

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

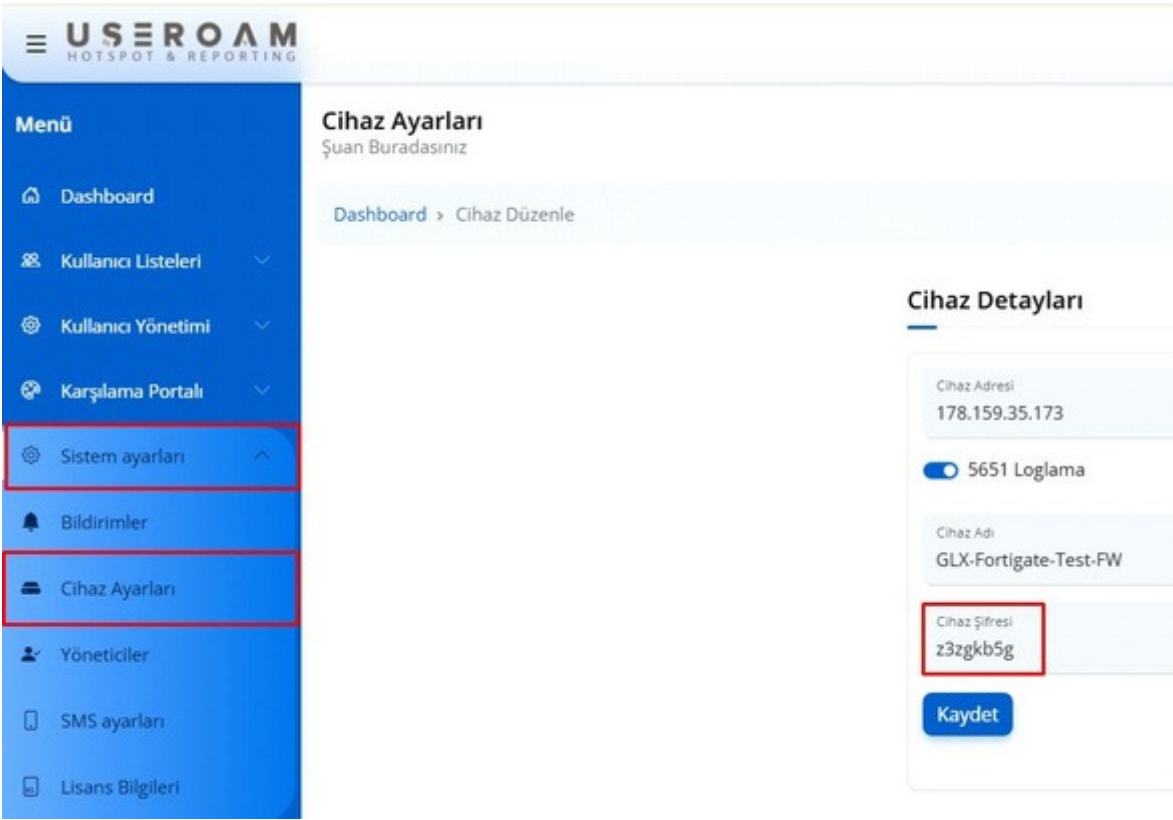
Kaydet

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.



