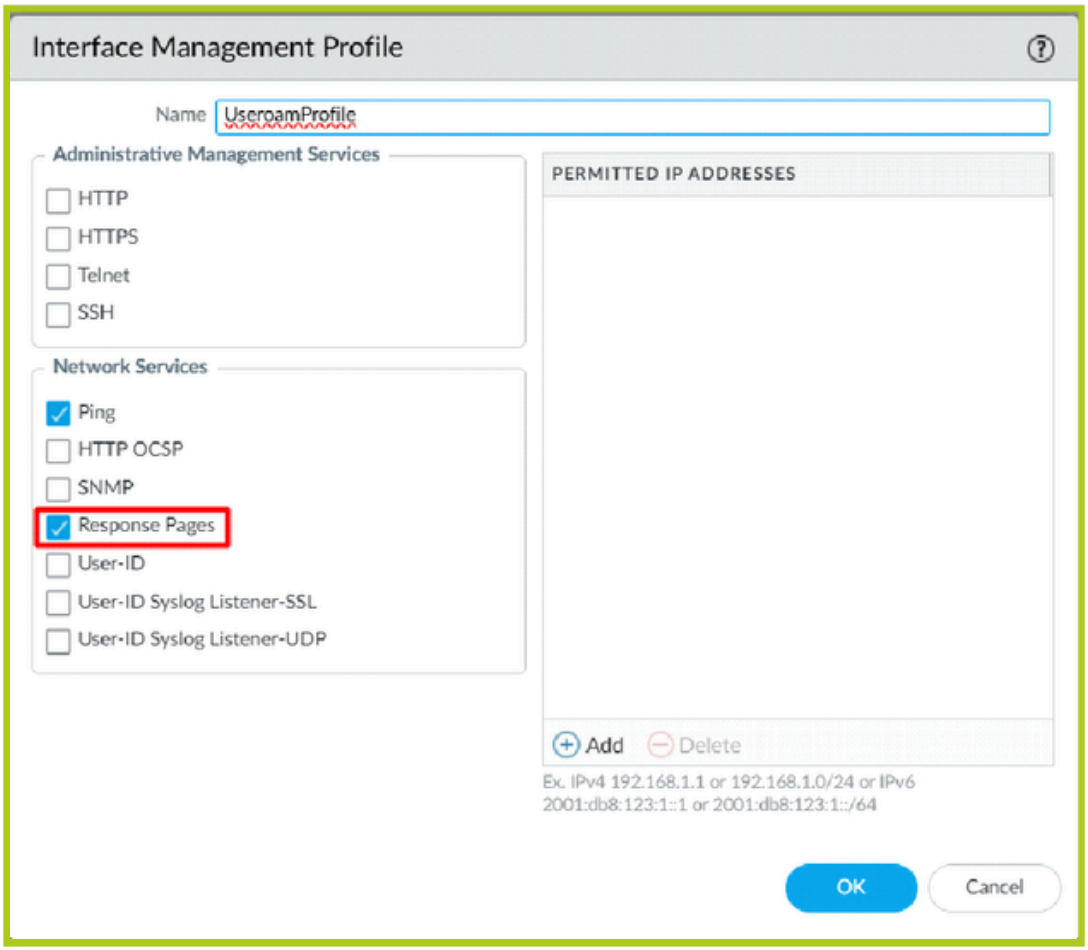
Useroam’u aktif edeceğimiz interface için **Network / Zone** menüsünden yeni bir zone oluşturup, “Enable User Identification” kutucuğunu seçiyoruz.



3 Interface ve Pro l Ayarları

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





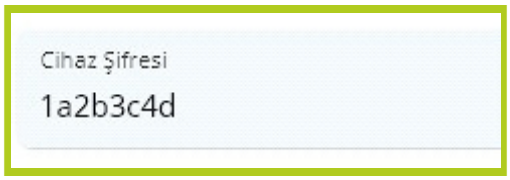
4 Radius Ayarları

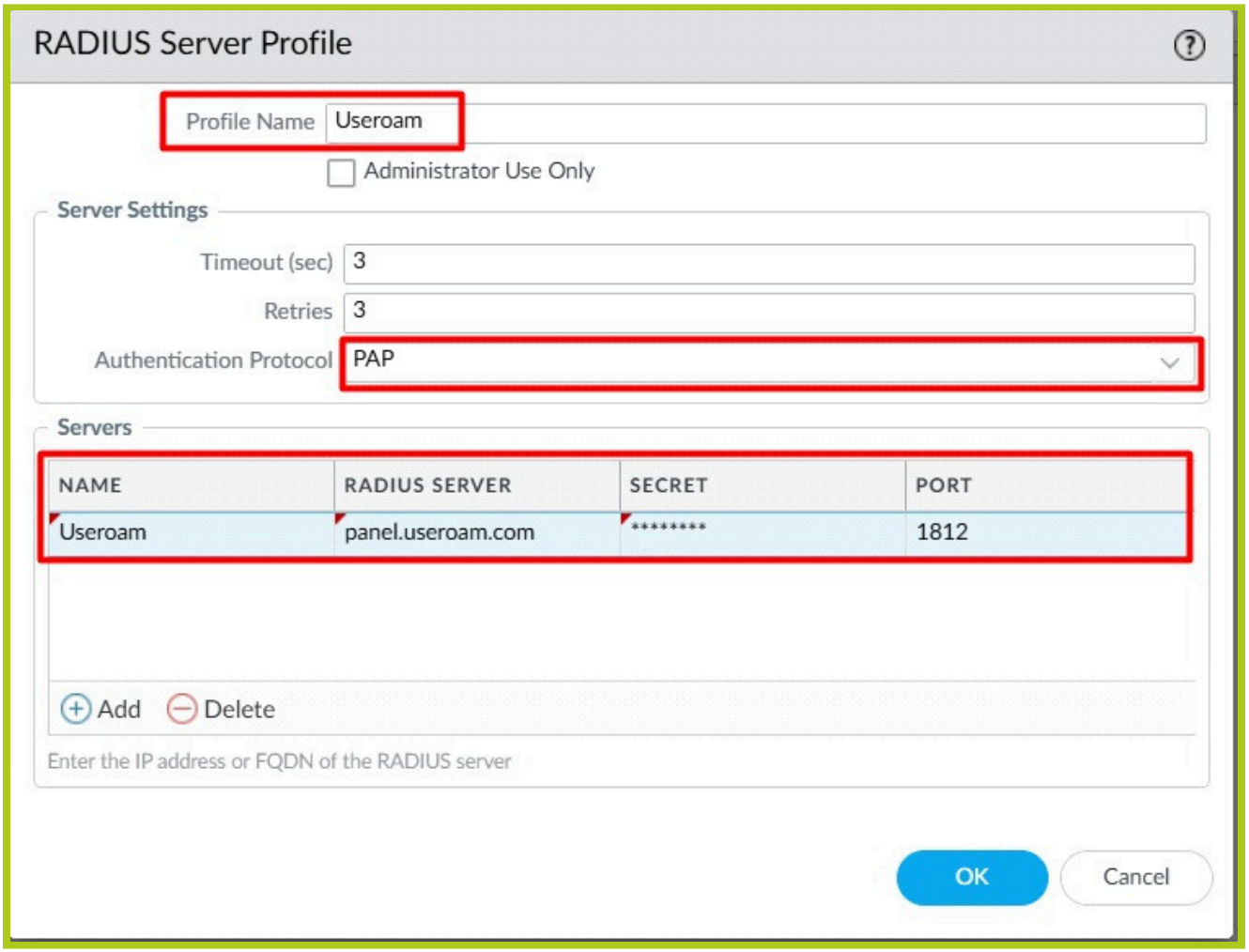
İlgili ayarları **Device \ Server Profiles \ Radius** menüsünden şu şekilde uyguluyoruz;

Authentication Portal : PAP

Radius Server : panel.useroam.com

Secret : Panel.useroam.com da **Sistem Ayarları / Cihaz Detaylarından** almış olduğunuz cihaz şifresi





