

Fortigate Integration Guide

This guide covers the full integration between a **FortiGate firewall** and Useroam Cloud: RADIUS authentication, the captive portal replacement messages, the firewall policies, and 5651 syslog forwarding.

“ **Before you start:** you need administrator access to the FortiGate web interface (and CLI access if a second syslog server is required), plus the WAN IP address of the firewall.

1 - Adding the device to the Useroam panel

Sign in to your panel at panel.useroam.com and add a **New Device**. The system selects your license automatically.

- **Device type:** select **Fortinet**.
- **Device address:** enter the WAN IP address of the firewall. If you have more than one WAN IP, the firewall usually sends this request from the first WAN interface by default.

Note: if you want the traffic to leave over a different WAN interface, create an SNAT rule to route it through the interface you want.

Yeni Cihaz

 **Cihaz Detayları**

JS0Q8GFCWM3OM2YAH27U629YKAH3

Cihaz Tipi
Fortinet

☒ 5651 Loglama

Cihaz Adresi
178.159.35.173

Cihaz Adı
GLX-Fortigate-FW

Kaydet

2 - Adding the RADIUS server

On your firewall, go to **User & Authentication > RADIUS Servers** and click **Create New** to define the Useroam Cloud server.

- **Authentication method:** Specify / PAP
- **Primary Server IP/Name:** , or by IP address:
- **Secret:** after adding the device in Useroam Cloud, copy the automatically generated **device password** from **Settings > Device Settings** and paste it here.

Test Connectivity: you can run a RADIUS test from your firewall against Useroam Cloud.

USEROAM

HOTSPOT & REPORTING

Menü

Dashboard

Kullanıcı Listeleri

Kullanıcı Yönetimi

Karşılama Portali

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

z3zgb5g

Kaydet

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

Manage Images
Edit
Search

Simple ViewExtended View

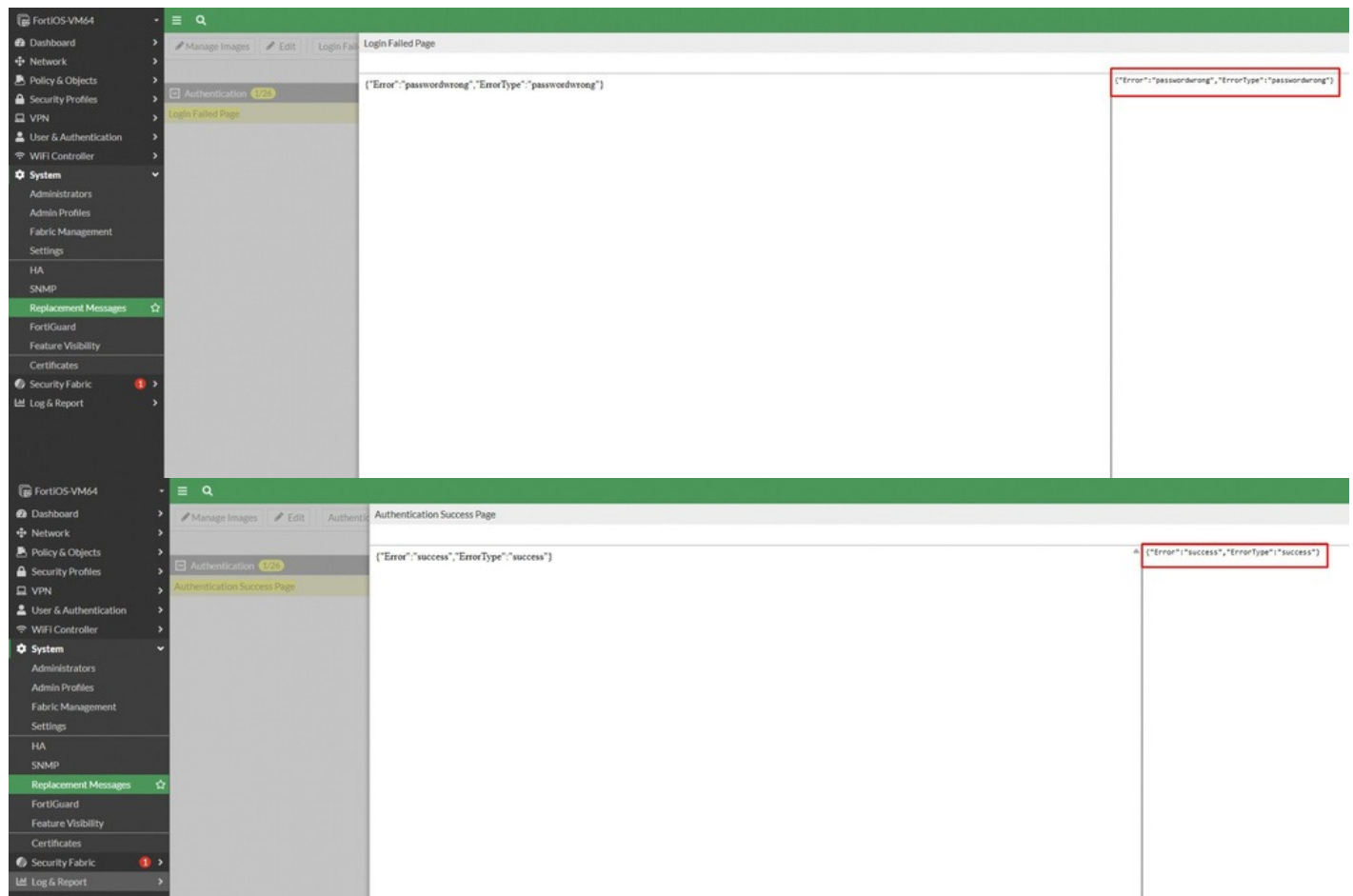
Name	Description
Admin 2	
Post-login Disclaimer Message	Replacement message for post-login disclaimer
Pre-login Disclaimer Message	Replacement message for pre-login disclaimer
Alert E-mail 5	
Block Message	Alert email text for block incidents
Critical Event Message	Alert email text for critical event 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 - Captive portal messages (Replacement Messages)

