



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.

1

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 Authentication

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

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

Sophos
 5651 Loglama

178.159.35.173

GLX-Sophos-FW

4444

useroam

Useroam112233

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		
	HTTPS	SSH	AD SSO	Captive portal *	Radius SSO	Clients	Chromebook SSO	Ping/Ping6	DNS	IP
LAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
WAN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DMZ	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VPN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
WiFi	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GUEST	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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

<input type="checkbox"/>	#	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

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

Add external server

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.

The screenshot shows the Sophos firewall configuration interface. The main window is titled "Add external server" and has a sidebar on the left with various navigation options. The "Servers" tab is selected and highlighted with a red box. The main content area shows the configuration for a RADIUS server. The "Server type" is set to "RADIUS server". The "Server name" is "Useroam", "Server IP" is "104.247.174.120", "Authentication port" is "1812", and "Time-out" is "3". There is an option to "Enable accounting" which is currently unchecked. The "Domain name" field is empty, and the "Group name attribute" is set to "Filter-Id". There is a toggle for "Enable additional settings" which is currently turned off. At the bottom of the main window, there are three buttons: "Test connection" (highlighted with a red box), "Save", and "Cancel".

A "Test connection" dialog box is open in the foreground. It has a title bar with a close button (X). The dialog contains two input fields: "Username *" with the value "test1" and "Password *" with a masked password. Below the input fields is a "Test connection" button, which is also highlighted with a red box.

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

The screenshot shows the Sophos Web Authentication configuration interface. The left sidebar contains navigation options like 'Control center', 'Reports', 'Diagnostics', 'Rules and policies', 'Web', 'Applications', 'Wireless', 'Email', 'Web server', 'Active threat response', 'Remote access VPN', 'Site-to-site VPN', 'Network', 'Routing', 'Authentication', 'System services', 'Sophos Central', 'Profiles', 'Hosts and services', 'Administration', 'Backup & firmware', and 'Certificates'. The main content area is titled 'Authorize unauthenticated users for web access' and includes sections for 'If Active Directory (AD) SSO is configured', 'If AD SSO isn't configured', 'Captive portal behavior', and 'Sign out user'. The 'Sign out user' section has three radio button options: 'When captive portal page is closed or redirected', 'When user is inactive' (selected), and 'Never'. Below this, there is a checkbox for 'Use insecure HTTP instead of HTTPS' which is checked. The 'Traffic flow required to consider the user active' section shows '100 bytes in 1440 minutes'. An 'Apply' button is at the bottom left.

8

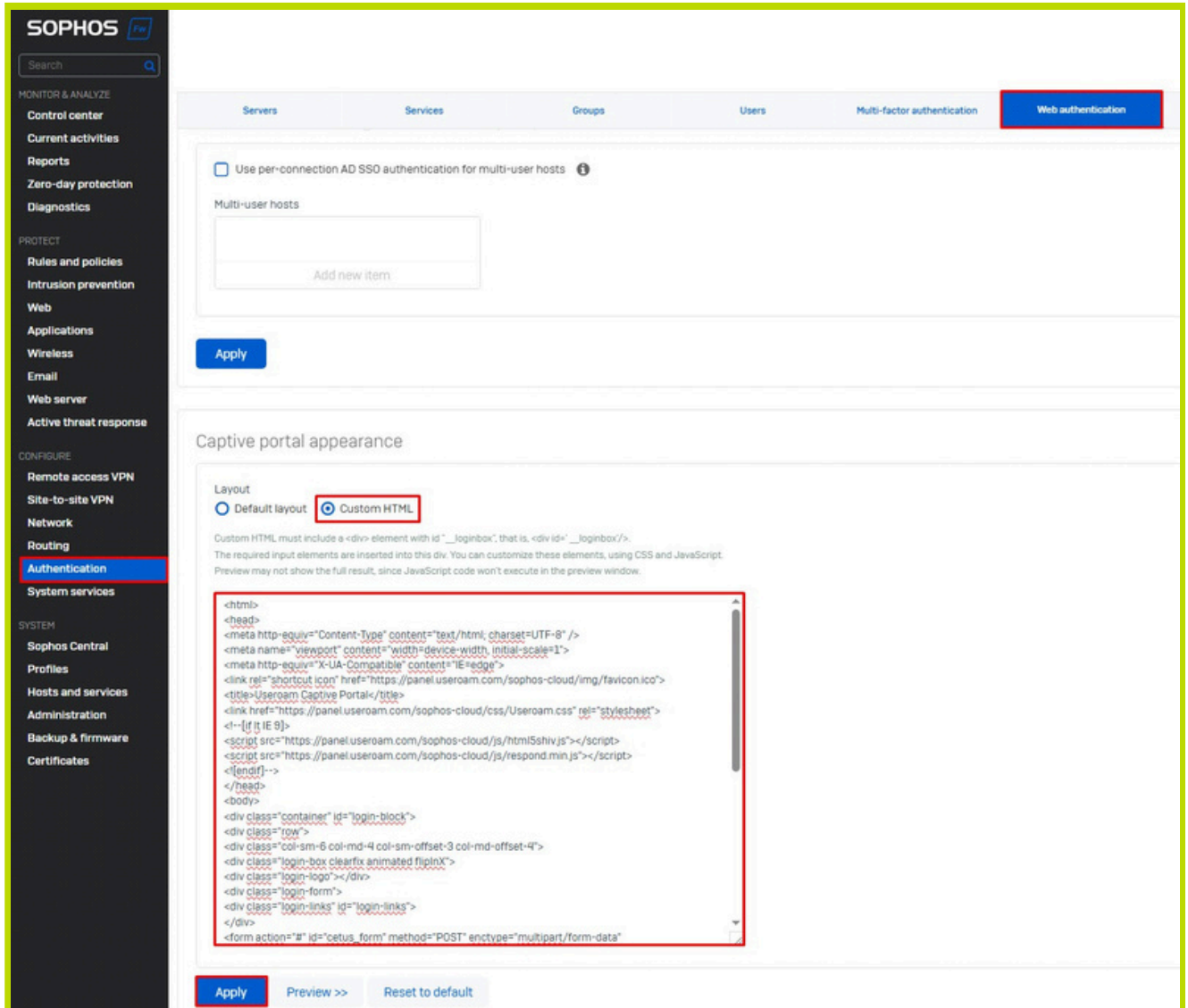
Useroam > Sistem Ayarları > Template kısmından <html> kod satırı ile başlayan bölümün hepsini alarak, Sophos Firewall'daki **Authentication > Web Authentication > Captive portal appearance > Custom HTML** kısmına yapıştırdınız ve kaydediniz.



```

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="https://panel.useroam.com/sophos-cloud/img/favicon.ico">
7 <title>Useroam Captive Portal</title>
8 <link href="https://panel.useroam.com/sophos-cloud/css/Useroam.css" rel="stylesheet">
9 <!-- [if lt IE 9]
10 <script src="https://panel.useroam.com/sophos-cloud/js/html5shiv.js"></script>
11 <script src="https://panel.useroam.com/sophos-cloud/js/respond.min.js"></script>
12 <![endif]-->
13 </head>
14 <body>
15 <div class="container" id="login-block">
16 <div class="row">
17 <div class="col-sm-6 col-md-4 col-sm-offset-3 col-md-offset-4">
18 <div class="login-box clearfix animated flipInX">
19 <div class="login-logo"></div>
20 <div class="login-form">

