epati

Log İzleme

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı

Kılavuzlar

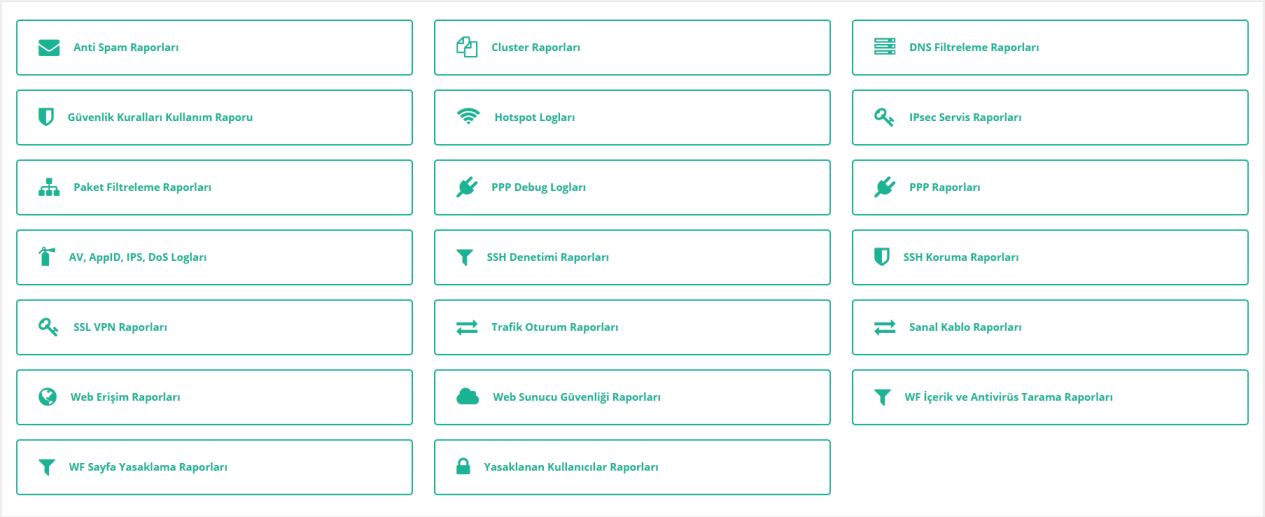
www.epati.com.tr

title: Log izleme
—

Log İzleme

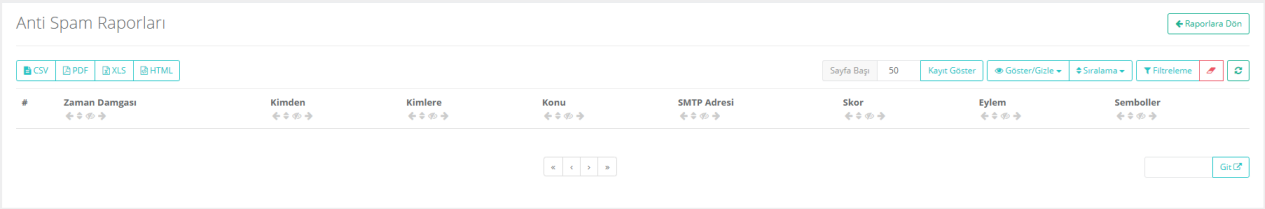
20 farklı rapor çeşidi dinamik olarak buradan görüntülenmekte ve listelenmektedir.

- Anti Spam Logları
- Cluster Logları
- DHCPv4 Logları
- DHCPv6 Logları
- Dışa Atılan İstek Logları
- DNS Filtreleme Logları
- Doğrulama Logları
- Güvenlik Kuralları Kullanım Logları
- Hotspot Logları
- IPsec Servis Logları
- Oturum Geçmişi Logları
- Paket Filtreleme Logları
- PPP Debug Logları
- PPP Logları
- AV, AppID, IPS, DoS Logları
- SSH Denetimi Logları
- SSH Koruma Logları
- SSL VPN Logları
- Trafik Oturum Logları
- Sanal Kablo Logları
- Web Erişim Logları
- Web Sunucu Güvenliği Logları
- WF İçerik ve Antivirüs Tarama Logları
- WF Sayfa Yasaklama Logları
- Yasaklanan Kullanıcılar Logları



Anti Spam Logları

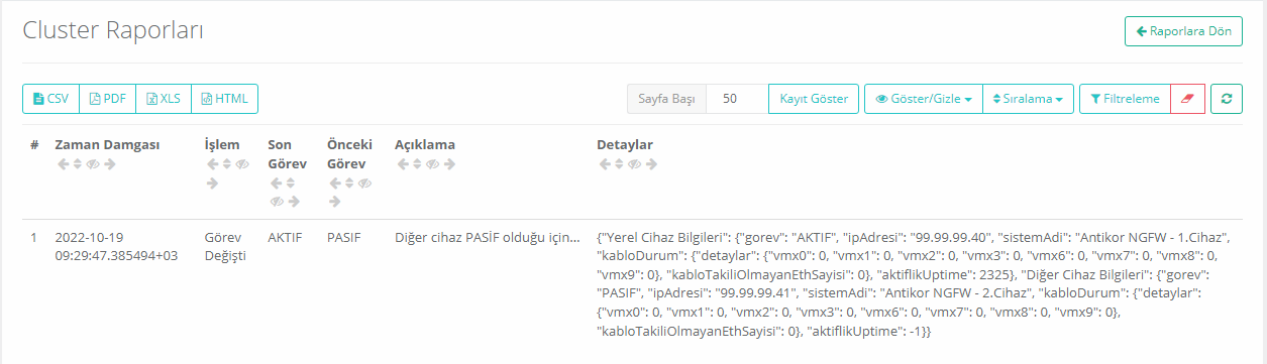
Anti-spam raporları, e-postaların spam filtrelerinden geçme sürecini detaylandıran kayıtlardır.



