

USEROAM CLOUD paloalto ENTEGRASYONU

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 kuracaksınız, ilgili dış bacak ip adresini giriniz. **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 Ayarları

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

Zone

Name: Misafir

Log Setting: None

Type: Layer3

INTERFACES ^

ethernet1/2

Zone Protection Profile: None

Enable Packet Buffer Protection

Enable L3 & L4 Header Inspection

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

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

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

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

OK Cancel

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

Cihaz şifresi
1a2b3c4d

RADIUS Server Profile

Profile Name

Administrator Use Only

Server Settings

Timeout (sec)

Retries

Authentication Protocol

Servers

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

Enter the IP address or FQDN of the RADIUS server

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**ize **all** ediyoruz.

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

Account Lockout

Failed Attempts: [0 - 10]

Lockout Time (min): 0

OK Cancel

6 Sertifikasyon 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.

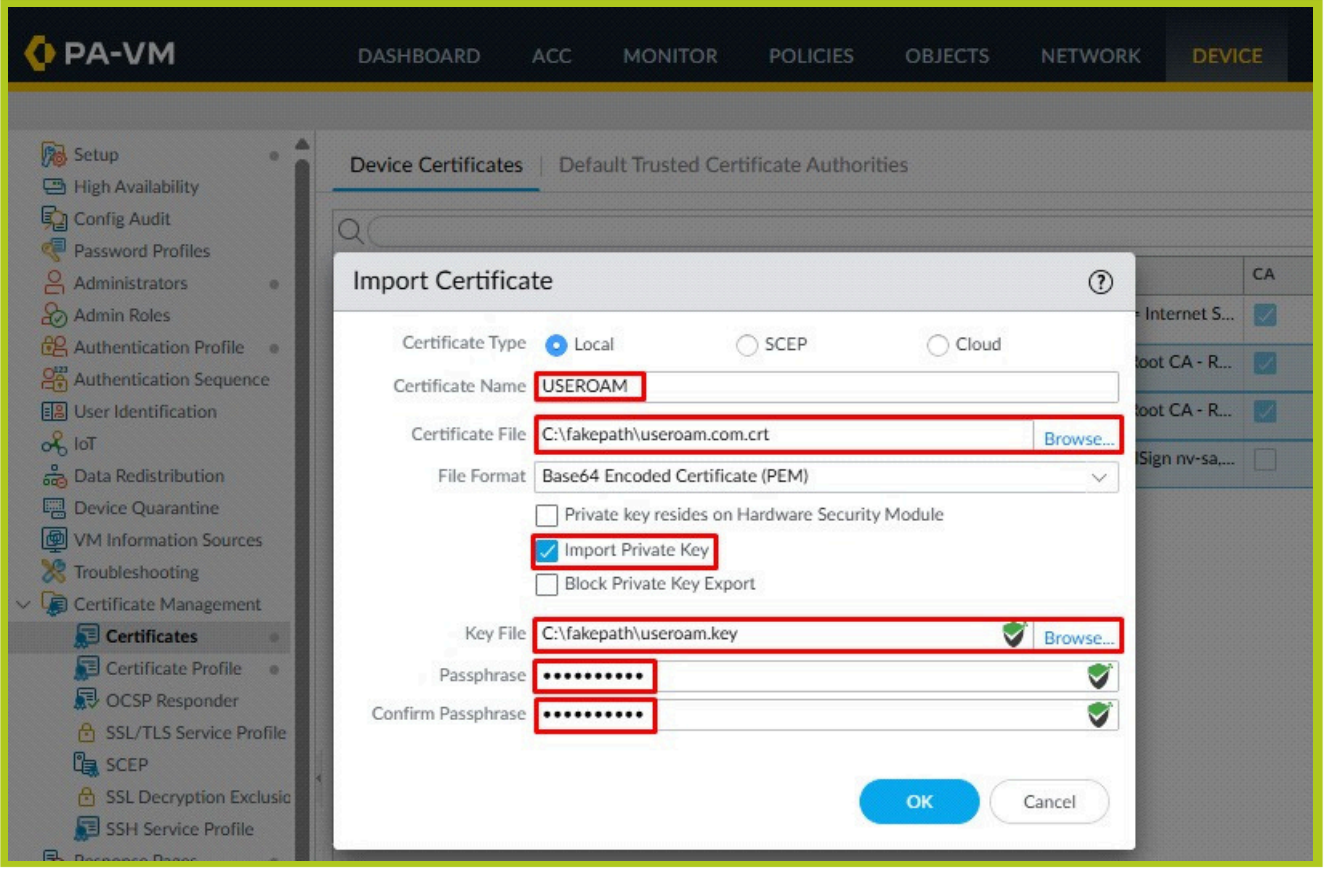
6a İlk adım olarak, **Root CA veya CA sertifikasını** import ediniz.