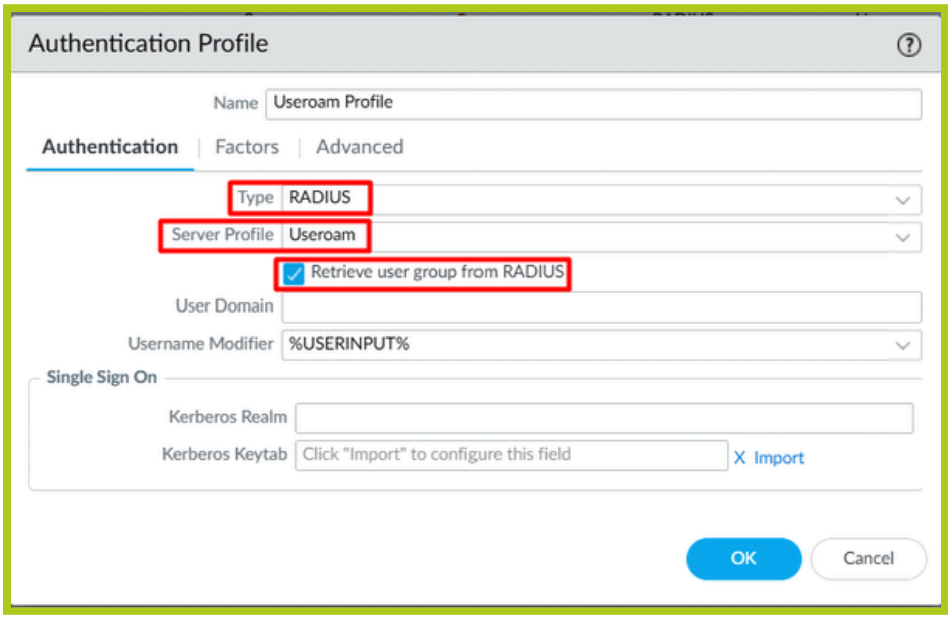
5 Authentication Profile ayarı

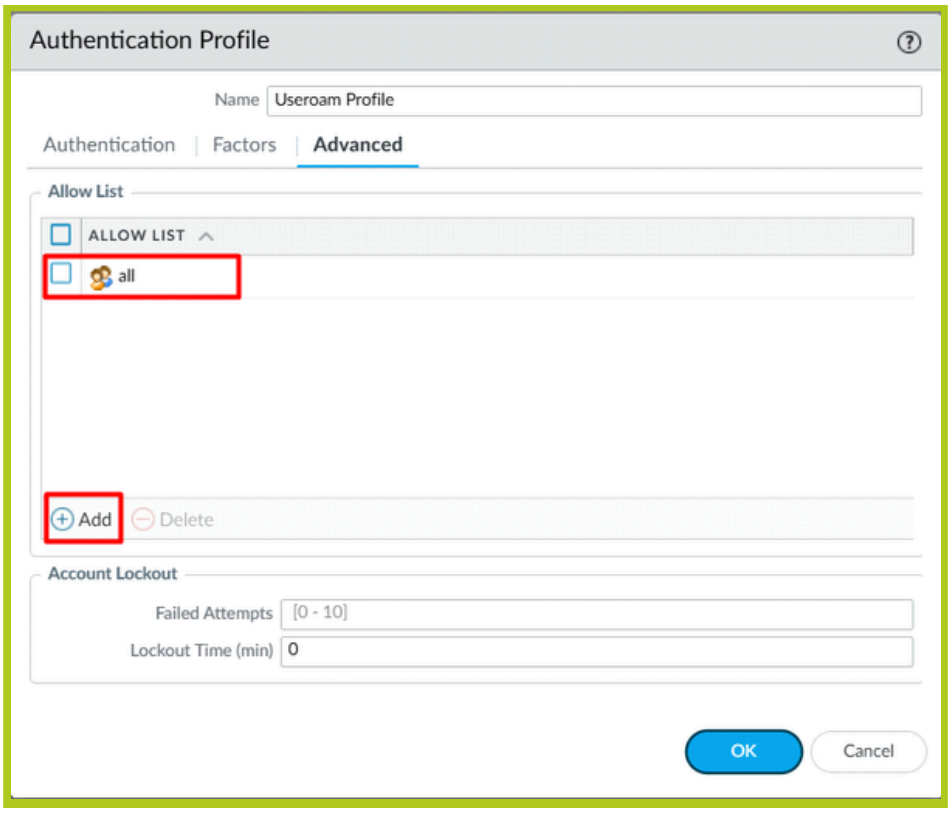
Device \ Authentication Profile menüsünden yeni profilimizi tanımlıyoruz.

Type: Radius

Server Profile :Oluşturmuş olduğumuz Radius Server Profilini seçiyoruz.

Retrieve user group from RADIUS kutucuğunu işaretleyerek, seçili olduğundan emin oluyoruz.
Advanced kısmında ise **Allow List**'e **all** ekliyoruz.

