

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 kuracaksınız, ilgili dış bacak IP adresini giriniz.

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

Yeni Cihaz

 **Cihaz Detayları**

AUVA3RYOZQ4E7F0LR7Z1640QD7XZ

Cihaz Tipi
PaloAlto

☒ 5651 Loglama

Cihaz Adresi
173.73.73.73

Cihaz Adı
Glox-Palo-Alto

SSL Port
443

2 - Zone Ayarlar?

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

Zone

NameMisafir

Log SettingNone

TypeLayer3

INTERFACES

ethernet1/2

Zone Protection

Zone Protection ProfileNone

Enable Packet Buffer Protection

Enable L3 & L4 Header Inspection

User Identification ACL

Enable User Identification

INCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Add

Delete

Users from these addresses/subnets will be identified.

EXCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Add

Delete

Users from these addresses/subnets will not be identified.

Device-ID ACL

Enable Device Identification

INCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Add

Delete

Devices from these addresses/subnets will be identified.

EXCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Add

Delete

Devices from these addresses/subnets will not be identified.

OK

Cancel

3 - Interface ve Profil Ayarlar?

Firewall üzerinden Useroam'u aktif edeceğimiz interface'de (arayüz) **Advanced** Kısımından 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

Cihaz Şifresi
1a2b3c4d

RADIUS Server Profile

Profile Name

Useroam

☐ Administrator Use Only

Server Settings

Timeout (sec)

3

Retries

3

Authentication Protocol

PAP

Servers

NAME	RADIUS SERVER	SECRET	PORT
Useroam	panel.useroam.com	*****	1812

+ Add

- Delete

Enter the IP address or FQDN of the RADIUS server

OK

Cancel

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.

Authentication Profile

?

NameUseroam Profile

AuthenticationFactorsAdvanced

TypeRADIUS

Server ProfileUseroam

☒ Retrieve user group from RADIUS

User Domain

Username Modifier%USERINPUT%

Single Sign On

Kerberos Realm

Kerberos KeytabClick "Import" to configure this fieldX Import

OKCancel

Authentication Profile

?

NameUseroam Profile

AuthenticationFactorsAdvanced

Allow List

☐ ALLOW LIST ^

☐ all

☒ Add☐ Delete

Account Lockout

Failed Attempts[0 - 10]

