



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.

1

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 bacağı**ndan gönderir.

Farklı bir WAN bacağından gönderim yapmak isterseniz, bir **SNAT kuralı** oluşturarak ilgili trađi istediđiniz 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.

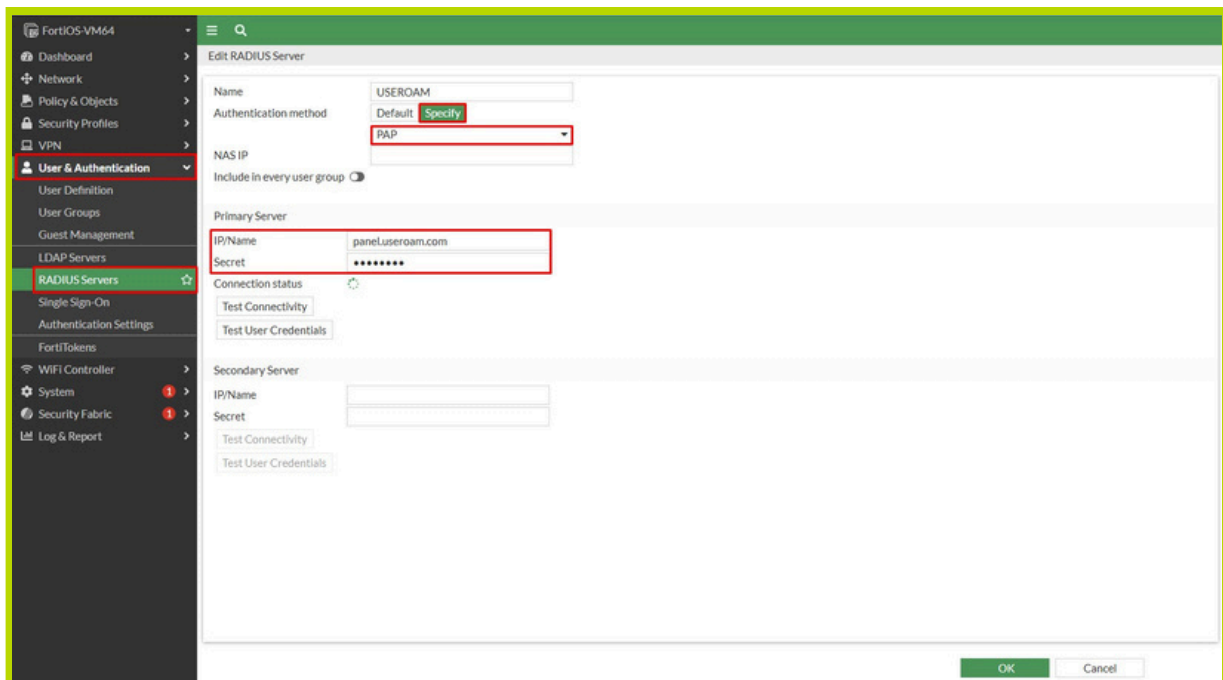
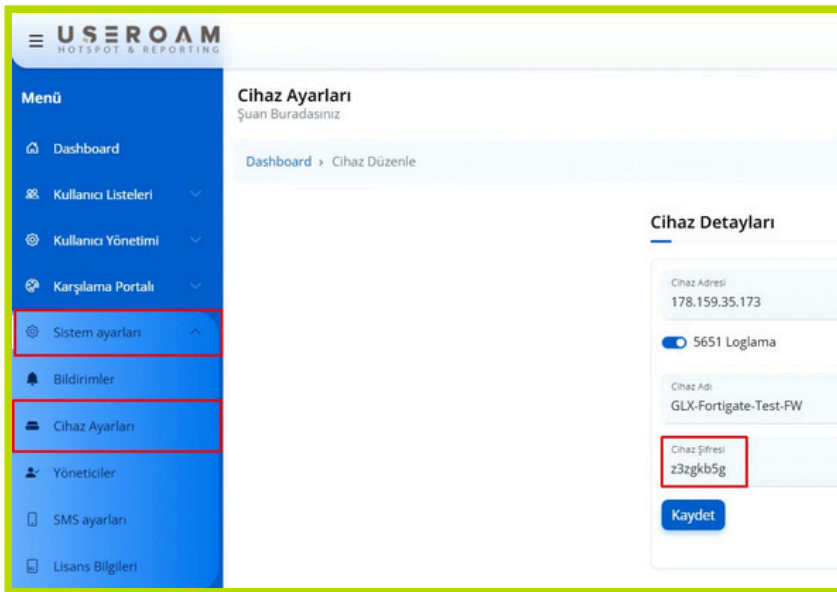
Authentication method : Specify / PAP

