Palo Alto Entegrasyon Rehberi

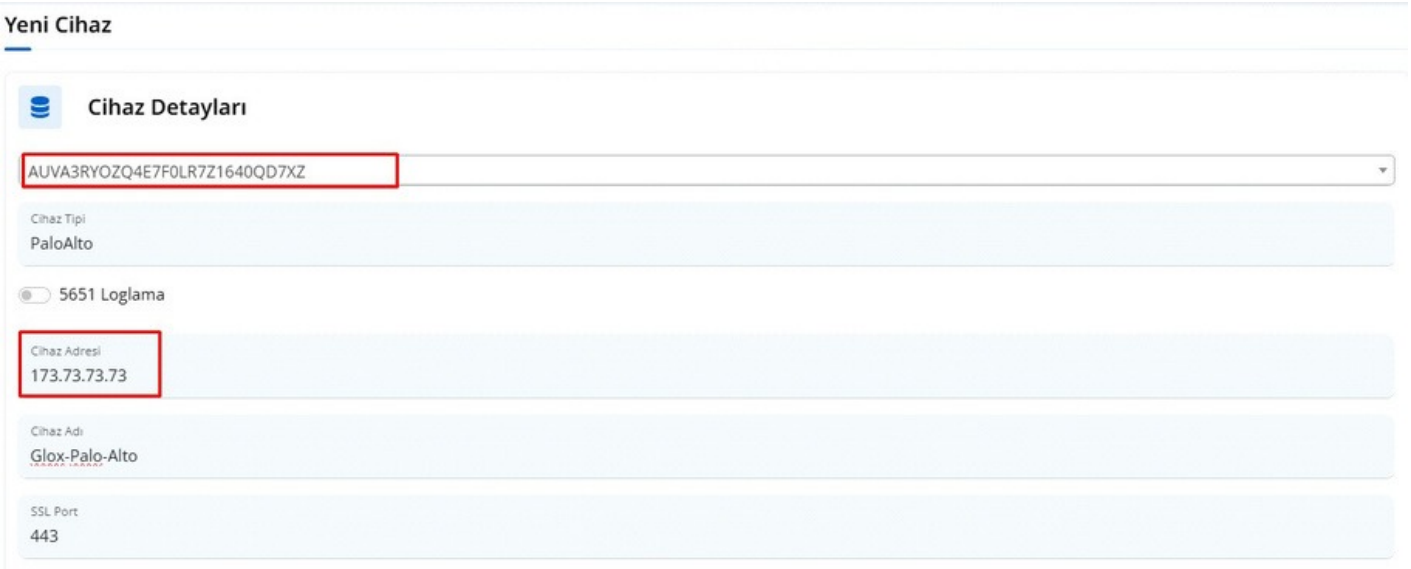
Bu rehber, bir **Palo Alto firewall** ile Useroam Cloud arasındaki entegrasyonun tamamını anlatır: zone ve interface yapılandırması, RADIUS kimlik doğrulama, sertifikalar, Authentication Portal, DNS, log yönlendirme ve firewall kuralları.

> **Başlamadan önce:** Palo Alto web arayüzüne yönetici erişimi, firewall'un Useroam ile konuşurken kullanacağı dış bacak IP adresi ve SSL sertifikanız ile anahtar dosyası ve parolası gerekir.

1 - Panele Güvenlik Duvarının Eklenmesi

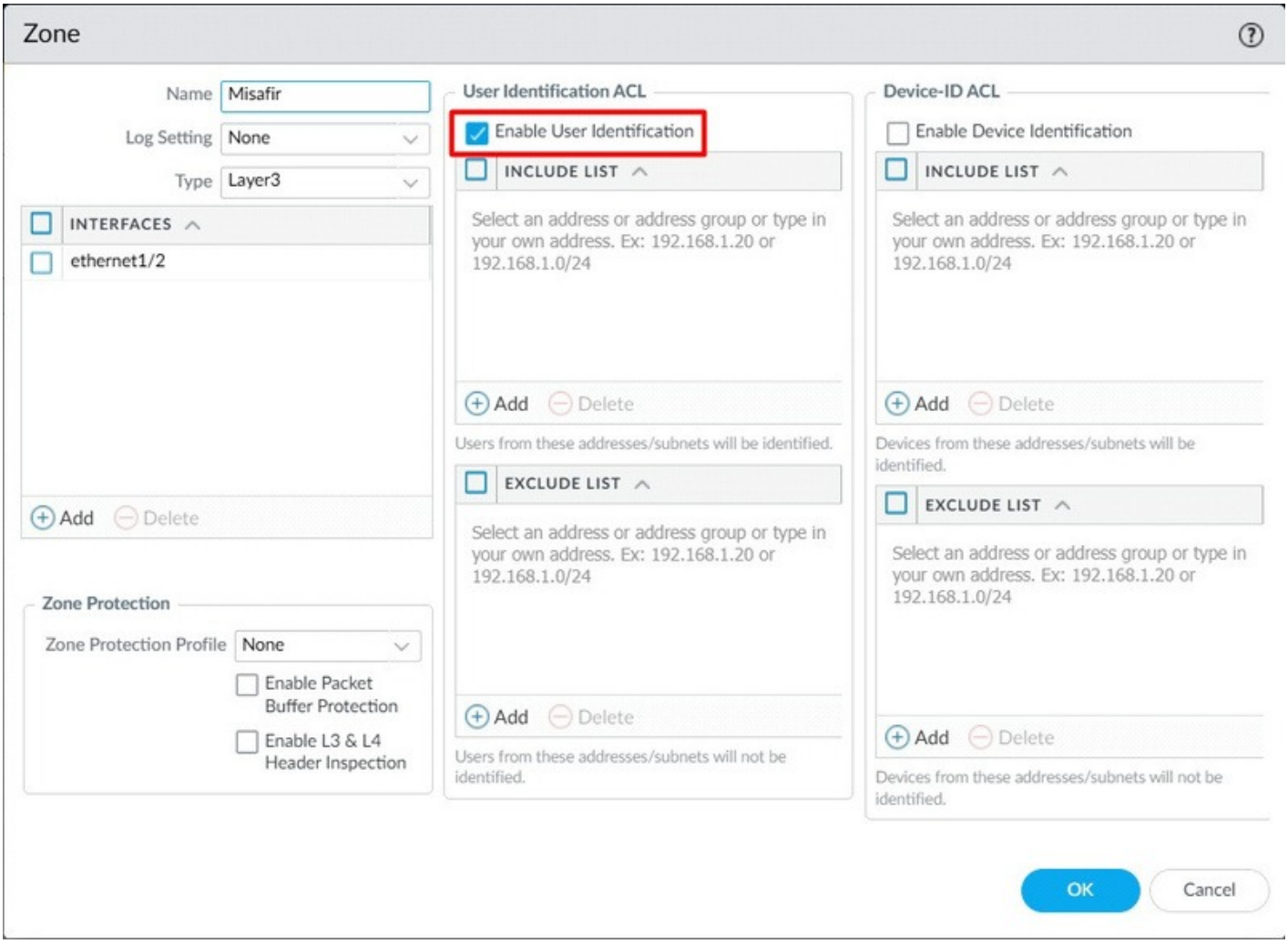
İlk olarak **panel.useroam.com** panelinize giriş yapıp **"Yeni Cihaz"** ekleyiniz. Cihaz Adresi kısmına firewall üzerinden hangi IP adresi ile iletişim kuracaksanız, ilgili dış bacak IP adresini giriniz.