Three fields under **System > Replacement Messages** need their code replaced. Switch to **Extended View** from the top-right corner first.

3A - Login Failed Page

Search for **Login Failed Page**. On the screen that opens, clear the code area on the right, paste in `{"Error": "passwordwrong", "ErrorType": "passwordwrong"}` and save.



3B - Authentication Success Page & Login Page

Search for **Authentication Success Page**. Clear the code area on the right, paste in `{"Error": "success", "ErrorType": "success"}` and save.

Finally, for **Login Page**, paste the entire code you copied from the Useroam Cloud panel (**Settings > Device Settings**).

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 fadeInX">

```

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

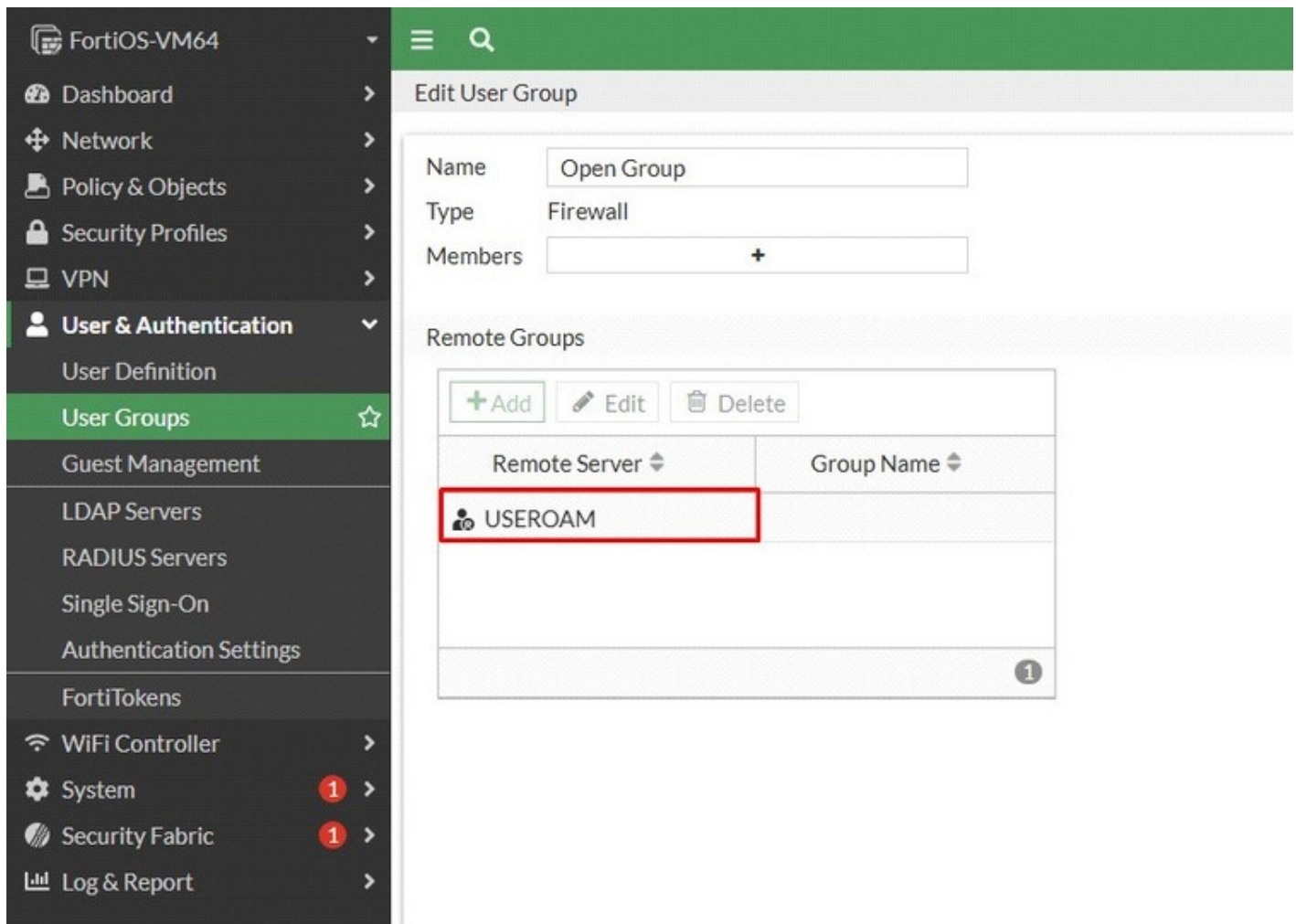
```