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.



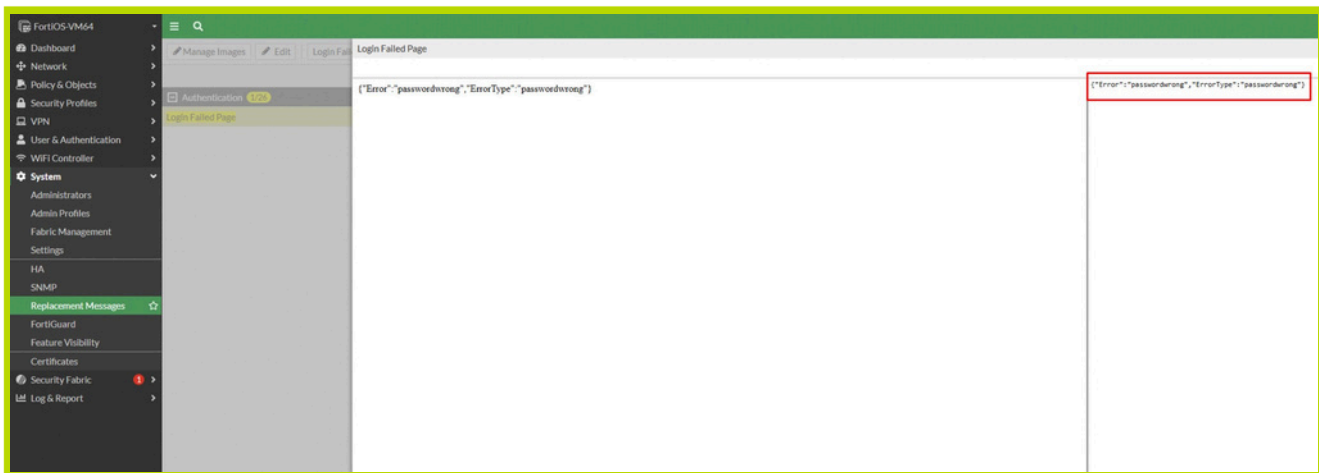
3

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

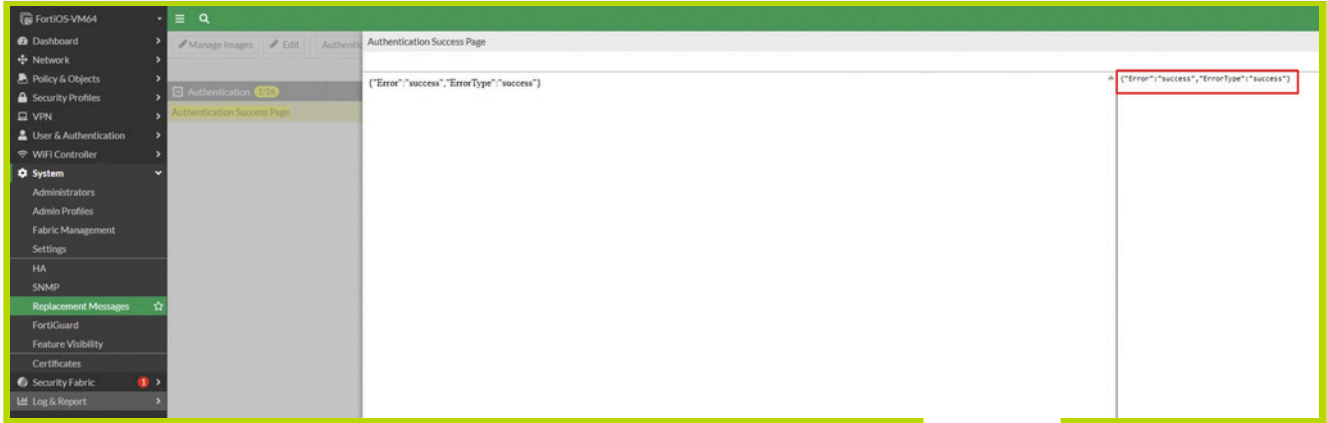
Name	Description
Admin (2)	
Post-login Disclaimer Message	Replacement message for post-login disclaimer
Pre-login Disclaimer Message	Replacement message for pre-login disclaimer
Alert E-mail (3)	
Block Message	Alert email text for block incidents
Critical Event Message	Alert email text for critical event 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