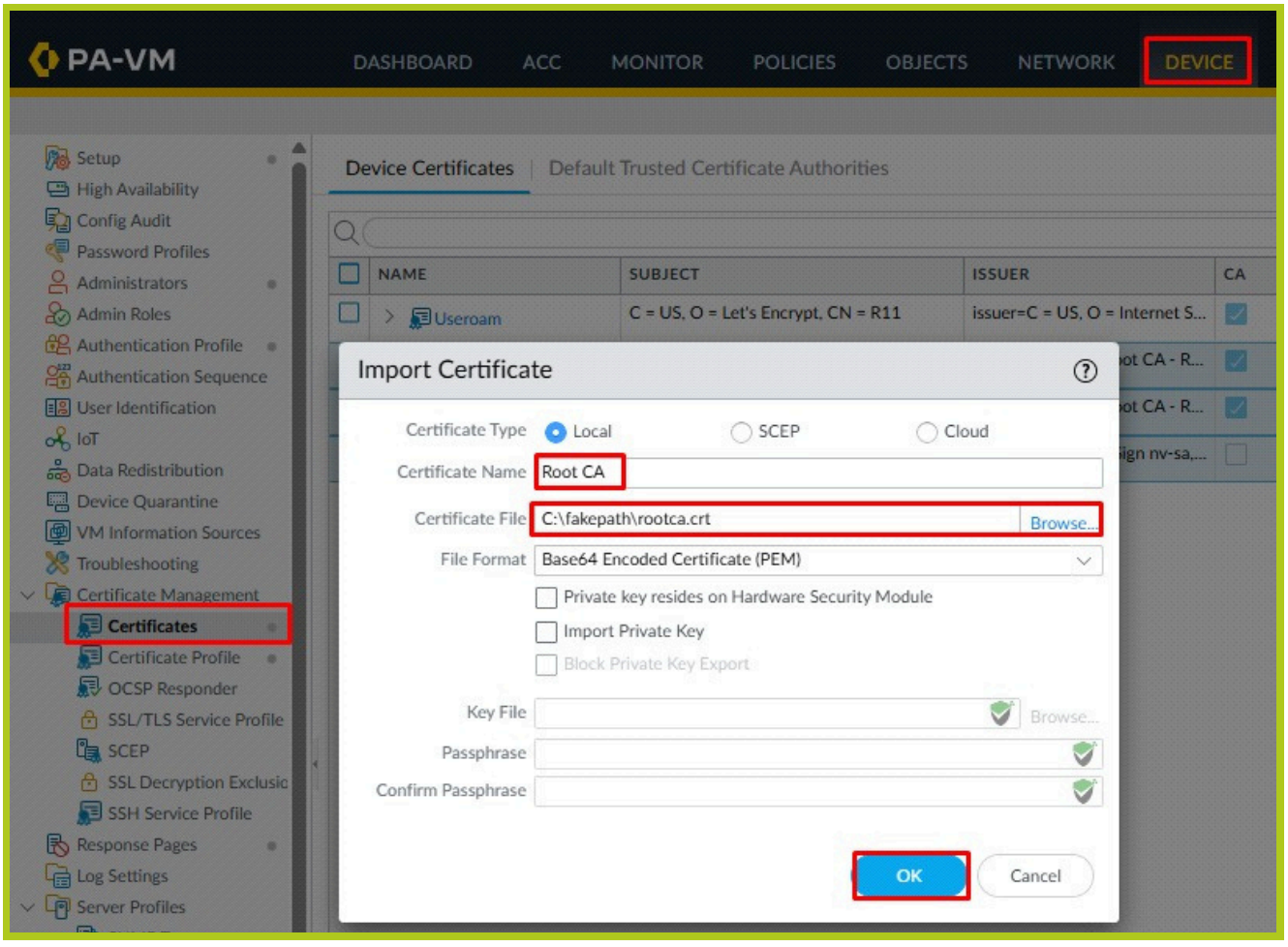




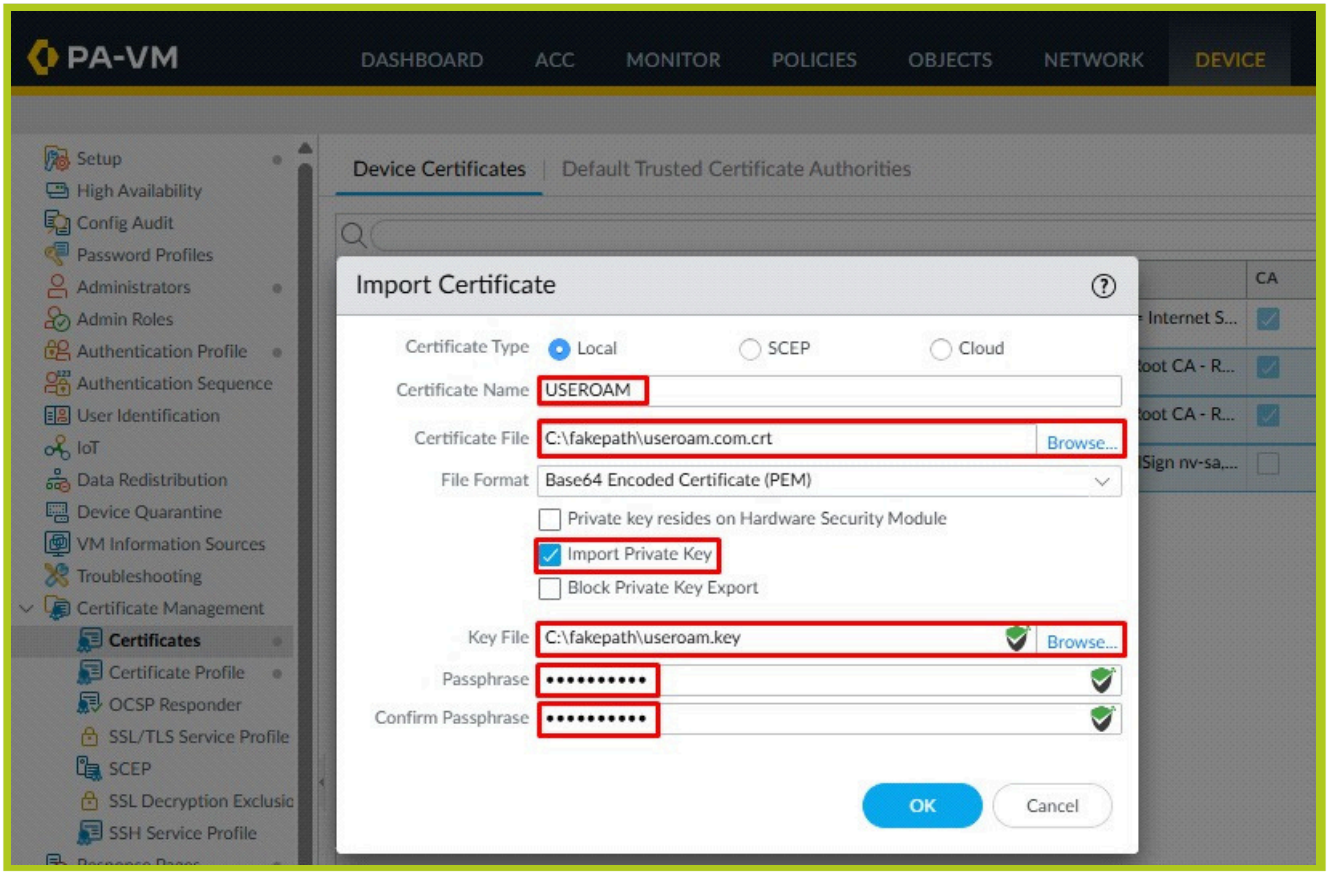
6 Sertifika ayarlarının yapılması

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. Bunun için aşağıdaki adımları takip edebilirsiniz.

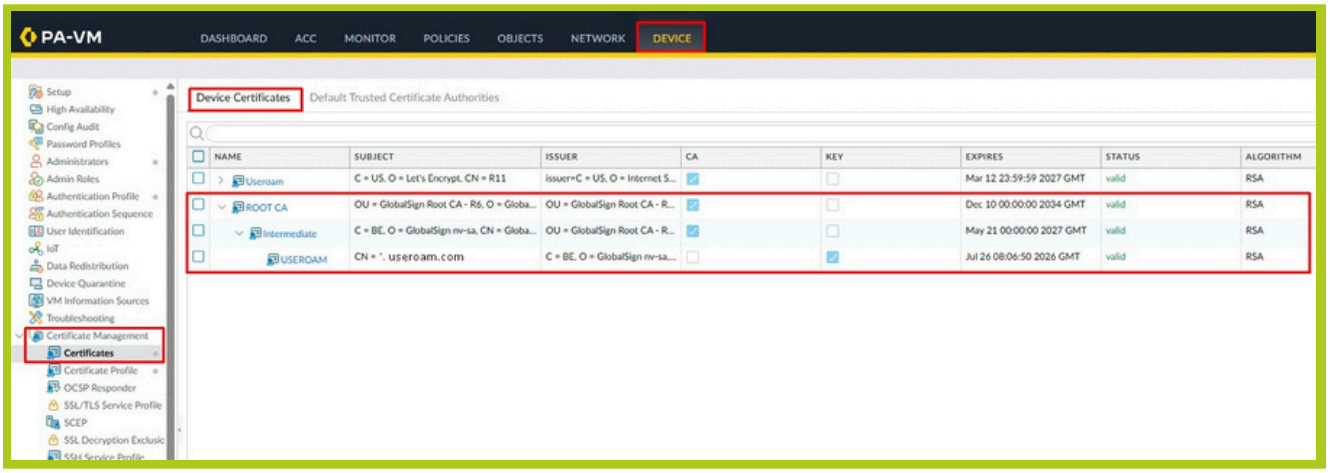
6a İlk adım olarak,**Root CA veya CA sertifikasını** import ediniz.



6b Sonraki adımda; sertifika dosyasını, anahtar dosyası ve şifreyle birlikte güvenlik duvarına yükleyiniz.

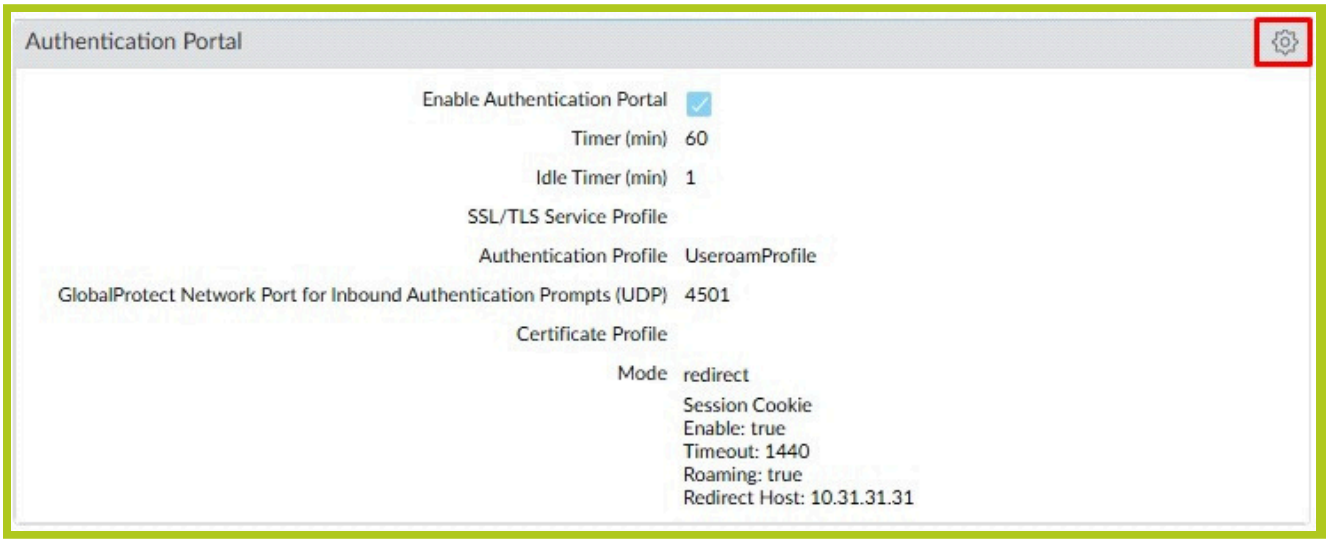


6c Yükleme işlemi tamamlandığında, karşımıza çıkan görüntü; katmanlı bir yapı şeklinde, birbirine bağlı bir sertifika zinciri şeklinde olmalıdır.



