

USEROAM CLOUD FortiGate ENTEGRASYONU

Useroam Cloud'a hoş geldiniz!

Bu rehber Useroam Cloud ile FortiGate güvenlik duvarınızın entegrasyon sürecini hızlı ve sorunsuz bir şekilde tamamlamanıza yardımcı olmak için detaylı talimatları içermektedir.

Aşağıda verilen adımları takip ederek entegrasyon sürecinizi kolayca tamamlayabilirsiniz.

I

İlk olarak **panel.useroam.com** adresinden panelinize giriş yapıp Yeni Cihaz ekleyiniz.

Sistem, lisansınızı otomatik olarak seçecektir.

Cihaz tipinden **Fortinet'i** seçiniz.

Cihaz adresi olarak **Firewall'un WAN IP adresini** seçiniz. Eğer birden fazla WAN IP adresiniz varsa, firewall cihazı genelde bu isteği varsayılan olarak **ilk WAN** bacağından gönderir.

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

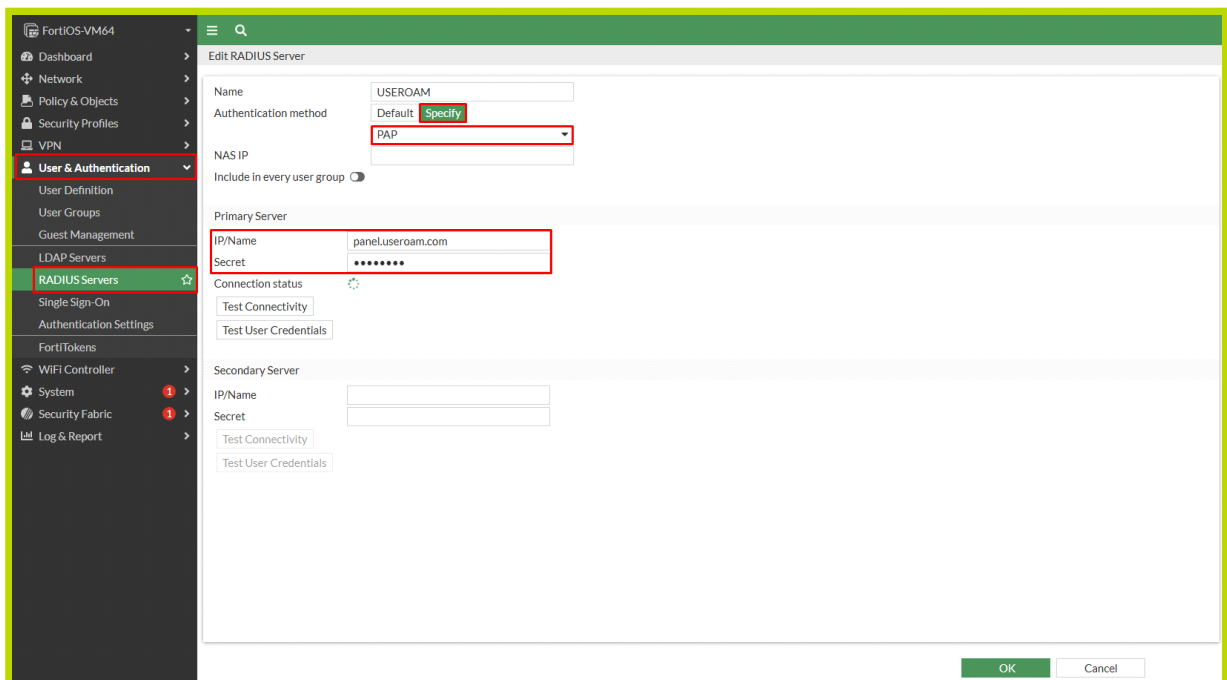
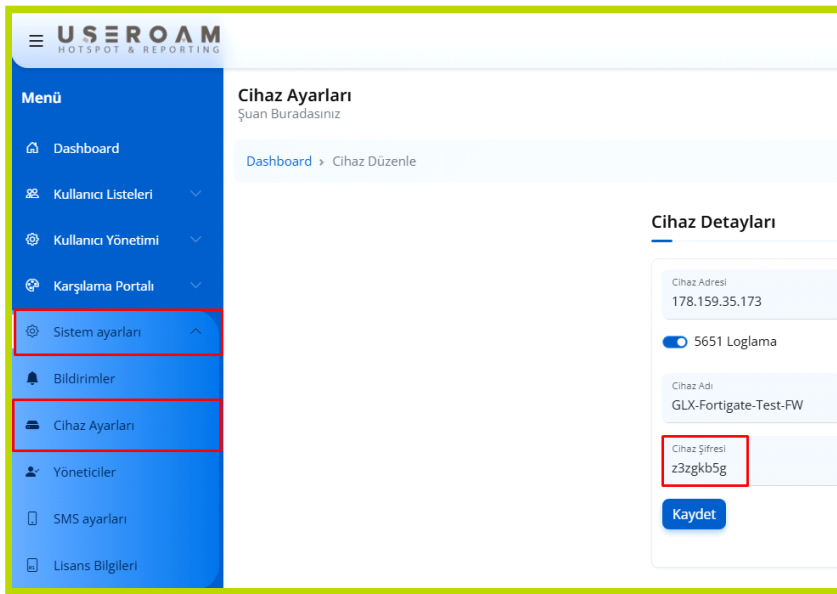
178.159.35.173