Alan	Açıklama
`Zaman Damgası`	E-postanın işlendiği tarih bilgisini gösterir.
`Kimden`	E-postayı gönderen kişinin veya sistemin e-posta adresini belirtir.
`Kimlere`	E-postanın gönderildiği alıcı veya alıcıların e-posta adreslerini gösterir.
`Konu`	E-postanın içerik bilgisini içerir.
`SMTP Adresi`	E-postayı gönderen sunucunun IP adresi veya alan adını belirtir.
`Skor`	E-postanın spam olasılığını gösteren sayısal bir değerdir.
`Eylem`	Anti-spam sisteminin e-postaya uyguladığı işlemi belirtir.
`Semboller`	E-postanın spam olarak işaretlenmesine katkıda bulunan belirli anti-spam kontrollerinin sonuçlarını gösteren kodlardır.

Cluster Logları

Cluster ile ilgili oluşan durumları ve durumların gerçekleştiği arayüzleri tarihe göre raporlamaktadır.



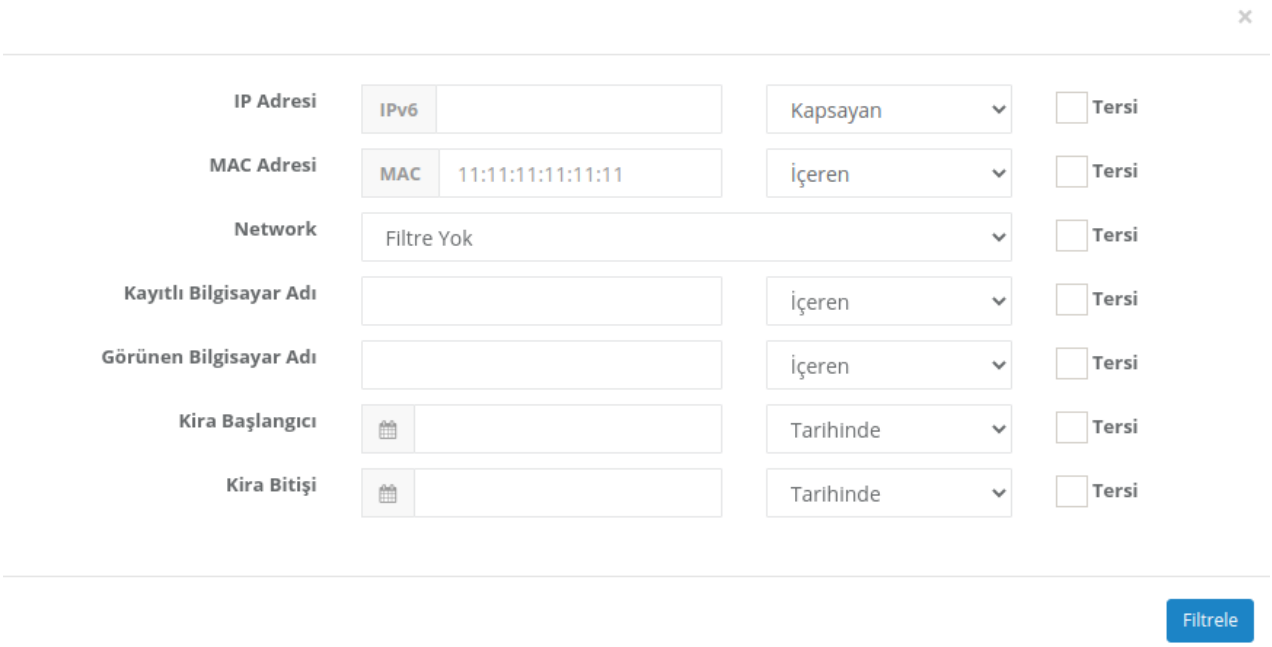
Alan	Açıklama
Zaman Damgası	Zaman damgası, olayın tam olarak ne zaman gerçekleştiğini gösterir.
İşlem	Cluster üzerindeki işlemlerin neler olduğu açıklanmaktadır. (Ne yapılmış).
Son Görev	Cluster içindeki ilgili node'un şu anda bulunduğu durumu veya en son gerçekleştirdiği geçişi gösterir.
Önceki Görev	Bu node'un önceki rolü neydi, hangi durumdan geldiğini gösterir.
Açıklama	Bu kısımda olayın kısa özeti yer alır.
Detaylar	Bu bölümde olayın arka planı yani teknik ayrıntılar yer alır.

DHCPv4 Logları

Seçilen tarih için DHCPv4 servisi tarafından IPv4 adresi atanmış olan istemcilere ait DHCPv4 raporlarını gösterir.

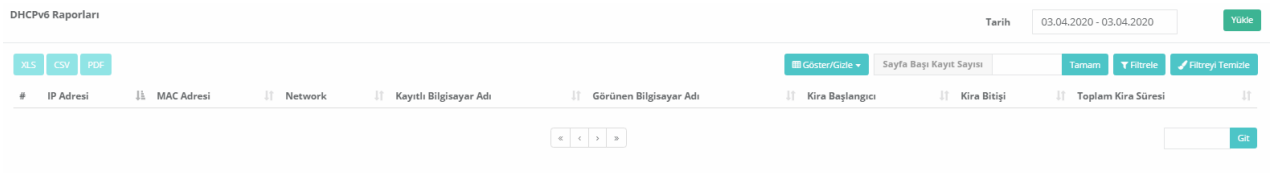
ALAN	AÇIKLAMA
IP Adresi	DHCP servisi tarafından istemciye atanmış IPv4 adresini gösterir.
MAC Adresi	IPv4 adresini alan istemciye ait MAC adresini gösterir.
Network	İstemcinin bağlı olduğu IPv4 ağı (network) gösterir.
Kayıtlı Bilgisayar Adı	İstemci Tanımlarında kayıtlı olan bilgisayar adını gösterir.
Görünen Bilgisayar Adı	Bilgisayarın işletim sisteminde tanımlı olan bilgisayar adını gösterir.
Kira Başlangıcı	IPv4 adresinin istemciye atanma tarihini gösterir.
Kira Bitişi	IPv4 adresinin istemci tarafından bırakıldığı tarihi gösterir.
Toplam Kira Süresi	İstemcinin IPv4 adresini toplamda ne kadar süre kullandığını gösterir.