3A

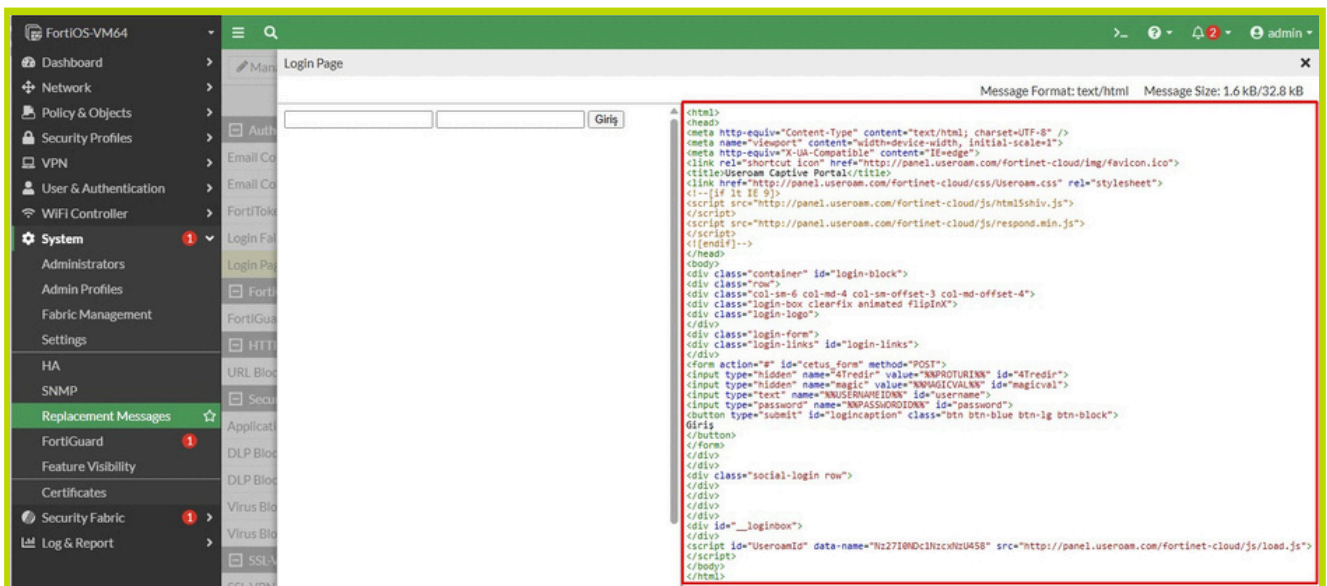
Login Failed Page'i aratın, karşınıza gelen ekranda sağ taraftaki kod kısmını temizleyerek, {"Error": "passwordwrong", "ErrorType": "passwordwrong"} kodunu içine yapıştırarak, kaydediniz.



3B Authentication Success Page'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.

