epati

Rapor Şablonu Yönetimi

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı

Kılavuzlar

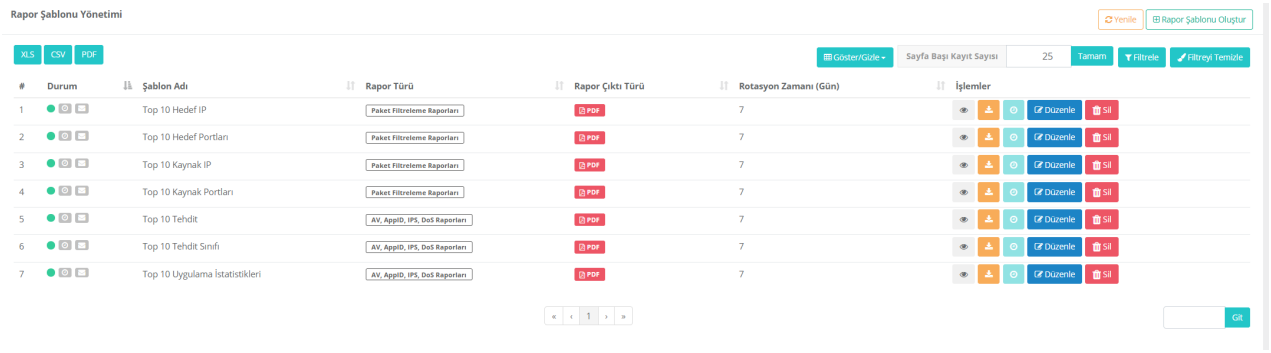
www.epati.com.tr

Rapor Şablonu Yönetimi

Bu sayfada **Rapor Şablonu Yönetimi** işlemleri gerçekleştirilmektedir.
Rapor şablonları, sistem üzerinde toplanan güvenlik ve trafik verilerinin belirli periyotlarla otomatik olarak raporlanmasını sağlar.

Oluşturulan rapor şablonları sayesinde;
paket filtreleme, tehdit, uygulama ve güvenlik istatistikleri düzenli olarak çıktı alınabilir ve ilgili kullanıcılara iletilebilir.

Raporlama süreci; **şablon tanımı**, **rapor türü seçimi**, **çıktı formatı** ve **rotasyon zamanı** gibi adımlardan oluşur.



Rapor Şablonu Listesi

Bu ekranda sistemde tanımlı olan tüm rapor şablonları listelenmektedir.
Her satır, ayrı bir rapor şablonunu temsil eder.

Listede yer alan bilgiler aşağıdaki gibidir:

- **Durum**: Rapor şablonunun aktif veya pasif olduğunu gösterir.
- **Şablon Adı**: Rapor şablonuna verilen tanımlayıcı isimdir.
- **Rapor Türü**: Raporun hangi veri kümesine ait olduğunu belirtir.
- **Rapor Çıktı Türü**: Raporun hangi formatta üretileceğini gösterir.
- **Rotasyon Zamanı (Gün)**: Raporun kaç günde bir otomatik oluşturulacağını belirtir.
- **İşlemler**: Rapor şablonu üzerinde yapılabilecek işlemleri içerir.

Ön Tanımlı Rapor Türleri

Sistem üzerinde desteklenen rapor türleri aşağıdaki gibidir:

- **Paket Filtreleme Raporları**
  - Top 10 Hedef IP
  - Top 10 Hedef Portları
  - Top 10 Kaynak IP
  - Top 10 Kaynak Portları
- **AV, AppID, IPS, DoS Raporları**
  - Top 10 Tehdit

- Top 10 Tehdit Sınıfı
- Top 10 Uygulama İstatistikleri

Her rapor türü, ilgili güvenlik modülünden toplanan veriler üzerinden oluşturulur.

Rapor Çıktı Türü

Raporlar aşağıdaki çıktı formatlarında üretilebilir:

- **PDF**
- **XLS**
- **CSV**

Seçilen çıktı türüne göre rapor, indirmeye veya paylaşmaya uygun şekilde oluşturulur.

