

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.

Yeni Cihaz

**Cihaz Detayları**

AUVA3RYOZQ4E7F0LR7Z1640QD7XZ

Cihaz Tipi

Sophos

☒ 5651 Loglama

Cihaz Adresi

178.159.35.173

Cihaz Adı

GLX-Sophos-FW

2- Cihaz Erişim Ayarları (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.

The screenshot shows the Sophos Administration web interface. The left sidebar contains navigation menus for 'MONITOR & ANALYZE', 'PROTECT', 'CONFIGURE', and 'SYSTEM'. The 'Administration' menu is highlighted. The main content area is titled 'Administration' and shows a 'Local service ACL' configuration page. The 'Device access' tab is selected. A table lists various services for different zones. The 'GUEST' zone is highlighted with a red box, showing that 'Captive portal' is enabled. Below the table, there is a note about turning off access to the captive portal and an 'Apply' button. At the bottom, there is a section for 'Local service ACL exception rule' which is currently empty.

Zone	Admin services		Authentication services					Network services		
	HTTPS	SSH	AD SSO	Captive portal *	Radius SSO	Clients	Chromebook SSO	Ping/Ping6	DNS	IP
LAN	☒	☒	☐	☒	☒	☒	☒	☒	☒	☐
WAN	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
DMZ	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
VPN	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
WiFi	☒	☒	☐	☒	☒	☒	☒	☒	☒	☐
GUEST	☐	☐	☐	☒	☐	☐	☐	☐	☒	☐

Turning off access to captive portal stops user notifications from appearing. Example: Web filter and zero-day protection notification pages.

Apply

Local service ACL exception rule

Show additional properties

#	Name	Source zone	Source	Destination
No records found				

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.

Cihaz Detayları

Cihaz Adresi

178.159.35.173

☒ 5651 Loglama

Cihaz Adı

Sophos-GLX-Test

Cihaz Şifresi

bjhcqhml

SOPHOS FW

Search

MONITOR & ANALYZE

Control center

Current activities

Reports

Zero-day protection

Diagnostics

PROTECT

Rules and policies

Intrusion prevention

Web

Applications

Wireless

Email

Web server

Active threat response

CONFIGURE

Remote access VPN

Site-to-site VPN

Network

Routing

Authentication

System services

SYSTEM

Sophos Central

Profiles

Hosts and services

Administration

Backup & firmware

Certificates

Edit external server

Servers

Services

Groups

Users

Multi-factor authentication

Server type

RADIUS server

Server name *

Useroam

Server IP *

104.247.174.120

Authentication port *

1812

Time-out *

3

☒ Enable accounting

Accounting port

1813

Shared secret *

***** [Change Shared secret](#)

Domain name ⁱ

Enter Domain name

Group name attribute *

Filter-Id

☐ Enable additional settings

Test connection

Save

Cancel

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.

SOPHOS FW

Search

MONITOR & ANALYZE

- Control center
- Current activities
- Reports
- Zero-day protection
- Diagnostics

PROTECT

- Rules and policies
- Intrusion prevention
- Web
- Applications
- Wireless
- Email
- Web server
- Active threat response

CONFIGURE

- Remote access VPN
- Site-to-site VPN
- Network
- Routing
- Authentication**
- System services

SYSTEM

- Sophos Central
- Profiles
- Hosts and services
- Administration
- Backup & firmware
- Certificates

Add external server

Servers Services Groups Users Multi-factor authentication Web authentication Guest users

Server type: RADIUS server

Server name *: Useroam

Server IP *: 104.247.174.120

Authentication port *: 1812

Time-out *: 3

☐ Enable accounting

Accounting port:

Shared secret *:

Domain name: Enter Domain name

Group name attribute *: Filter-Id

☐ Enable additional settings

Test connection

Username *: test1

Password *:

Test connection

Test connection Save Cancel

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.

SOPHOS Fw

Search 

MONITOR & ANALYZE
Control center
Current activities
Reports
Zero-day protection
Diagnostics

PROTECT
Rules and policies
Intrusion prevention
Web
Applications
Wireless
Email
Web server
Active threat response

CONFIGURE
Remote access VPN
Site-to-site VPN
Network
Routing
Authentication
System services

Authentication

Servers **Services** Groups

Firewall authentication methods

Authentication server list

type to search...

☒ Local
☒ Useroam

Selected authentication server

Useroam 

Local 

drag to change priority

Default group

Open Group 

Apply

User portal authentication methods

☒ Set authentication methods same as firewall

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.

SOPHOS FW

Search

MONITOR & ANALYZE

- Control center
- Current activities
- Reports
- Zero-day protection
- Diagnostics

PROTECT

- Rules and policies
- Intrusion prevention
- Web
- Applications
- Wireless
- Email
- Web server
- Active threat response

CONFIGURE

- Remote access VPN
- Site-to-site VPN
- Network
- Routing
- Authentication**
- System services

SYSTEM

- Sophos Central
- Profiles
- Hosts and services
- Administration
- Backup & firmware
- Certificates

Servers Services Groups Users Multi-factor authentication **Web authentication** Guest users Clientless

Authorize unauthenticated users for web access

If Active Directory (AD) SSO is configured

AD SSO mechanism

☐ NTLM only ☒ Kerberos & NTLM

If AD SSO fails, captive portal appears.

If AD SSO isn't configured

When unauthenticated user reaches a block page

☒ Show captive portal link

Captive portal behavior

☒ Show user portal link

☒ Show web page after sign-in

Open web page

☒ In new browser window

☐ In captive portal window

Web page

☒ Originally requested by user

☐ Custom

Sign out user

These options don't apply to Azure AD. Users are signed out based on the Azure AD token expiration time.

☐ When captive portal page is closed or redirected

☒ When user is inactive

☐ Never

☒ Use insecure HTTP instead of HTTPS

Traffic flow required to consider the user active

100 bytes in 140 minutes

Apply

7 - Captive Portal Tasarımın 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.

Kurulum Dökümanı

Template

```
1 <html>
2 <head>
3 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
4 <meta name="viewport" content="width=device-width, initial-scale=1">
5 <meta http-equiv="X-UA-Compatible" content="IE=edge">
6 <link rel="shortcut icon" href="https://panel.useroam.com/sophos-cloud/img/favicon.ico">
7 <title>Useroam Captive Portal</title>
8 <link href="https://panel.useroam.com/sophos-cloud/css/Useroam.css" rel="stylesheet">
9 <!--[if lt IE 9]>
10 <script src="https://panel.useroam.com/sophos-cloud/js/html5shiv.js"></script>
11 <script src="https://panel.useroam.com/sophos-cloud/js/respond.min.js"></script>
12 <![endif]-->
13 </head>
14 <body>
15 <div class="container" id="login-block">
16 <div class="row">
17 <div class="col-sm-6 col-md-4 col-sm-offset-3 col-md-offset-4">
18 <div class="login-box clearfix animated flipInX">
19 <div class="login-logo"></div>
20 <div class="login-form">
```

Cihazı Sil

Servers Services Groups Users Multi-factor authentication **Web authentication**

☐ Use per-connection AD SSO authentication for multi-user hosts ⓘ

Multi-user hosts

Add new item

Apply

Captive portal appearance

Layout

☐ Default layout ☒ Custom HTML

Custom HTML must include a <div> element with id "loginbox", that is, <div id="loginbox">.

The required input elements are inserted into this div. You can customize these elements, using CSS and JavaScript.

Preview may not show the full result, since JavaScript code won't execute in the preview window.