7 Authentication Portal ayarları

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

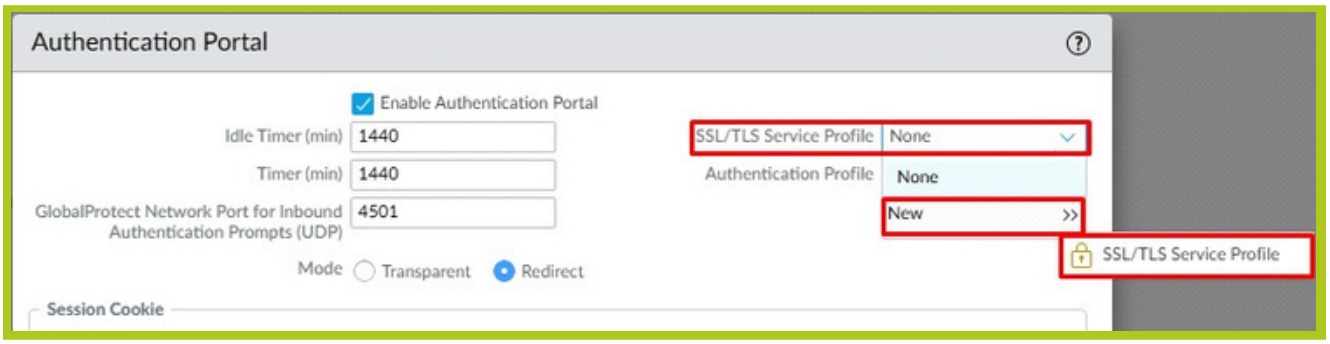


Enable Authentication Portal: Bu seçeneği işaretleyerek hotspotu aktif hale getiriniz.

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 Profile: Bu alandan, daha önce oluşturulan SSL profilini seçiniz. Ancak burada şuna dikkat etmeniz gerekmektedir: Palo Alto'nun bazı sürümlerinde, önceden oluşturulmuş profiller bu alanda görünmeyebilir. Bu durumda, "New" seçeneği ile bu ekrandan yeni bir SSL/TLS profili oluşturularak işlem tamamlanmalıdır.

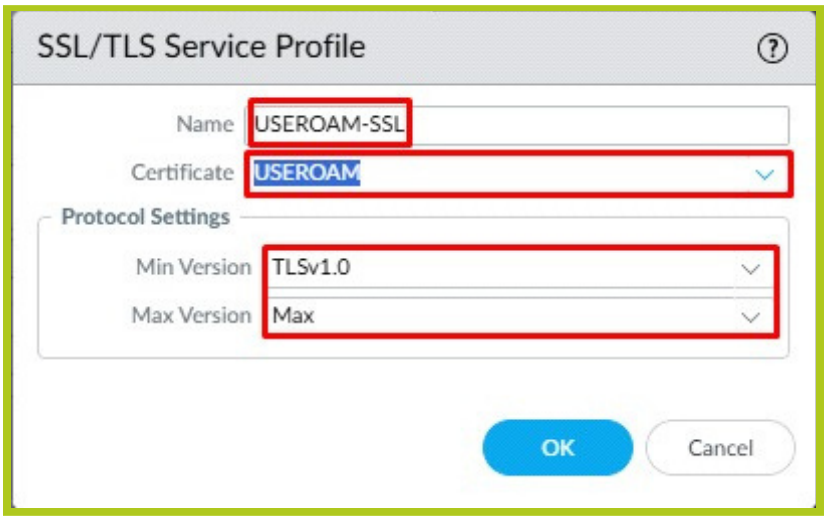
Eğer sisteminizde seçim yapılabiliyorsa, önceden oluşturulmuş profil kullanılabilir.

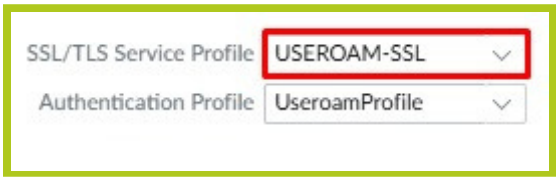


Yeni bir pro□l oluşturmanız gerekiyorsa aşağıdaki adımları izleyiniz.

- Pro□le bir isim vererek, kullanılacak SSL serti□kasını seçiniz.
- Protocol Settings bölümünden, çalışması istenen minimum ve maksimum SSL/TLS versiyon değerlerini seçiniz.
- Ayarlar tamamlandıktan sonra OK butonuna tıklanarak pro□l kaydediniz.

Bu işlemlerin ardından, oluşturulan yeni pro□l sistem tarafından otomatik olarak seçilmiş şekilde görünecektir.

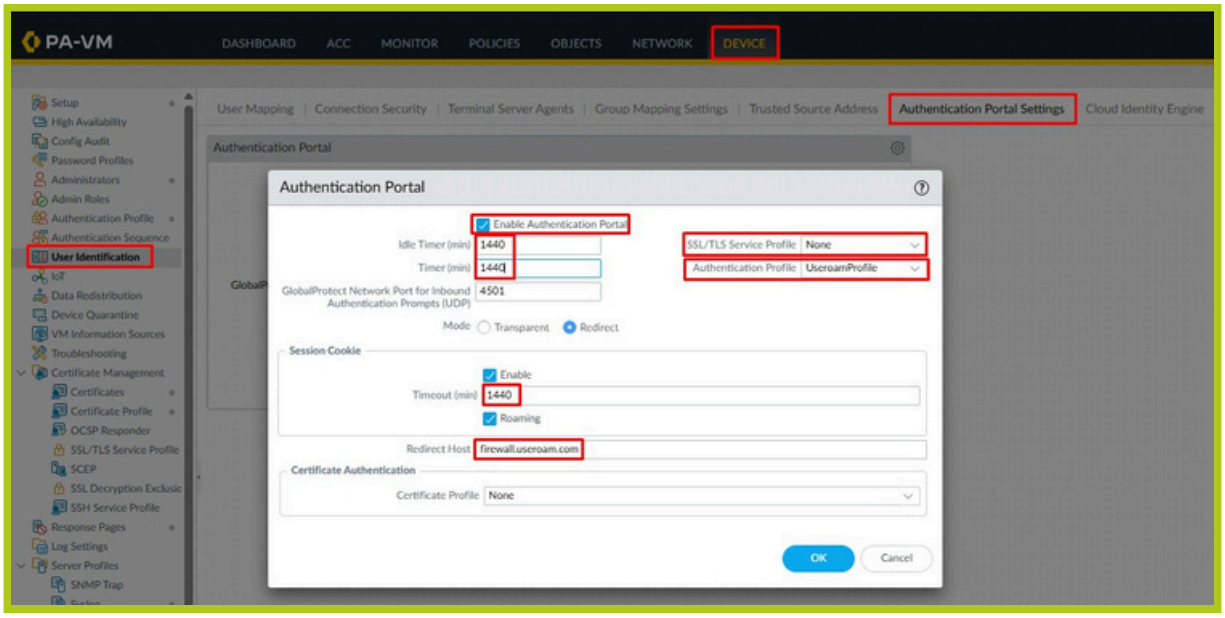




Authentication Pro□le : Oluşturulan Useroam pro□lini seçerek devam ediniz.