Cihaz Adı

GLX-Fortigate-FW

Kaydet

- 2 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.



3

System > Replacement Messages menüsünde bulunan 3 alanın kodlarını değiştirmek için önce sağ üst köşeden **Extended View** moduna geçiniz.

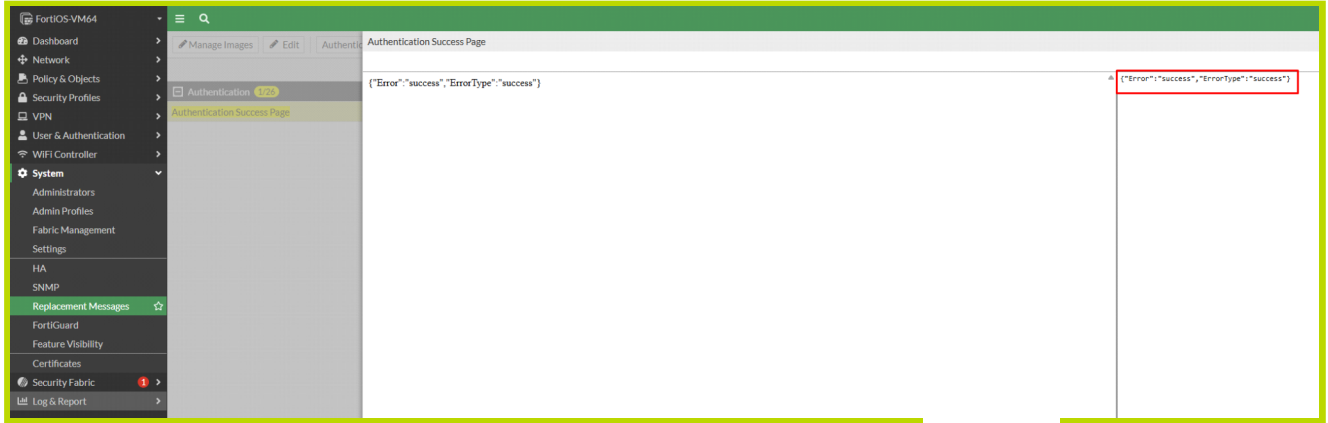
Dashboard	Manage Images	Edit	Search	Simple View	Extended View
Network	Name	Description			
Policy & Objects	Admin 2				
Security Profiles	Post-login Disclaimer Message	Replacement message for post-login disclaimer			
VPN	Pre-login Disclaimer Message	Replacement message for pre-login disclaimer			
User & Authentication	Alert E-mail 5				
WiFi Controller	Block Message	Alert email text for block incidents			
System	Critical Event Message	Alert email text for critical event notification			
Administrators	Disk Full Message	Alert email text for disk full events			
Admin Profiles	Intrusion Message	Alert email text for IPS events			
Fabric Management	Virus Message	Alert email text for virus incidents			
Settings	Authentication 26				
HA	Authentication Rejection Page	Replacement HTML for authentication rejection page			
SNMP	Authentication Success Page	Replacement HTML for authentication success page			
Replacement Messages	Block Notification Page	Replacement HTML for block notification page			
FortiGuard	Certificate Password Page	Replacement HTML for certificate password page			
Feature Visibility	Declined Disclaimer Page	Replacement HTML for user declined disclaimer page			
Certificates	Declined Quarantine Page	Replacement HTML for user declined quarantine page			
Security Fabric	Disclaimer Page	Replacement HTML for authentication disclaimer page			
Log & Report					