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<link rel="shortcut icon" href="https://panel.useroam.com/sophos-cloud/img/favicon.ico">
<title>Useroam Captive Portal</title>
<link href="https://panel.useroam.com/sophos-cloud/css/Useroam.css" rel="stylesheet">
<!--[if IE 9]>
<script src="https://panel.useroam.com/sophos-cloud/js/html5shiv.js"></script>
<script src="https://panel.useroam.com/sophos-cloud/js/respond.min.js"></script>
<![endif]-->
</head>
<body>
<div class="container" id="login-block">
<div class="row">
<div class="col-sm-6 col-md-4 col-sm-offset-3 col-md-offset-4">
<div class="login-box clearfix animated flipInX">
<div class="login-logo"></div>
<div class="login-form">
<div class="login-links" id="login-links">
</div>
<form action="#" id="cetus_form" method="POST" enctype="multipart/form-data">
```

Apply Preview >> Reset to default

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.

SOPHOS FW

Search

MONITOR & ANALYZE

- Control center
- Current activities
- Reports
- Zero-day protection
- Diagnostics

PROTECT

- Rules and policies
- Intrusion prevention
- Web
- Applications
- Wireless
- Email
- Web server
- Active threat response

CONFIGURE

- Remote access VPN
- Site-to-site VPN
- Network
- Routing
- Authentication**
- System services

SYSTEM

- Sophos Central
- Profiles
- Hosts and services
- Administration
- Backup & firmware
- Certificates

Authentication

Servers Services Groups Users Multi-factor authentication

☒ Local
☐ Useroam

drag to change priority

Apply

Global settings

Maximum session time-out * ☒ Unlimited Minutes (between 3-1440)

Simultaneous logins * ☒ Unlimited (1-99)

Apply

AD SSO settings (NTLM and Kerberos)

Inactivity time 6 Minutes (between 6-1440)

Data transfer threshold 1024 bytes

HTTP challenge redirect on "Intranet zone" ☒ Enable

Apply

Firewall Kuralları'nın Oluşturulması?

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.

SOPHOS FW

Search

MONITOR & ANALYZE

Control center

Current activities

Reports

Zero-day protection

Diagnostics

PROTECT

Rules and policies

Intrusion prevention

Web

Applications

Wireless

Email

Web server

Active threat response

CONFIGURE

Remote access VPN

Site-to-site VPN

Network

Routing

Authentication

System services

SYSTEM

Sophos Central

Profiles

Hosts and services

Administration

Backup & firmware

Certificates

Add firewall rule

How-to guides Log viewer

☒ Rule status

Rule name *
GUEST TO DNS

Action
Accept

☒ Log firewall traffic
Log traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.

Description
GUEST TO DNS

Rule position
Top

Rule group
GUEST

Source

Select the source zones, networks, and devices.
The rule applies to traffic from these sources during the scheduled time period.

Source zones *
GUEST

Source networks and devices *
Any

During scheduled time
All the time

Destination and services

Select the destination zones, networks, devices, and services.
The rule applies to traffic to these destinations.

Destination zones *
WAN

Destination networks *
Any

Services *
DNS

KURAL 2: Guest to Useroam

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

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

SOPHOS FW

Search

MONITOR & ANALYZE

Control center

Current activities

Reports

Zero-day protection

Diagnostics

PROTECT

Rules and policies

Intrusion prevention

Web

Applications

Wireless

Email

Web server

Active threat response

CONFIGURE

Remote access VPN

Site-to-site VPN

Network

Routing

Authentication

System services

SYSTEM

Sophos Central

Profiles

Hosts and services

Administration

Backup & firmware

Certificates

Edit firewall rule

How-to guides Log viewer

☒ Rule status

Rule name *
GUEST TO USEROAM

Action
Accept

☒ Log firewall traffic
Log traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.

Description
GUEST TO USEROAM

Rule group
GUEST

Source

Select the source zones, networks, and devices.
The rule applies to traffic from these sources during the scheduled time period.

Source zones *
GUEST

Source networks and devices *
Any

During scheduled time
All the time

Destination and services

Select the destination zones, networks, devices, and services.
The rule applies to traffic to these destinations.

Destination zones *
WAN

Destination networks *
panel.useroam.com

Services *
HTTP
HTTPS

☐ Match known users

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.

MONITOR & ANALYZE

- Control center
- Current activities
- Reports
- Zero-day protection
- Diagnostics

PROTECT

- Rules and policies**
- Intrusion prevention
- Web
- Applications
- Wireless
- Email
- Web server
- Active threat response

CONFIGURE

- Remote access VPN
- Site-to-site VPN
- Network
- Routing
- Authentication
- System services

SYSTEM

- Sophos Central
- Profiles
- Hosts and services
- Administration
- Backup & firmware
- Certificates

Web server

- Active threat response

CONFIGURE

- Remote access VPN
- Site-to-site VPN
- Network
- Routing
- Authentication
- System services

SYSTEM

- Sophos Central
- Profiles
- Hosts and services
- Administration
- Backup & firmware
- Certificates

Rule status

Rule name *
GUEST TO INTERNET

Action
Accept

☒ Log firewall traffic
Log traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.

Description
GUEST TO INTERNET

Rule position
Bottom

Rule group
GUEST

Source
Select the source zones, networks, and devices.
The rule applies to traffic from these sources during the scheduled time period.

Source zones *
GUEST

Source networks and devices *
Any

During scheduled time
All the time

Destination and services
Select the destination zones, networks, devices, and services.
The rule applies to traffic to these destinations.

Destination zones *
WAN

Destination networks *
Any

Services *
Any

☒ Match known users
☒ Use web authentication for unknown users

User or groups *
Any

☐ Exclude this user activity from data accounting

Security features

Web filtering

Web policy
Allow All

☐ Apply web category-based traffic shaping

☒ Block QUIC protocol

Malware and content scanning

☐ Scan HTTP and decrypted HTTPS

☐ Use zero-day protection

☐ Scan FTP for malware

Filtering common web ports

☐ Use web proxy instead of DPI engine

☒ DPI engine or web proxy?

Web proxy options

☐ Decrypt HTTPS during web proxy filtering

Configure Synchronized Security Heartbeat

Other security features

Identify and control applications (App control)
Allow All

☐ Apply application-based traffic shaping policy

Detect and prevent exploits (IPS)
None

Scan email content

Shape traffic
User's policy applied

DSCP marking
Select DSCP marking

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

SOPHOS Firewall

Rules and policies

Firewall rules NAT rules

IPv4 IPv6 Disable filter Test your policies

Rule type Source zone Destination zone Status Rule ID Add Filter

#	Name	Source	Destination	What
1	GUEST TO DNS in 0 B, out 0 B	GUEST, Any host	WAN, Any host	DNS
2	GUEST TO USEROAM in 0 B, out 0 B	GUEST, Any host	WAN, panel.useroam.com	HTTP, HTTPS
3	GUEST TO INTERNET in 0 B, out 0 B	GUEST, Any host, Any live user...	WAN, Any host	Any service

Loglar?n Useroam Cihaz?na Yönlendirilmesi

1 - Syslog Server Tan?mlama

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

SOPHOS Firewall

System services

High availability Traffic shaping settings RED Malware protection Log settings

Name * Useroam Cloud

IP address / Domain * panel.useroam.com

Secure log transmission ☐

Port * 514

Facility * DAEMON

Severity level * Information

Format * Standard syslog protocol

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]

Name *	UseroamCloud
IP address / Domain *	104.247.174.120
Secure log transmission	☐
Port *	514
Facility *	DAEMON
Severity level *	Debug
Format *	Standard syslog protocol

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

SOPHOS
Search
MONITOR & ANALYZE
Control center
Current activities
Reports
Zero-day protection
Diagnostics
PROTECT
Rules and policies
Intrusion prevention
Web
Applications
Wireless
Email
Web server
Active threat response
CONFIGURE
Remote access VPN
Site-to-site VPN
Network
Routing
Authentication
System services
SYSTEM
Sophos Central
Profiles
Hosts and services
Administration
Backup & firmware
Certificates

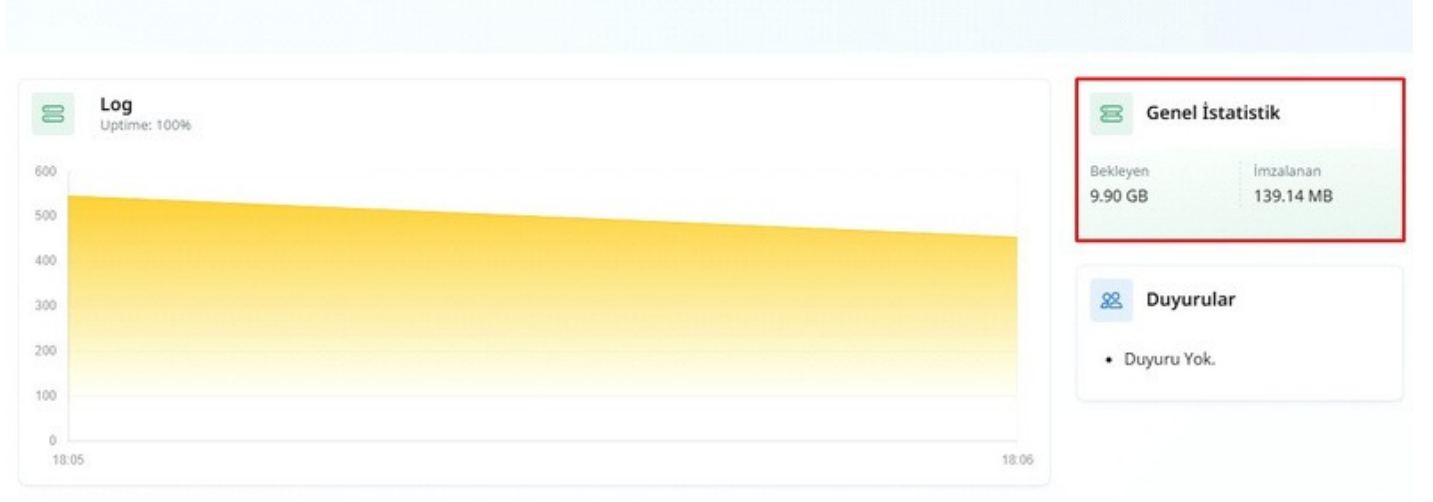
Feedback How-to guides Log viewer Help GLOX TEKNO

High availability	Traffic shaping settings	RED	Malware protection	Log settings	Notification list	Data anonymization	Traffic shaping
Anti-spam	☐	☐	☐	☐		☐	
SMTP		☒	☐	☐		☐	
POP3		☒	☐	☐		☐	
IMAP		☒	☐	☐		☐	
SMTPS		☒	☐	☐		☐	
POPS		☒	☐	☐		☐	
IMAPS		☒	☐	☐		☐	
Content filtering	☐	☐	☐	☐		☒	
Web filter		☒	☐	☐		☒	
Application filter		☒	☐	☐		☒	
Web content policy		☒	☐	☐		☒	
SSL/TLS filter		☒	☐	☐		☒	
Events	☐	☐	☐	☐		☐	
Admin events		☒	☐	☐		☐	
Authentication events		☒	☐	☐		☐	
System events		☒	☐	☐		☐	
Web server protection	☐	☐	☐	☐		☐	
Web server protection events		☒	☐	☐		☐	
Active threat response	☐	☐	☐	☐		☐	

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** alanının 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.

Yeni Cihaz



Cihaz Detayları

JS0Q8GFCWM3OM2YAH27U629YKAH3

Cihaz Tipi
Fortinet

☒ 5651 Loglama

Cihaz Adresi
178.159.35.173

Cihaz Adı
GLX-Fortigate-FW

Kaydet

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.

USEROAM
HOTSPOT & REPORTING

Menü

- Dashboard
- Kullanıcı Listeleri
- Kullanıcı Yönetimi
- Karşılama Portalı
- Sistem ayarları**
- Bildirimler
- Cihaz Ayarları**
- Yöneticiler
- SMS ayarları
- Lisans Bilgileri

Cihaz Ayarları
Şuan Buradasınız

Dashboard > Cihaz Düzenle

Cihaz Detayları

Cihaz Adresi
178.159.35.173

5651 Loglama

Cihaz Adı
GLX-Fortigate-Test-FW

Cihaz Şifresi
z3zgkb5g

Kaydet

Dashboard	Manage Images	Edit	Search	Simple View	Extended View
Network					
Policy & Objects					
Security Profiles					
VPN					
User & Authentication					
WiFi Controller					
System					
Administrators					
Admin Profiles					
Fabric Management					
Settings					
HA					
SNMP					
Replacement Messages					
FortiGuard					
Feature Visibility					
Certificates					
Security Fabric					
Log & Report					

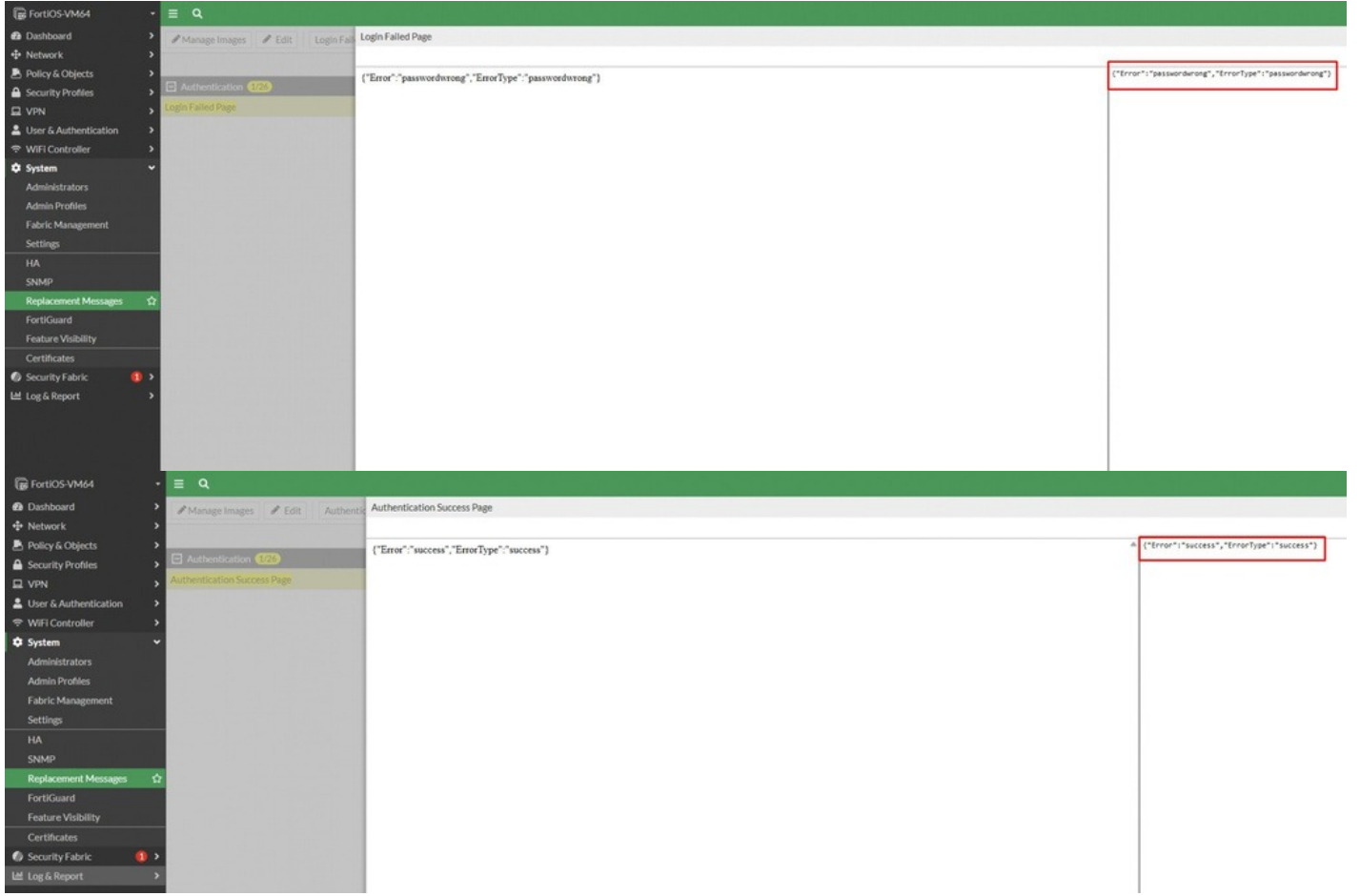
Name	Description
Admin 2	
Post-login Disclaimer Message	Replacement message for post-login disclaimer
Pre-login Disclaimer Message	Replacement message for pre-login disclaimer
Alert E-mail 5	
Block Message	Alert email text for block incidents
Critical Event Message	Alert email text for critical event notification
Disk Full Message	Alert email text for disk full events
Intrusion Message	Alert email text for IPS events
Virus Message	Alert email text for virus incidents
Authentication 26	
Authentication Rejection Page	Replacement HTML for authentication rejection page
Authentication Success Page	Replacement HTML for authentication success page
Block Notification Page	Replacement HTML for block notification page
Certificate Password Page	Replacement HTML for certificate password page
Declined Disclaimer Page	Replacement HTML for user declined disclaimer page
Declined Quarantine Page	Replacement HTML for user declined quarantine page
Disclaimer Page	Replacement HTML for authentication disclaimer page

3 - Karşılama Ekranı Mesajları (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.

Template