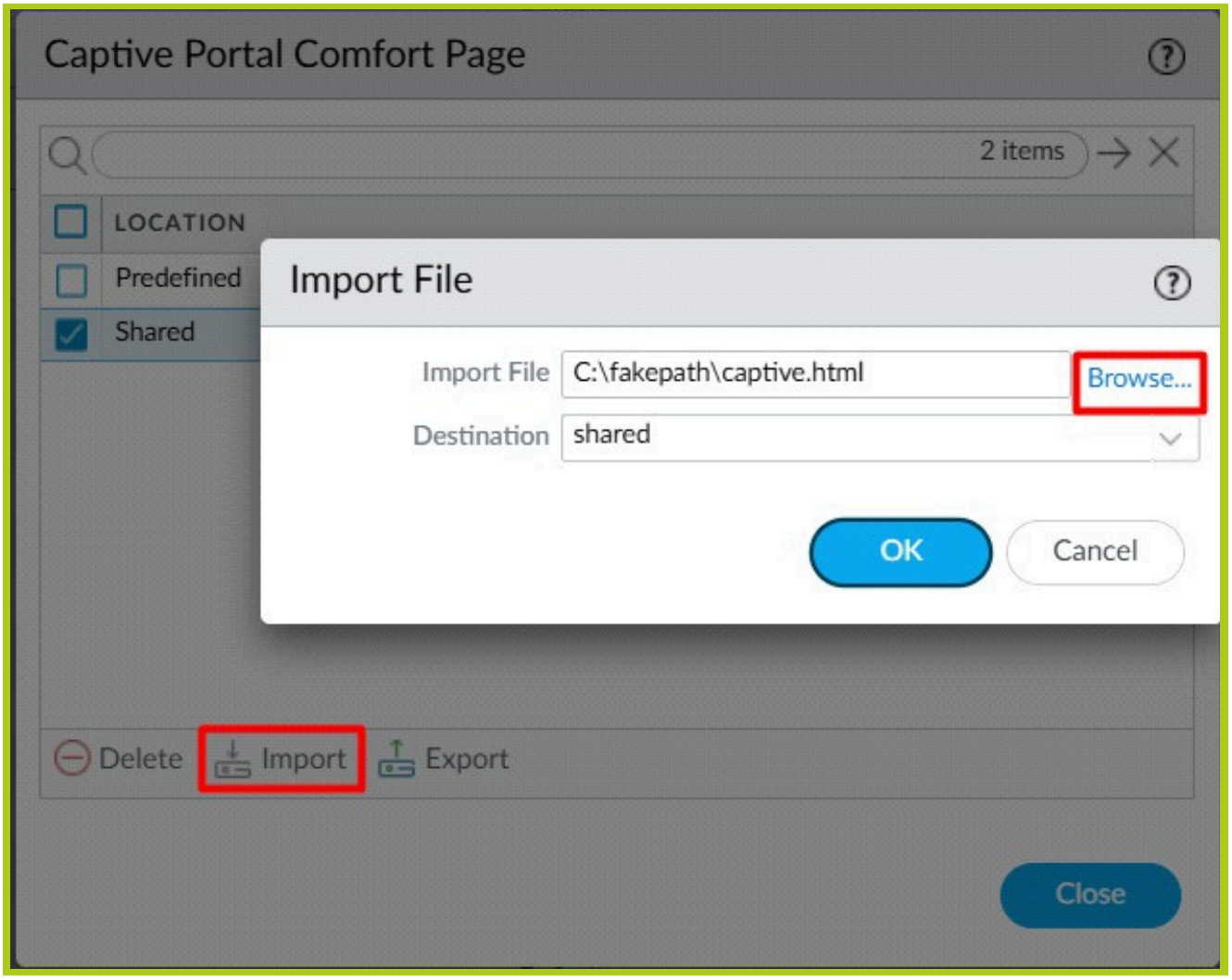
Session Cookie / Timeout : Bu alanda da daha önce belirlediğimiz gibi **1440 dakika (24 saat)** değerini girerek oturum süresini tanımlayınız.

Redirect Host : Buraya serti□ka üzerinden yönlendirme yapılacağı için subdomaini giriniz.



8 Captive Portal Ayarları

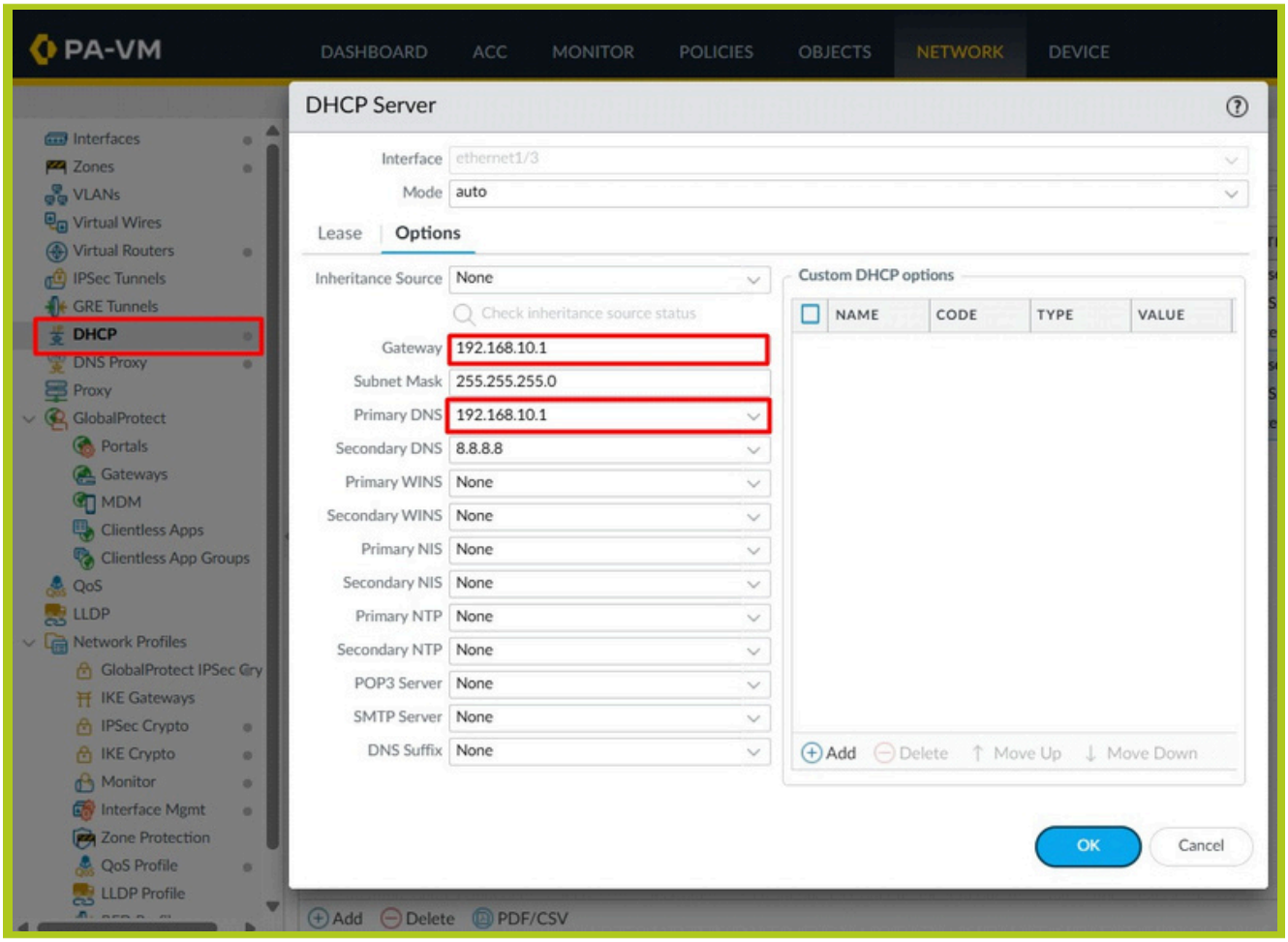
Panel.useroam.com dan **Sistem Ayarları / Cihaz Detayları**'nda bulunan **<html>**olarak başlayan kod satırının hepsini kopyalayıp, not defteri veya benzeri bir uygulamaya yapıştırıp, ilgili kodu **"captive.html"** gibi bir isimle, html formatında olacak şekilde, kaydedip sonrasında, rewall'da **Device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



9 **DHCP Ayarları** (İçerde bir DNS sunucunuz varsa static entries kısmına gireceğiniz URL'yi orada tanımlayarak 11. Adımdan devam edebilirsiniz)

İç ağdan yapılacak DNS sorgularının sorunsuz şekilde işlenebilmesi için, eğer ayrı bir DNS sunucusu bulunmuyorsa, DHCP ve DNS Proxy kısmının aşağıdaki şekilde güncellenmesi gerekmektedir. Mevcutta bir DNS sunucunuz varsa alan adı yönlendirmesi için gerekli kaydı iç dns ağınızda da girebilirsiniz.