Lockout Time (min)0

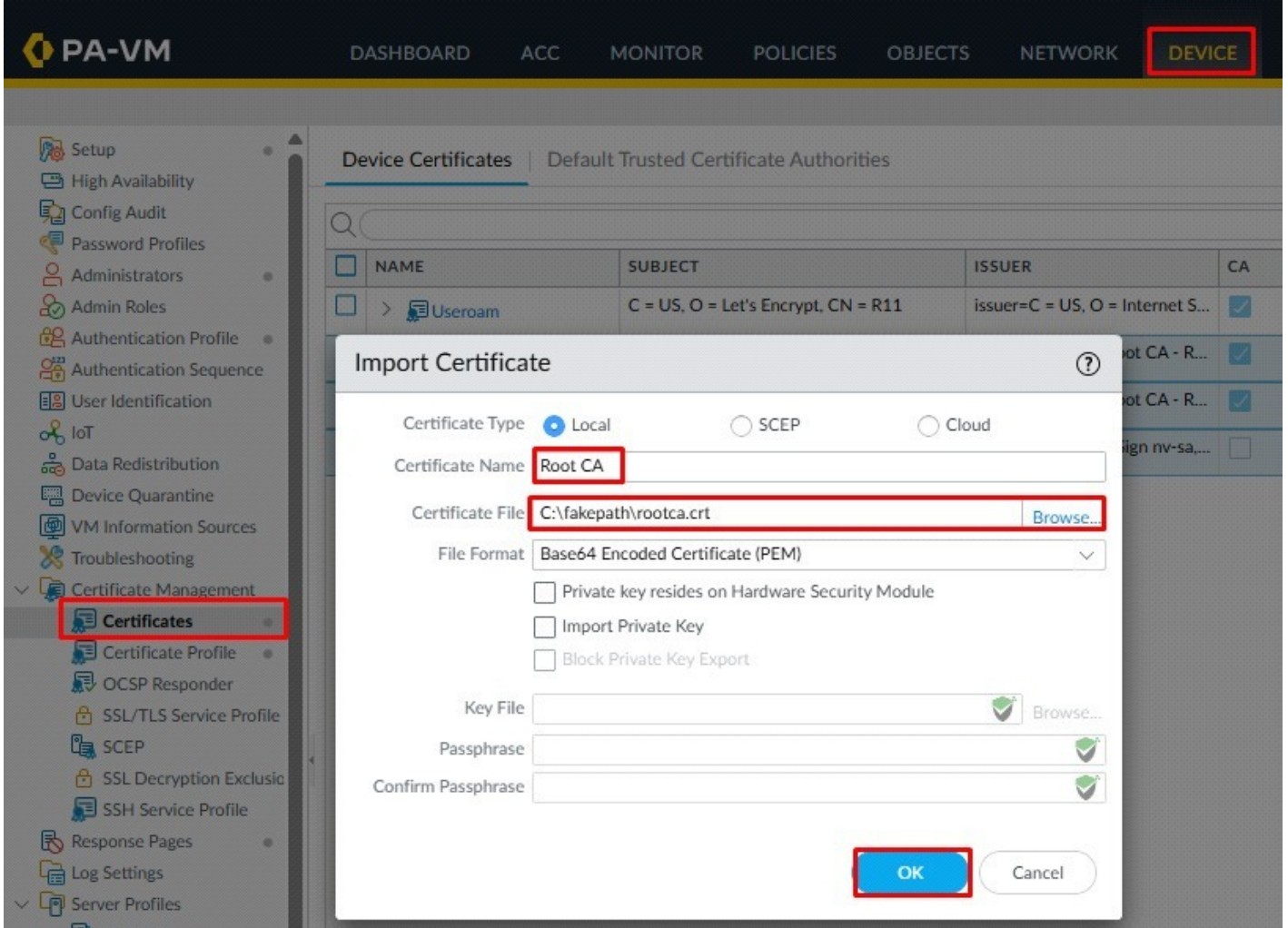
OKCancel

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.