```

1      <html>
2      <head>
3      <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
4      <meta name="viewport" content="width=device-width, initial-scale=1">
5      <meta http-equiv="X-UA-Compatible" content="IE=edge">
6      <link rel="shortcut icon" href="http://panel.useroam.com/fortinet-cloud/img/favicon.ico">
7      <title>Useroam Captive Portal</title>
8      <link href="http://panel.useroam.com/fortinet-cloud/css/Useroam.css" rel="stylesheet">
9      <!--[if lt IE 9]>
10     <script src="http://panel.useroam.com/fortinet-cloud/js/html5shiv.js">
11     </script>
12     <script src="http://panel.useroam.com/fortinet-cloud/js/respond.min.js">
13     </script>
14     <![endif]-->
15     </head>
16     <body>
17     <div class="container" id="login-block">
18     <div class="row">
19     <div class="col-sm-6 col-md-4 col-sm-offset-3 col-md-offset-4">
20     <div class="login-box clearfix animated flipInX">

```

Cihazı Sil

FortiOS-VM64

Dashboard

Network

Policy & Objects

Security Profiles

VPN

User & Authentication

WiFi Controller

System

Administrators

Admin Profiles

Fabric Management

Settings

HA

SNMP

Replacement Messages

FortiGuard

Feature Visibility

Certificates

Security Fabric

Log & Report

Login Page

Message Format: text/html Message Size: 1.6 kB/32.8 kB

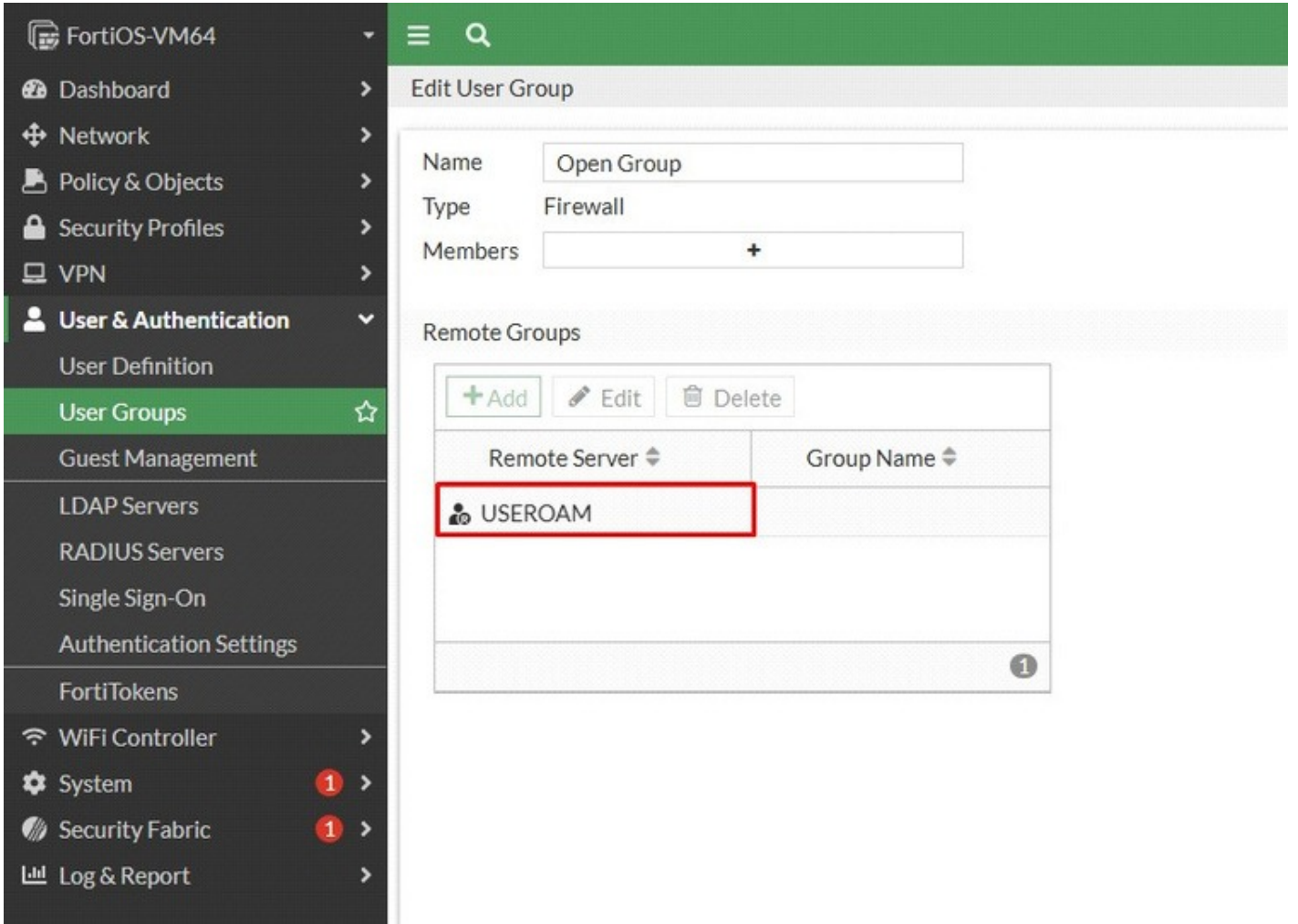
```