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



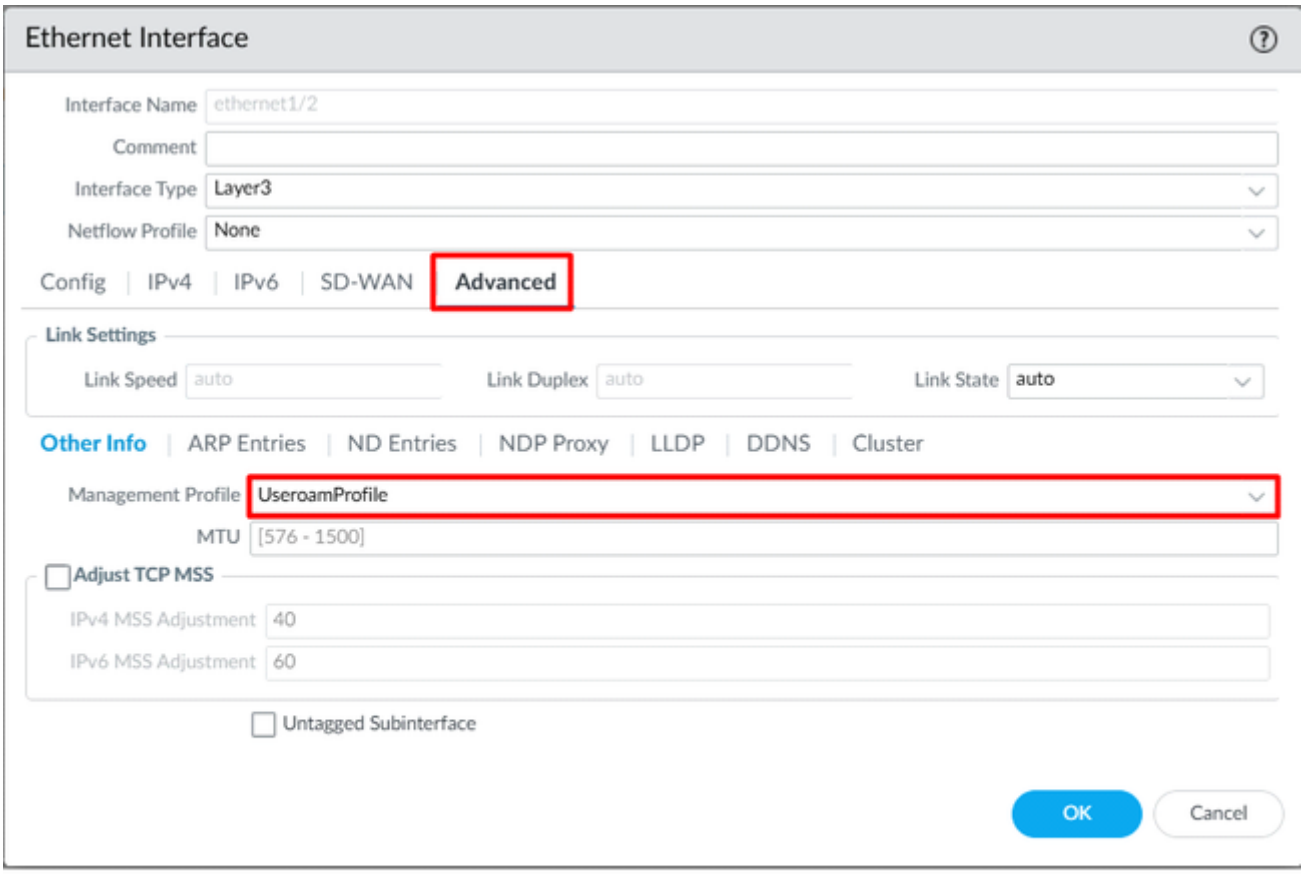
2 - Zone Ayarları

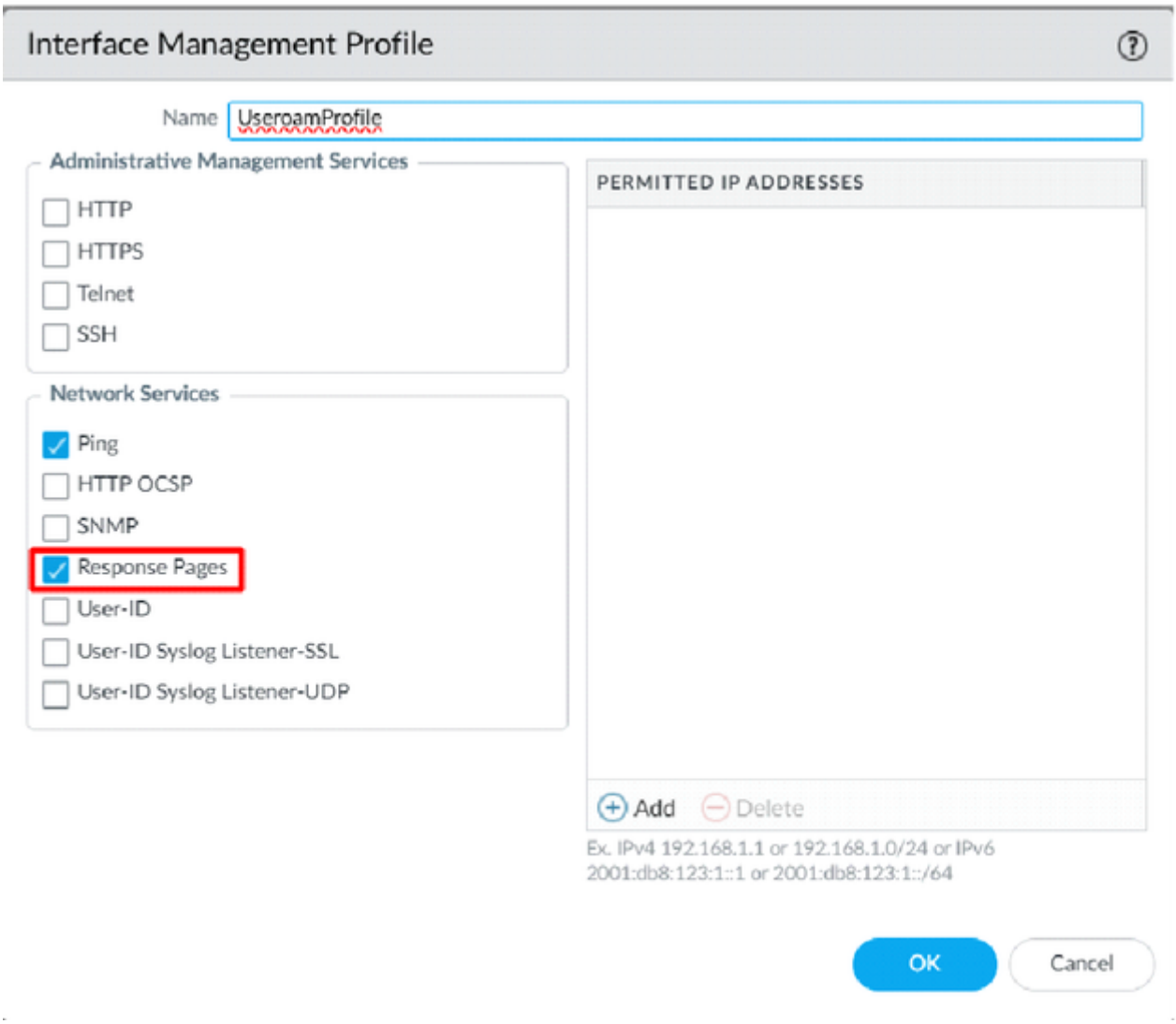
Useroam'u aktif edeceğimiz interface için **Network / Zone** menüsünden yeni bir zone oluşturup, **"Enable User Identification"** kutucuğunu seçiyoruz.



3 - Interface ve Profil Ayarları

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

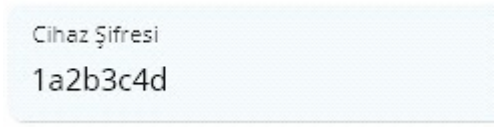

Ethernet Interface
Interface Name
ethernet1/2
Comment
Interface Type
Layer3
Netflow Profile
None
Config
IPv4
IPv6
SD-WAN
Advanced
Link Settings
Link Speed
auto
Link Duplex
auto
Link State
auto
Other Info
ARP Entries
ND Entries
NDP Proxy
LLDP
DDNS
Cluster
Management Profile
UseroamProfile
MTU
[576 - 1500]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