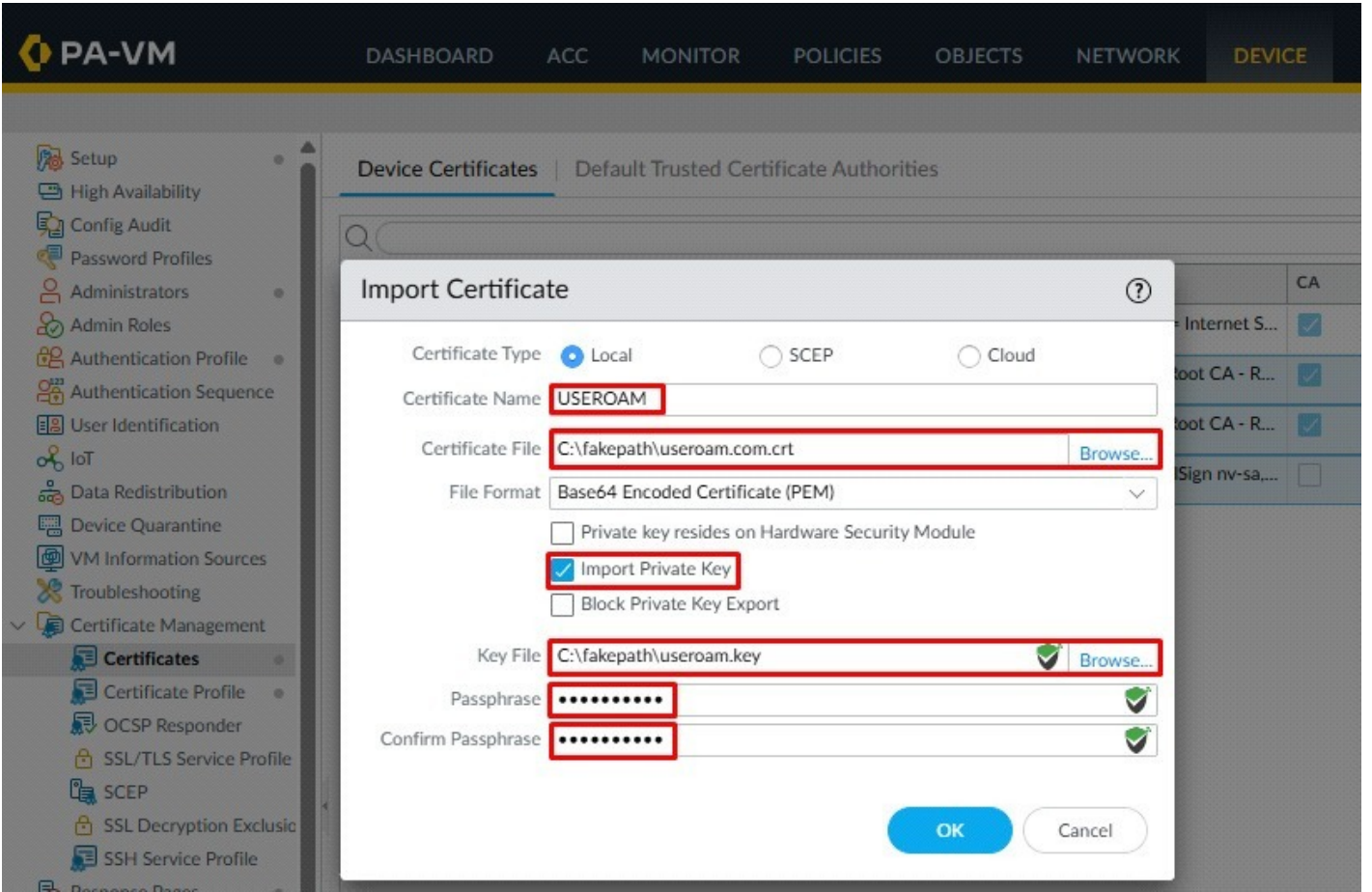
6A - Root CA Import ??lemi

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



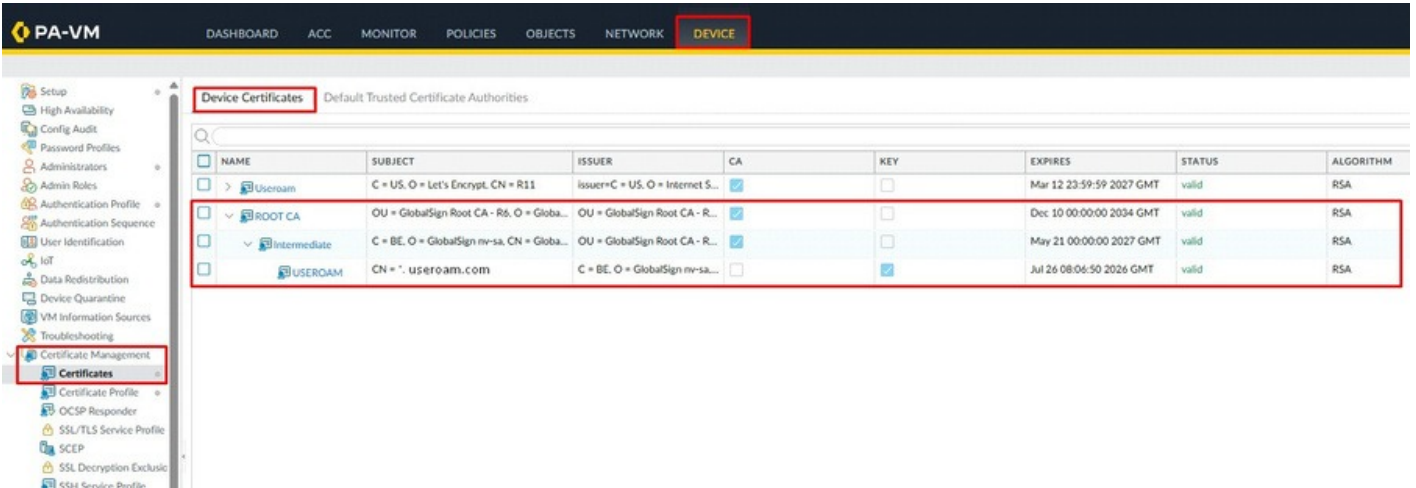
6B - Sertifika ve Anahtar Dosyası'nın Yüklenmesi

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 Ayarlar?