<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 fadeInX">
<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="NKPOTURINX" id="4fredis">
<input type="hidden" name="magic" value="NNUAGICVALNN" id="magicval">
<input type="text" name="NNUSENAMEIDNN" id="username">
<input type="password" name="NKPASSWORDIDNN" id="password">
<button type="submit" id="logincaption" class="btn btn-blue btn-lg btn-block">
Giris
</button>
</form>
</div>
</div>
<div class="social-login row">
</div>
</div>
</div>
<div id="__loginbox">
</div>
<script id="UseroamId" data-name="Nz2710NDc1NiczNzU45B" src="http://panel.useroam.com/fortinet-cloud/js/load.js">
</script>
</body>
</html>

```

4 - Creating the user group (User Groups)

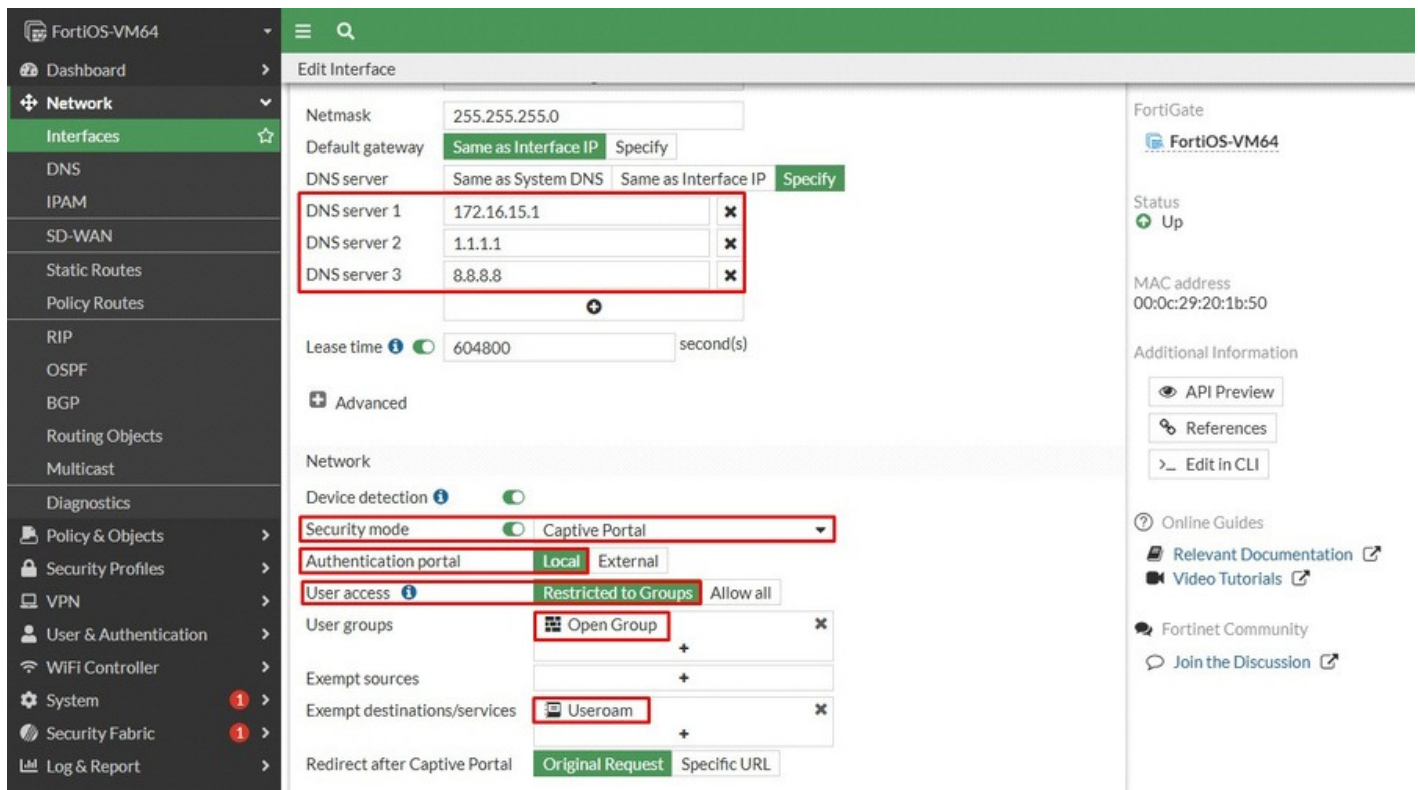
Go to **User & Authentication > User Groups** and create a group for Useroam Cloud.



5 - Interface configuration

On the firewall, edit the relevant port from the **Interface** menu.

- **DNS Server:** first enter the firewall's gateway IP for this interface, then define the DNS servers.
