

USEROAM CLOUD SOPHOS ENTEGRASYONU

Useroam Cloud'a hoş geldiniz!

Bu rehber Useroam Cloud ile Sophos 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 Sophos Firewall'da **Authentication > Users** menüsünden yeni bir yetkili kullanıcı oluşturup firewall tarafındaki iletişimi kurmasını sağlayınız.

User type olarak **Administrator; Profile** olarak **Administrator** seçiniz. Ardından **Group** kısmında sınırsız erişimi olan herhangi bir grup seçerek kullanıcıyı oluşturunuz.

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

Add user

Username * useroam

Name * useroam

Description Description

User type * ☐ User ☒ Administrator

Profile * Administrator

Password *

Email * admin@admin.com Quarantine digest will be sent to

Policies

Group * Open Group

Surfing quota * Unlimited Internet Access

Access time * Allowed all the time

Network traffic None

Traffic shaping None

VPN

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

Sistem, lisansınızı otomatik olarak seçecektir.

2

Cihaz tipinden **Sophos**'u seçiniz.

Cihaz adresi olarak **Firewall'un WAN IP adresini** seçiniz. Eğer birden fazla WAN IP adresiniz varsa, Sophos cihazı 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

AUVA3RYOZQ4E7F0LR7Z1640QD7XZ

Cihaz Tipi

Sophos

☒ 5651 Loglama

Cihaz Adresi

178.159.35.173

Cihaz Adı

GLX-Sophos-FW

SSL Port

4444

Kullanıcı Adı

useroam

Şifre

Useroam112233

Kaydet

Sonra **Administration > Device Access** menüsüne gidiniz. Burada **Useroam'u** kullanacağınız **Zone'da sadece Captive Portal ve DNS** seçeneklerini işaretleyerek aktif hale getiriniz.

3



Dikkat: Radius SSO gibi farklı kimlik doğrulama mekanizmalarını aktif hale getirmeniz durumunda, yönlendirme sorunları veya Captive Portal sayfasının yavaş açılması gibi problemler yaşanabilir.

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

Administration

Licensing

Device access

Admin and user settings

Time

Notification

Local service ACL

Zone	Admin services		Authentication services				Network services			IP
	HTTPS	SSH	AD SSO	Captive portal *	Radius SSO	Clients	Chromebook SSO	Ping/Ping6	DNS	
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				

4

Authentication > Servers menüsünden yeni bir Radius sunucu ekleyiniz. Server IP kısmında, **panel.useroam.com** adresini pingleyerek, çıkan IP adresini buraya 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 Add external server

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

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

Bu noktada bir test yapmak isterseniz,

5

Useroam Cloud panelinden **Kullanıcı Yönetimi> Yeni Kullanıcı** adımlarıyla yeni kullanıcı oluşturabilir;

Firewall'da Radius Sunucu ayarının içinden Test Connection ile bağlantıyı kontrol edebilirsiniz.

SOPHOS Add external server

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

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

6

Sonra **Authentication > Services** menüsünden **Useroam'u Firewall Authentication Methods** kısmında 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

7

Ardından **Authentication > Web Authentication** menüsüne geçiniz. Burada **Sign Out User** kısmına gelerek, **When User is Inactive** seçeneğini işaretleyiniz. Yan taraftaki **Traffic flow** kısmında ise **100bytes için 1440 dk** olarak ayarlayınız - bu süre 24 saate denk gelmektedir; 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 Clients

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

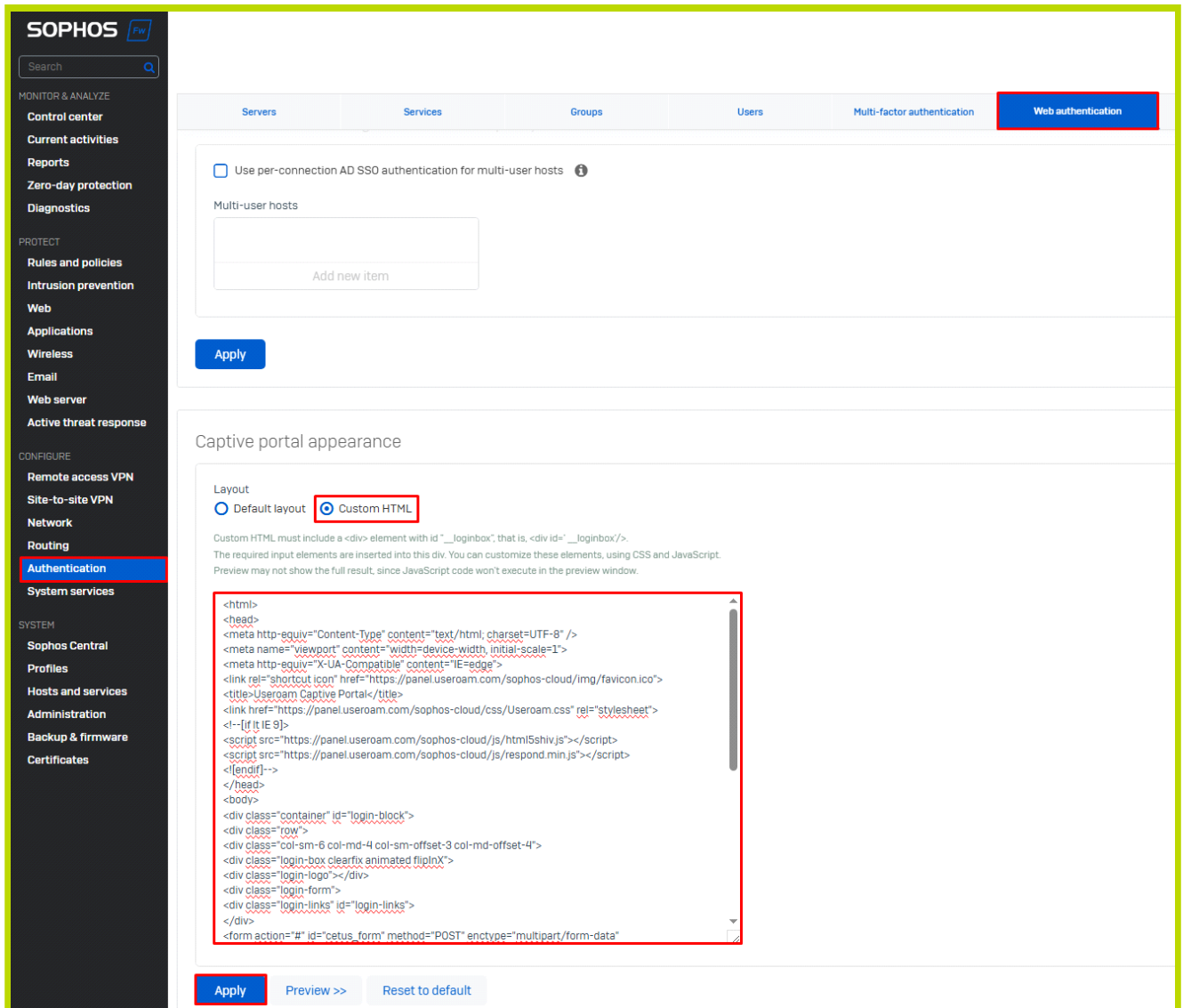
Traffic flow required to consider the user active