3A

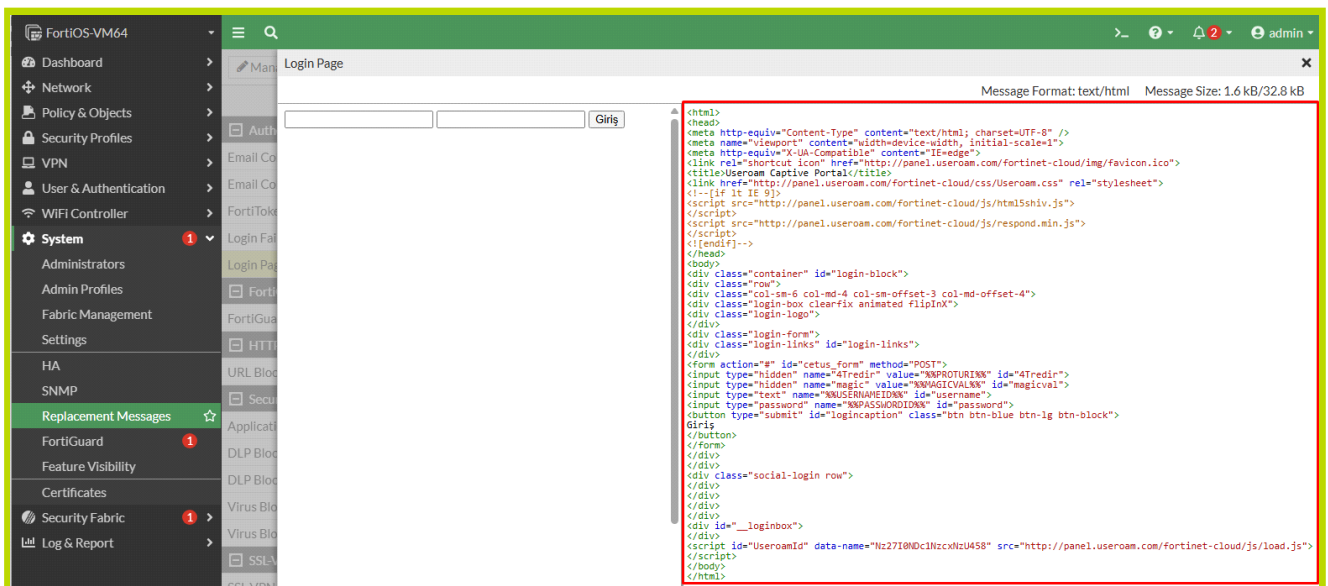
Login Failed Page'i aratın, karşınıza gelen ekranda sağ taraftaki kod kısmını temizleyerek, `{"Error":"passwordwrong","ErrorType":"passwordwrong"}` kodunu içine yapıştırarak, kaydediniz.

FortiOS-VM64	Manage Images	Edit	Login Failed Page
Dashboard	Authentication 122		
Network	Login Failed Page		
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			

- 3B** **Authentication Success Page**'i aratın, karşınıza gelen ekranda sağ taraftaki kod kısmını temizleyerek, {"Error": "success", "ErrorType": "success"} kodunu içine yapııştırarak, kaydediniz.



- 3C** Son olarak **Login Page** kısmına **Useroam Cloud** panelinden (Sistem Ayarları / Cihaz Ayarları) kopyaladığınız kodun hepsini yapıştırınız.