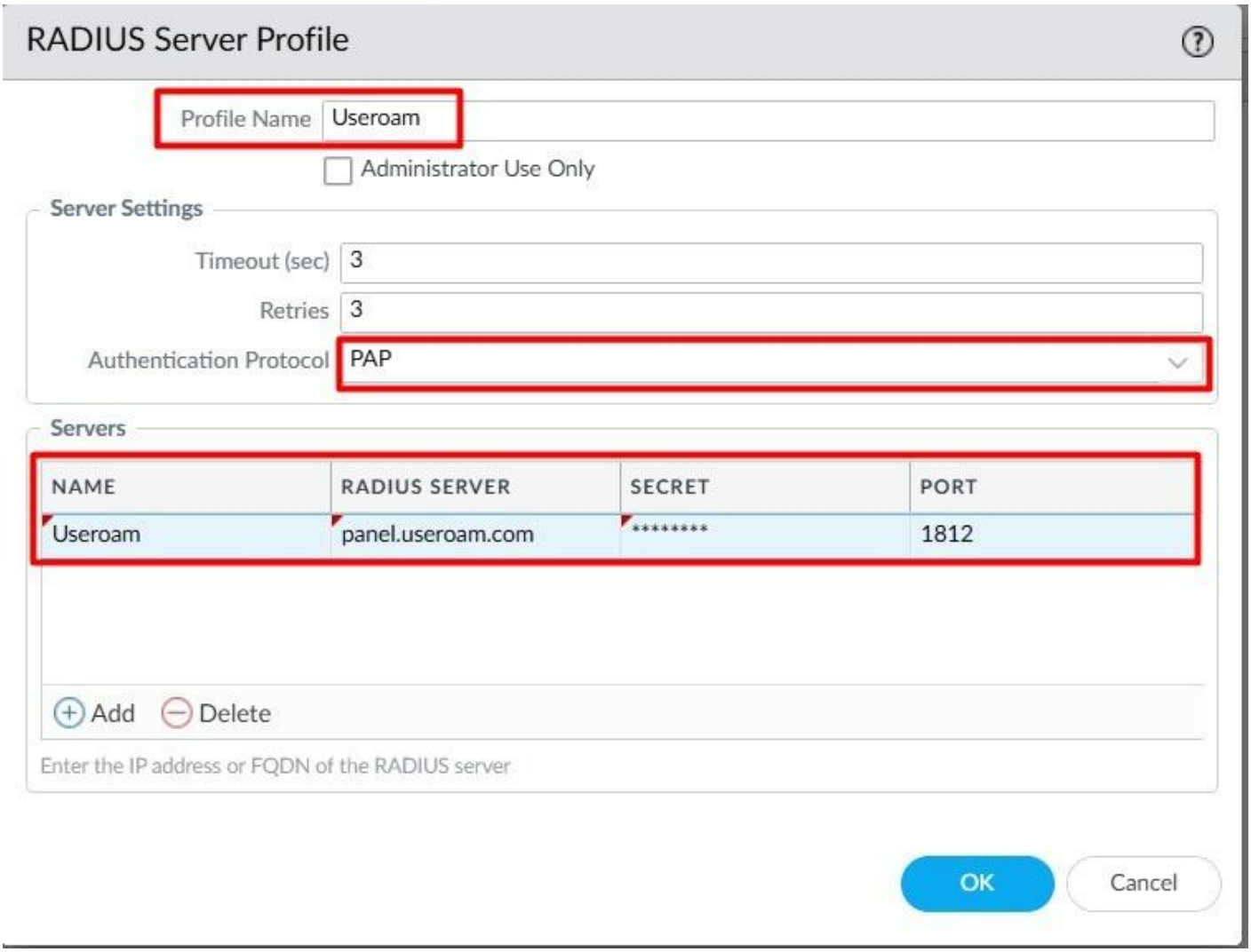

Interface Management Profile
Name
UseroamProfile
Administrative Management Services
HTTP
HTTPS
Telnet
SSH
Network Services
Ping
HTTP OCSP
SNMP
Response Pages
User-ID
User-ID Syslog Listener-SSL
User-ID Syslog Listener-UDP
PERMITTED IP ADDRESSES
Add
Delete
Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6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

4 - Radius Ayarları

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

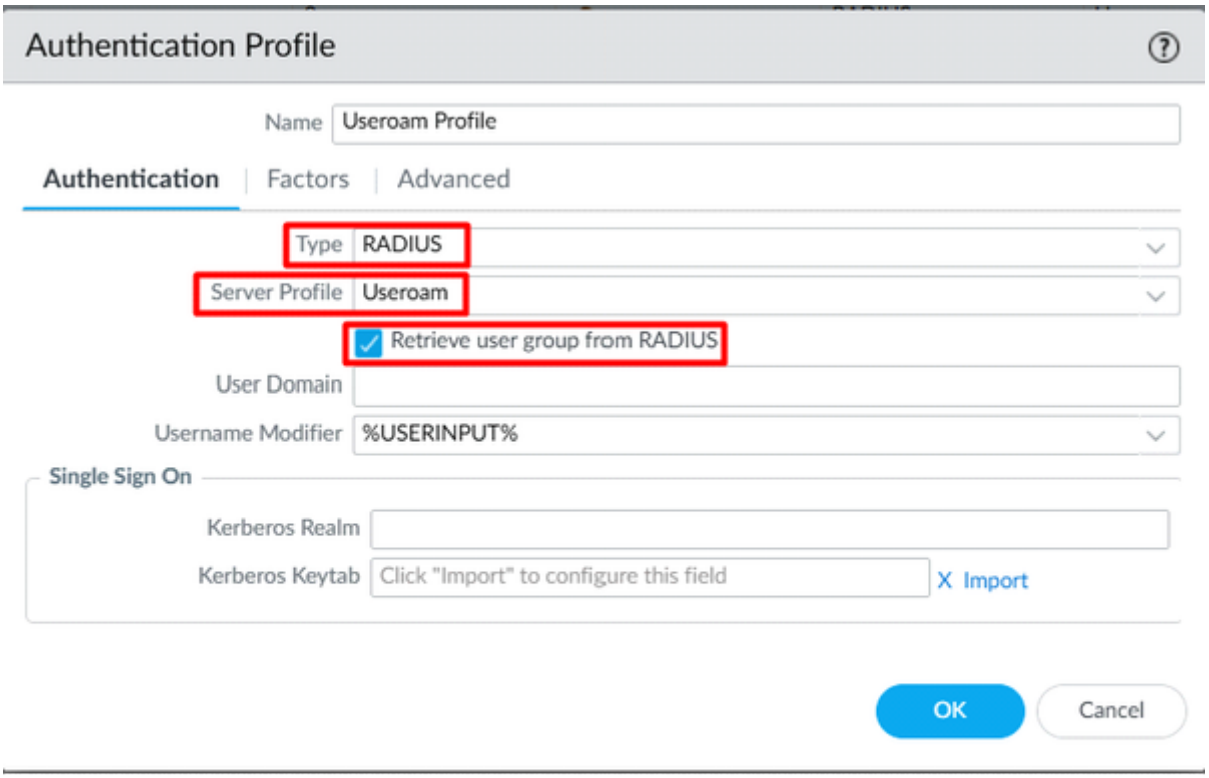


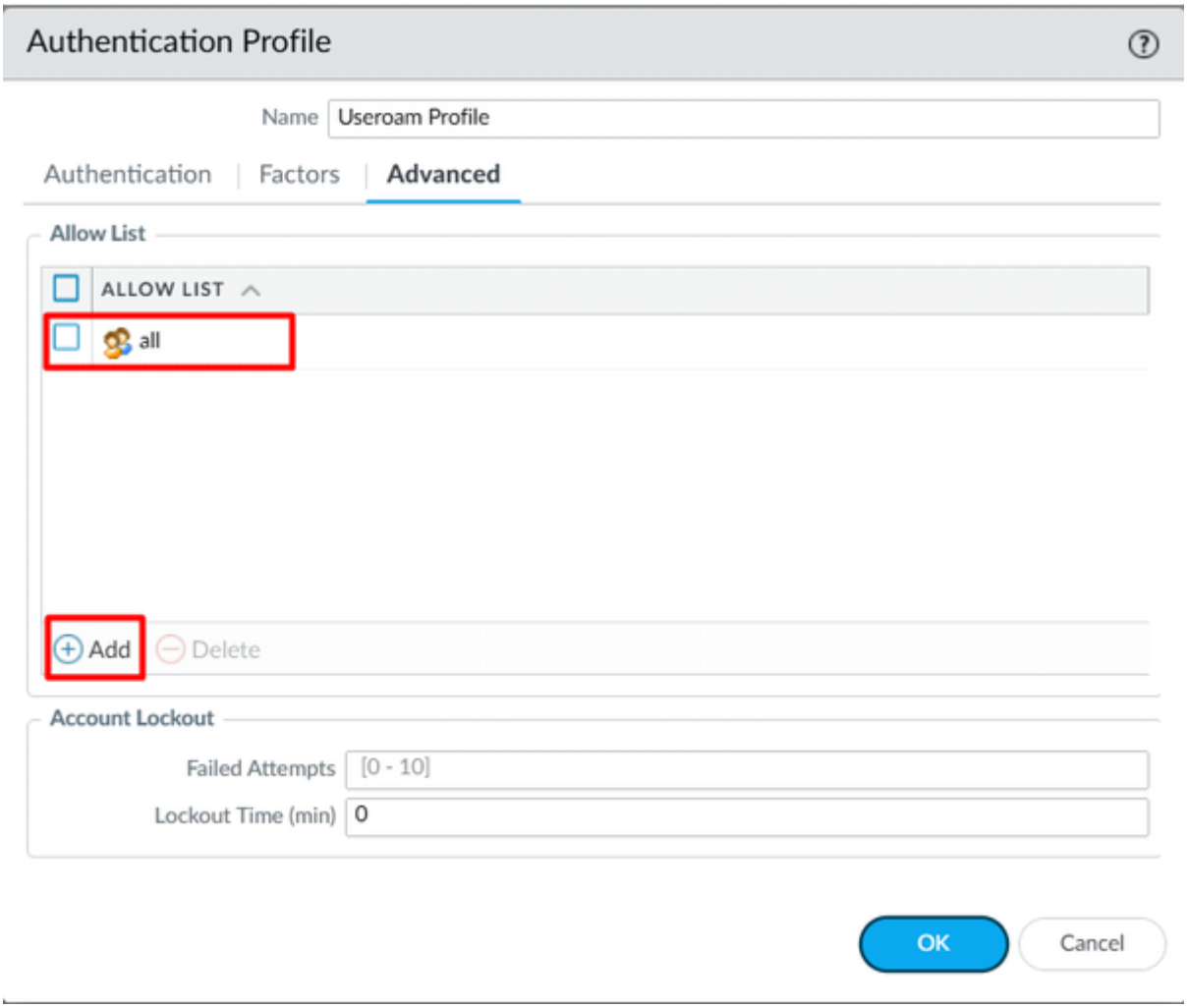


5 - Authentication Profile Ayarı

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.