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

Authentication Portal



Enable Authentication Portal ☒

Timer (min) 60

Idle Timer (min) 1

SSL/TLS Service Profile

Authentication Profile UseroamProfile

GlobalProtect Network Port for Inbound Authentication Prompts (UDP) 4501

Certificate Profile

Mode redirect

Session Cookie

Enable: true

Timeout: 1440

Roaming: true

Redirect Host: 10.31.31.31

- 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 proller bu alanda görünmeyebilir. Bu durumda, "New" seçeneği ile bu ekrandan yeni bir SSL/TLS proli oluşturularak işlem tamamlanmalıdır.
- Eğer sisteminizde seçim yapılabilirse, önceden oluşturulmuş proli kullanılabilir

Authentication Portal



☒ Enable Authentication Portal

Idle Timer (min) 1440

Timer (min) 1440

GlobalProtect Network Port for Inbound Authentication Prompts (UDP) 4501

Mode ☐ Transparent ☒ Redirect

Session Cookie

SSL/TLS Service Profile None

Authentication Profile None

New >>

SSL/TLS Service Profile

Yeni bir profil oluşturmanız gerekiyorsa aşağıdaki adımları izleyiniz.

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

SSL/TLS Service Profile ?

Name: **USEROAM-SSL**

Certificate: **USEROAM**

Protocol Settings

Min Version: **TLV1.0**

Max Version: **Max**

OK **Cancel**

SSL/TLS Service Profile: **USEROAM-SSL**

Authentication Profile: **UseroamProfile**

Authentication Prole : Oluřturulan Useroam prolini seęerek devam ediniz.

Session Cookie / Timeout : Bu alanda da daha nce belirledięimiz gibi 1440 dakika (24 saat)d eęerini girerek oturum sresini tanımlayınız.

Redirect Host : Buraya sertika zerinden ynlendirme yapılacaęı iin subdomaini giriniz.

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK **DEVICE**

User Mapping | Connection Security | Terminal Server Agents | Group Mapping Settings | Trusted Source Address | **Authentication Portal Settings** | Cloud Identity Engine

Authentication Portal

User Identification

Authentication Portal ?