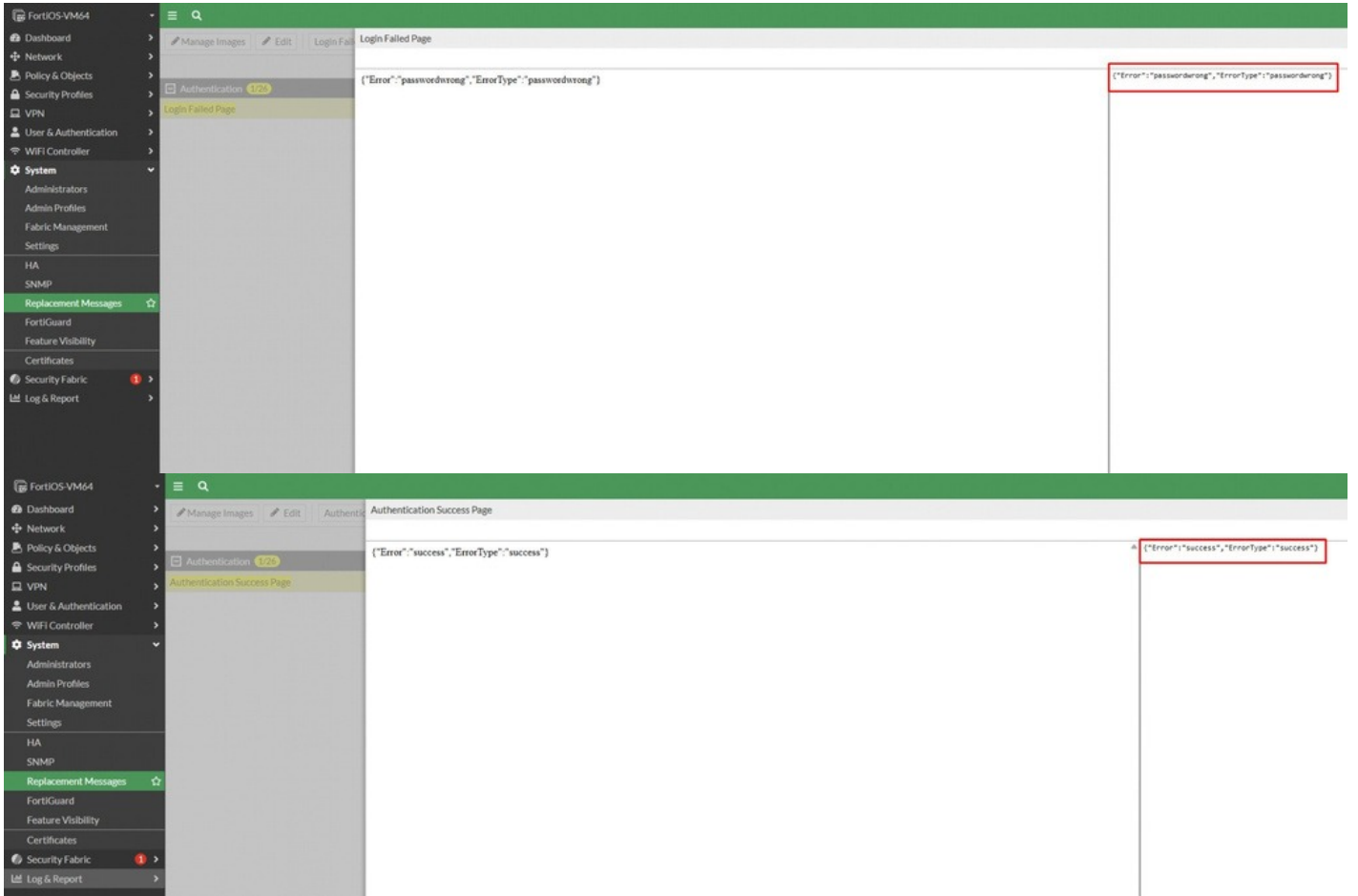
Dashboard	Manage Images	Edit	Search	Simple View	Extended View
Name	Description				
Admin 2					
Post-login Disclaimer Message	Replacement message for post-login disclaimer				
Pre-login Disclaimer Message	Replacement message for pre-login disclaimer				
Alert E-mail 5					
Block Message	Alert email text 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">

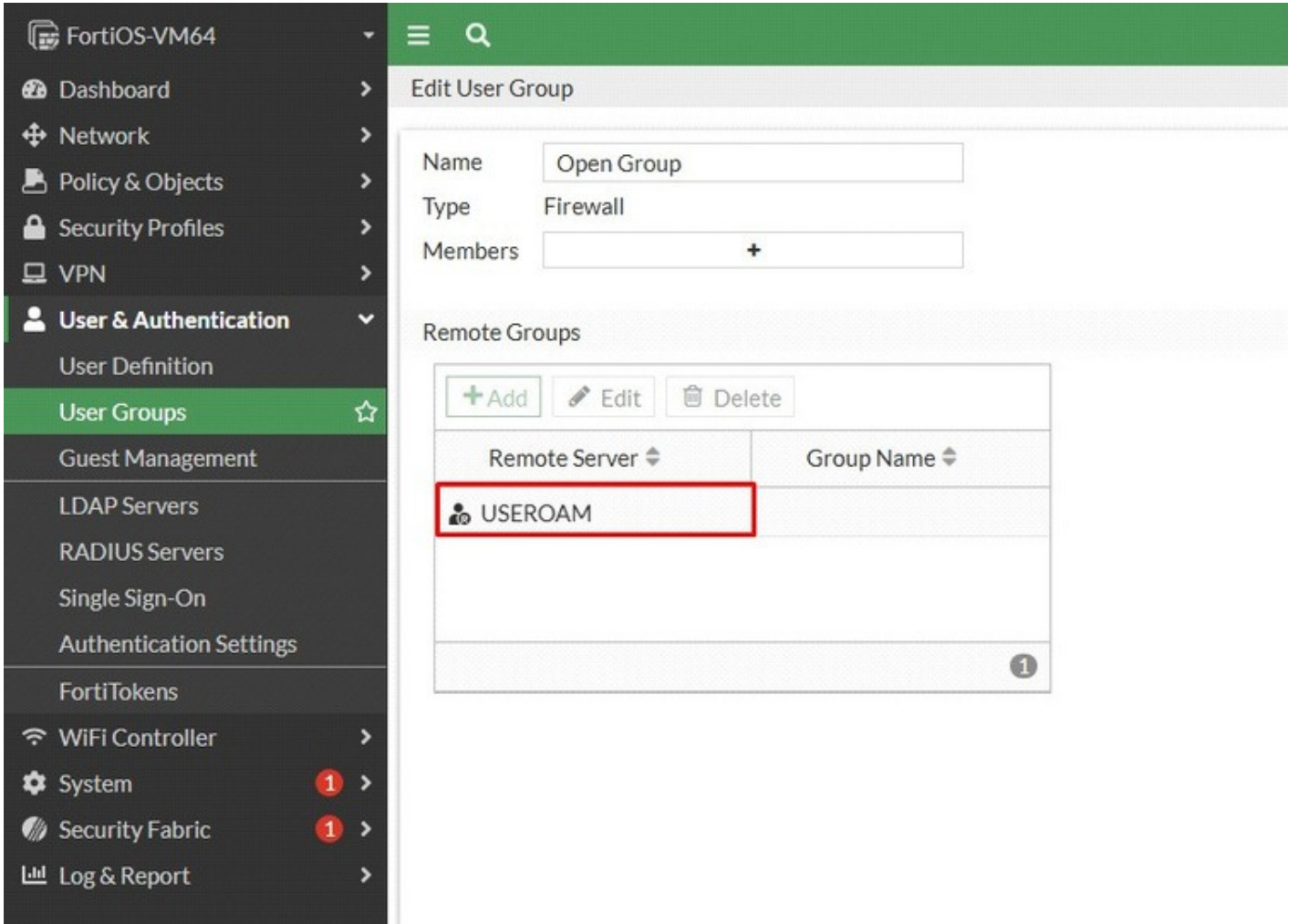
```

Cihazı Sil

The screenshot shows the FortiOS-VM64 interface. The left sidebar lists various system settings, including System, Administrators, Admin Profiles, Fabric Management, Settings, HA, SNMP, Replacement Messages, FortiGuard, Feature Visibility, Certificates, Security Fabric, and Log & Report. The main area displays the Login Page configuration. The HTML code for the login page is shown, including meta tags, CSS links, and form elements for user login.