Authentication Profile
Name
Useroam Profile
Authentication
Factors
Advanced
Type
RADIUS
Server Profile
Useroam
Retrieve user group from RADIUS
User Domain
Username Modifier
%USERINPUT%
Single Sign On
Kerberos Realm
Kerberos Keytab
Click "Import" to configure this field
X Import
OK
Cancel

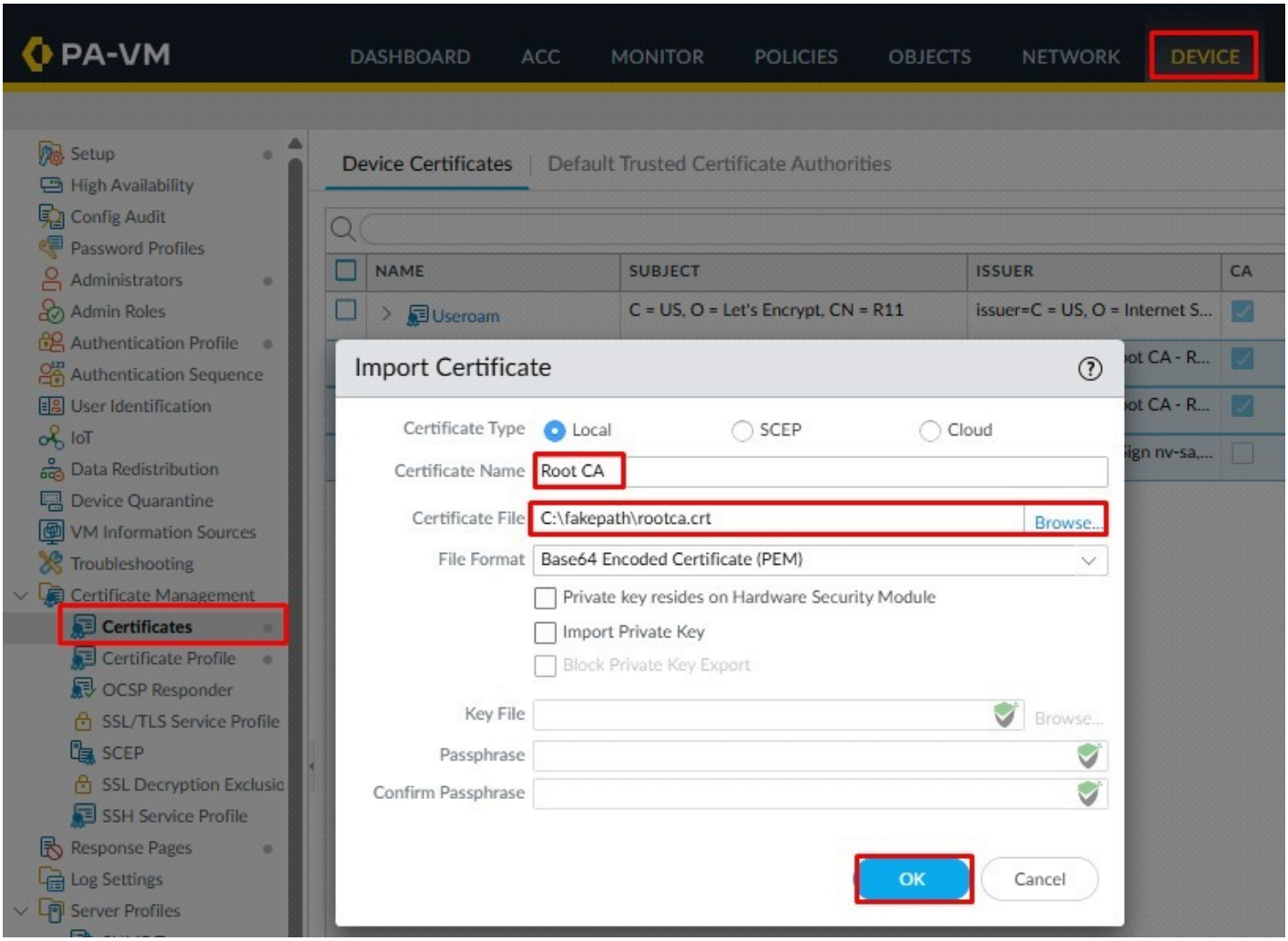

Authentication Profile
Name
Useroam Profile
Authentication
Factors
Advanced
Allow List
ALLOW LIST
all
Add
Delete
Account Lockout
Failed Attempts
[0 - 10]
Lockout Time (min)
0
OK
Cancel

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.