☒ **Enable Authentication Portal**

Idle Timer (min): **1440**

Timer (min): **1440**

GlobalProtect Network Port for Inbound Authentication Prompts (UDP): **4501**

Mode: ☐ Transparent ☒ **Redirect**

Session Cookie

☒ **Enable**

Timeout (min): **1440**

☒ **Roaming**

Redirect Host: **firewall.useroam.com**

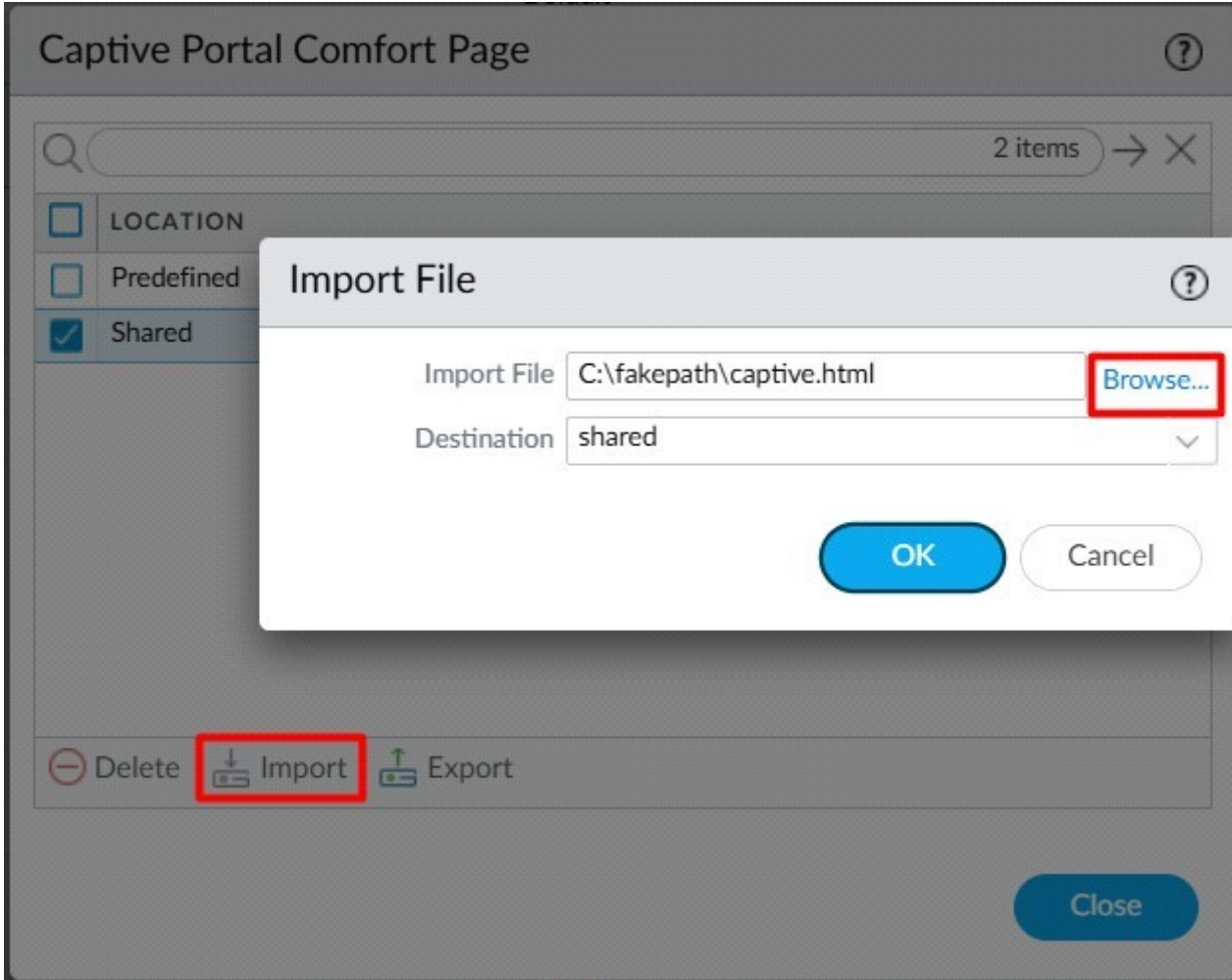
Certificate Authentication

Certificate Profile: **None**

OK **Cancel**

8 - Captive Portal Tasarımının Yklenmesi (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.