4

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

FortiOS-VM64

- Dashboard
- Network
- Policy & Objects
- Security Profiles
- VPN
- User & Authentication**
 - User Definition
 - User Groups** ☆
 - Guest Management
 - LDAP Servers
 - RADIUS Servers
 - Single Sign-On
 - Authentication Settings
 - FortiTokens
- WiFi Controller
- System 1
- Security Fabric 1
- Log & Report

Edit User Group

Name: Open Group

Type: Firewall

Members: +

Remote Groups

Remote Server	Group Name
USEROAM	

1

5

Firewall'da **Interface** menüsünden ilgili Portunuzu düzenleyiniz.

DNS Server: Bu kısımda, önce bu Interface'in **Firewall'un Gateway IP'sini** giriniz. Ardından DNS serverlarını tanımlayınız.

Security Mode: Bu özelliği açınız.

User Access: Retricted to Groups

User Groups: Bir önceki adımda oluşturduğunuz Open Group'u seçiniz.

Exempt destinations/services: panel.useroam.com **fqdn** objesini oluşturup seçiniz

The screenshot displays the FortiGate FortiOS-VM64 web interface. The left sidebar shows the navigation menu with 'Network' and 'Interfaces' highlighted. The main content area is titled 'Edit Interface'. The 'DNS server' section is highlighted with a red box, showing three servers: 172.16.15.1, 1.1.1.1, and 8.8.8.8. The 'Advanced' section is also highlighted with a red box, showing 'Security mode' set to 'Captive Portal', 'Authentication portal' set to 'Local', 'User access' set to 'Restricted to Groups', 'User groups' set to 'Open Group', and 'Exempt destinations/services' set to 'Useroam'.

FIREWALL KURALLARININ OLUŞTURULMASI

Kuralları oluşturmak için önce FortiGate Firewall altında **Policy & Objectives > Firewall Policy** menüsüne geliniz.

KURAL I.

Önce **DNS** kuralınızı oluşturunuz. Bunun için sadece DNS servisinin seçili olması yeterli olacaktır.

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: default

Security Profiles

AntiVirus: ☐

Web Filter: ☐

DNS Filter: ☐

Application Control: ☐

IPS: ☐

File Filter: ☐

SSL Inspection: 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.

Bu kural ile Useroam'u aktiveleştireceğiniz Zone'daki kullanıcıların **Panel.useroam.com** paneline erişmesi sağlanacak.

The screenshot shows the FortiGate Firewall Policy configuration interface. The policy is named 'GUEST-TO-USEROAM' and is applied to the 'GUEST (port3)' interface. The source is 'all' and the destination is 'panel.useroam.com'. The service is set to 'HTTP' and 'HTTPS'. The action is 'ACCEPT'. The policy is scheduled 'always'. The security profiles are 'no-inspection'. The logging options are 'Security Events' and 'All Sessions'.

Policy Configuration:

- ID:** 4
- Name:** GUEST-TO-USEROAM
- Incoming Interface:** GUEST (port3)
- Outgoing Interface:** INTERNET
- Source:** all
- Negate Source:** ☐
- Destination:** panel.useroam.com
- Negate Destination:** ☐
- Schedule:** always
- Service:** HTTP, HTTPS
- 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:** ☐
- DNS Filter:** ☐
- Application Control:** ☐
- IPS:** ☐
- File Filter:** ☐
- SSL Inspection:** no-inspection

Logging Options:

- Log Allowed Traffic:** ☒ Security Events, All Sessions
- Generate Logs when Session Starts:** ☐
- Capture Packets:** ☐

Advanced:

- WCCP:** ☐
- Exempt from Captive Portal:** ☒

Buttons: OK, Cancel

KURAL 3.

Bu kural ile internet çıkış kuralınızı da oluşturacaksınız.