Filtreleme



DHCPv6 Logları

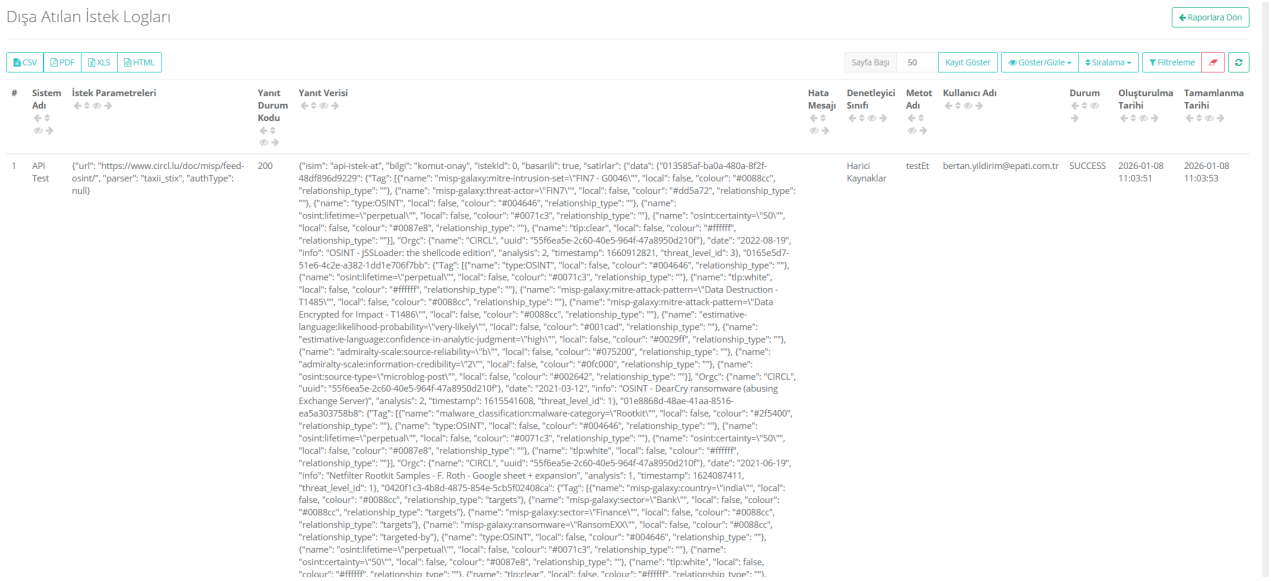
Seçilen tarih için DHCPv6 servisi tarafından IPv6 adresi atanmış olan istemcilere ait DHCPv6 raporlarını gösterir.



ALAN	AÇIKLAMA
IP Adresi	DHCP servisi tarafından istemciye atanmış IPv6 adresini gösterir.
MAC Adresi	IPv6 adresini alan istemciye ait MAC adresini gösterir.
Network	İstemcinin bağlı olduğu IPv6 ağı (network) gösterir.
Kayıtlı Bilgisayar Adı	İstemci Tanımlarında kayıtlı olan bilgisayar adını gösterir.
Görünen Bilgisayar Adı	Bilgisayarın işletim sisteminde tanımlı olan bilgisayar adını gösterir.
Kira Başlangıcı	IPv6 adresinin istemciye atanma tarihini gösterir.
Kira Bitişi	IPv6 adresinin istemci tarafından bırakıldığı tarihi gösterir.
Toplam Kira Süresi	İstemcinin IPv6 adresini toplamda ne kadar süre kullandığını gösterir.