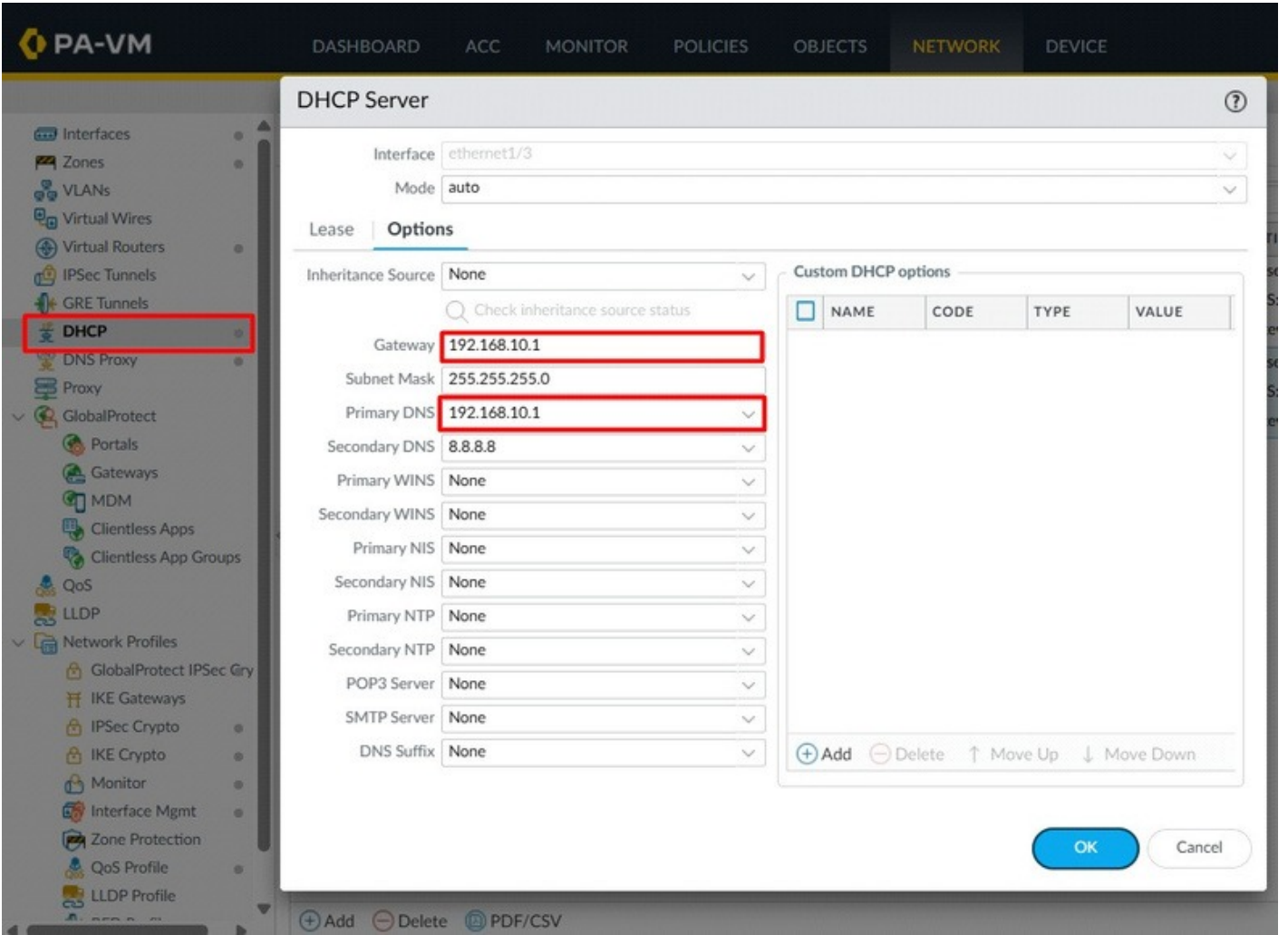


9 - DHCP Ayarlar?

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).