- **Security Mode:** enable **Captive Portal**.
- **User Access:** Restricted to Groups
- **User Groups:** select the group you created in the previous step (for example *Open Group*).
- **Exempt destinations/services:** create an FQDN object for `panel.useroam.com` and select it.



Creating the firewall policies

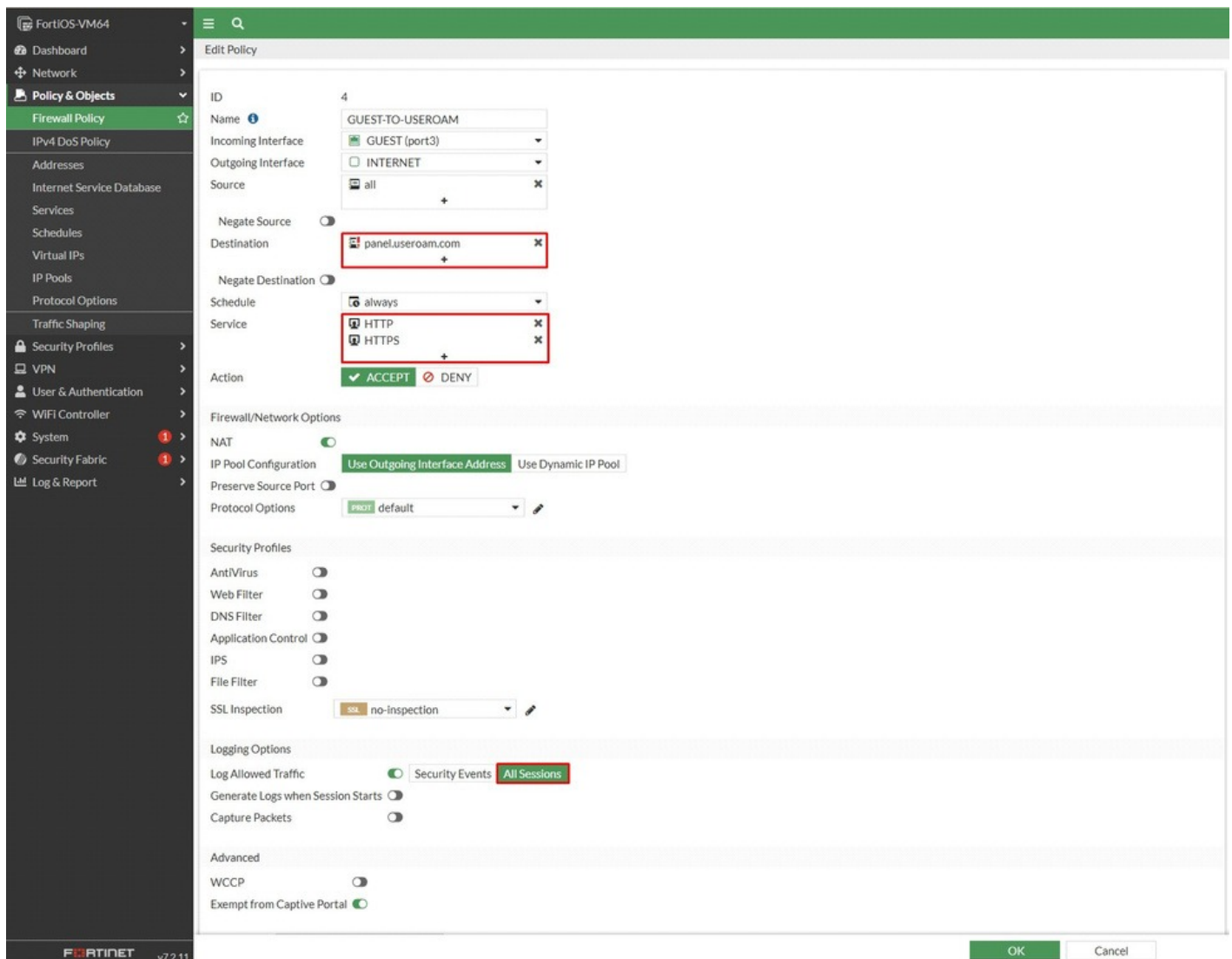
To create the rules, go to **Policy & Objects > Firewall Policy** on the FortiGate firewall.

RULE 1: Guest to DNS

Create your DNS rule first. Selecting only the **DNS** service is enough.

RULE 2: Guest to Useroam

This rule lets users in the zone where you enable Useroam reach the **panel.useroam.com** panel. Under Service, select the **HTTP/HTTPS** services.



RULE 3: Guest to Internet

This rule is your general internet access rule. Add the **User Group (Open Group)** object you created as the Source, and the **ALL** service under Service.

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 ☒

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

Preserve Source Port ☐

Protocol Options **default**