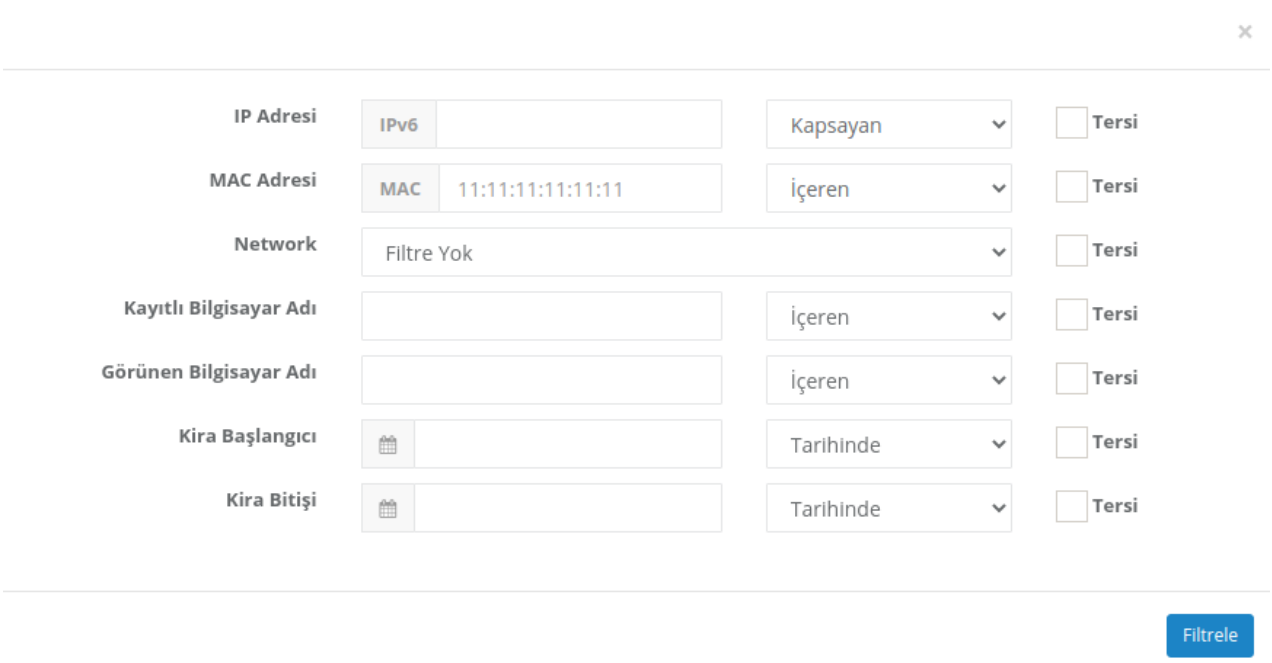
Dışa Atılan İstek Logları

Dışa Atılan İstek Logları, sistem tarafından dış sistemlere yapılan isteklerin ve bu isteklere ait yanıtların detaylarını kayıt altına alır.



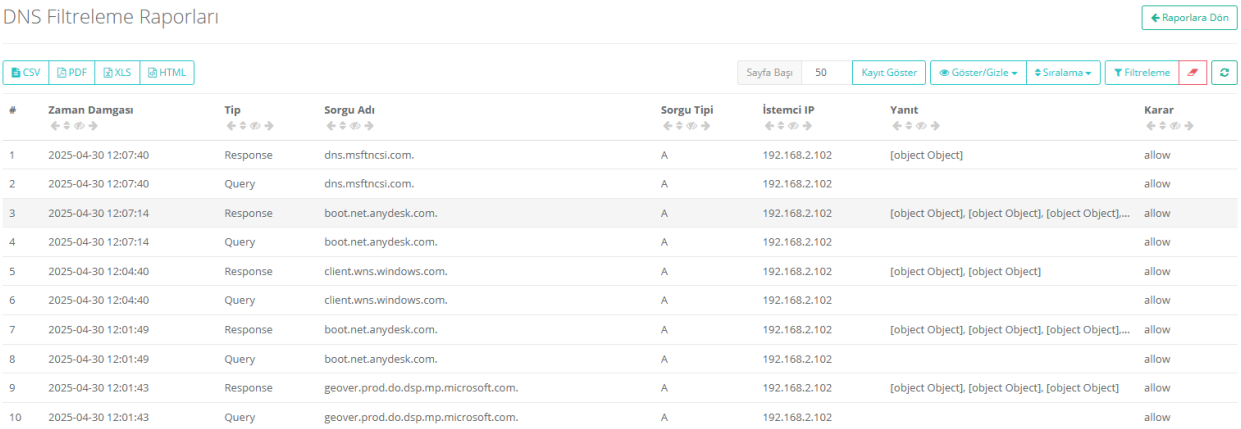
Alan	Açıklama
`Sistem Adı`	İsteğin hangi sistem veya modül tarafından oluşturulduğunu gösterir.
`İstek Parametreleri`	Dış sisteme gönderilen isteğe ait parametre bilgilerini gösterir.
`Yanıt Durum Kodu`	Dış sistemden dönen yanıtın HTTP durum kodunu gösterir.
`Yanıt Verisi`	Dış sistemden dönen yanıt içeriğini gösterir.
`Hata Mesajı`	İstek sırasında oluşan hata varsa hata mesajını gösterir.
`Denetleyici Sınıfı`	İsteği işleyen denetleyici (controller) sınıfını gösterir.
`Metot Adı`	Denetleyici içerisinde çağrılan metot adını gösterir.
`Kullanıcı Adı`	İsteği başlatan kullanıcı hesabını gösterir.
`Durum`	İsteğin başarılı veya hatalı sonuçlandığını gösterir.
`Oluşturulma Tarihi`	İsteğin sisteme kaydedildiği tarih ve saat bilgisidir.
`Tamamlanma Tarihi`	İsteğin tamamlandığı tarih ve saat bilgisidir.

Filtreleme



DNS Filtreleme Logları

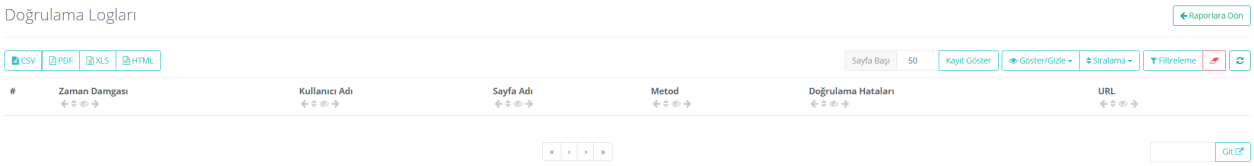
DNS filtreleme logları, bir ağda yapılan DNS sorgularını ve bu sorgulara verilen yanıtları takip eder.



Alan	Açıklama
`Zaman Damgası`	DNS filtrelemesinin sistemde gerçekleştiği tarih ve saattir.
`Tip`	DNS filtrelemesinin türünü belirtir
`Sorgu Adı`	Erişilmek istenen alan adını (domain) gösterir.
`Sorgu Tipi`	Yapılan DNS sorgusunun tipidir.
`İstemci IP`	DNS sorgusunu yapan cihazın IP adresidir.
`Yanıt`	DNS sunucusunun bu sorguya verdiği cevaptır.
`Karar`	Sorguya izin verildi mi yoksa engellendi mi, bunu belirtir.