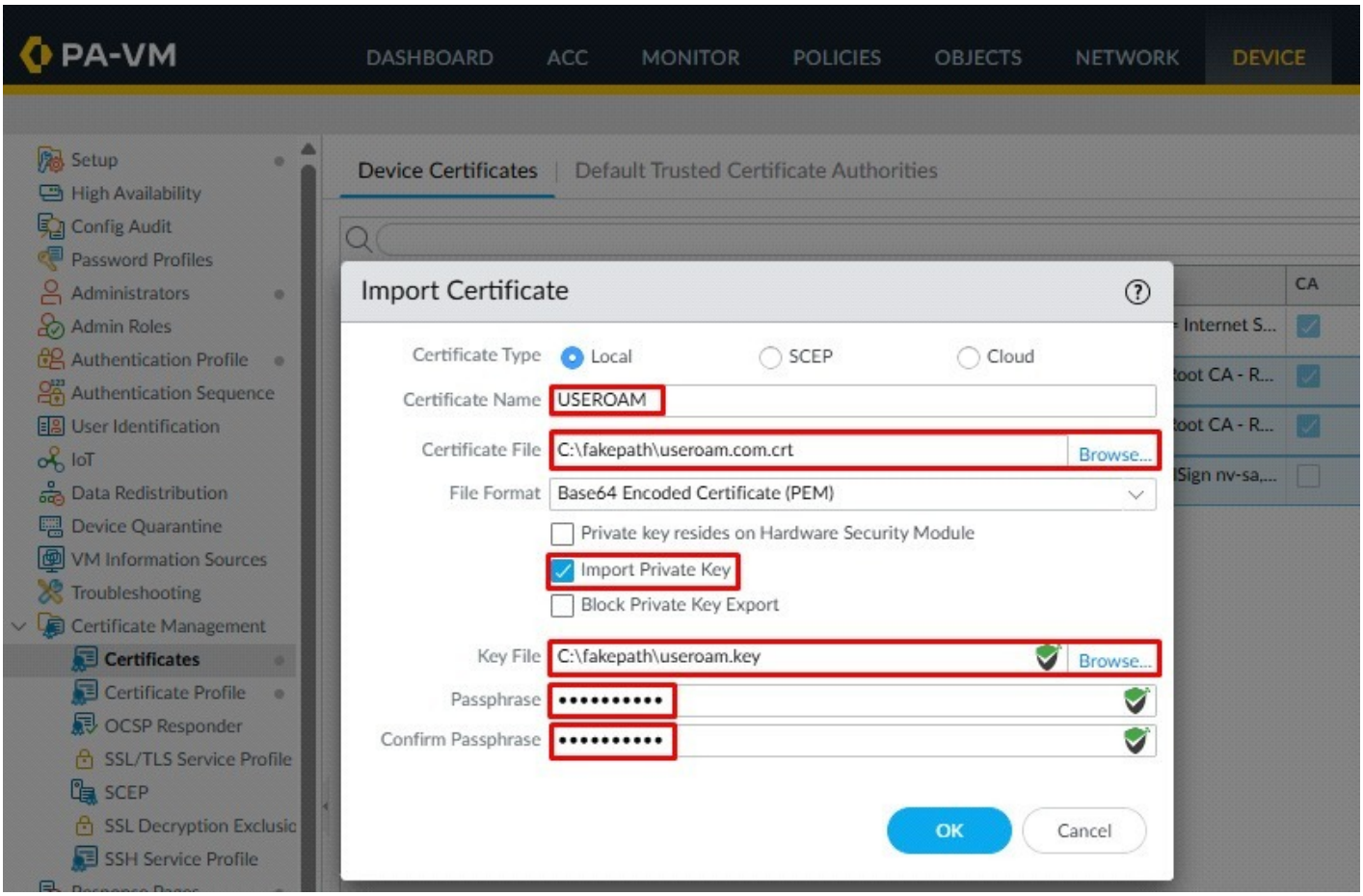
6A - Root CA Import İşlemi

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



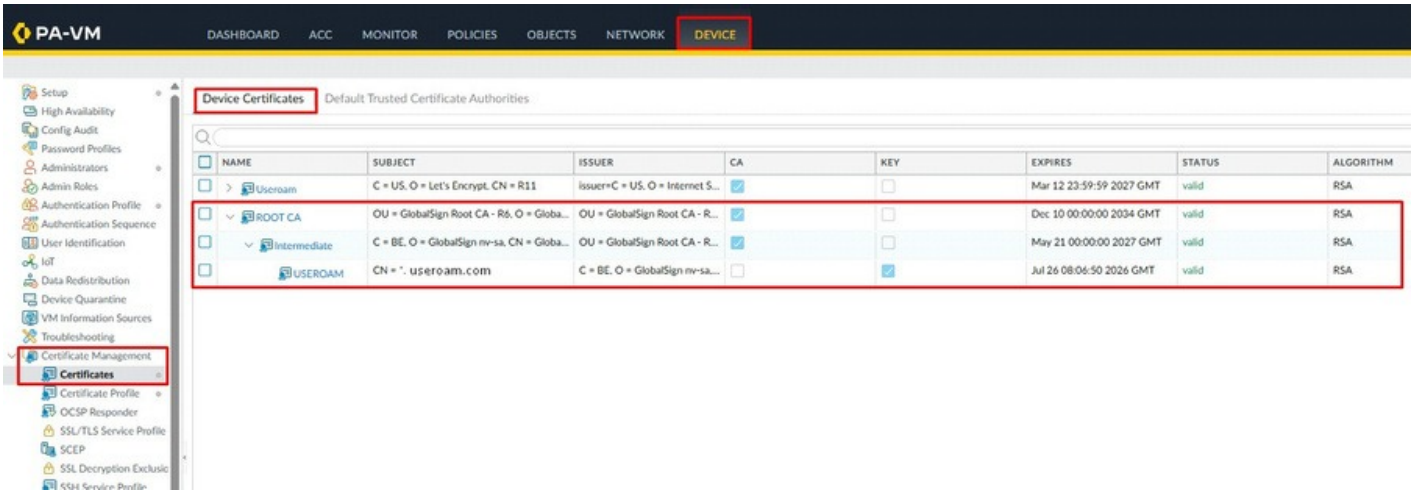
6B - Sertifika ve Anahtar Dosyasının Yüklenmesi

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



6C - Katmanlı Sertifika Zinciri Kontrolü

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

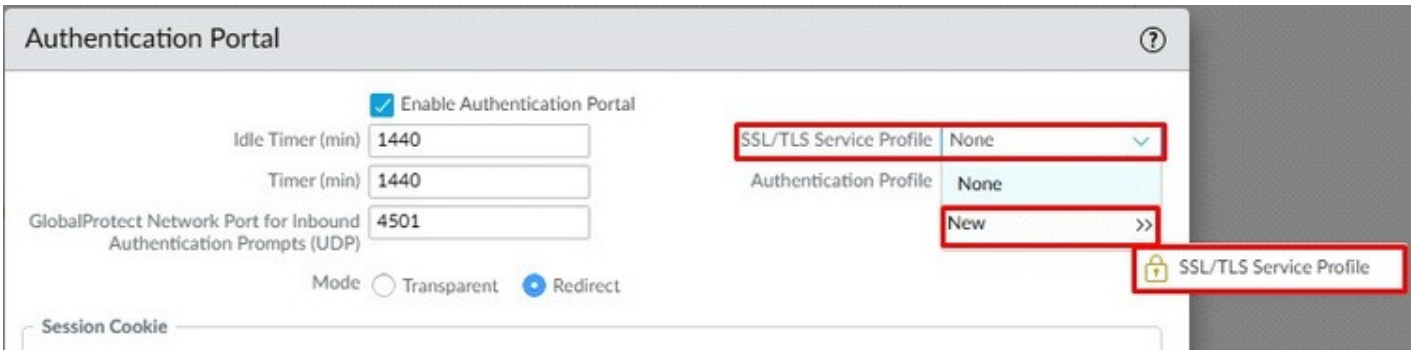


7 - Authentication Portal Ayarları

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

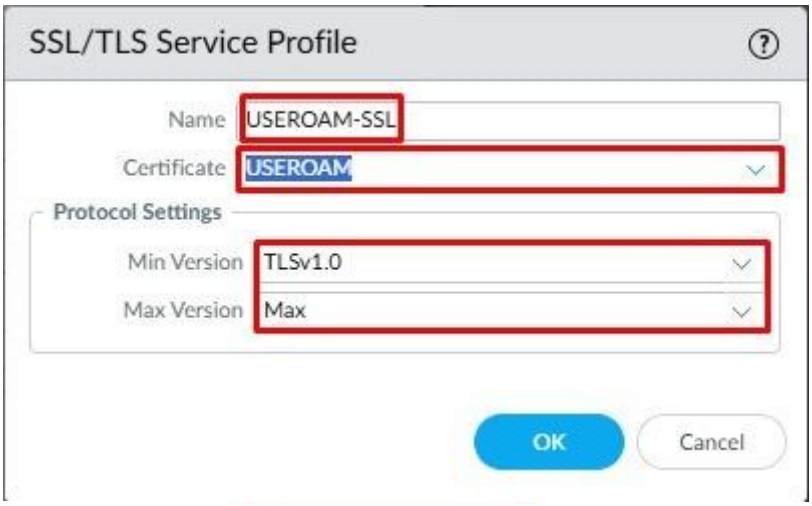


- Enable Authentication Portal: Bu seçeneği işaretleyerek hotspotu aktif hale getiriniz.
- Idle Timer ve Timer: Her iki alan için de maksimum değer olan 1440 dakika (24 saat) girilir. Bu, bir kullanıcının hotspot ekranını günde yalnızca bir kez görmesini sağlar. Biz bir kullanıcının önüne hotspot ekranının 24 saatte bir gelmesini istediğimiz için bu değeri giriyoruz. Daha kısa oturum süreleri tercih ediyorsanız, bu değeri ihtiyacınıza göre güncelleyebilirsiniz.
- SSL/TLS Service 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.