Rotasyon Zamanı

Rotasyon Zamanı (Gün) alanı, raporun otomatik olarak hangi periyotlarla oluşturulacağını belirtir.

Örnek:

- 7 gün seçilmesi durumunda, rapor her 7 günde bir otomatik olarak üretilir.

Bu sayede periyodik raporlama süreçleri manuel işleme gerek kalmadan yönetilebilir.

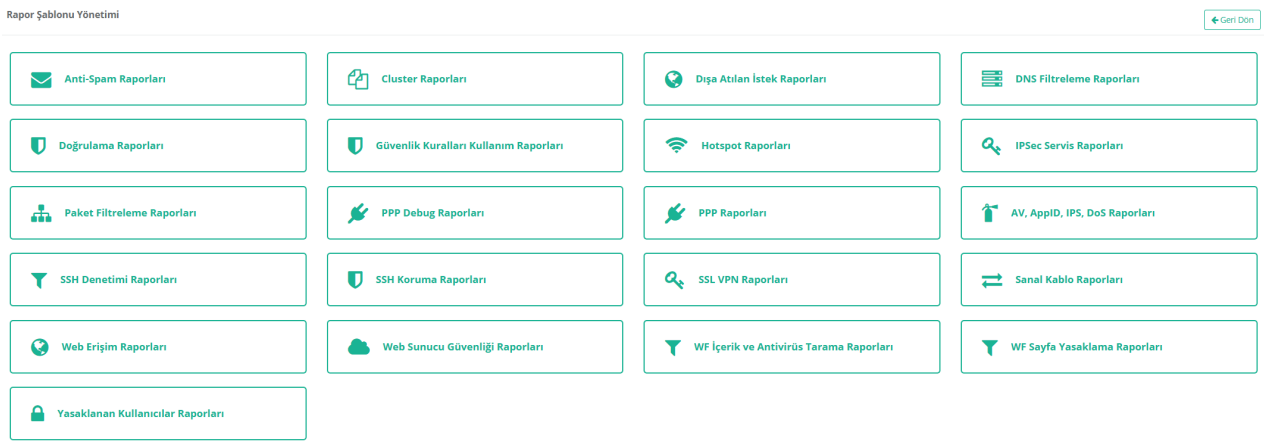
İşlemler

Her rapor şablonu için aşağıdaki işlemler gerçekleştirilebilir:

İşlem	Açıklama
□ Görüntüle	Rapor şablonuna ait detayları görüntüler.
⬇ İndir	Manuel olarak rapor çıktısını indirir.
□ Zamanla	Raporun zamanlama ayarlarını gösterir.
✏ Düzenle	Rapor şablonunda değişiklik yapılmasını sağlar.
□ Sil	Rapor şablonunu sistemden siler.

Rapor Kategorileri

Aşağıda listelenen rapor kategorilerinden biri seçilerek şablon oluşturma işlemine devam edilir:



- **Anti-Spam Raporları**
  E-posta trafiği üzerinde yapılan spam tespit ve engelleme işlemlerine ait raporları içerir.
- **Cluster Raporları**
  Cluster mimarisi üzerinde çalışan cihazların durum ve kullanım bilgilerini kapsar.
- **Dışa Atılan İstek Raporları**
  Sistem üzerinden dış ağlara yapılan isteklerin analizini ve istatistiklerini sunar.
- **DNS Filtreleme Raporları**
  DNS tabanlı erişim kontrolleri ve engelleme kayıtlarına ait raporları içerir.
- **Doğrulama Raporları**
  Kullanıcı doğrulama ve kimlik denetimi süreçlerine ait kayıtları raporlar.
- **Güvenlik Kuralları Kullanım Raporları**
  Tanımlı güvenlik kurallarının ne sıklıkla ve hangi trafik üzerinde çalıştığını gösterir.
- **Hotspot Raporları**
  Hotspot kullanıcıları ve bağlantı hareketlerine ait verileri içerir.
- **IPSec Servis Raporları**
  IPSec VPN bağlantıları ve servis durumları hakkında rapor üretir.
- **Paket Filtreleme Raporları**
  Paket filtreleme kurallarına takılan veya geçen trafiğin analizini sunar.
- **PPP Debug Raporları**
  PPP bağlantılarına ait hata ve debug kayıtlarını raporlar.
- **PPP Raporları**
  PPP servislerinin kullanım ve bağlantı istatistiklerini içerir.
- **AV, AppID, IPS, DoS Raporları**
  Tehdit tespiti, uygulama tanımlama ve saldırı önleme sistemlerine ait raporları kapsar.
- **SSH Denetimi Raporları**
  SSH erişim denemeleri ve denetim kayıtlarını içerir.
- **SSH Koruma Raporları**
  SSH saldırı engelleme ve koruma mekanizmalarına ait raporları sunar.
- **SSL VPN Raporları**
  SSL VPN bağlantıları ve kullanıcı hareketlerini raporlar.
- **Sanal Kablo Raporları**
  Sanal kablo (virtual wire) yapılandırmaları ve trafik bilgilerini içerir.

- **Web Erişim Raporları**
  Web erişim kayıtları ve kullanıcı bazlı erişim istatistiklerini sunar.
- **Web Sunucu Güvenliği Raporları**
  Web sunucularına yönelik güvenlik olaylarını raporlar.
- **WF İçerik ve Antivirüs Tarama Raporları**
  Web filtreleme ve antivirüs tarama sonuçlarına ait raporları içerir.
- **WF Sayfa Yasaklama Raporları**
  Yasaklanan web sayfaları ve erişim denemelerini raporlar.
- **Yasaklanan Kullanıcılar Raporları**
  Sistem tarafından engellenmiş kullanıcıları ve engelleme nedenlerini listeler.