Doğrulama Logları

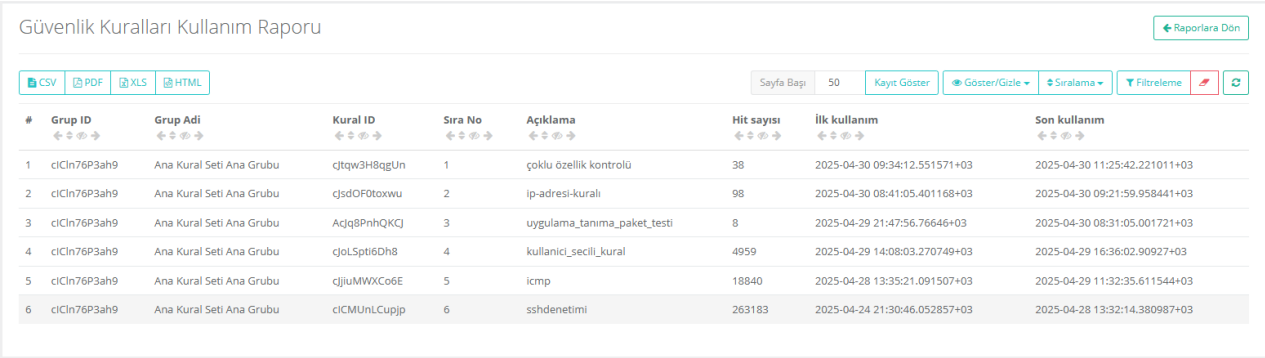
Doğrulama Logları, sistem üzerinde yapılan kullanıcı doğrulama (authentication / validation) işlemlerine ait kayıtları gösterir. Bu loglar sayesinde hangi kullanıcı tarafından, hangi sayfa veya URL üzerinde, hangi metot ile doğrulama hatası oluştuğu detaylı olarak izlenebilir.



Alan	Açıklama
`#`	Log kaydının tablo üzerindeki sıra numarasını gösterir.
`Zaman Damgası`	Doğrulama işleminin gerçekleştiği tarih ve saat bilgisidir.
`Kullanıcı Adı`	Doğrulama işlemini gerçekleştiren kullanıcı hesabını gösterir.
`Sayfa Adı`	Doğrulama işleminin yapıldığı sayfanın adını gösterir.
`Metod`	Doğrulama sırasında kullanılan HTTP metodunu gösterir (GET, POST vb.).
`Doğrulama Hataları`	Doğrulama sırasında oluşan hata veya hata mesajlarını gösterir.
`URL`	Doğrulama işleminin gerçekleştiği tam URL bilgisini gösterir.

Güvenlik Kuralları Kullanım Logları

Güvenlik kuralı kullanım logları, Güvenlik Kuralları sayfasında oluşturduğumuz kuralların kullanım loglarıdır.



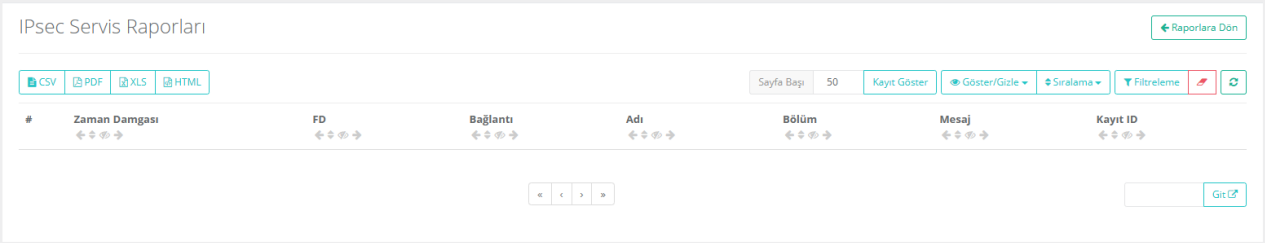
Alan	Açıklama
`Grup ID`	Bu kuralın ait olduğu grubun benzersiz kimlik numarasını belirtir.
`Grup Adı`	Kuralın yer aldığı güvenlik grubunun adını belirtir.
`Kural ID`	Her bir güvenlik kuralının kendine ait benzersiz kimlik numarasını gösterir.
`Sıra No`	Kuralın sıralandığı yerin numarasını belirtir. En düşük numara ilk dikkate alınan kural.
`Açıklama`	Bu güvenlik kuralının ne işe yaradığını açıklayan kısa bir tanımlamadır.
`Hit Sayısı`	Bu güvenlik kuralının kaç kez tetiklendiğini veya kaç kez kullanıldığını gösteren sayıdır.
`İlk Kullanım`	Kuralın ilk kez ne zaman tetiklendiğini veya uygulandığını gösterir.
`Son Kullanım`	Kuralın son kez ne zaman tetiklendiğini veya kullanıldığını gösterir.

Hotspot Logları

Alan	Açıklama
Kullanıcı Adı	Ağda oturum açan kullanıcının kimlik bilgilerini belirtir.
Kullanılan Süre (Sn)	Kullanıcının ağa bağlandığı andan itibaren toplamda kaç saniye süreyle bağlantı sağladığını gösterir.
Kullanılan Boyut (KB)	Kullanıcının oturum sırasında kullandığı toplam veri miktarını kilobayt (KB) cinsinden belirtir.
IP Adresi	Kullanıcının oturum açtığı cihazın IP adresini gösterir.
Oturum Açma Zamanı	Kullanıcının ağa bağlandığı ilk zaman veya oturum açtığı anı gösterir.
Oturum Kapatma Zamanı	Kullanıcının ağdan çıkış yaptığı veya oturumunun sonlandığı zamanı belirtir.