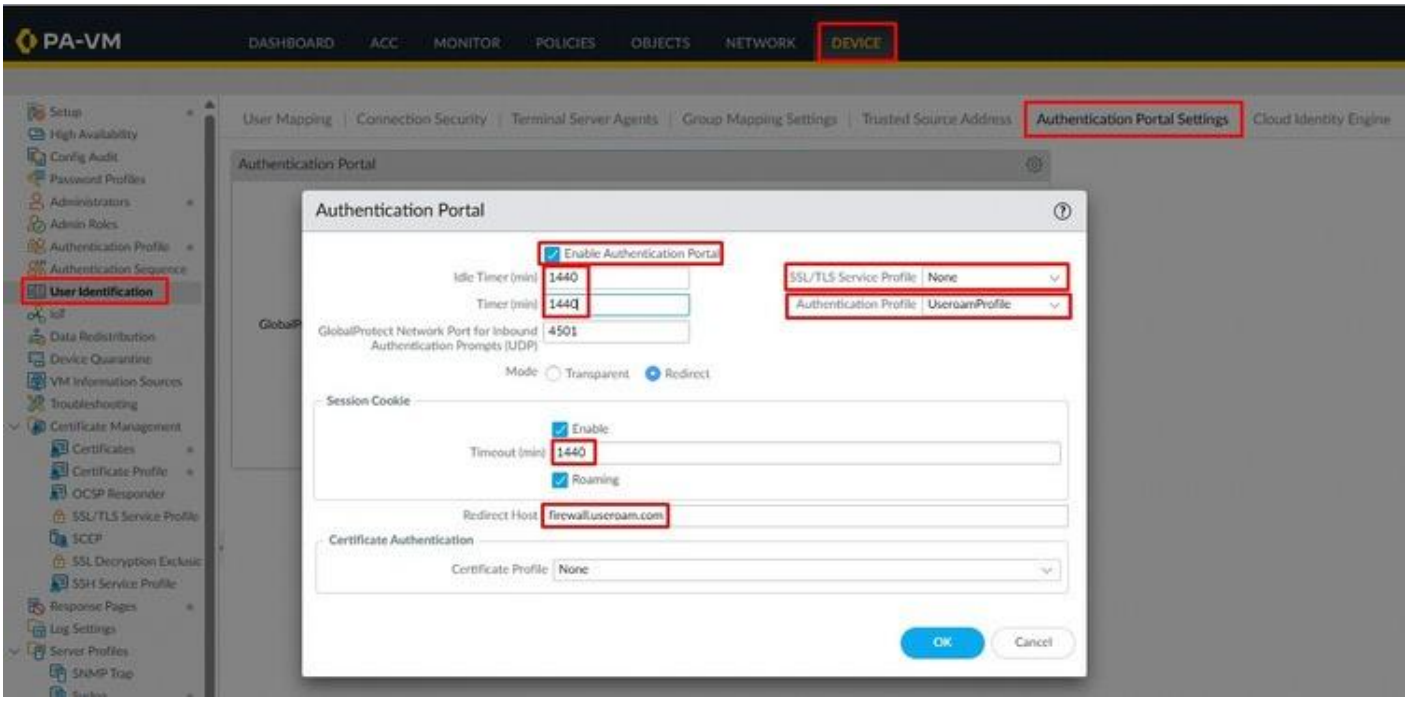




Authentication Prole : Oluşturulan Useroam prolini seçerek devam ediniz.

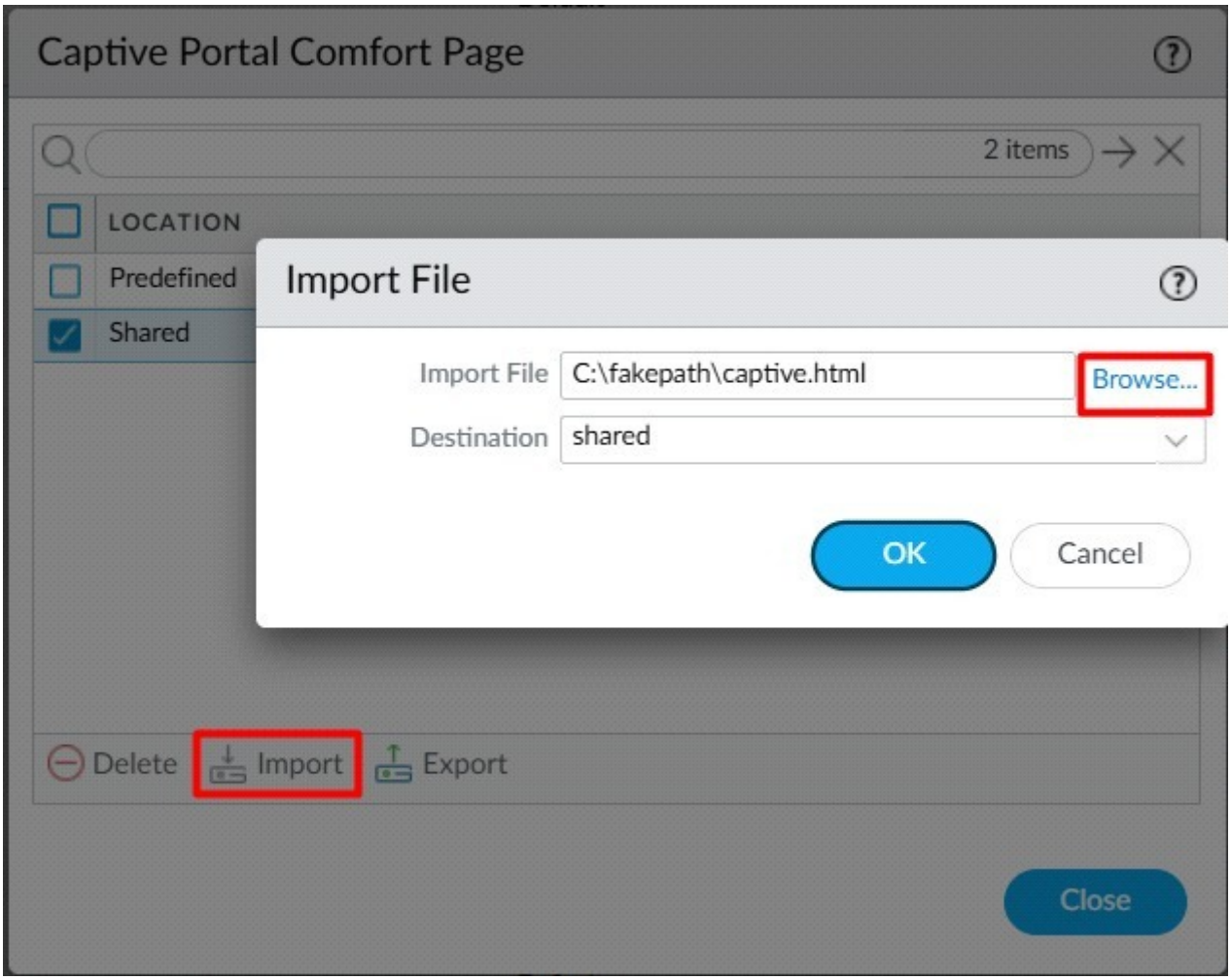
Session Cookie / Timeout : Bu alanda da daha önce belirlediğimiz gibi 1440 dakika (24 saat)d eğerini girerek oturum süresini tanımlayınız.

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



8 - Captive Portal Tasarımının 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.

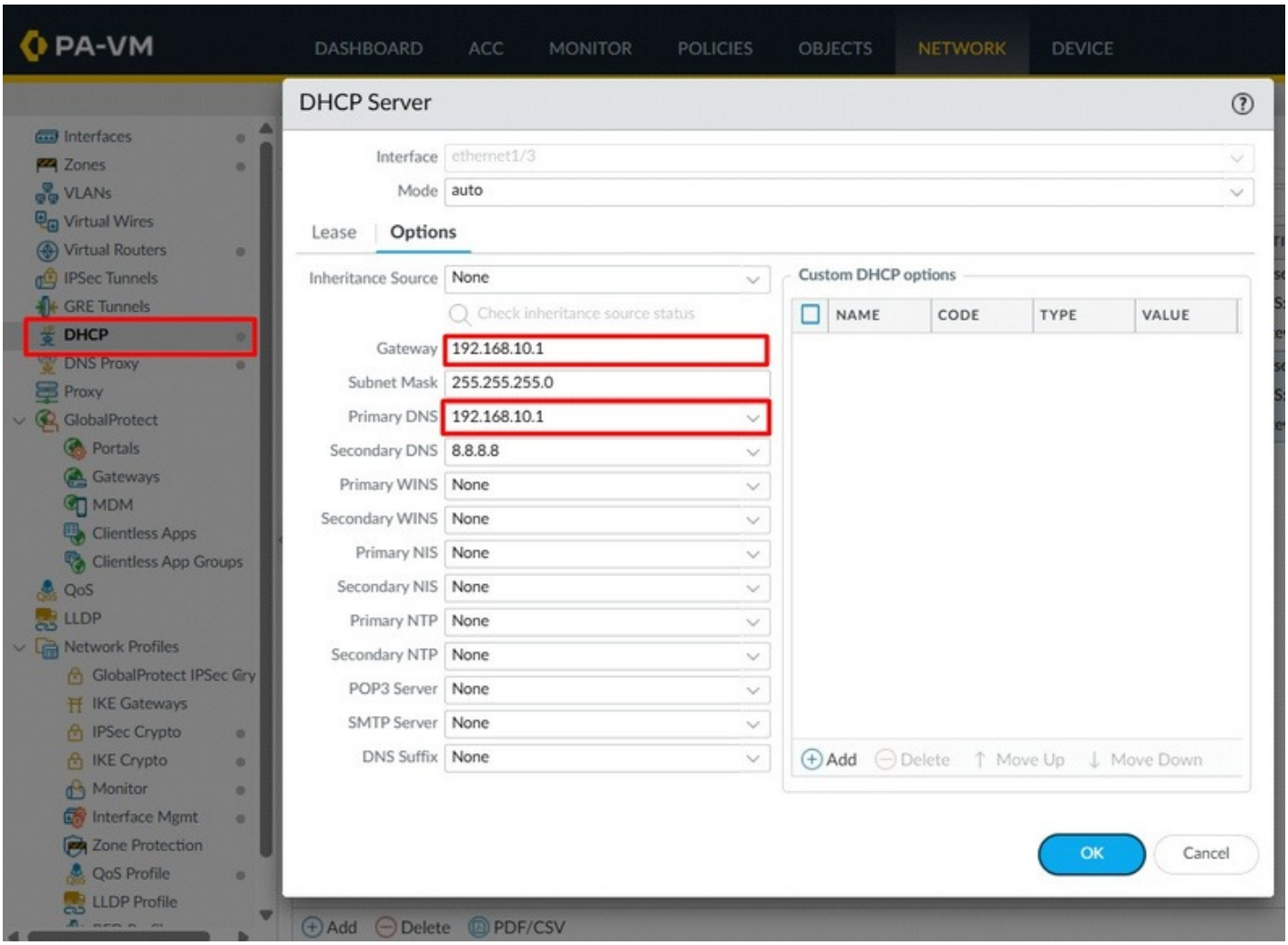


9 - DHCP Ayarları

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).