The screenshot shows the Palo Alto VM console interface. The 'DEVICE' tab is selected. The 'Device Certificates' section is active, showing a table with columns for NAME, SUBJECT, ISSUER, and CA. A table entry is visible for 'Useroam' with subject 'C = US, O = Let's Encrypt, CN = R11' and issuer 'issuer=C = US, O = Internet S...'. The 'Import Certificate' dialog box is open, showing the following fields:

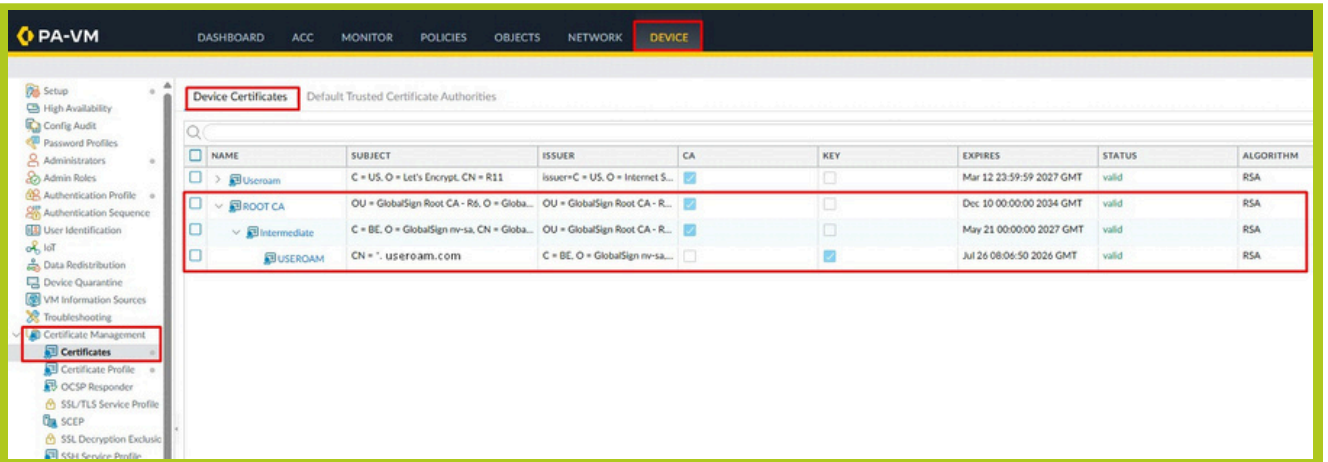
- Certificate Type: Local (selected), SCEP, Cloud
- Certificate Name: Root CA
- Certificate File: C:\fakepath\rootca.crt (with a 'Browse...' button)
- File Format: Base64 Encoded Certificate (PEM)
- Private key resides on Hardware Security Module:
- Import Private Key:
- Block Private Key Export:
- Key File: (with a 'Browse...' button)
- Passphrase: (with a 'Browse...' button)
- Confirm Passphrase: (with a 'Browse...' button)

The 'OK' button is highlighted in blue.

6b Sonraki adımda; serti ka dosyasını, anahtar dosyası ve Őifreyle birlikte g venlik duvarına y kleyiniz.



6c Y kleme iŐlemi tamamlandığında, karŐımıza  ıkan g r nt ; katmanlı bir yapı Őeklinde, birbirine baėlı bir serti ka zinciri Őeklinde olmalıdır.



7 Authentication Portal ayarları

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

Eğer sisteminizde seçim yapılabilirse, önceden oluşturulmuş profil 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 profil kaydediniz.