<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<link rel="shortcut icon" href="http://panel.useroam.com/fortinet-cloud/img/favicon.ico">
<title>Useroam Captive Portal</title>
<link href="http://panel.useroam.com/fortinet-cloud/css/Useroam.css" rel="stylesheet">
<!--[if lt IE 9]>
<script src="http://panel.useroam.com/fortinet-cloud/js/html5shiv.js">
</script>
<script src="http://panel.useroam.com/fortinet-cloud/js/respond.min.js">
</script>
<![endif]-->
</head>
<body>
<div class="container" id="login-block">
<div class="row">
<div class="col-sm-6 col-md-4 col-sm-offset-3 col-md-offset-4">
<div class="login-box clearfix animated flipInX">
<div class="login-logo">
</div>
<div class="login-form">
<div class="login-links" id="login-links">
</div>
<form action="#" id="cetus_form" method="POST">
<input type="hidden" name="4fredis" value="4fredis">
<input type="hidden" name="magic" value="4fredis">
<input type="text" name="4fredis" id="username">
<input type="password" name="4fredis" id="password">
<button type="submit" id="loginbutton" class="btn btn-blue btn-lg btn-block">
Giriş
</button>
</form>
</div>
</div>
<div class="social-login row">
</div>
</div>
</div>
<div id="__loginbox">
</div>
<script id="UseroamId" data-name="Nz2710NDc1NzcxNzU458" src="http://panel.useroam.com/fortinet-cloud/js/load.js">
</script>
</body>
</html>

```

4 - Kullanıcı Grubu Oluşturma (User Groups)

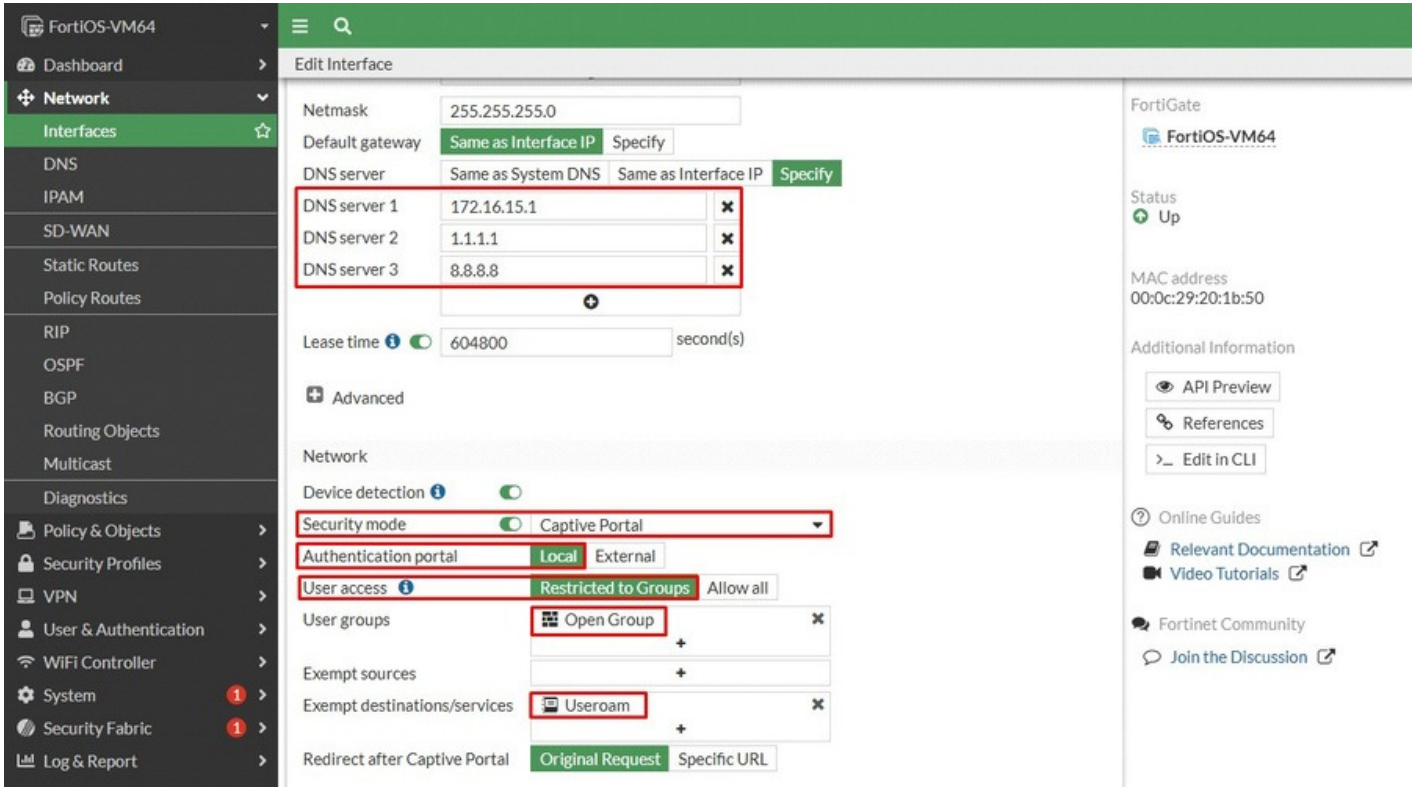
User & Authentication > User Groups menüsünden kendinize Useroam Cloud için bir grup oluşturunuz.



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.

FortiOS-VM64

Dashboard

Network

Policy & Objects

Firewall Policy

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

Security Profiles

VPN

User & Authentication

WiFi Controller

System

Security Fabric

Log & Report

Edit Policy

Name: GUEST TO DNS

Incoming Interface: GUEST (port3)

Outgoing Interface: INTERNET

Source: all

Destination: all

Schedule: always

Service: DNS

Action: ACCEPT DENY

Firewall/Network Options

NAT: ☒

IP Pool Configuration: Use Outgoing Interface Address Use Dynamic IP Pool