4 - Kullanıcı Grubu Oluşturma (User Groups)

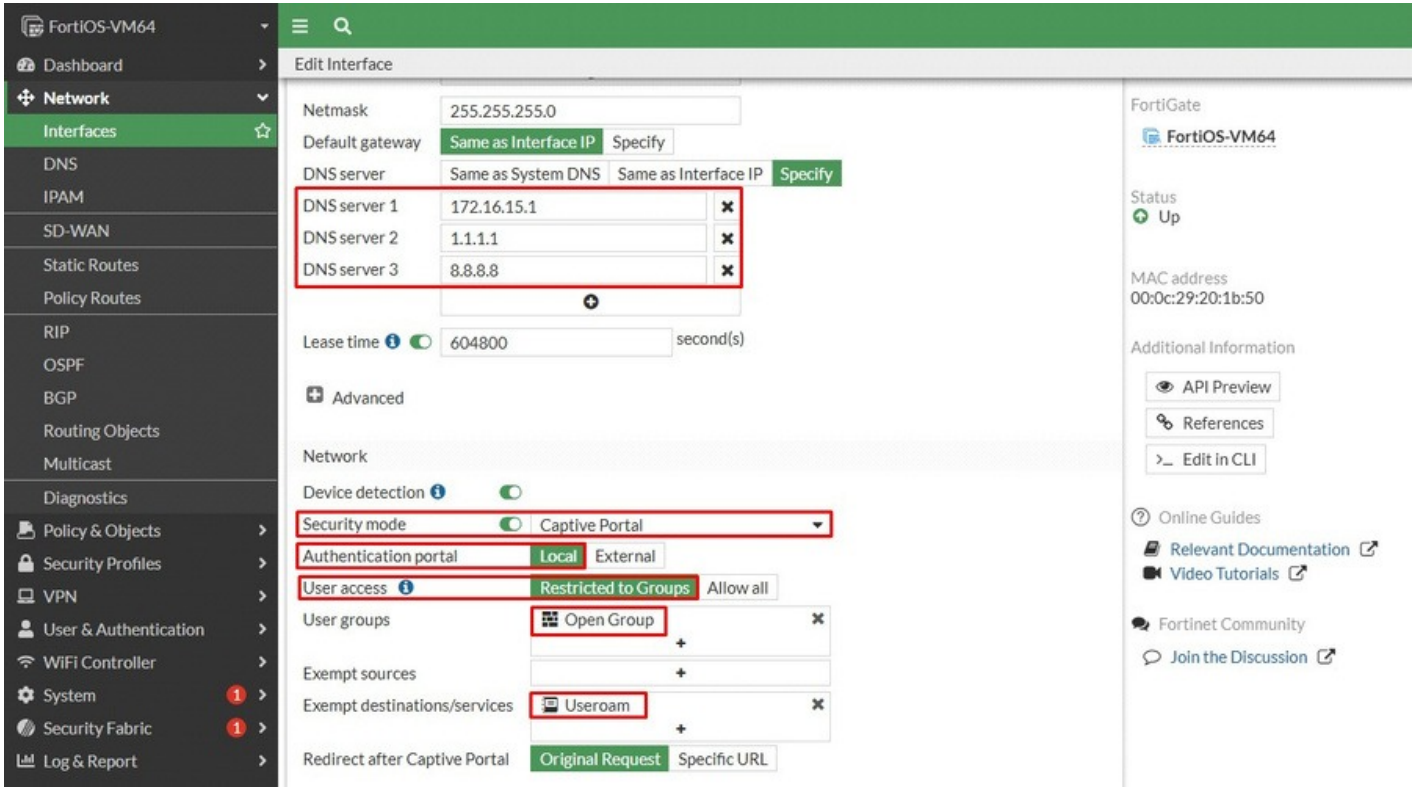
User & Authentication > User Groups menüsünden kendinize Useroam Cloud için bir grup oluşturunuz.