Bu işlemlerin ardından, oluşturulan yeni profil sistem tarafından otomatik olarak seçilmiş şekilde görünecektir.

SSL/TLS Service Profile

Name: USEROAM-SSL

Certificate: USEROAM

Protocol Settings

Min Version: TLSv1.0

Max Version: Max

OK Cancel

SSL/TLS Service Profile: USEROAM-SSL

Authentication Profile: UseroamProfile

Authentication Profile : Oluşturulan Useroam profilini 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 sertifika üzerinden yönlendirme yapılacağı için 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

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

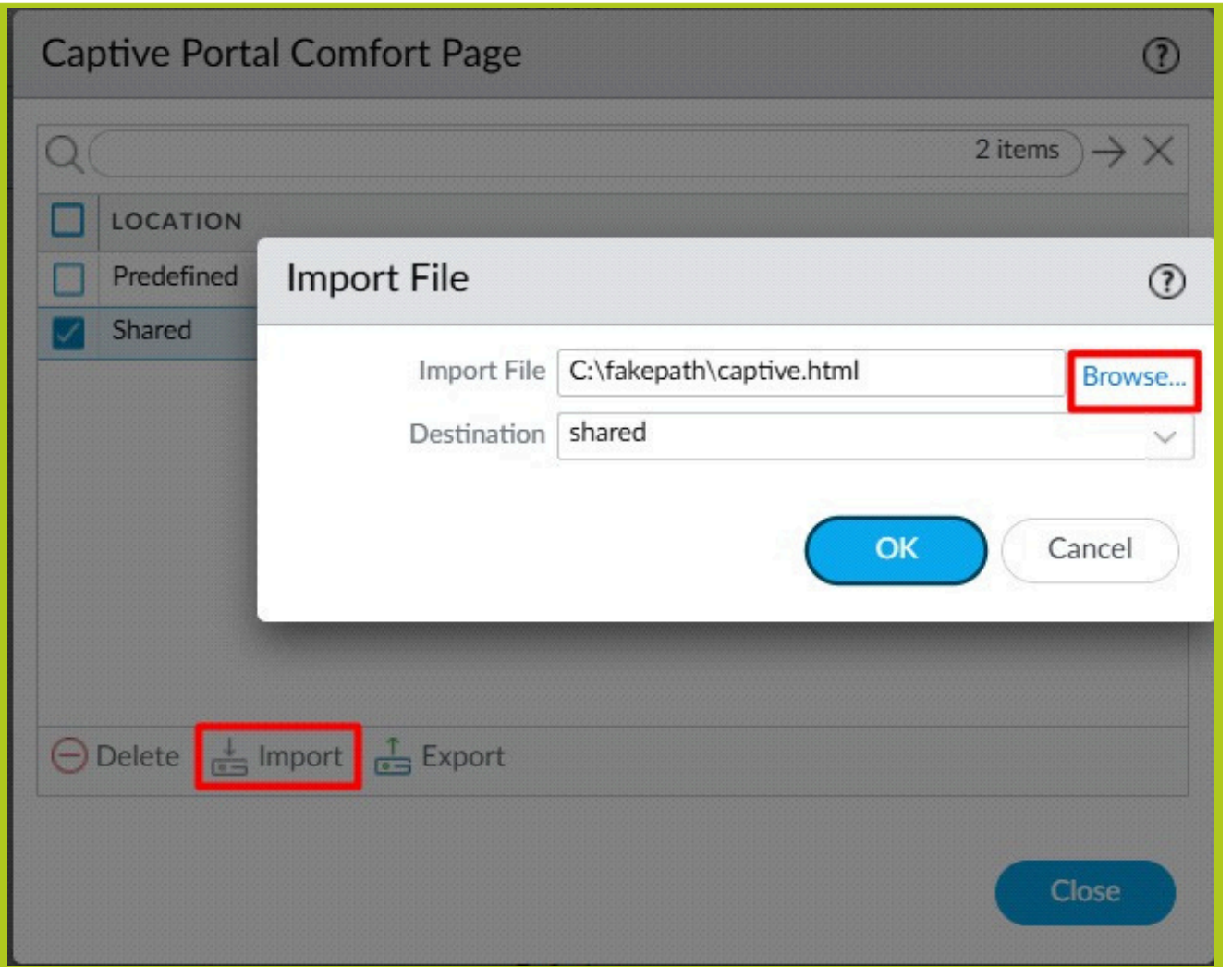
Certificate Authentication

Certificate Profile: None

OK Cancel

8 Captive Portal 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, Firewall'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).