- **Network > DHCP > Options** menüsüne gidilir.
- **Primary DNS** alanına, firewall cihazının **kendi IP adresi** yazılır.
- **Secondary DNS** olarak ise global bir DNS sunucusu tanımlanabilir (örnek: 8.8.8.8 – Google DNS).



10 **DNS Ayarları**

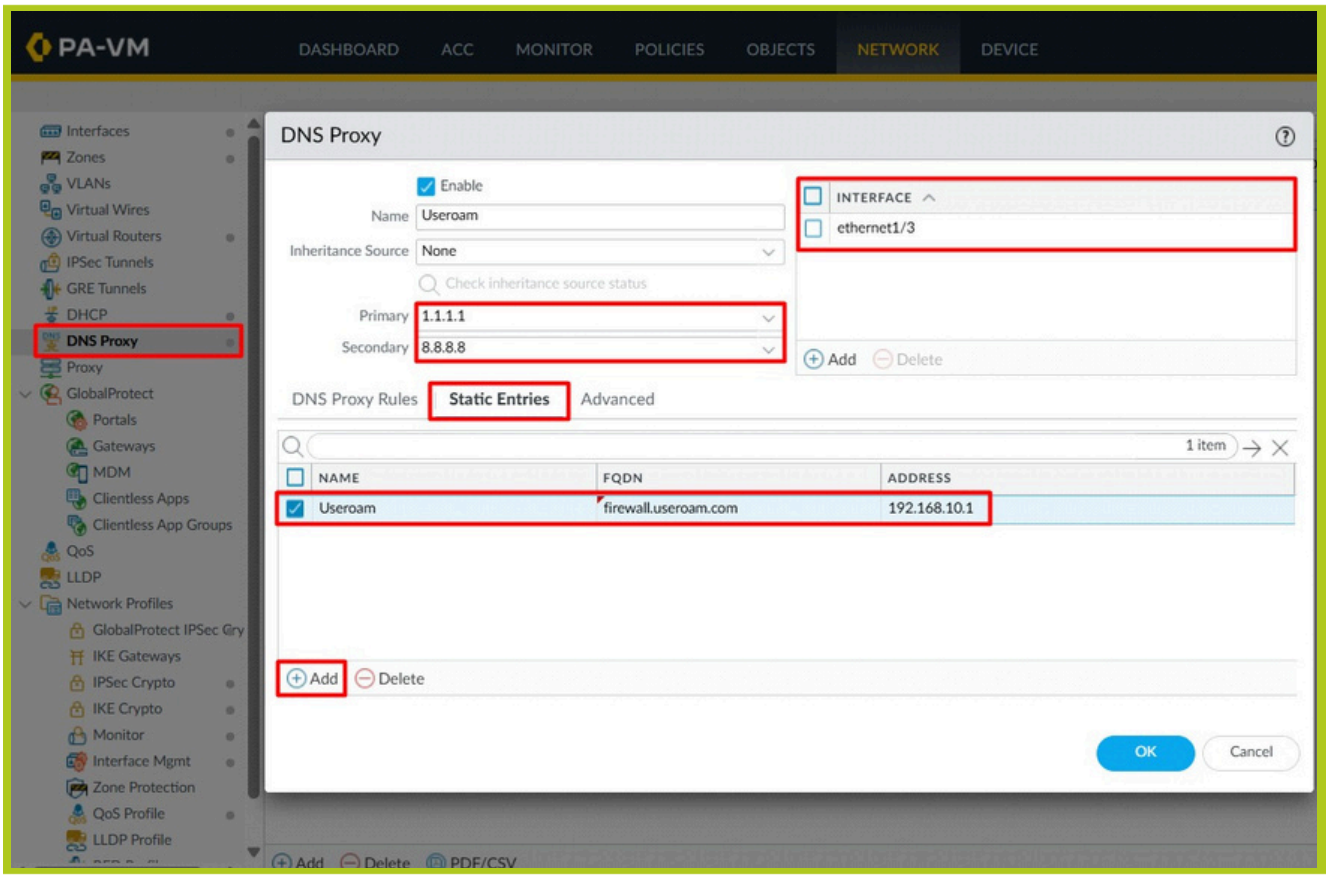
Ardından DNS sorgularının doğru şekilde çözümlenebilmesi için yeni bir proxy tanımlanır. İşlem adımları aşağıdaki gibidir: **Network > DNS Proxy** menüsünden

Name: Pro□le bir isim veriniz.

Primary / Secondary DNS: Global DNS sunucuları giriniz.

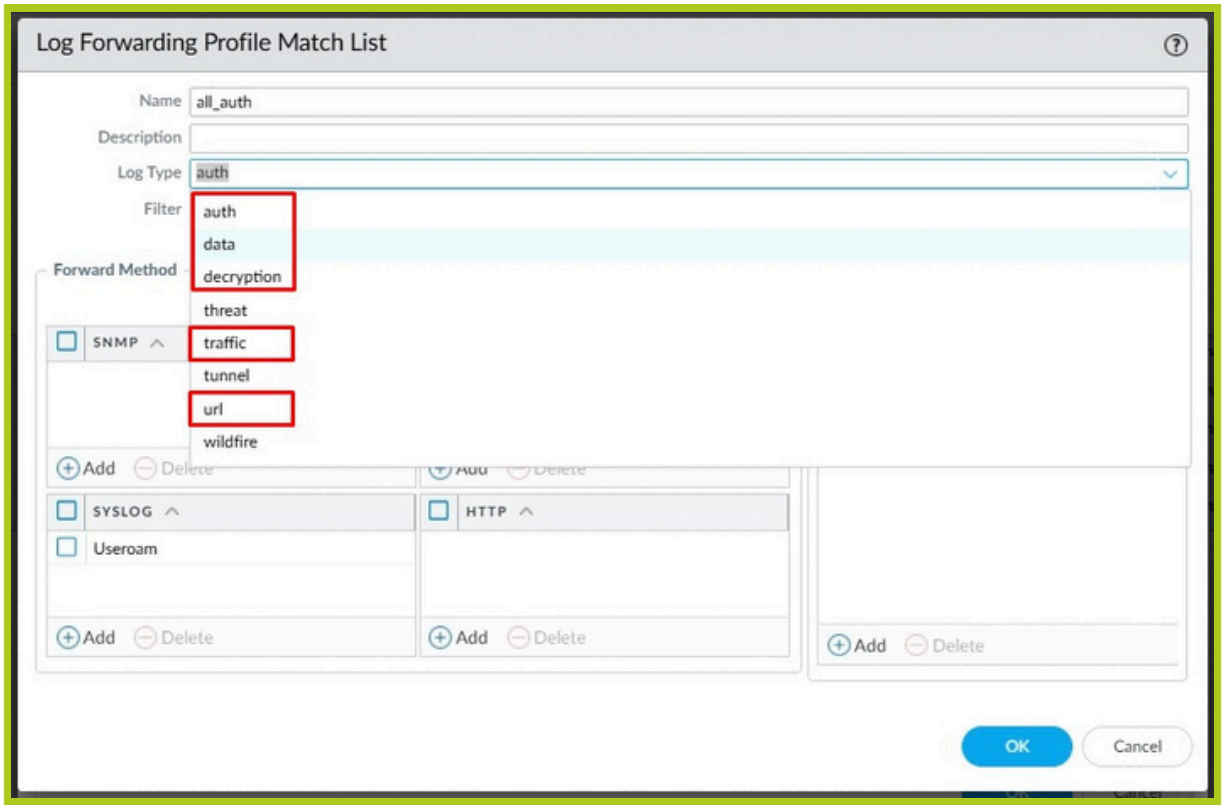
Interface: Bu kısımda Useroam'un aktif olacağı interface veya intefaceleri seçiniz.