Preserve Source Port: ☐

Protocol Options: PROXY default

Security Profiles

AntiVirus: ☐

Web Filter: ☐

DNS Filter: ☐

Application Control: ☐

IPS: ☐

File Filter: ☐

SSL Inspection: SSL no-inspection

Logging Options

Log Allowed Traffic: ☒ Security Events All Sessions

Generate Logs when Session Starts: ☐

Capture Packets: ☐

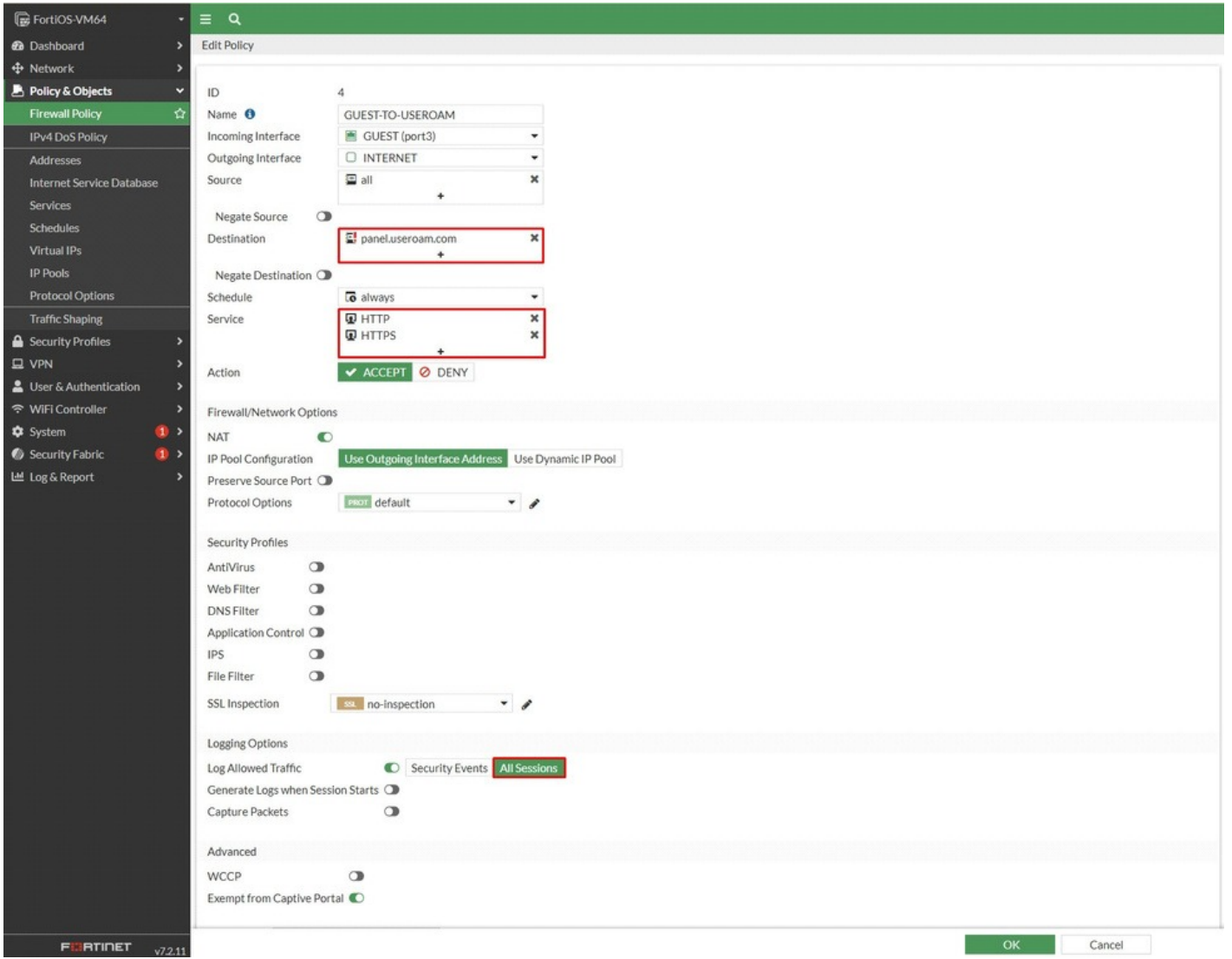
Comments: Write a comment... 0/1023

Enable this policy: ☒

OK Cancel

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.

New Policy

Name: GUEST TO INTERNET

Incoming Interface: GUEST (port3)

Outgoing Interface: INTERNET

Source: all, Open Group

Destination: all

Schedule: always

Service: ALL

Action: ACCEPT, DENY

Firewall/Network Options

NAT: ☒ NAT

IP Pool Configuration: Use Outgoing Interface Address, Use Dynamic IP Pool

Preserve Source Port: ☐

Protocol Options: default

Security Profiles

AntiVirus: ☐

Web Filter: ☒ WEB default

DNS Filter: ☐

Application Control: ☒ APP default

IPS: ☐

File Filter: ☐

SSL Inspection: ☐ SSL no-inspection

Logging Options

Log Allowed Traffic: ☒ Security Events, All Sessions

Generate Logs when Session Starts: ☐

Capture Packets: ☐

Comments: Write a comment... 0/1023

Enable this policy: ☒

OK Cancel

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

FortiOS-VM64

Dashboard

Network

Policy & Objects

Firewall Policy

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Create New

Edit

Edit in CLI

Delete

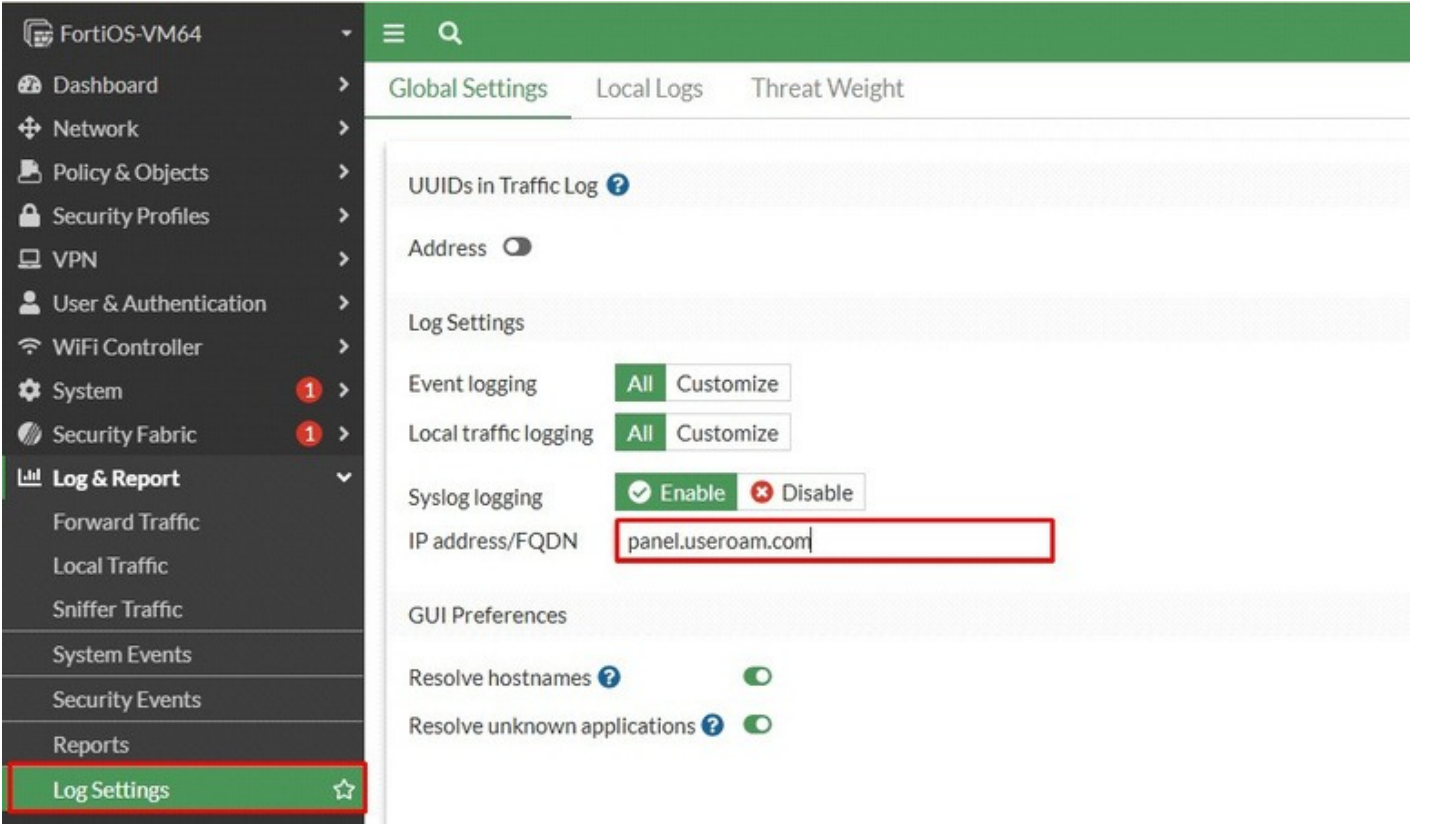
Policy lookup

Search

Name	Source	Destination	Schedule	Service	Action	NAT
GUEST (port3) → INTERNET						
GUEST TO DNS	all	all	always	DNS	ACCEPT	Enabled
GUEST-TO-USEROAM	all	panel.useroam.com	always	HTTP HTTPS	ACCEPT	Enabled
GUEST TO INTERNET	Open Group all	all	always	ALL	ACCEPT	Enabled
Implicit						
Implicit Deny	all	all	always	ALL	DENY	

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 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

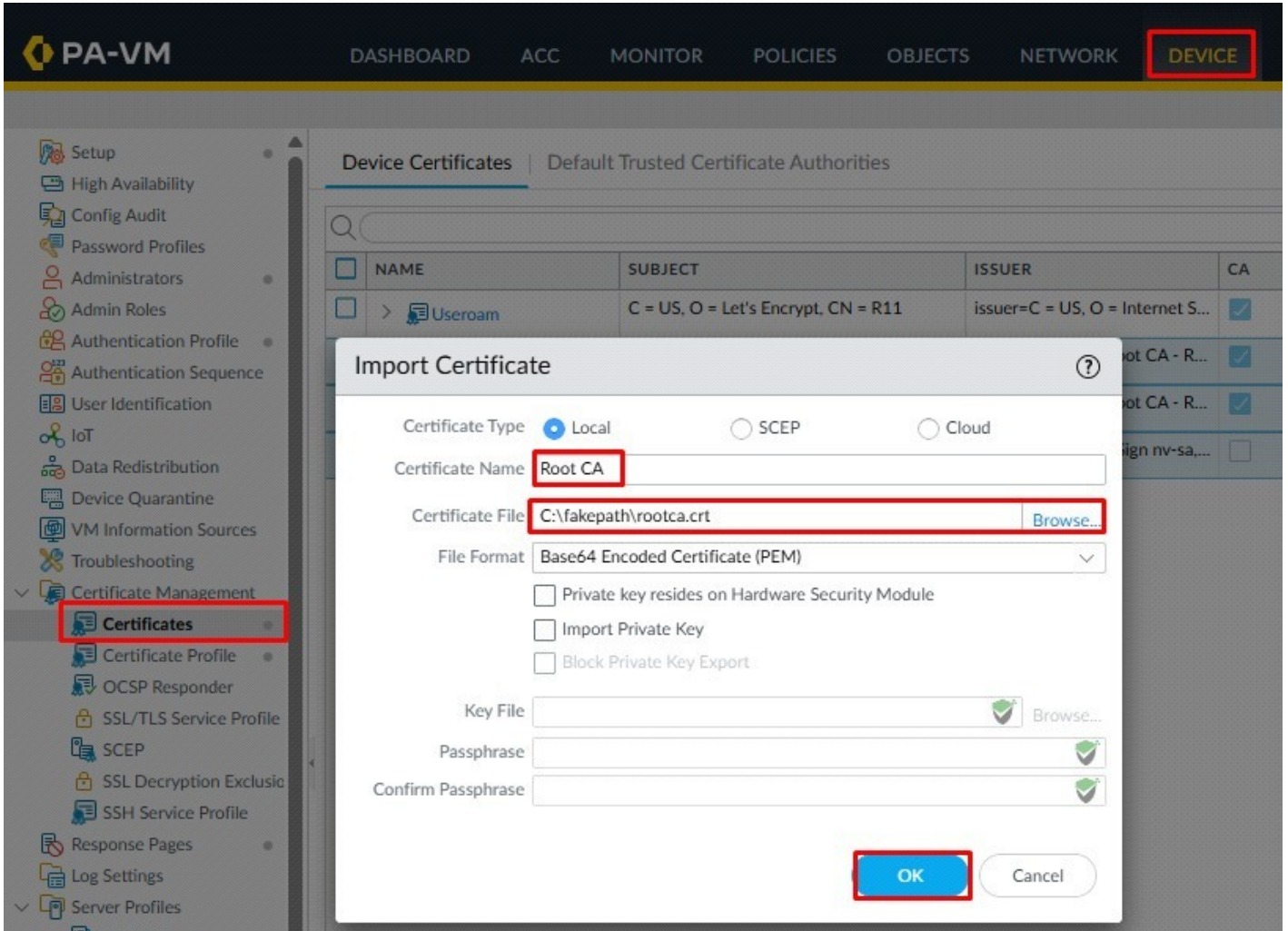
OKCancel

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.