The screenshot shows the DHCP Server configuration page in the Palo Alto VM interface. The 'Options' tab is active, displaying a list of DHCP options. The 'Primary DNS' field is highlighted with a red box and contains the value '192.168.10.1'. The 'Secondary DNS' field contains '8.8.8.8'. The 'Interface' is set to 'ethernet1/3' and 'Mode' is 'auto'. The 'Inheritance Source' is 'None'. A 'Custom DHCP options' table is visible on the right, currently empty. The interface includes navigation tabs (Dashboard, Acc, Monitor, Policies, Objects, Network, Device) and a sidebar menu with 'DHCP' highlighted in red.

NAME	CODE	TYPE	VALUE

10

DNS Ayarları

Ardından DNS sorgularının doğru şekilde çözümlenebilmesi için yeni bir proxy tanımlanır. İşlem adımları aşağıdaki gibidir:

Network > DNS Proxy menüsünden

Name: Proxyle 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, Firewall cihazının Management Interface nin gateway IP adresi** olması önemlidir. Ok butonuna tıklanarak işlemi tamamlayınız.

The screenshot shows the Palo Alto VM configuration interface for DNS Proxy. The 'DNS Proxy' section is active, and the 'Static Entries' tab is selected. The configuration includes the following details:

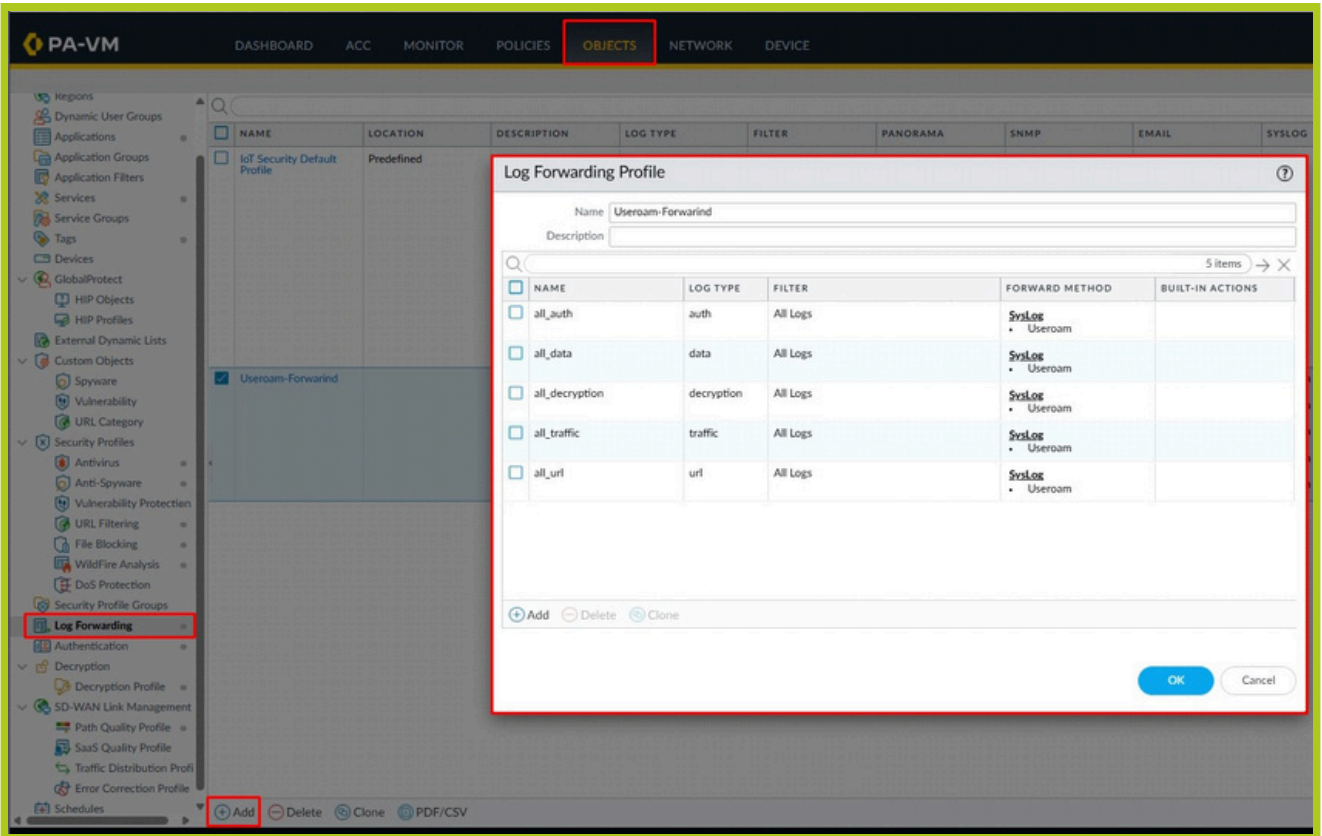
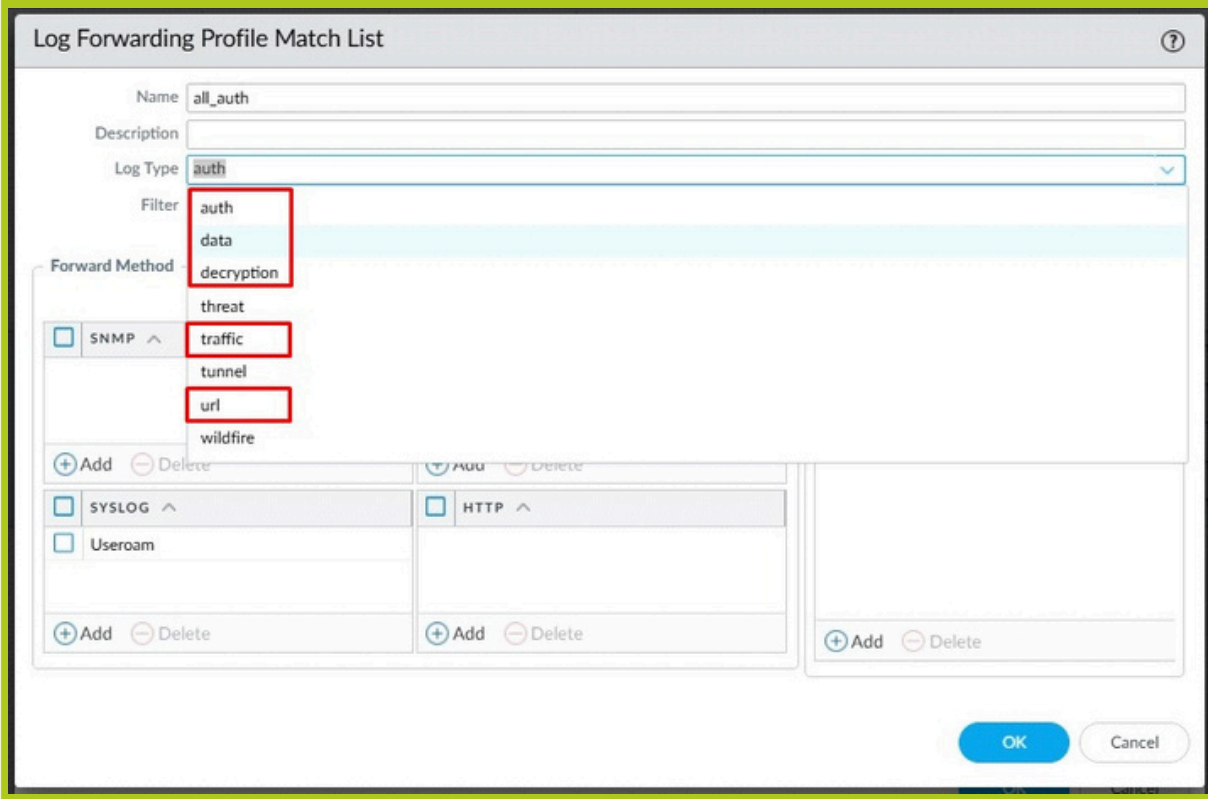
- Enable:** Checked
- Name:** Useroam
- Inheritance Source:** None
- Primary:** 1.1.1.1
- Secondary:** 8.8.8.8
- INTERFACE:** ethernet1/3
- DNS Proxy Rules:** Static Entries
- Static Entries Table:**