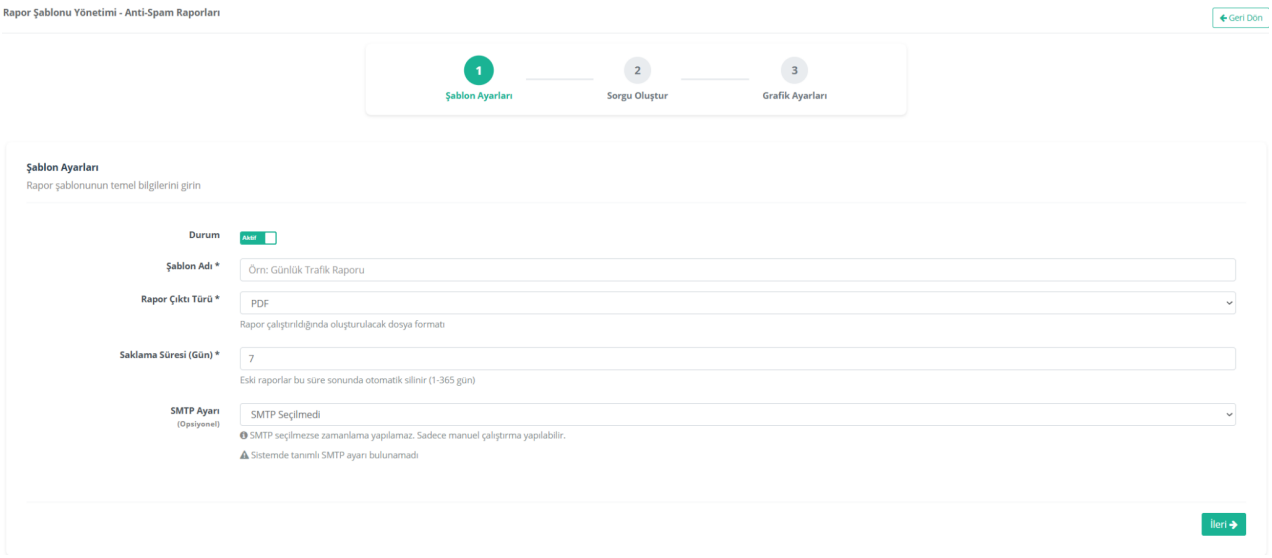
Rapor Şablonu Oluşturma

Rapor şablonu oluşturma süreci, tüm rapor türleri için aynı adımlardan oluşur.
Bu bölümde süreç, **Anti-Spam Raporları** üzerinden örneklenerek anlatılmıştır.

Oluşturma işlemi toplam **3 adımdan** oluşur:

1. Şablon Ayarları
2. Sorgu Oluştur
3. Grafik Ayarları

1. Şablon Ayarları



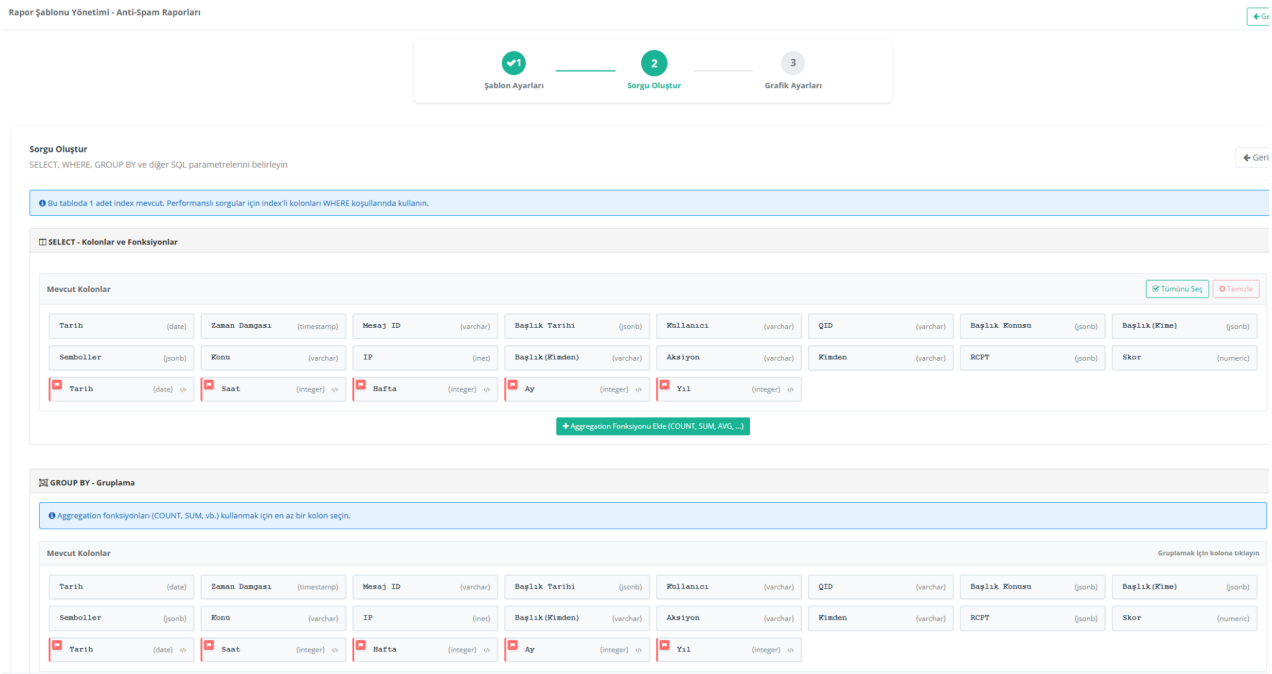
Bu adımda rapor şablonuna ait temel bilgiler tanımlanır.