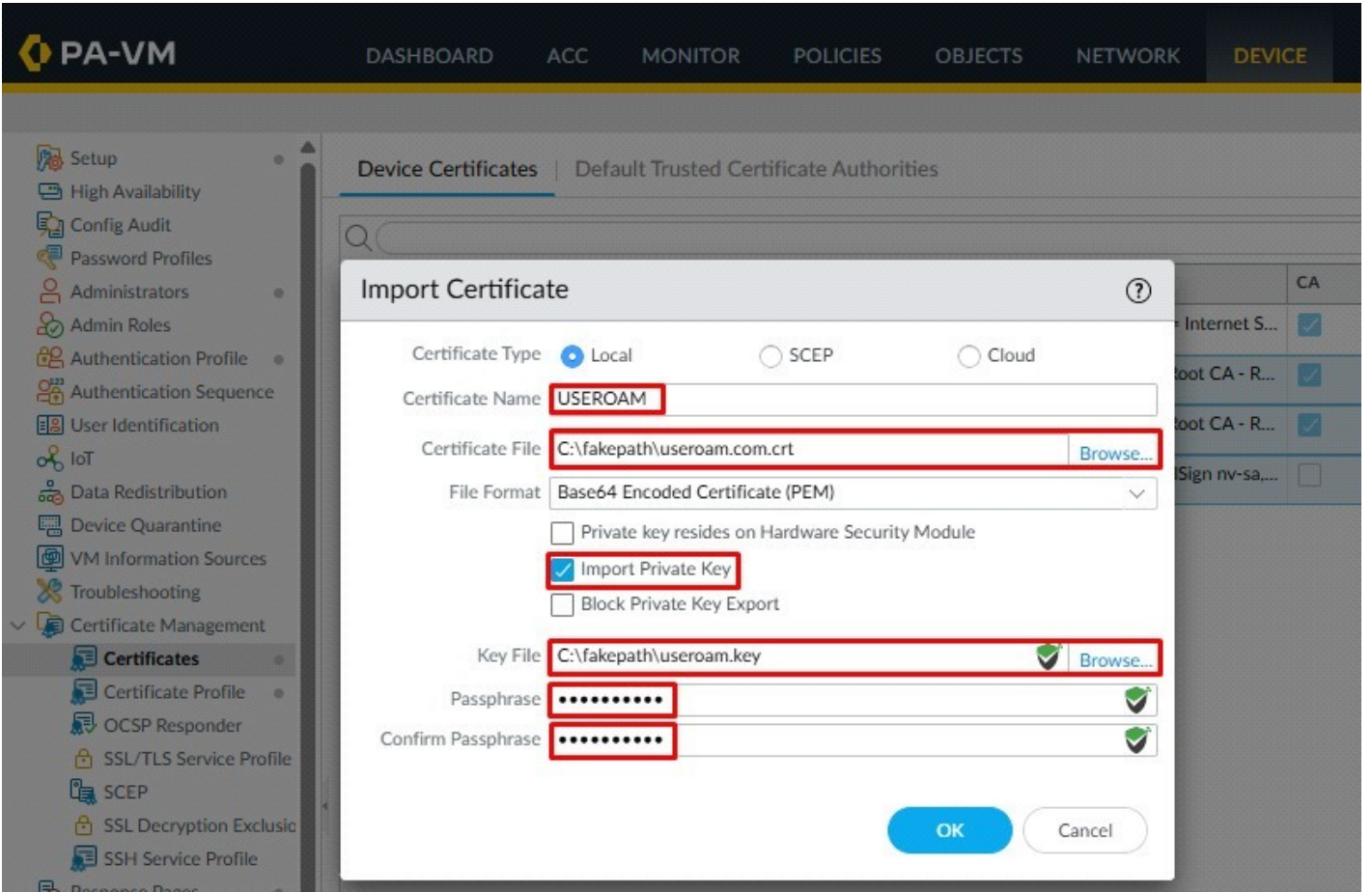
6A - Root CA Import ??lemi

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



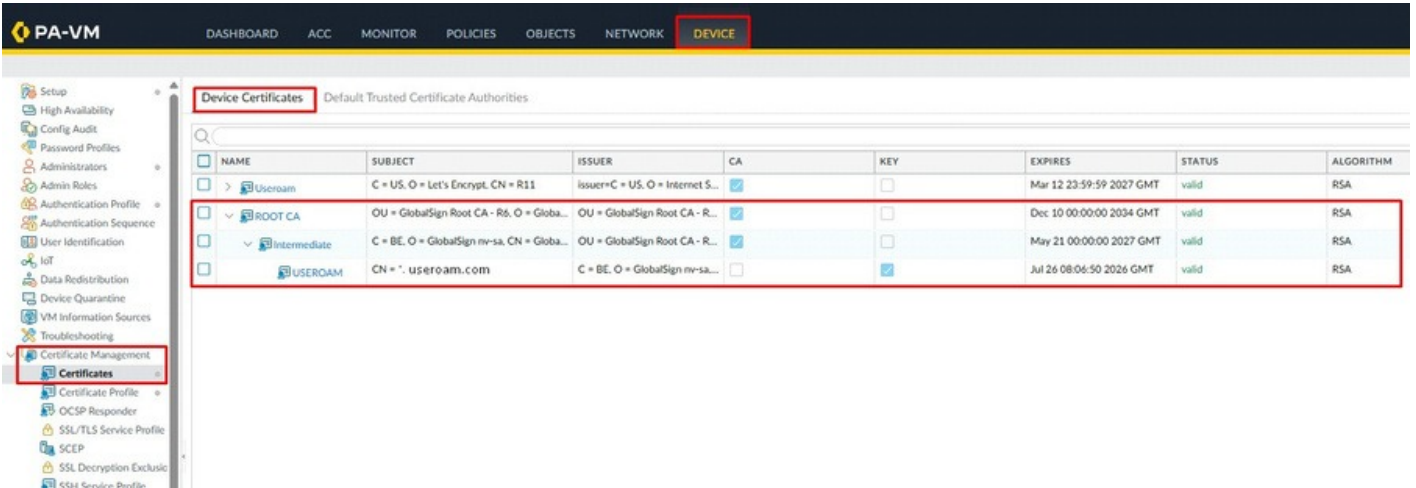
6B - Sertifika ve Anahtar Dosyası'nın Yüklenmesi

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: **TLsv1.0**

Max Version: **Max**

OK **Cancel**

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

Authentication Profile: **UseroamProfile**

Authentication Prole : Oluřturulan Useroam prolini seerek devam ediniz.

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

Redirect Host : Buraya sertika zerinden ynlendirme yapılacağı 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**

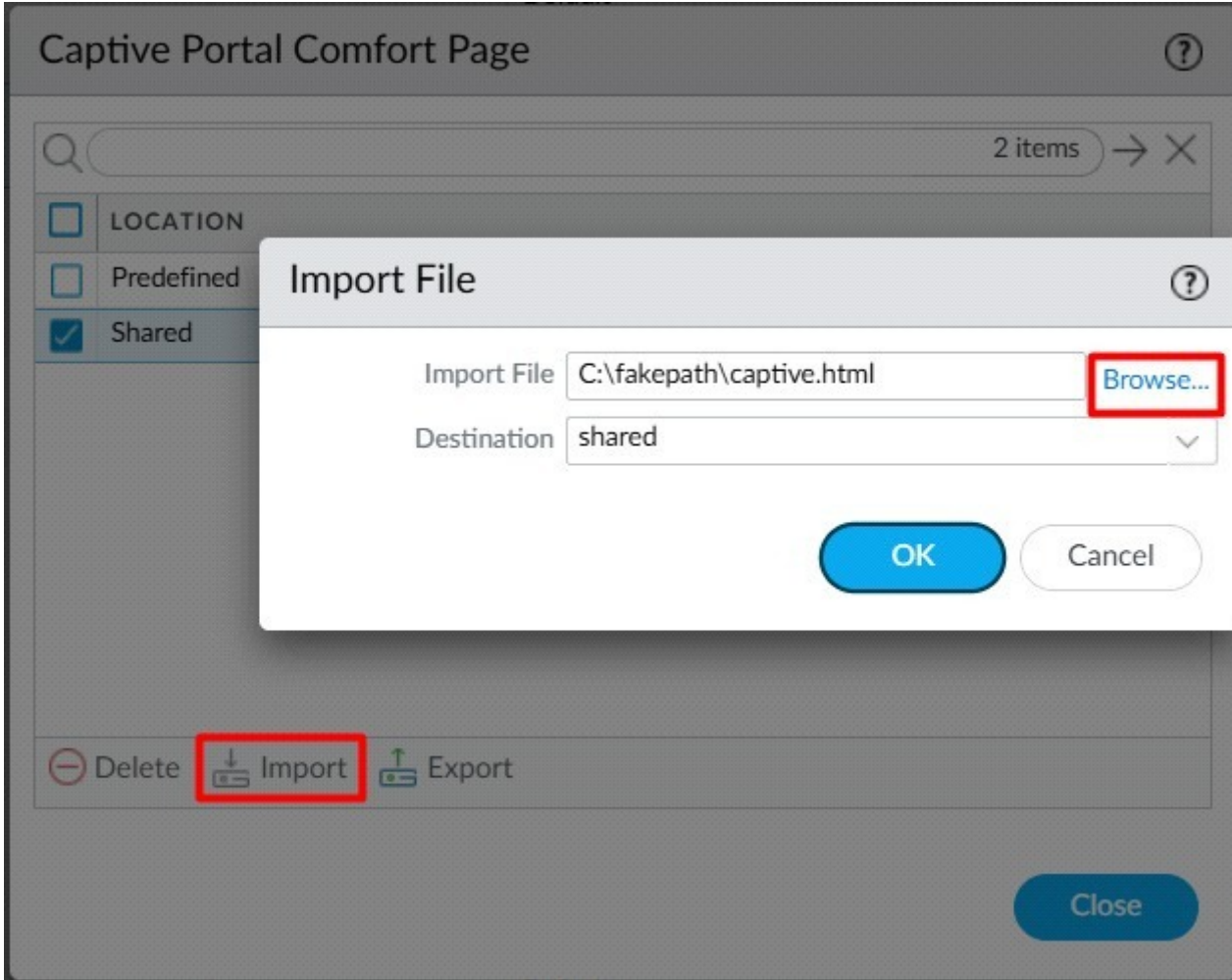
Certificate Authentication

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.

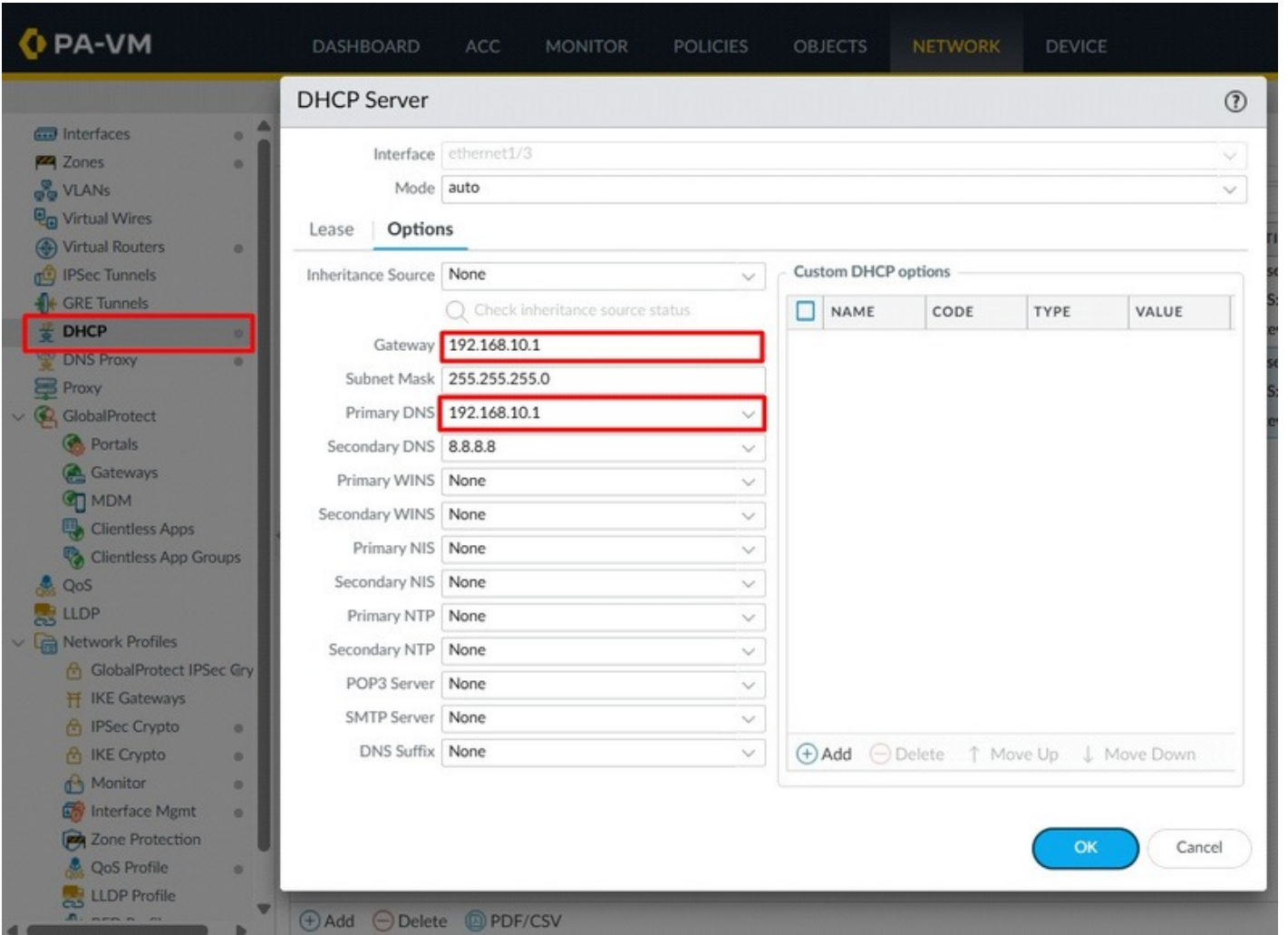


9 - DHCP Ayarlar?

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).

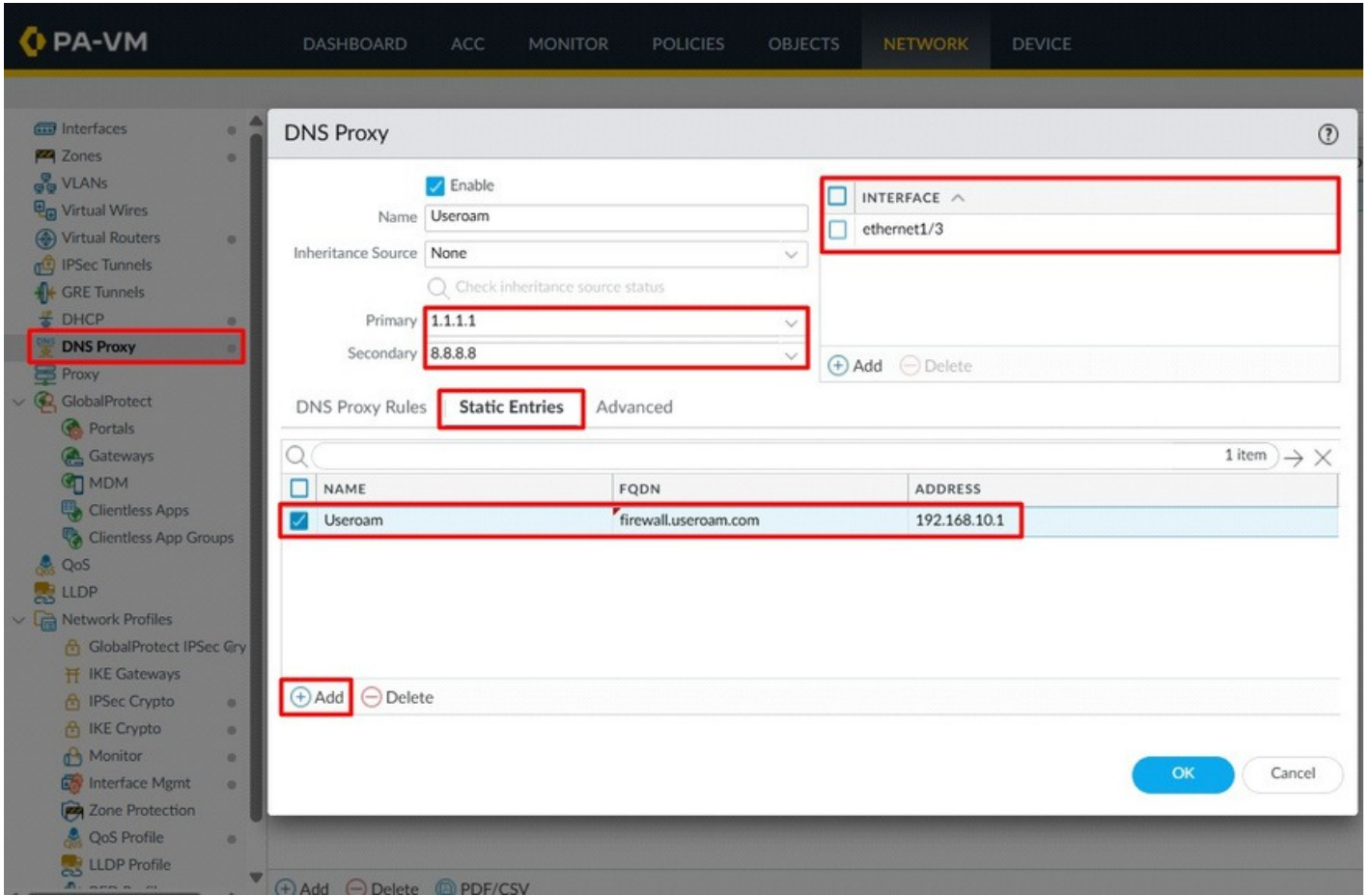
Not: Mevcutta içeride bir DNS sunucunuz varsa alan adı yönlendirmesi için gerekli kaydı iç DNS ağınızda da (Static Entries kısmında) tanımlayarak 11. adımdan devam edebilirsiniz.



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.

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 kuracaksınız onu tanımlayınız.

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

2 - Bridge ve Port Yapılandırması

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 Ağ 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=P00L-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 içerisinde **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 Sıkılaştırma (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 Görünürlüğü 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 Doğrulama Adımları

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 Tamamlandı?

Hepsi bu kadar! MikroTik mevcut cihaz üzerinde misafir ağı, Hotspot ve Useroam entegrasyon işlemlerinizi başarıyla tamamladı. 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.

USEROAM
HOTSPOT & REPORTING

Yeni Cihaz

Cihaz Detayları

Useroam Teknoloji LTD. ŞTİ. ▼