NAME	FQDN	ADDRESS
<input checked="" type="checkbox"/> Useroam	firewall.useroam.com	192.168.10.1
- Buttons:** Add, Delete, OK, Cancel

11 LOGLARIN USEROAM'A YÖNLENDİRİLMESİ

OBJECTS > Log Forwarding kısmından **Add** proflidekle yapınız. Buradaherlemede gerekmektedir.

ileyeniprofl oluşturunuz. 5 farklı log tipi için ayrı ayrı **Syslog** kısmında **Useroam** proflini seçmeniz



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

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-Forward

OK
Cancel

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** i seçerek izin veriyoruz.

PA-VM											
DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE											
Commit											
Security											
<ul style="list-style-type: none"> NAT QoS Policy Based Forwarding Decryption Tunnel Inspection Application Override Authentication DoS Protection SD-WAN 											
Q											
Source											
Destination											
NAME	TAGS	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	SERVICE	AUTHENTICATION ENFORCEMENT	
1	DNS ALLOW	none	LAN	any	any	WAN	any	any	DNS	default-no-captive-por...	
2	NoAuthCloud	none	LAN	any	any	WAN	UseroamCloud	any	service-http	default-no-captive-por...	
3	UseroamAuth	none	LAN	any	unknown	WAN	any	any	service-http	default-web-form	
									service-https		

KURAL 2:

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

PA-VM											
DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE											
Commit											
Security											
<ul style="list-style-type: none"> NAT QoS Policy Based Forwarding Decryption Tunnel Inspection Application Override Authentication DoS Protection SD-WAN 											
Q											
Source											
Destination											
NAME	TAGS	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	SERVICE	AUTHENTICATION ENFORCEMENT	
1	NoAuthCloud	none	LAN	any	any	WAN	UseroamCloud	any	service-http	default-no-captive-por...	
2	UseroamAuth	none	LAN	any	unknown	WAN	any	any	service-http	default-web-form	
									service-https		

KURAL 3:

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

	NAME	TAGS	Source				Destination			SERVICE	AUTHENTICATION ENFORCEMENT
			ZONE	ADDRESS	USER	DEVICE	ZONE	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

12b KURAL SETİ 2 (Security)

Bunun için **Policies > Security** menüsüne geliniz. Buradan üç kural oluşturacaksınız. Kurallar ilk oluşturulurken Palo Altonun trafiği 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.

Security Policy Rule

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

Action Setting
 Action: Allow
 Send ICMP Unreachable

Profile Setting
 Profile Type: None

Log Setting
 Log at Session Start
 Log at Session End
 Log Forwarding: Useroam-Forwarding

Other Settings
 Schedule: None
 QoS Marking: None
 Disable Server Response Inspection

OK Cancel

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.

	NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE				
1	Allow DNS	none	universal	LAN	any	any	any	WAN	any	any	dns	application...	Allow	none

KURAL 2:

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

	NAME	TAGS	TYPE	Source			Destination			APPLICATION	SERVICE	ACTION	
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS				DEVICE
1	Allow DNS	none	universal	LAN	any	any	any	WAN	any	any	dns	application...	Allow
2	LarfiUseroam	none	universal	LAN	any	any	any	WAN	UseroamCloud	any	any	application...	Allow
3	CaptivePortal	none	universal	LAN	any	known-user	any	WAN	any	any	any	application...	Allow

KURAL 3:

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

	NAME	TAGS	TYPE	Source			Destination			APPLICATION	SERVICE	ACTION	PROFILE	
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS					DEVICE
1	Allow DNS	none	universal	LAN	any	any	any	WAN	any	any	dns	application...	Allow	none
2	LarfiUseroam	none	universal	LAN	any	any	any	WAN	UseroamCloud	any	any	application...	Allow	none
3	CaptivePortal	none	universal	LAN	any	known-user	any	WAN	any	any	any	application...	Allow	none

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](mailto:destek@useroamteknoloji.com) adresinden bizimle iletişime geçebilirsiniz.