100 bytes in 1440 minutes

Apply

8

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.





Dikkat: 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 KURALLARININ OLUŞTURULMASI

Kuralları oluşturmak için önce Sophos Firewall altında **Protect > Rules and Policies** menüsünden **Add Firewall Rule** sayfasına geliniz.

KURAL I.

Guest to DNS: Tüm cihazlar, bağlandıkları ağda internet erişimi olup olmadığını anlamak için cihaza özel alan adına bir DNS sorgusu atar. Örneğin *captive.apple.com*; bu sorgu sonucu gelince, cihaz, ağda internet olduğunu anlayıp, trafik akışını başlatır. Aksi takdirde, hotspot yönlendirmesi de yapılmayacaktır. Bu kuralın misafirlerin internet çıkışı kuralının üstünde olması gerekiyor.

SOPHOS Add firewall rule

How-to guides Log viewer

Rule status ☒

Rule name *
GUEST TO DNS

Description
GUEST TO DNS

Rule position
Top

Action
Accept

Rule group
GUEST

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

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

Source zones *
GUEST
Add new item

Source networks and devices *
Any
Add new item

During scheduled time
All the time
Select to apply the rule to a specific time period and day of the week.

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

Destination zones *
WAN
Add new item

Destination networks *
Any
Add new item

Services *
DNS
Add new item
Services are traffic types based on a combination of protocols and ports.

KURAL 2.

Guest to Useroam: Bu kural ile misafir ağındaki cihazların **panel.useroam.com** a erişmesini sağlayacaksınız. Bunun için **Services** kısmında **HTTP/HTTPS** seçmeniz yeterli olacaktır.

SOPHOS **FW** **How-to guides** **Log viewer**

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

Rule status

Rule name *
GUEST TO USEROAM

Action
Accept

☒ **Log firewall traffic**
Logs 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. **Match Known Users ve Use Web Authentication For Unknown Users** kutucuklarını da tanımsız kullanıcılara Hotspot ekranı gelmesi için seçiniz. **Web Policy ve Identify And Control Applications (App Control)** kısımlarında **Allow All** ya da herhangi bir politika seçiniz.

Rule status

Rule name *

Description

Rule position

Rule group

Action

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

Source

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

Source zones *

Source networks and devices *

During scheduled time

Destination and services

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

Destination zones *

Destination networks *

Services *

☒ Match known users

☒ Use web authentication for unknown users

User or groups *

☐ Exclude this user activity from data accounting

Security features

Web filtering

Web policy

☐ 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

Other security features

Identify and control applications (App control)

☐ Apply application-based traffic shaping policy

Shape traffic

DSCP marking

Detect and prevent exploits (IPS)

☐ Scan email content

İşlemler sonucunda **Protect > Rules and Policies** menüsü aşağıdaki şekilde görünecektir.

Rule type	Source zone	Destination zone	Status	Rule ID	Add Filter
IPv4	IPv6	Disable filter			Test your policies
#	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	

LOGLARIN USEROAM CİHAZINA YÖNLENDİRİLMESİ**I.**

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

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 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.

Ardından loglarınızı göndermek için yeni bir **syslog server** eklenerek aşağıdaki bilgiler girilir.

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 sadece **Content Filtering** alanları seçilerek loglama Useroam'a doğru başlatılır.

SOPHOS FW

Feedback [How-to guides](#) [Log viewer](#) [Help](#) [GLOX TEKNO](#)

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

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.

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.

**Hepsi bu kadar.**

Entegrasyon işleminiz tamamlandı. İşlem sırasında bir sorun yaşarsanız destek@glox.com.tr adresinden bizimle iletişime geçebilirsiniz.