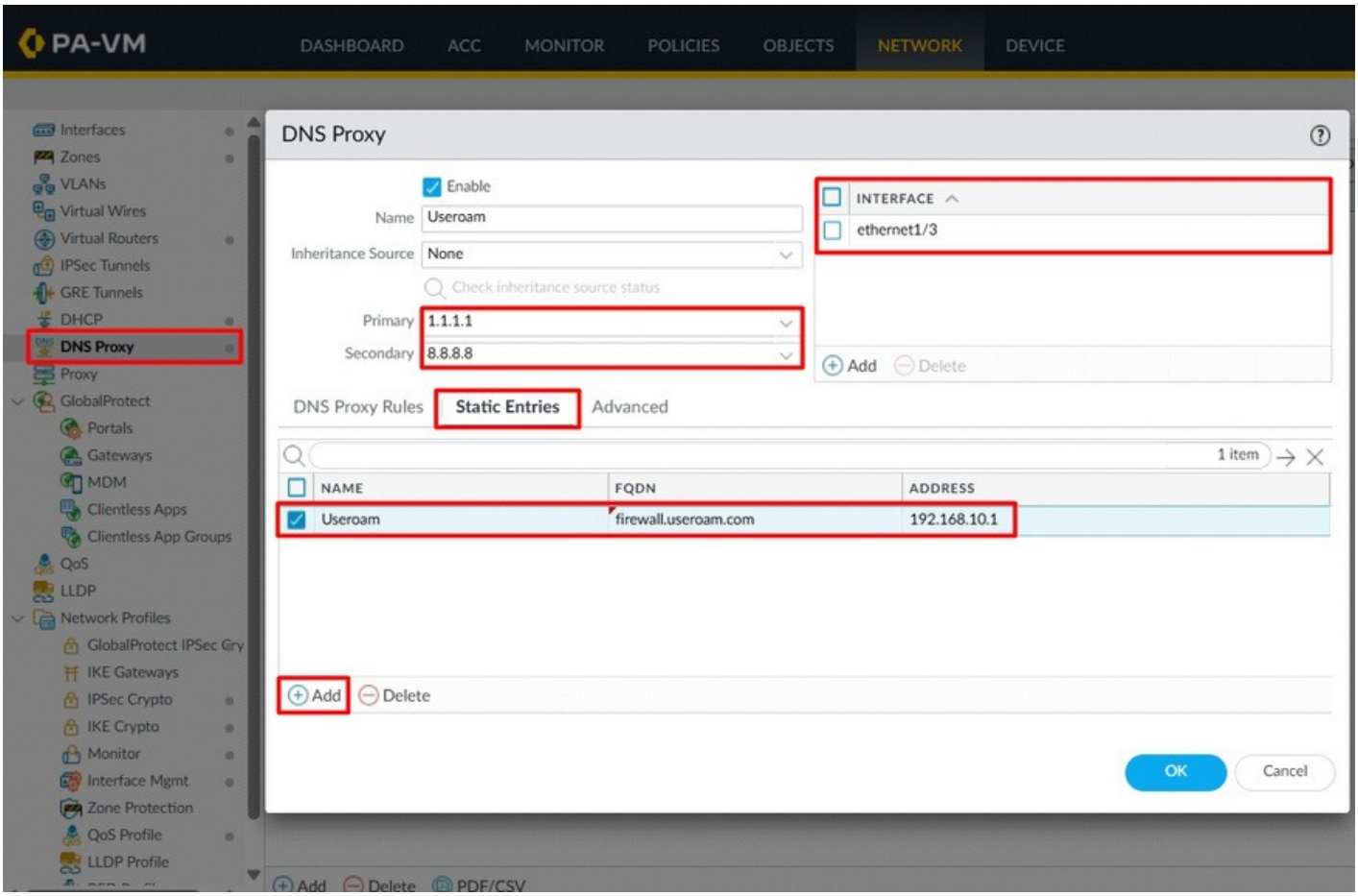
`Not: Mevcutta içeride bir DNS sunucunuz varsa alan adı yönlendirmesi için gerekli kaydı iç DNS ağınızda da (Static Entries kısmında) tanımlayarak 11. adımdan devam edebilirsiniz.`



10 - DNS Proxy Ayarları

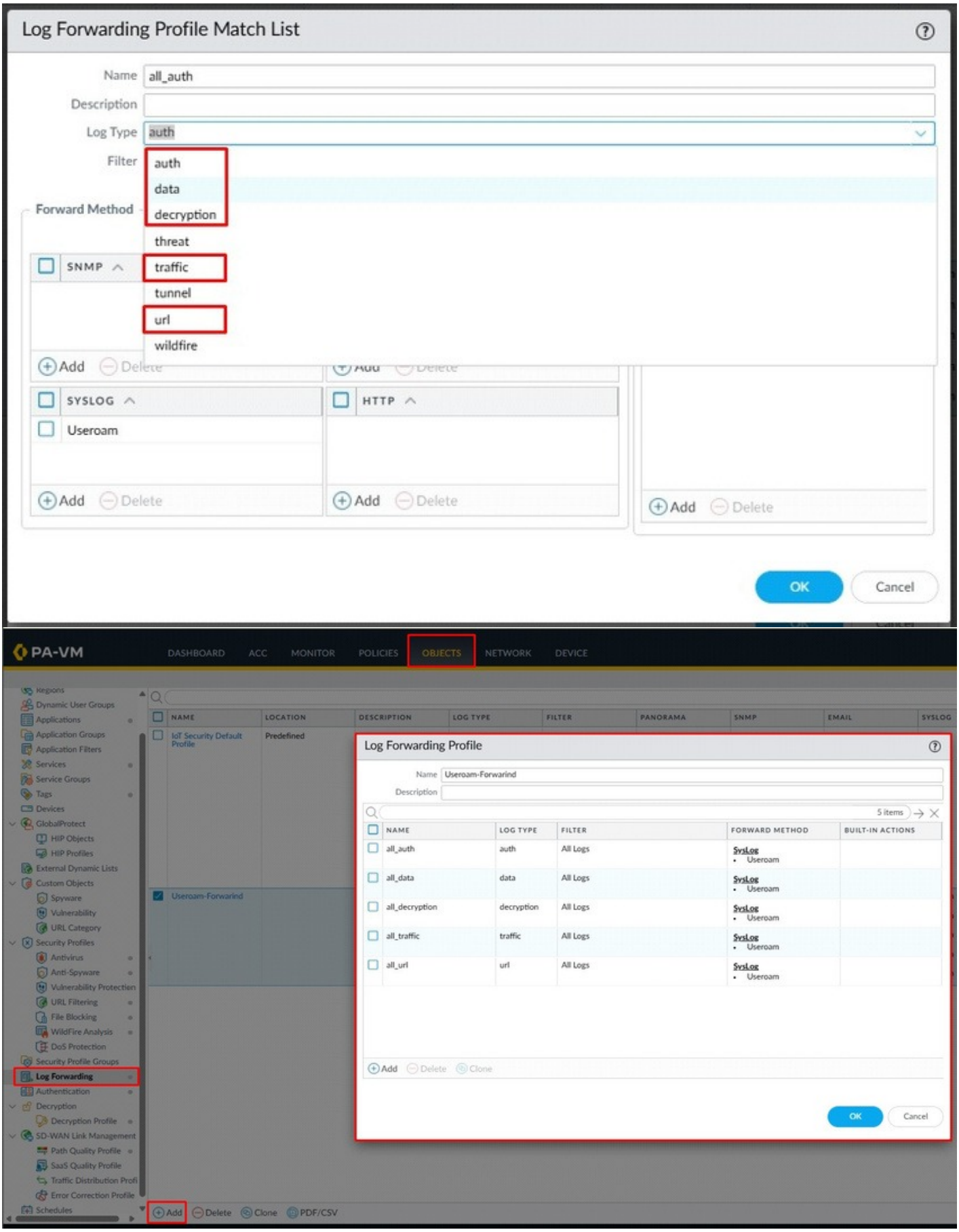
Ardından DNS sorgularının doğru şekilde çözümlenebilmesi için **Network > DNS Proxy** menüsünden yeni bir proxy tanımlanır.