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: ☐

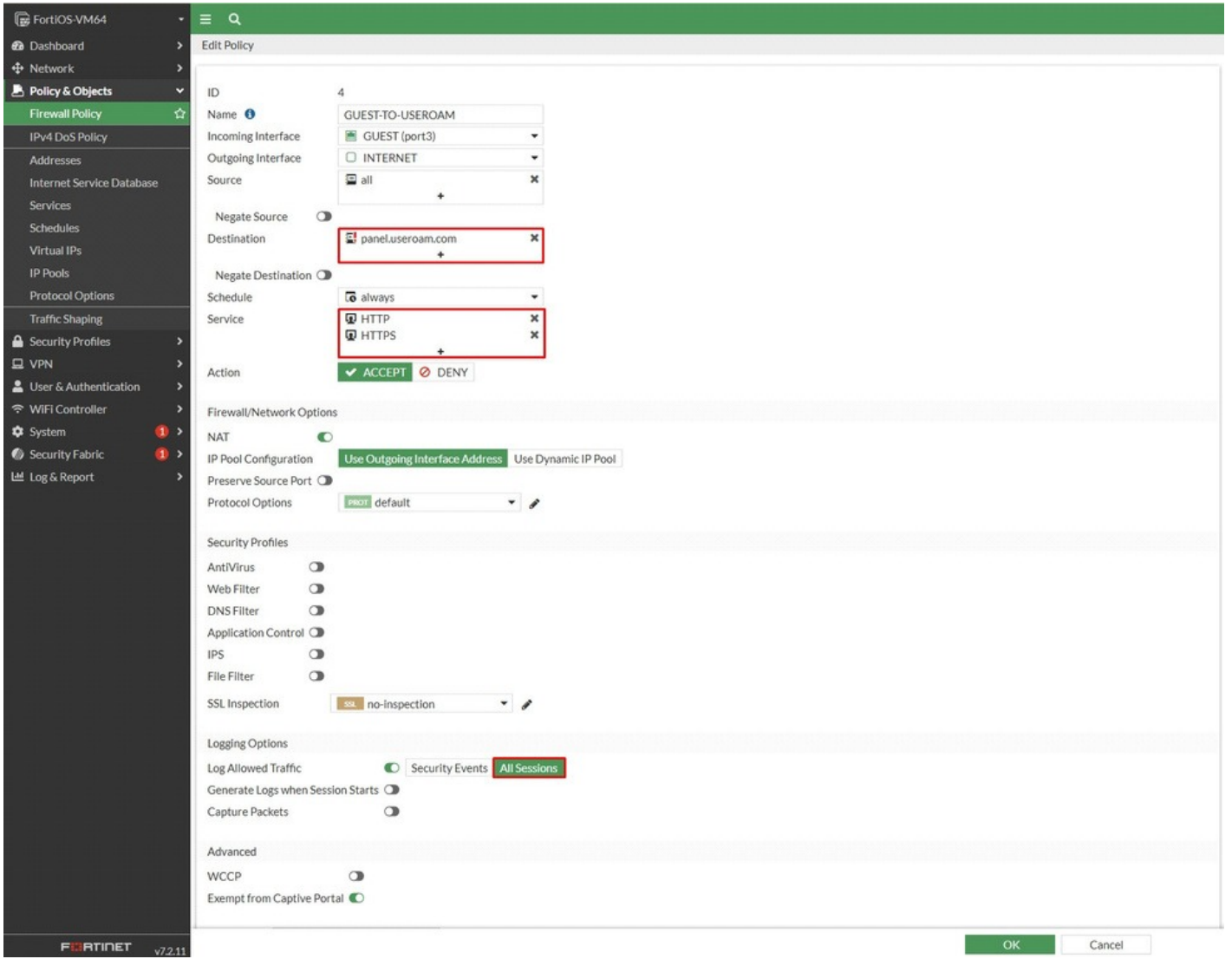
Comments: Write a comment... 0/1023

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

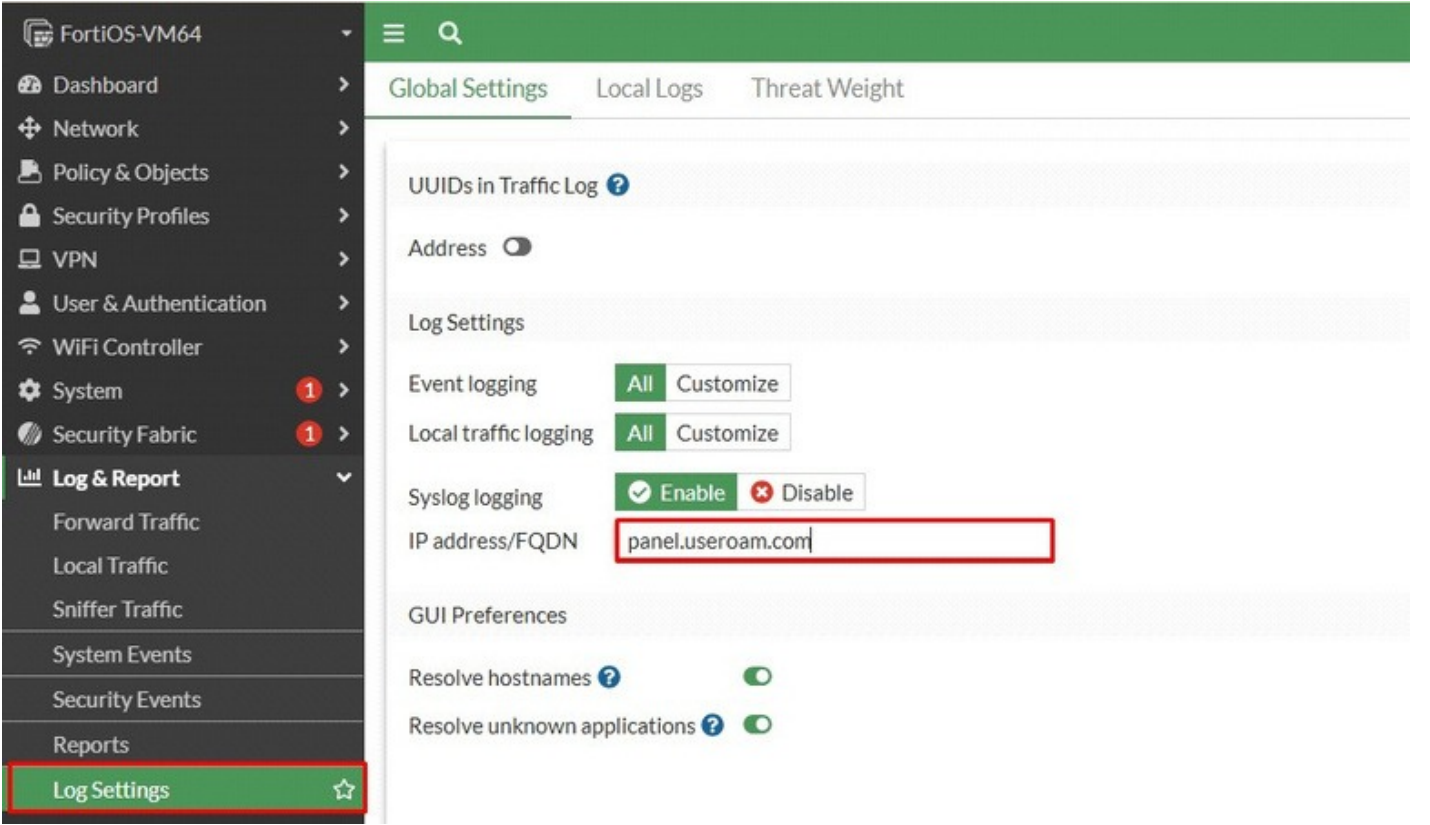
Policy lookup

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.

WhatsApp ile Giriş — Firewall ?zin Listesi (Walled Garden)

Misafir henüz internete çıkmadan (captive portal / giriş öncesi aşamada) **WhatsApp ile Giriş** akışının çalışabilmesi için, firewall veya walled-garden yapılandırmasında aşağıdaki adreslere **izin verilmesi zorunludur**. Bu izinler tanımlanmadan WhatsApp giriş ekranı açılmaz ve teslim

(delivered) onayına dayalı otomatik giriş çalışmaz.

?zin verilecek alan adlar? (FQDN)

- *.wa.me
- *.whatsapp.com
- *.whatsapp.net
- g.whatsapp.net
- mmg.whatsapp.net
- fbsbx.com
- *.useroam.com

?zin verilecek IP adresleri

- 157.240.0.0 — Meta / Facebook ağ bloğu
- 31.13.0.0 — Meta / Facebook ağ bloğu
- 104.247.174.120 — Useroam panel

Not: 157.240.0.0 ve 31.13.0.0 tipik olarak /16 ağ bloklarıdır (Meta altyapısı); firewall'da blok olarak (157.240.0.0/16, 31.13.0.0/16) tanımlanması önerilir. 104.247.174.120 Useroam panel IP'sidir (/32). FQDN tabanlı filtreleme destekleniyorsa alan adı listesi, desteklenmiyorsa IP blokları kullanılmalıdır.

Revizyon #4

tugay tarafından 6 Temmuz 2026 10:03:05 oluşturuldu

tugay tarafından 27 Temmuz 2026 17:56:10 güncellendi