IPsec Servis Logları

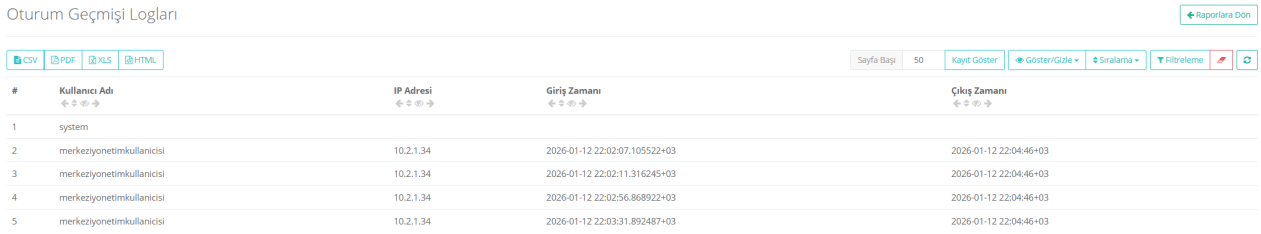
IPsec (Internet Protocol Security), IP tabanlı ağlarda veri güvenliğini sağlamak amacıyla kullanılan bir güvenlik protokolüdür. Bu güvenliği sağlama sürecinde karşılaşılan raporlara buradan ulaşmak mümkündür.



Alan	Açıklama
Zaman Damgası	Bu alan, raporun oluşturulduğu veya olayın gerçekleştiği tam zamanı belirtir.
FD	Bu, IPsec trafiğinin yönünü belirtir.
Bağlantı	IPsec ile kurulan ağ bağlantısının kimliğini belirtir.
Adı	Bağlantının tanımlayıcı ismini belirtir.
Bölüm	Olayın veya raporun hangi bölümde gerçekleştiğini belirtir.
Mesaj	Bu, IPsec ile ilgili olay hakkında daha ayrıntılı bilgi verir.
Kayıt ID	Her raporun benzersiz bir kimlik numarasını belirtir.

Oturum Geçmişi Logları

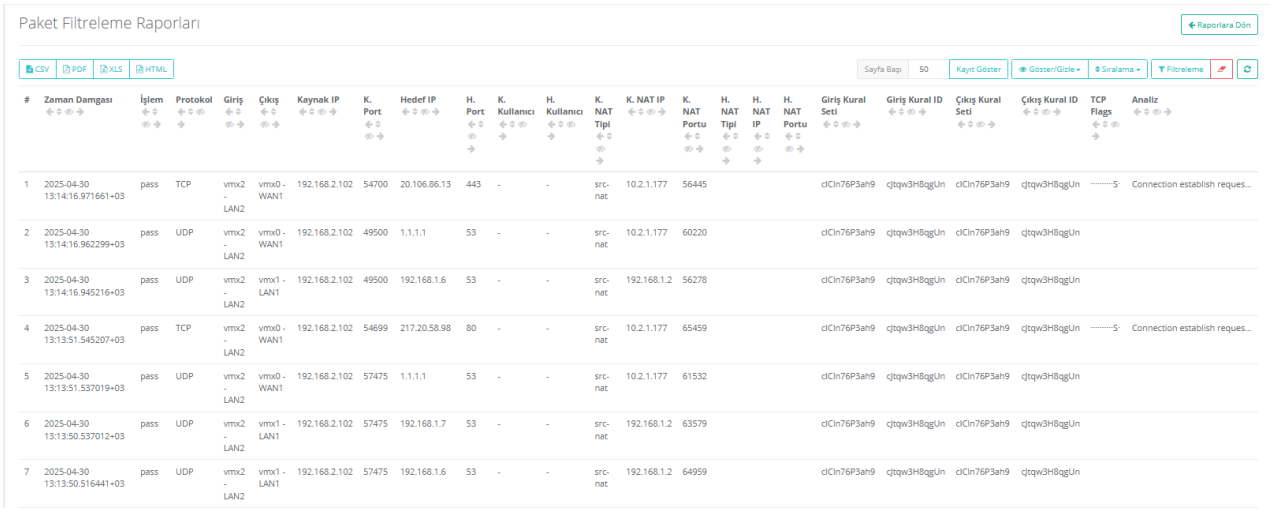
Oturum Geçmişi Logları, sistem kullanıcılarının oturum açma ve kapatma işlemlerine ait kayıtları gösterir. Bu loglar sayesinde hangi kullanıcının, hangi IP adresinden, ne zaman giriş yaptığı ve oturumunu ne zaman sonlandırdığı izlenebilir.



Alan	Açıklama
`#`	Log kaydının tablo üzerindeki sıra numarasını gösterir.
`Kullanıcı Adı`	Oturum açan kullanıcı hesabını gösterir.
`IP Adresi`	Kullanıcının oturum açtığı istemci IP adresini gösterir.
`Giriş Zamanı`	Kullanıcının sisteme giriş yaptığı tarih ve saat bilgisidir.
`Çıkış Zamanı`	Kullanıcının sistemden çıkış yaptığı tarih ve saat bilgisidir.