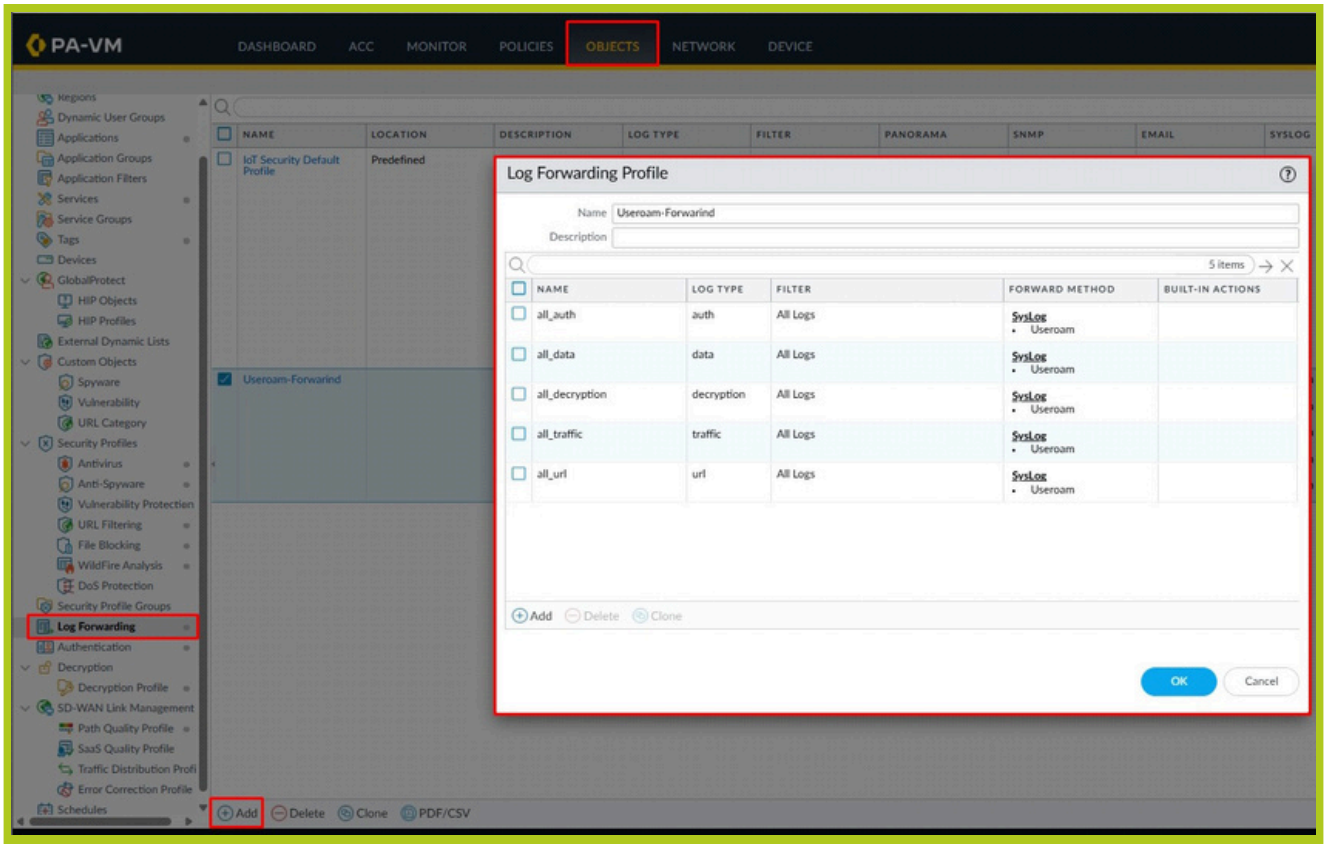
Static Entries: Burada **Add** butonuna tıklanarak yeni bir kayıt oluşturunuz. Bu aşamada, yönlendirme yapılacak **IP'nin, □rewall cihazının Management Interface nin gateway IP adresi** olması önemlidir. Ok butonuna tıklanarak işlemi tamamlayınız.



11 LOGLARIN USEROAM'A YÖNLENDİRİLMESİ

OBJECTS > Log Forwarding kısmından **Add** ileyeniprol oluşturunuz. 5 farklı log tipi için ayrı ayrı prolideeklemeyapınız.Buradahereklemede **Syslog** kısmında **Useroam** prolini seçmeniz gerekmektedir.



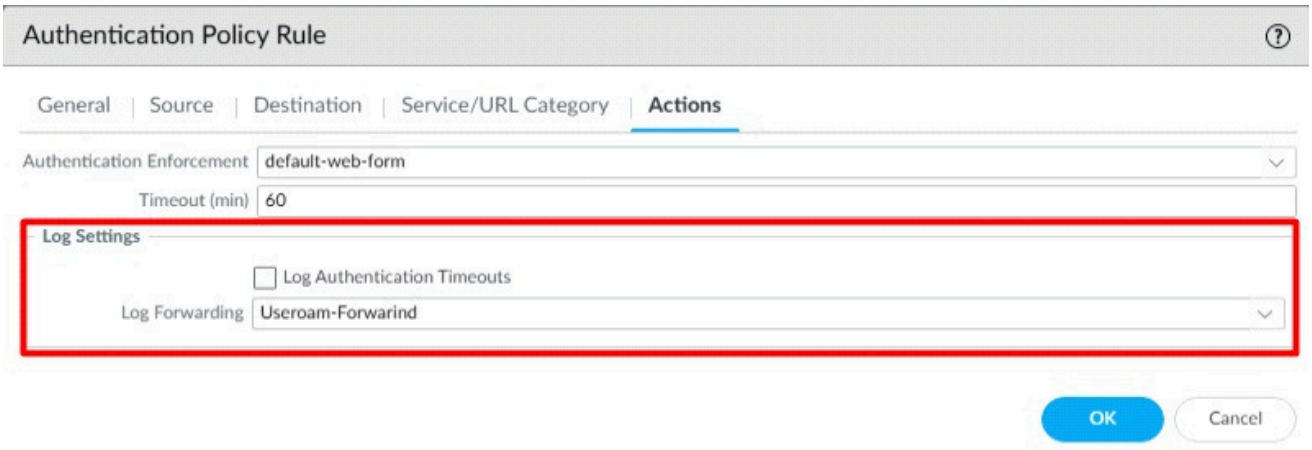


12 FIREWALL KURALLARININ OLUŞTURULMASI

Palo Alto Firewall entegrasyonunda iki grup kural oluşturulması gerekmektedir. Bunun için ilk olarak **Policies > Authentication** menüsüne geliniz. Buradan iki kural oluşturacaksınız.

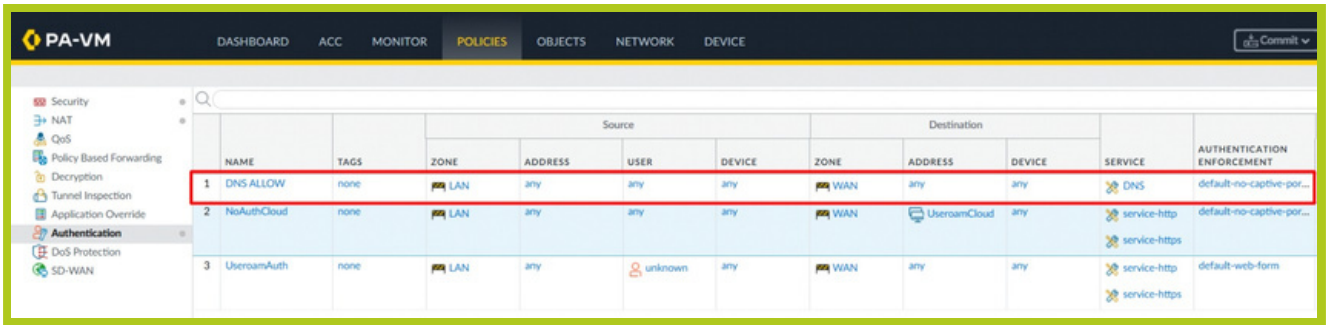
12a KURAL SETİ 1 (Authentication)

Kurallar ilk oluşturulurken Palo Altonun trafiği öğrenmesi gerekeceğinden **Service** kısmını **Any** olarak kullanıp sonra **application-default** olarak değiştirebilirsiniz. Tüm kurallarda **Log Forwarding** te **Useroam** seçili olmalı



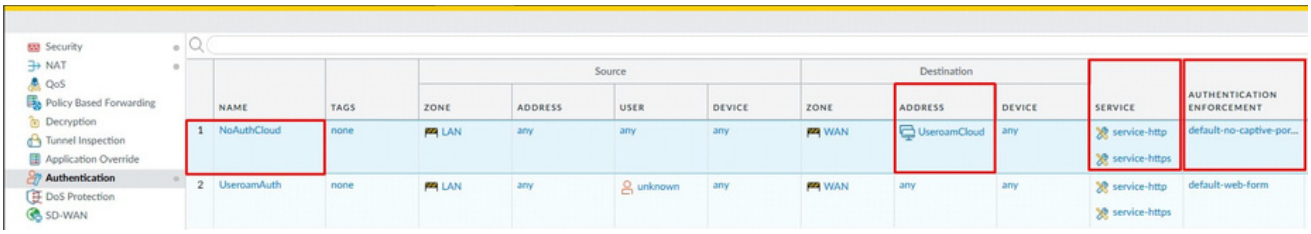
KURAL 1:

DNS sorgularının authentication dan sorunsuz geçebilmesi için bu kuralı oluşturuyoruz. WAN a doğru tüm DNS sorgularına **Authentication Enforcement** da **default-no-captive-portal** ı seçerek izin veriyoruz.