- **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 - Logların 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.

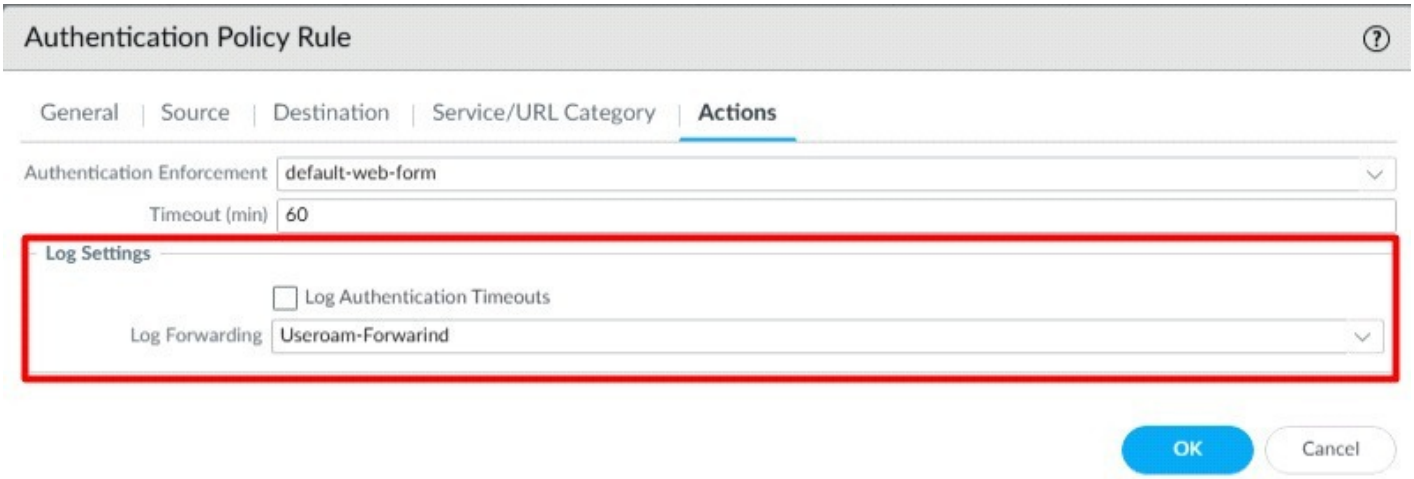

Log Forwarding Profile Match List
Name
all_auth
Description
Log Type
auth
Filter
auth
data
decryption
threat
traffic
tunnel
url
wildfire
Forward Method
SNMP
Add
Delete
SYSLOG
Useroam
HTTP
Add
Delete
Add
Delete
OK
Cancel
PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Dynamic User Groups
Applications
Application Groups
Application Filters
Services
Service Groups
Tags
Devices
GlobalProtect
HIP Objects
HIP Profiles
External Dynamic Lists
Custom Objects
Spyware
Vulnerability
URL Category
Security Profiles
Antivirus
Anti-Spyware
Vulnerability Protection
URL Filtering
File Blocking
WildFire Analysis
DoS Protection
Security Profile Groups
Log Forwarding
Authentication
Decryption
Decryption Profile
SD-WAN Link Management
Path Quality Profile
SaaS Quality Profile
Traffic Distribution Profi
Error Correction Profile
Schedules
NAME
LOCATION
DESCRIPTION
LOG TYPE
FILTER
PANORAMA
SNMP
EMAIL
SYSLOG
IoT Security Default Profile
Predefined
Useroam-Forwarind
Add
Delete
Clone
PDF/CSV
Log Forwarding Profile
Name
Useroam-Forwarind
Description
5 items
NAME
LOG TYPE
FILTER
FORWARD METHOD
BUILT-IN ACTIONS
all_auth
auth
All Logs
SysLog
Useroam
all_data
data
All Logs
SysLog
Useroam
all_decryption
decryption
All Logs
SysLog
Useroam
all_traffic
traffic
All Logs
SysLog
Useroam
all_url
url
All Logs
SysLog
Useroam
Add
Delete
Clone
OK
Cancel

Firewall Kurallarının Oluşturulması

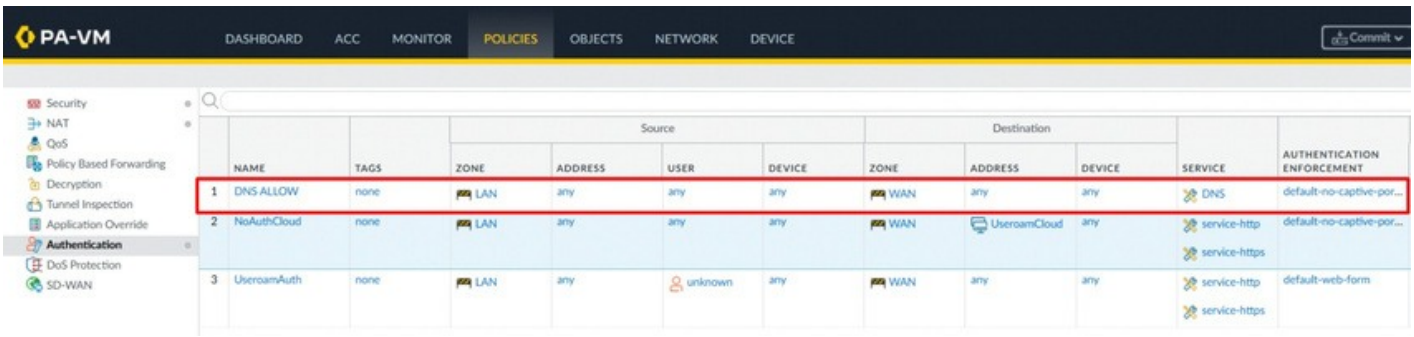
Palo Alto Firewall entegrasyonunda iki grup kural oluşturulması gerekmektedir. Kurallar ilk oluşturulurken Palo Alto'nun trafiği öğrenmesi gerekeceğinden Service kısmını öncelikle **Any** olarak kullanıp, sonrasında **application-default** olarak değiştirebilirsiniz.

12A - KURAL SETİ 1: Authentication Kuralları

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

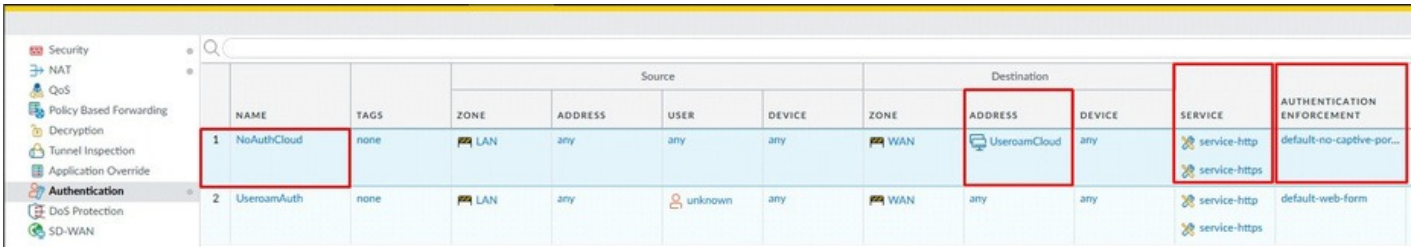


- **KURAL 1 (DNS İzni):** DNS sorgularının authentication aşamasından sorunsuz geçebilmesi için oluşturulur. WAN yönüne doğru tüm DNS sorgularına Authentication Enforcement alanında **default-no-captive-portal** seçilerek izin verilir.
- **KURAL 2 (Useroam Cloud İzni):** Bu kural sayesinde Useroam Cloud'a 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 SETİ 2: Security Kuralları

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 Tamamlandı

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.

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 #8
tugay tarafından 6 Temmuz 2026 12:34:28 oluşturuldu
tugay tarafından 13 Ekim 2026 12:43:20 güncellendi