```



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**

Use per-connection AD SSO authentication for multi-user hosts

Multi-user hosts

Add new item

Apply

Captive portal appearance

Layout

Default layout Custom HTML

Custom HTML must include a <div> element with id "_loginbox", that is, <div id="_loginbox">.

The required input elements are inserted into this div. You can customize these elements, using CSS and JavaScript.

Preview may not show the full result, since JavaScript code won't execute in the preview window.

```

<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="https://panel.useroam.com/sophos-cloud/img/favicon.ico">
<title>Useroam Captive Portal</title>
<link href="https://panel.useroam.com/sophos-cloud/css/Useroam.css" rel="stylesheet">
<!-- [if lt IE 9]
<script src="https://panel.useroam.com/sophos-cloud/js/html5shiv.js"></script>
<script src="https://panel.useroam.com/sophos-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 flipInX">
<div class="login-logo"></div>
<div class="login-form">
<div class="login-links" id="login-links">
</div>
<form action="#" id="cetus_form" method="POST" enctype="multipart/form-data"

```

Apply Preview >> Reset to default

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 Firewall

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 1.

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.

The screenshot shows the 'Add firewall rule' configuration page in the Sophos Firewall interface. The page is titled 'Add firewall rule' and includes a search bar and navigation links for 'How-to guides' and 'Log viewer'. The configuration is organized into several sections:

- Rule status:** A toggle switch is turned on.
- Rule name:** 'GUEST TO DNS' is entered in the text field.
- Description:** 'GUEST TO DNS' is entered in the text field.
- Action:** 'Accept' is selected from the dropdown menu.
- Log firewall traffic:** This checkbox is checked.
- Rule position:** 'Top' is selected from the dropdown menu.
- Rule group:** 'GUEST' is selected from the dropdown menu.
- Source:**
 - Source zones:** 'GUEST' is selected from the dropdown menu.
 - Source networks and devices:** 'Any' is selected from the dropdown menu.
- Destination and services:**
 - Destination zones:** 'WAN' is selected from the dropdown menu.
 - Destination networks:** 'Any' is selected from the dropdown menu.
 - Services:** 'DNS' is selected from the dropdown menu.
- During scheduled time:** 'All the time' is selected from the dropdown menu.

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 Edit firewall rule 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

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.

The screenshot shows the configuration page for a rule named 'GUEST TO INTERNET'. The 'Action' is set to 'Accept' and 'Log firewall traffic' is checked. The 'Source' is 'GUEST' and 'Destination' is 'WAN'. Under 'Security features', 'Web policy' is set to 'Allow All', 'Match known users' and 'Use web authentication for unknown users' are checked, and 'Identify and control applications (App control)' is set to 'Allow All'. The 'User or groups' field is set to 'Any'.

The screenshot shows the 'Security features' configuration page. Under 'Web filtering', 'Web policy' is set to 'Allow All'. Under 'Other security features', 'Identify and control applications (App control)' is set to 'Allow All'. The 'Shape traffic' is set to 'User's policy applied' and 'DSCP marking' is set to 'Select DSCP marking'.

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

The screenshot shows the 'Rules and policies' overview page. The 'Firewall rules' tab is selected. A table lists the rules:

Rule type	Source zone	Destination zone	Status	Rule ID	Add Filter
#	Name	Source	Destination	What	
	GUEST in 0 B, out 0 B	GUEST			
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**1.**

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

The screenshot displays the 'System services' configuration page in the Sophos Firewall interface. The 'Log settings' tab is selected. The configuration form includes the following fields:

- 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	<input type="checkbox"/>
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.

The screenshot shows the Sophos Firewall configuration interface. The 'Log settings' tab is selected, and the 'Content filtering' section is expanded. The following options are checked:

- Anti-spam
- SMTP
- POP3
- IMAP
- SMTSPS
- 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@useroamteknoloji.com adresinden bizimle iletişime geçebilirsiniz.