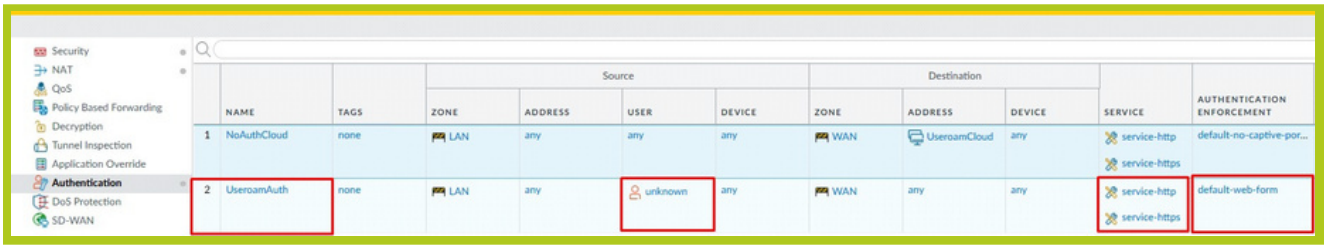
KURAL 2:

Bu kural sayesinde Useroam Cloud'a sorunsuz erişim sağlanacaktır. Destination Address'te oluşturduğunuz UseroamCloud (panel.useroam.com) adresini seçiniz.



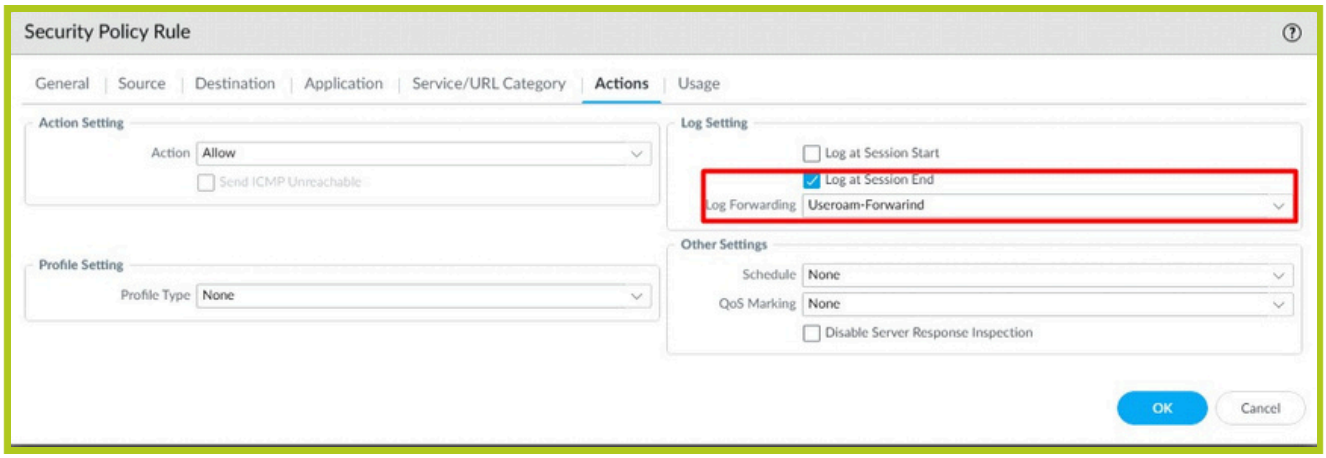
KURAL 3:

Captive de oturum açmamış veya ilk defa giren kullanıcıların http ve https tra□klerinde default-web-form yani captive portal 'a yönlenmesi için gerekli kuralımız



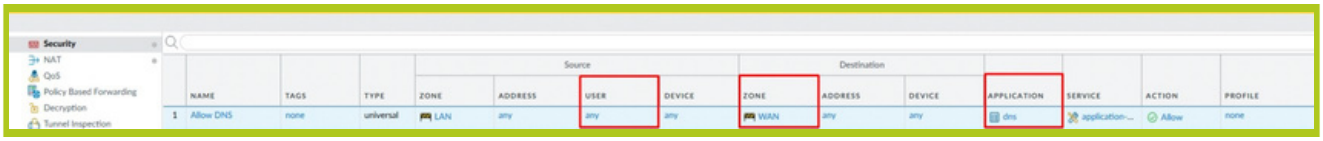
12b KURAL SETİ 2 (Security)

Bunun için **Policies > Security** menüsüne geliniz. Buradan üç kural oluşturacaksınız.
Kurallar ilk oluşturulurken Palo Altonun tra□ği öğrenmesi gerekeceğinden **Service** kısmını **Any** olarak kullanıp sonra **application-default** olarak değiştirebilirsiniz. Her kuralda **Log Settings** kısmında **"Log at Session End"** kısmı seçili olmalı ve **Log Forwarding** te **Useroam** seçili olmalı.



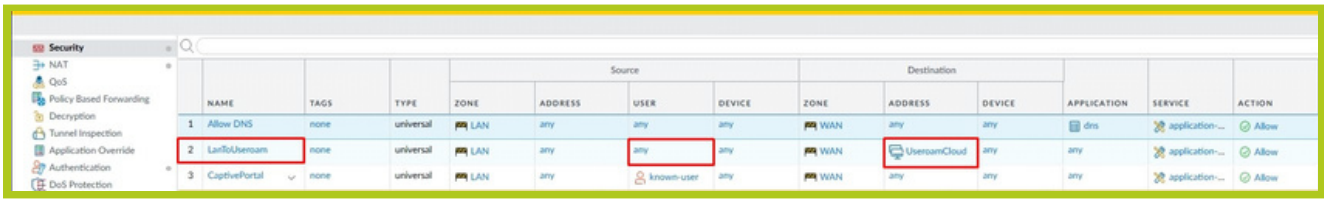
KURAL 1:

Bu kural, tüm cihazların **Captive Portal**'a takılmadan WAN üzerinden DNS sorguları gerçekleştirebilmesini sağlar. Bu kural, bağlanan cihazın kendi global captive alan adına erişip (örnek; captive.apple.com), bağlandığı ağda internetin gerçekten olduğunu anlayıp firewall hotspot yönlendirmesine erişmesini amaçlamaktadır.



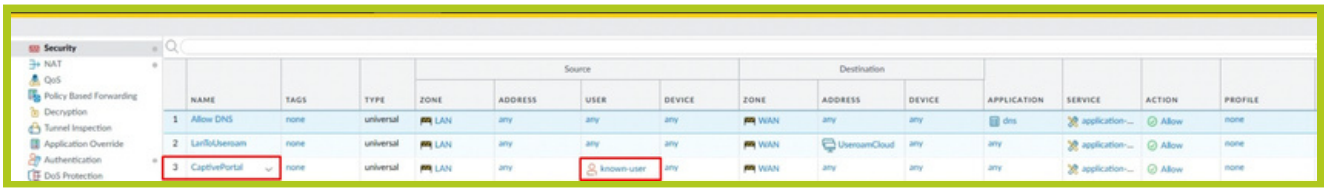
KURAL 2:

Bu kural Captive Portal Zone'undaki cihazların panel.useroam.com'a sorunsuz erişmesi için gereklidir.



KURAL 3:

Bu kural misafir ağınızın internete çıkışını sağlar. Burada **Source** kısmında **Source User'ı known-user** olarak seçerek, son kuralı da oluşturunuz.



Ek Bilgi :

Giriş yapmış kullanıcıyı düşürmek için CLI girişi yapılır.

show user ip-user-mapping all

bu komut size giriş yapmış tüm kullanıcıları verir. Buradan alınan IP adresi aşağıdaki kodlarla birlikte çalıştırılır.

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

Hepsi bu kadar!

Entegrasyon işleminiz tamamlandı.

İşlem sırasında bir sorun yaşarsanız destek@useroamteknoloji.com adresinden bizimle iletişime geçebilirsiniz.