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

Use Outgoing Interface Address

Use Dynamic IP Pool

Preserve Source Port

Protocol Options

default

Security Profiles

AntiVirus

Web Filter

DNS Filter

Application Control

IPS

File Filter

SSL Inspection

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

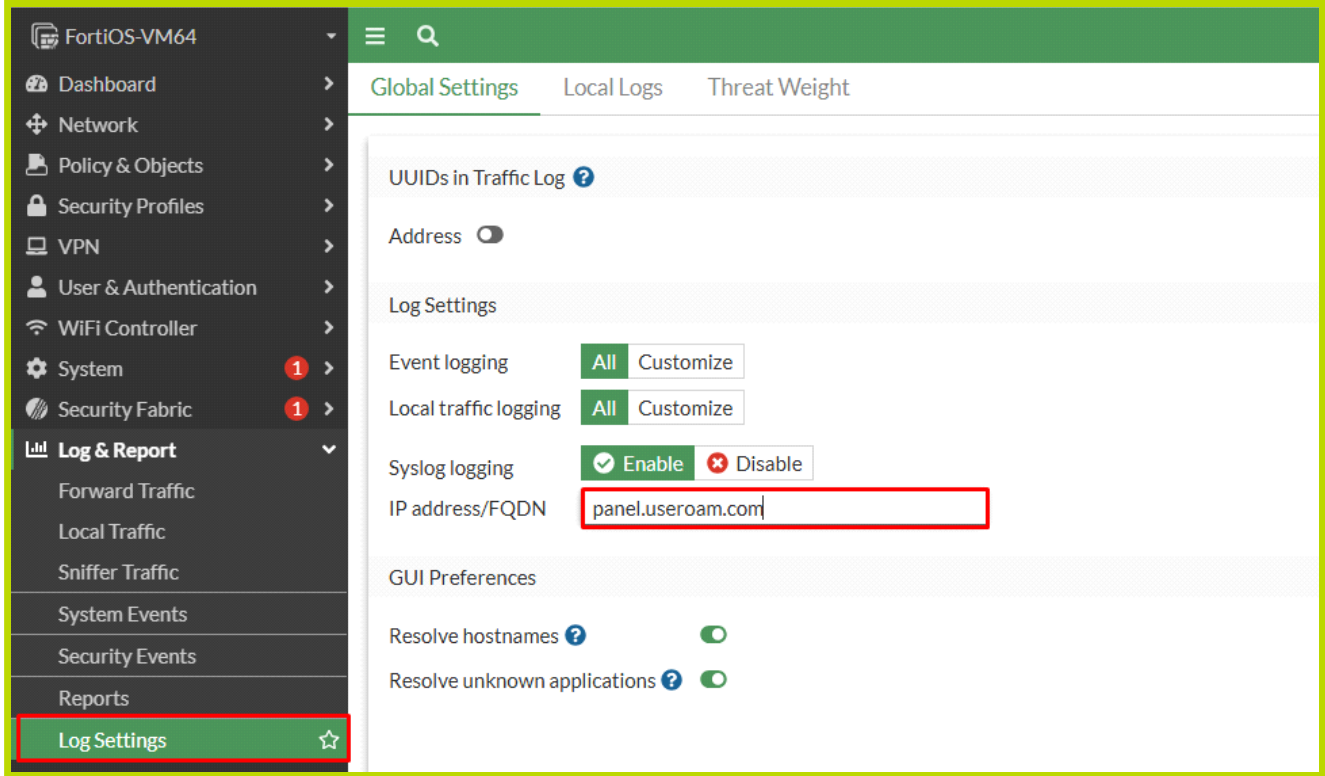
Cancel

Üç kuralı da oluşturmanızın ardından **Policy & Objectives > Firewall Policy** menüsü ekranı aşağıdaki şekilde görünecektir.

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	

LOGLARIN USEROAM'A YÖNLENDİRİLMESİ

Log & Report > Log Settings > Global Settings menüsü altından **Syslog logging** kısmını **Enable** konumuna getiriniz. Ardından **IP Address/FQDN** kısmına sunucunu bilgilerinizi **panel.useroam.com** olarak giriniz.



Dikkat: Eğer bu kısımda bir IP tanımlı ise ikinci Syslog sunucunuzu komut satırı üzerinden yapmanız gerekiyor. Örnek komut olarak aşağıdaki komutu kullanabilirsiniz. Öncesinde firewall üzerinden syslogd2'nin içinde konfigürasyon olup olmadığını lütfen kontrol ederek bu komutu kullanınız.

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

Hepsi bu kadar.

Entegrasyon işleminiz tamamlandı.

İşlem sırasında bir sorun yaşarsanız

destek@glox.com.tr

adresinden bizimle iletişime geçebilirsiniz.