Paket Filtreleme Logları

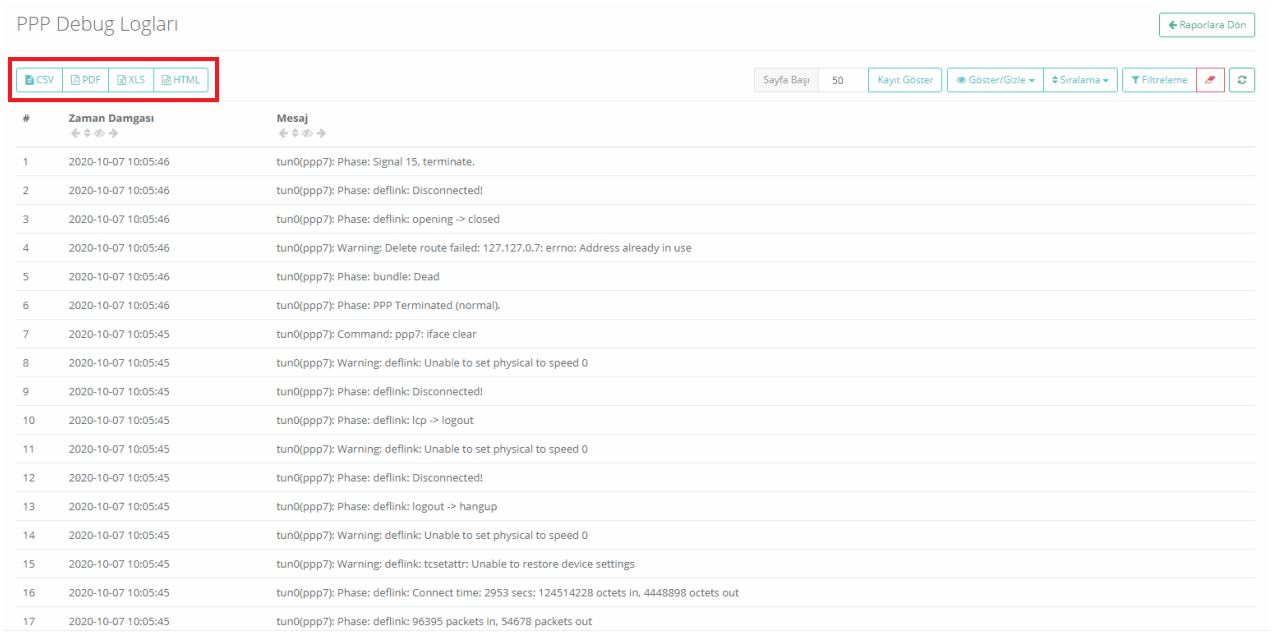
Paket filtreleme logları, ağdan geçen veri paketlerinin hangi kurallara göre işlendiğini, izin verilip verilmediğini ve paketin yönünü gösteren güvenlik kayıtlarıdır. Bu raporlar sayesinde, ağ trafiği gerçek zamanlı olarak analiz edilir ve olası tehditler tespit edilebilir.



Alan	Açıklama
`Zaman Damgası`	Paketin işlendiği tarih ve saat bilgisidir.
`İşlem`	Pakete uygulanan işlem türünü belirtir.(pass/block)
`Protokol`	Paket iletişiminin gerçekleştiği ağ protokolünü (örneğin TCP, UDP) gösterir.
`Giriş`	Paket ağda hangi arayüzden (interface) içeri girmişse onu belirtir.
`Çıkış`	Paket ağdan hangi arayüzden çıkmışsa onu gösterir.
`Kaynak IP`	Paketin geldiği cihazın IP adresidir.
`K.Port`	Paketi gönderen cihazın kullandığı port numarasıdır.
`Hedef IP`	Paketin ulaşmak istediği hedef IP adresidir.
`H.Port`	Paketin ulaştığı hedefteki port numarasıdır.
`K.Kullanıcı`	Kaynak tarafındaki oturumda kullanılan kullanıcı bilgisidir (varsa).
`H.Kullanıcı`	Hedef sistemdeki kullanıcı kimliğidir (varsa).
`K.NAT Tipi`	Kaynak tarafında uygulanan NAT (adres çevirme) türüdür.
`K.NAT IP`	NAT işleminde kullanılan yeni kaynak IP adresidir.
`K.NAT Portu`	NAT işleminde kullanılan yeni kaynak port numarasıdır.
`H.NAT Tipi`	Hedef tarafında uygulanan NAT türüdür.
`H.NAT IP`	NAT işleminde hedefe atanmış yeni IP adresidir.
`H.NAT Portu`	NAT işleminde hedefe atanmış yeni port numarasıdır.
`Giriş Kural Seti`	Paketin girişte karşılaştığı kural grubunun adıdır.
`Giriş Kural ID`	Girişte uygulanan belirli güvenlik kuralının kimlik numarasıdır.
`Çıkış Kural Seti`	Paketin çıkışta karşılaştığı kural grubunun adıdır.
`Çıkış Kural IP`	Çıkışta uygulanan belirli güvenlik kuralının kimlik numarasıdır.
`TCP Flags`	TCP paketleri için iletişim durumunu belirten bayrak (flag) bilgilerini gösterir.
`Analiz`	Bu paketin güvenlik açısından sistem tarafından yapılmış olan yorum veya işlem notudur.

PPP Debug Logları

PPP (Point-to-Point Protocol) Debug logları, iki cihaz arasında yapılan PPP bağlantısının kurulum, kimlik doğrulama ve veri iletim süreçlerini ayrıntılı olarak izleyen hata ayıklama kayıtlarıdır. Bu loglar, bağlantı hataları, oturum açma süreçleri ve iletişim adımlarını adım adım analiz etmek için kullanılır.

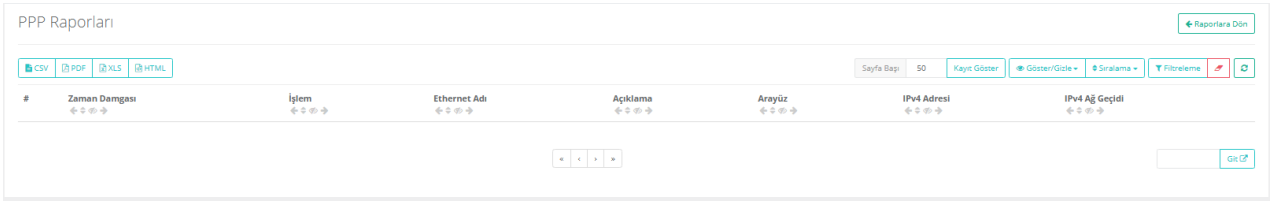


Alan	Açıklama
`Zaman Damgası`	Her bir PPP olayının veya mesajın gerçekleştiği tarih ve saat bilgisidir.
`Mesaj`	PPP bağlantısına ait olayın detayını içerir; örneğin, “CHAP authentication success”, “LCP terminated” gibi oturumun durumu veya hata mesajıdır.