Lütfen hesap seçiniz ▼

Cihaz Tipi
Ruijie

☒ 5651 Loglama

Cihaz Seri Numarası

Cihaz Adresi

Cihaz Adı

Kaydet

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.

Ruijie Cybrey

Home O&M Policy Object Network System

Search

Quick Onboarding Policy Wizard Customer Service English admin

Address App Service Region Time Plan User Authentication Authentication Settings Authentication Server Content Identification Lib. Content Template Security Rule Base ISP Address Library Certificate

Allowlist SSO Other Authentication Settings

Create Delete Refresh

Search whitelist

Src. IP Dest. IP URL Src. MAC

Allowlist	Description	Operation
☐	104.247.174.120	Edit Delete
☐	157.240.0.0/16	Edit Delete
☐	31.13.64.0/18	Edit Delete
☐	31.13.24.0/21	Edit Delete
☐	179.60.192.0/22	Edit Delete
☐	185.60.216.0/22	Edit Delete
☐	102.132.96.0/20	Edit Delete
☐	129.134.0.0/16	Edit Delete
☐	69.171.224.0/19	Edit Delete
☐	66.220.144.0/20	Edit Delete

Cancel

URL

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.

Ruijie Cybrey

Home O&M Policy Object Network System

Search

Quick Onboarding Policy Wizard Customer Service English admin

Address App Service Region Time Plan User Authentication Authentication Settings Authentication Server Content Identification Lib. Content Template Security Rule Base ISP Address Library Certificate

Allowlist SSO Other Authentication Settings

Create Delete Refresh

Search whitelist

Src. IP Dest. IP URL Src. MAC

Allowlist	Description	Operation
☐	whatsapp.net	Edit Delete
☐	whatsapp.com	Edit Delete
☐	g.whatsapp.net	Edit Delete
☐	v.whatsapp.net	Edit Delete
☐	mmg.whatsapp.net	Edit Delete
☐	media.whatsapp.net	Edit Delete
☐	static.whatsapp.net	Edit Delete
☐	cdn.whatsapp.net	Edit Delete
☐	web.whatsapp.com	Edit Delete
☐	*.useroam.com	Edit Delete

10 / Page Total:10

Go to 1 < 1 >

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:

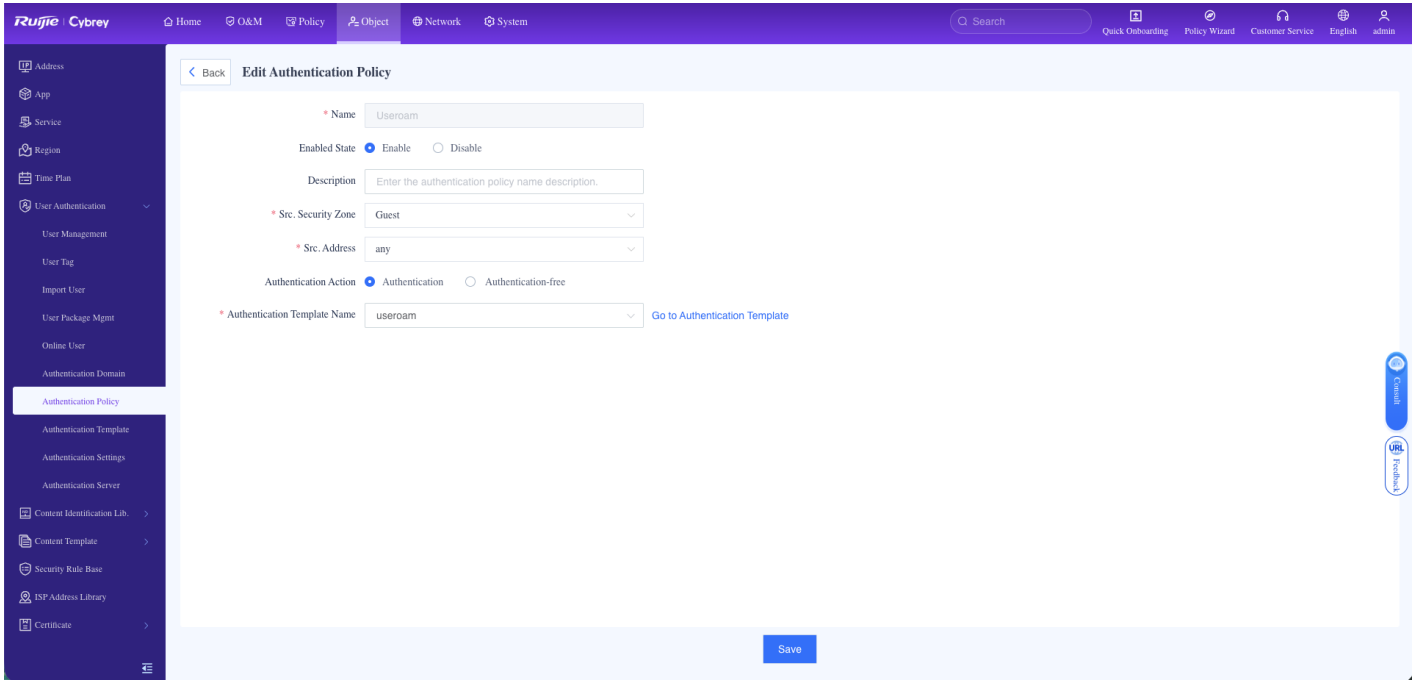
- **Version:** Wifidog V1 seçiniz.
- **Authentication Template Name:** useroam
- **Server URL:** `http://104.247.174.120/ruijie-cloud/`
- **Permission Mode:** Do Not Permit seçiniz.