Alan	Açıklama
`Durum`	Rapor şablonunun aktif veya pasif olma durumu belirlenir.
`Şablon Adı`	Oluşturulacak rapor şablonunun ismidir.
`Rapor Çıktı Türü`	Raporun hangi formatta oluşturulacağını belirtir (PDF, XLS, CSV).
`Saklama Süresi (Gün)`	Oluşturulan raporların sistemde kaç gün saklanacağını belirler.
`SMTP Ayarı`	Raporun e-posta ile gönderilmesi için kullanılacak SMTP ayarıdır (opsiyonel).

`Not:` SMTP ayarı seçilmezse rapor zamanlanamaz, yalnızca manuel olarak çalıştırılabilir.

Bu alanlar doldurulduktan sonra **İleri** butonuna tıklanarak ikinci adıma geçilir.

2. Sorgu Oluştur



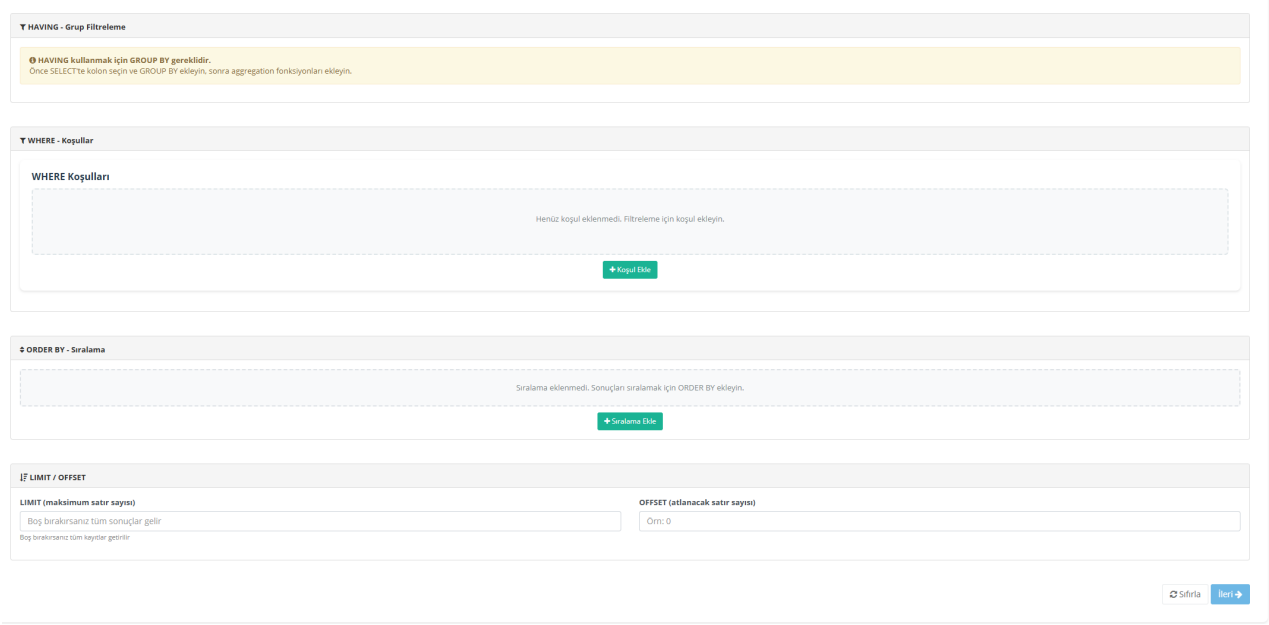
Bu adımda raporun hangi veriler üzerinden üretileceği belirlenir.
Sorgu yapısı, SQL mantığına benzer şekilde görsel olarak oluşturulur.