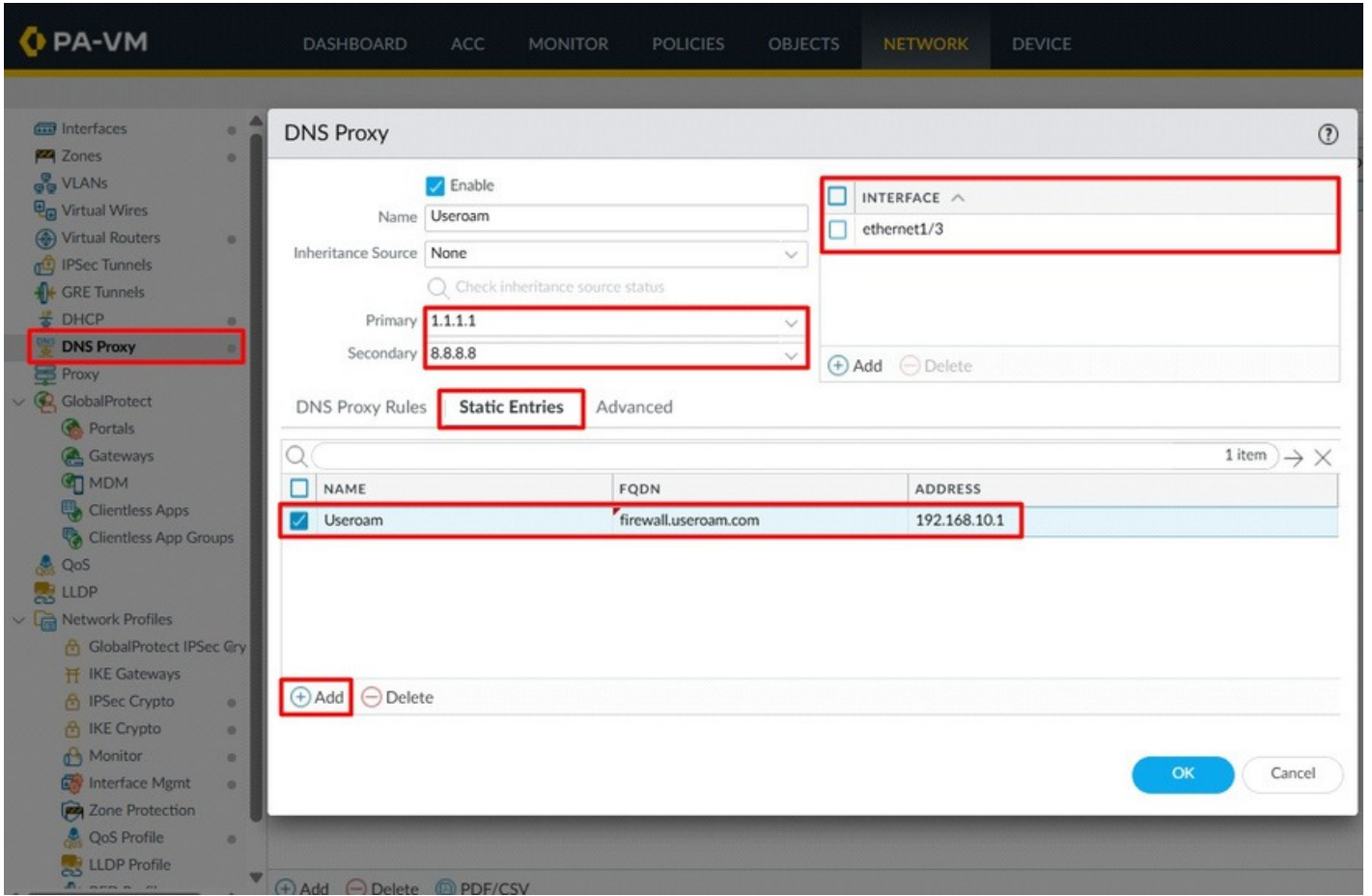
Not: Mevcutta içeride bir DNS sunucunuz varsa alan adı yönlendirmesi için gerekli kaydı iç DNS ağınızda da (Static Entries kısmında) tanımlayarak 11. adımdan devam edebilirsiniz.



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.

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.**

Authentication Policy Rule

General | Source | Destination | Service/URL Category | **Actions**

Authentication Enforcement: default-web-form

Timeout (min): 60

Log Settings

☐ Log Authentication Timeouts

Log Forwarding: Useroam-Forwardind

OK Cancel

- **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)** fqd'n 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 yönlendirmesini sağlayan ana kuraldır.

PA-VM DASHBOARD ACC MONITOR **POLICIES** OBJECTS NETWORK DEVICE

	NAME	TAGS	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	SERVICE	AUTHENTICATION ENFORCEMENT
1	DNS ALLOW	none	LAN	any	any	any	WAN	any	any	DNS	default-no-captive-por...
2	NoAuthCloud	none	LAN	any	any	any	WAN	UseroamCloud	any	service-http service-https	default-no-captive-por...
3	UseroamAuth	none	LAN	any	unknown	any	WAN	any	any	service-http service-https	default-web-form

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.**

	NAME	TAGS	ZONE	Source			ZONE	Destination		SERVICE	AUTHENTICATION ENFORCEMENT
				ADDRESS	USER	DEVICE		ADDRESS	DEVICE		
1	NoAuthCloud	none	LAN	any	any	any	WAN	UseroamCloud	any	service-http service-https	default-no-captive-por...
2	UseroamAuth	none	LAN	any	unknown	any	WAN	any	any	service-http service-https	default-web-form

- **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.

Revizyon #4

tugay tarafından 6 Temmuz 2026 12:34:28 oluşturuldu

tugay tarafından 6 Temmuz 2026 12:55:33 güncellendi