Security Profiles

AntiVirus ☐

Web Filter ☒ **default**

DNS Filter ☐

Application Control ☒ **default**

IPS ☐

File Filter ☐

SSL Inspection ☐ **no-inspection**

Logging Options

Log Allowed Traffic ☒ **Security Events** **All Sessions**

Generate Logs when Session Starts ☐

Capture Packets ☐

Comments 0/1023

Enable this policy ☒

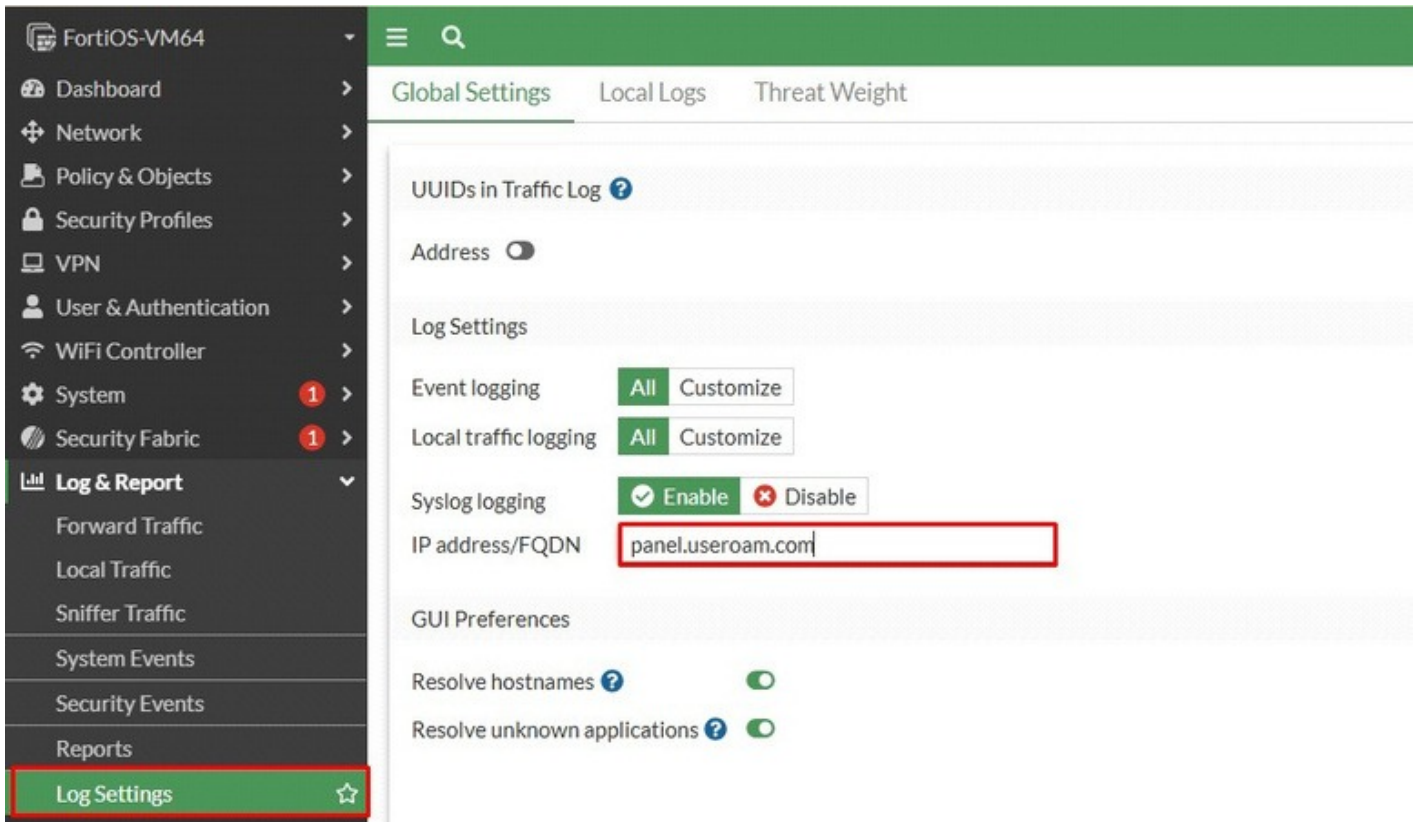
OK **Cancel**

Once all three rules are in place, the **Policy & Objects > Firewall Policy** list should be ordered as shown below.

Name	Source	Destination	Schedule	Service	Action	NAT
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	

Forwarding logs to the Useroam device

Under **Log & Report > Log Settings**, set **Syslog logging** to **Enable**. Then enter the server details in the IP Address/FQDN field as **panel.useroam.com**.



Caution: if a different IP is already defined here, you must configure your second syslog server from the command line (CLI).

After checking whether `syslogd2` already contains another configuration, you can use the example command block below:

```
config log syslogd2 setting
set status enable
set server "panel.useroam.com"
set port 514
set format default
end
```

Important — integration complete

That's it — your FortiGate integration is complete. If you run into any problems during the process, contact our support team at destek@useroamteknoloji.com.

Login with WhatsApp — firewall allowlist (walled garden)

For the **Login with WhatsApp** flow to work while the guest is still behind the captive portal (before internet access is granted), the following addresses **must be allowed** in your firewall or walled-garden configuration. Without these rules the WhatsApp login screen will not open and the

automatic login based on delivery confirmation will not work.

Domains to allow (FQDN)

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

IP addresses to allow

- 157.240.0.0 — Meta / Facebook network block
- 31.13.0.0 — Meta / Facebook network block
- 104.247.174.120 — Useroam panel

Note: 157.240.0.0 and 31.13.0.0 are typically /16 network blocks (Meta infrastructure); we recommend defining them as blocks in the firewall (157.240.0.0/16, 31.13.0.0/16). 104.247.174.120 is the Useroam panel IP (/32). Use the domain list if your firewall supports FQDN-based filtering; otherwise use the IP blocks.

Revizyon #1

tugay tarafından 10 Ağustos 2026 22:57:02 oluşturuldu

tugay tarafından 10 Ağustos 2026 22:57:02 güncellendi