Bu ekranda aşağıdaki bölümler yer alır:

- **SELECT – Kolonlar ve Fonksiyonlar**
  Raporda gösterilecek kolonlar seçilir.
  İhtiyaca göre `COUNT`, `SUM`, `AVG` gibi aggregation fonksiyonları eklenebilir.
- **GROUP BY – Gruplama**
  Verilerin belirli alanlara göre gruplanmasını sağlar.
  (Örn: Tarihe, IP'ye veya kullanıcıya göre gruplama)
- **HAVING – Grup Filtreleme**
  Gruplama sonrası oluşan sonuçlar üzerinde filtreleme yapılmasını sağlar.
- **WHERE – Koşullar**
  Rapor verilerinin filtrelenmesi için kullanılır.
  (Örn: tarih aralığı, IP adresi, skor değeri)

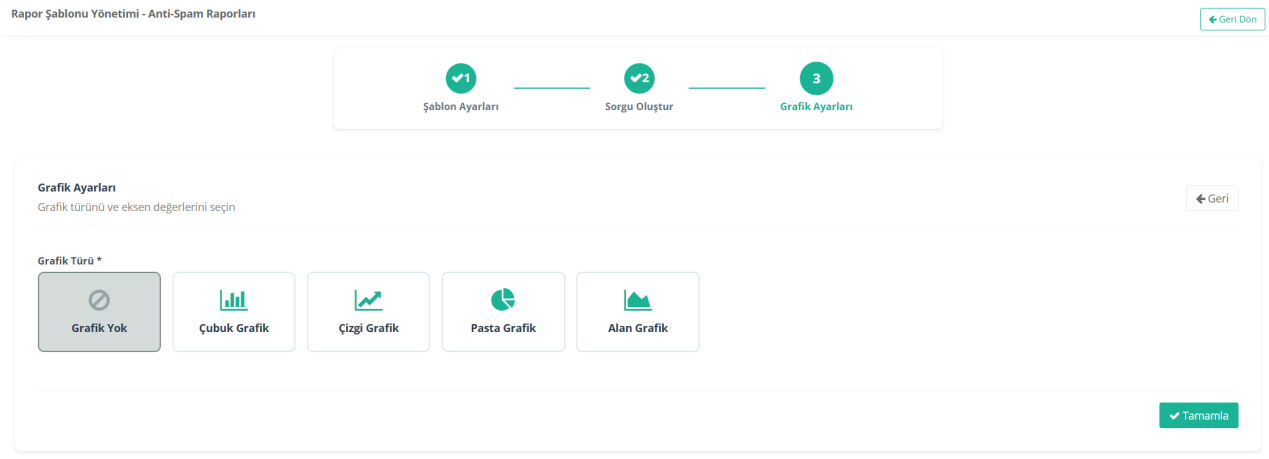
- **ORDER BY – Sıralama**
  Sonuçların artan veya azalan şekilde sıralanmasını sağlar.

- **LIMIT / OFFSET**
  Raporda getirilecek maksimum kayıt sayısını ve başlangıç satırını belirler.



Sorgu yapılandırması tamamlandıktan sonra **İleri** butonuna tıklanarak son adıma geçilir.

3. Grafik Ayarları



Bu adımda rapor çıktısında kullanılacak grafik ayarları belirlenir.

Seçilebilen grafik türleri:

- **Grafik Yok**
- **Çubuk Grafik**
- **Çizgi Grafik**
- **Pasta Grafik**
- **Alan Grafik**

Grafik seçimi opsiyoneldir.
Grafik seçilmediği durumda rapor yalnızca tablo formatında oluşturulur.

Tüm ayarlar tamamlandıktan sonra **Tamamla** butonuna tıklanarak rapor şablonu oluşturulur.

`Not:` Bu örnek Anti-Spam Raporları üzerinden anlatılmıştır. Diğer tüm rapor türleri için şablon oluşturma

adımları aynı şekilde çalışır.

ePati Siber Güvenlik Teknolojileri A.Ş.
Mersin Üniversitesi Çiftlikköy Kampüsü
Teknopark İdari Binası Kat: 4 No: 411
Posta Kodu: 33343 Yenişehir / MERSİN

www.epati.com.tr
bilgi@epati.com.tr
+90 324 361 02 33
+90 324 361 02 39