- **Sending Source:** Default olarak bırakınız.

The screenshot shows the Ruijie Cybrey web interface. The left sidebar contains a menu with options like Address, App, Service, Region, Time Plan, User Authentication, User Management, User Tag, Import User, User Package Mgmt, Online User, Authentication Domain, Authentication Policy, Authentication Template, Authentication Settings, Authentication Server, Content Identification Lib., Content Template, Security Rule Base, ISP Address Library, and Certificate. The main area is titled 'External Portal' and contains a 'WiFidog Authentication' section. This section has a toggle switch for 'WiFidog Authentication' which is turned on. Below it, there are radio buttons for 'Version' with 'Wifidog V1' selected. A message states 'The template has been referenced by authentication policy Useroam.' Below this is a 'Basic Info' section with fields for 'Authentication Template 1 Name' (useroam), 'Server URL' (http://104.247.174.120/ruijie-cloud/), and 'Default SSID' (Enter the default SSID.). There is a 'Configure SSID' button. Below the Basic Info is a 'Service Settings' section with a 'Basic Info' subsection. It contains a field for 'Authentication URL' (http://104.247.174.120/ruijie-cloud/), a 'Permission Mode' section with radio buttons for '(Temporary) Permit All', '(Temporary) Permit WeChat Only', 'Do Not Permit' (selected), and 'Permit All WeChat Traffic', and a 'Sending Source' section with radio buttons for 'Default' (selected) and 'Interface'. At the bottom right of the Service Settings section is an 'Apply' button.

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

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

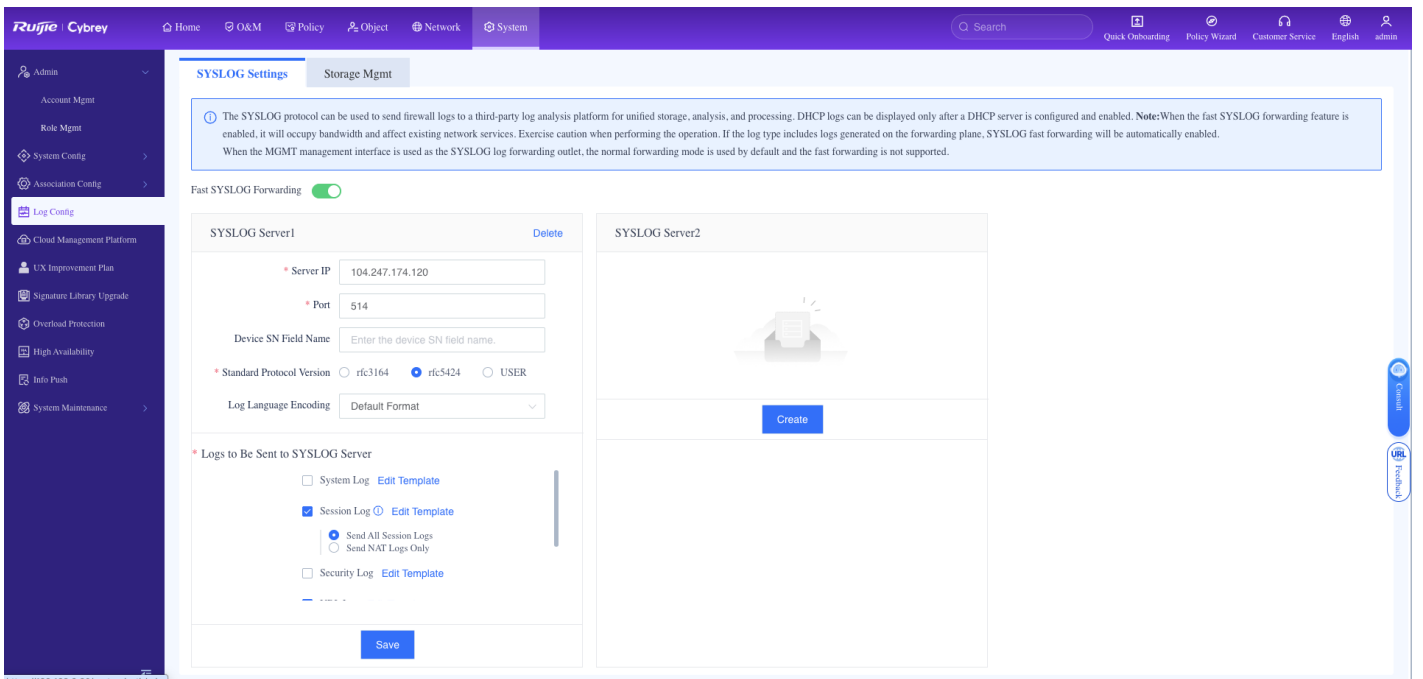
- **Name:** useroam
- **Enabled State:** Enable konumuna getiriniz.
- **Src. Security Zone:** Misafir ağınızın bağlı olduğu zone'u seçiniz (Örn: `Guest`).
- **Src. Address:** any
- **Authentication Action:** Authentication seçeneğini işaretleyiniz.
- **Authentication Template Name:** Bir önceki adımda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