The screenshot displays the FortiGate web interface for configuring a User Group. The left sidebar shows the navigation menu with 'User & Authentication' expanded and 'User Groups' selected. The main content area shows the 'Edit User Group' form with the following fields:

- Name: Open Group
- Type: Firewall
- Members: +

Below the form is a table for Remote Groups with the following columns: Remote Server and Group Name. The 'USEROAM' entry is highlighted with a red box.

Remote Server	Group Name
USEROAM	

- 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 shows the FortiGate web interface for editing an interface. The left sidebar shows the navigation menu with 'Network' and 'Interfaces' highlighted. The main content area is titled 'Edit Interface' and is divided into three sections: Network, Advanced, and Network. The Network section is highlighted in red and contains the following settings:

- Netmask: 255.255.255.0
- Default gateway: Same as Interface IP
- DNS server: Same as System DNS, Same as Interface IP, Specify
- DNS server 1: 172.16.15.1
- DNS server 2: 1.1.1.1
- DNS server 3: 8.8.8.8
- Lease time: 604800 second(s)

The Advanced section contains the following settings:

- Security mode: Captive Portal
- Authentication portal: Local
- User access: Restricted to Groups
- User groups: Open Group
- Exempt sources: (empty)
- Exempt destinations/services: Useroam
- Redirect after Captive Portal: Original Request

The Network section contains the following settings:

- Device detection: (checked)
- Security mode: Captive Portal
- Authentication portal: Local, External
- User access: Restricted to Groups, Allow all
- User groups: Open Group
- Exempt sources: (empty)
- Exempt destinations/services: Useroam
- Redirect after Captive Portal: Original Request, Specific URL

FIREWALL KURALLARININ OLUŞTURULMASI

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

KURAL 1.

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

The screenshot displays the FortiGate Firewall Policy configuration interface. The left sidebar shows the navigation menu with 'Policy & Objects' selected. The main area is titled 'Edit Policy' and shows the following configuration:

- Name: GUEST TO DNS
- Incoming Interface: GUEST (port3)
- Outgoing Interface: INTERNET
- Source: all
- Destination: all
- Schedule: always
- Service: DNS (highlighted with a red box)
- Action: ACCEPT (checked), DENY (unchecked)

Below the main configuration, there are sections for Firewall/Network Options, Security Profiles, and Logging Options:

- Firewall/Network Options: NAT is enabled. IP Pool Configuration is set to 'Use Outgoing Interface Address' and 'Use Dynamic IP Pool'. Protocol Options is set to 'default'.
- Security Profiles: AntiVirus, Web Filter, DNS Filter, Application Control, IPS, and File Filter are all disabled. SSL Inspection is set to 'no-inspection'.
- Logging Options: 'Log Allowed Traffic' is enabled, with 'Security Events' and 'All Sessions' selected. 'Generate Logs when Session Starts' and 'Capture Packets' are disabled.

At the bottom, there is a 'Comments' field with a character count of 0/1023 and an 'Enable this policy' checkbox which is checked. The 'OK' and 'Cancel' buttons are visible at the bottom right.

KURAL 2.

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

The screenshot displays the FortiGate Firewall Policy configuration interface. The policy is named "GUEST-TO-USEROAM" and is applied to the "GUEST (port3)" interface. The source is set to "all". The destination is "panel.useroam.com". The schedule is "always". The service is "HTTP" and "HTTPS". The action is "ACCEPT". The policy is configured with NAT, IP Pool Configuration, and Protocol Options. Security Profiles are set to "no-inspection". Logging Options are set to "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:

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:

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

Preserve Source Port:

Protocol Options: PROT 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:

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

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	

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.

The screenshot shows the FortiGate web interface. The left sidebar has 'Log & Report' selected, with 'Log Settings' highlighted. The main content area shows the 'Global Settings' tab. Under 'Log Settings', 'Syslog logging' is enabled, and the 'IP address/FQDN' field is set to 'panel.useroam.com'.



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@useroamteknoloji.com
adresinden bizimle iletişime geçebilirsiniz.