`Not:` Kullanıcılar bu raporları **csv, pdf, xls ve html** formatlarında indirebilmektedir.

PPP Logları

PPP (Point-to-Point Protocol) raporları, ağ üzerindeki PPP bağlantılarının genel durumu hakkında bilgi verir; özellikle IP atamaları ve bağlantı arayüzleri gibi detayları içerir.



Alan	Açıklama
`Zaman Damgası`	PPP bağlantı işleminin gerçekleştiği tarih ve saat bilgisidir.
`İşlem`	PPP bağlantısı için yapılan işlemi belirtir.
`Ethernet Adı`	PPP oturumunun bağlı olduğu fiziksel Ethernet arayüzünün adıdır.
`Açıklama`	Bağlantıya dair sistem tarafından girilen durum veya bilgilendirici nottur.
`Arayüz`	PPP oturumunun kurulduğu mantıksal arayüz adıdır.
`IPv4 Adresi`	PPP bağlantısı sırasında istemciye atanan IPv4 adresidir.
`IPv4 Ağ Geçidi`	PPP oturumu için kullanılan varsayılan ağ geçidinin IPv4 adresidir.

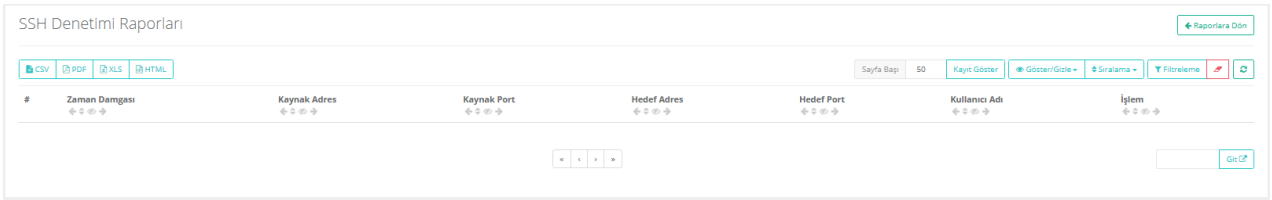
AV, AppID, IPS, DoS Logları

Antivirüs (AV), **Uygulama Tanımlama (AppID)**, **Saldırı Önleme Sistemi (IPS)** ve **Hizmet Dışı Bırakma (DoS)** olaylarına ilişkin güvenlik kayıtlarıdır. Ağdaki tehditleri, riskli uygulamaları ve saldırı girişimlerini tespit ederek yöneticilere detaylı güvenlik görünürlüğü sağlar.

Alan	Açıklama
Zaman Damgası	Olayın veya güvenlik işleminin gerçekleştiği tarih ve saat bilgisidir.
İşlem	Sistem tarafından yapılan güvenlik müdahalesinin türünü belirtir.
Karar	Olay sonucunda sistemin izin verip vermediğini veya engellediğini belirtir.
Protokol	İletişimin gerçekleştiği ağ protokolünü (örneğin TCP, UDP) gösterir.
Kaynak Kullanıcı	Olayın çıktığı istemcideki oturum açmış kullanıcıyı belirtir.
Kaynak IP	Trafiği başlatan cihazın IP adresidir.
Kaynak Port	Trafiği başlatan cihazın kullandığı port numarasıdır.
Hedef Kullanıcı	Trafiğin ulaştığı cihazda oturum açmış olan kullanıcı bilgisidir.
Hedef IP	Trafiğin yönlendirildiği hedef IP adresidir.
Hedef Port	Hedefte kullanılan servis port numarasıdır.
Servis	Belirli bir porta bağlı çalışan uygulama veya servis bilgisidir.
Ağ Arayüzü	Trafiğin geçtiği bağlantı noktasıdır.
VLAN	Olayın geçtiği sanal yerel ağdır.
AppID	Tanımlanan veya tespit edilen uygulama adıdır
Kural	Uygulanan güvenlik politikasının adıdır.
Açıklama	Olayla ilgili sistemin oluşturduğu açıklayıcı bilgidir.
Sistem	Olayı işleyen veya kaydeden güvenlik sistemi bileşenidir.
Kayıt ID	Her olaya özel oluşturulmuş benzersiz kimlik numarasıdır.
QoS Bilgisi	Olayın geçtiği trafiğe ait hizmet kalitesi seviyesidir.
Severity	Olayın önem derecesini ifade eder.

SSH Denetim Raporları

SSH denetim raporları, ağ üzerindeki cihazlara yapılan **SSH (Secure Shell)** bağlantı girişimlerini ve yönetim aktivitelerini izlemek amacıyla kaydedilen güvenlik kayıtlarıdır.



Alan	Açıklama
`Zaman Damgası`	SSH işleminin gerçekleştiği tarih ve saat bilgisidir.
`Kaynak Adres`	Bağlantıyı başlatan istemci cihazın IP adresidir.
`Kaynak Port`	İstemcinin SSH bağlantısı için kullandığı port numarasıdır.
`Hedef Adres`	Bağlantı kurulmak istenen sunucunun IP adresidir.
`Hedef Port`	SSH erişimi için hedef sistemde dinlenen port numarasıdır.
`Kullanıcı Adı`	SSH oturumu için kimlik doğrulama sırasında girilen kullanıcı hesabıdır.
`İşlem`	Gerçekleşen SSH işleminin türünü belirtir.

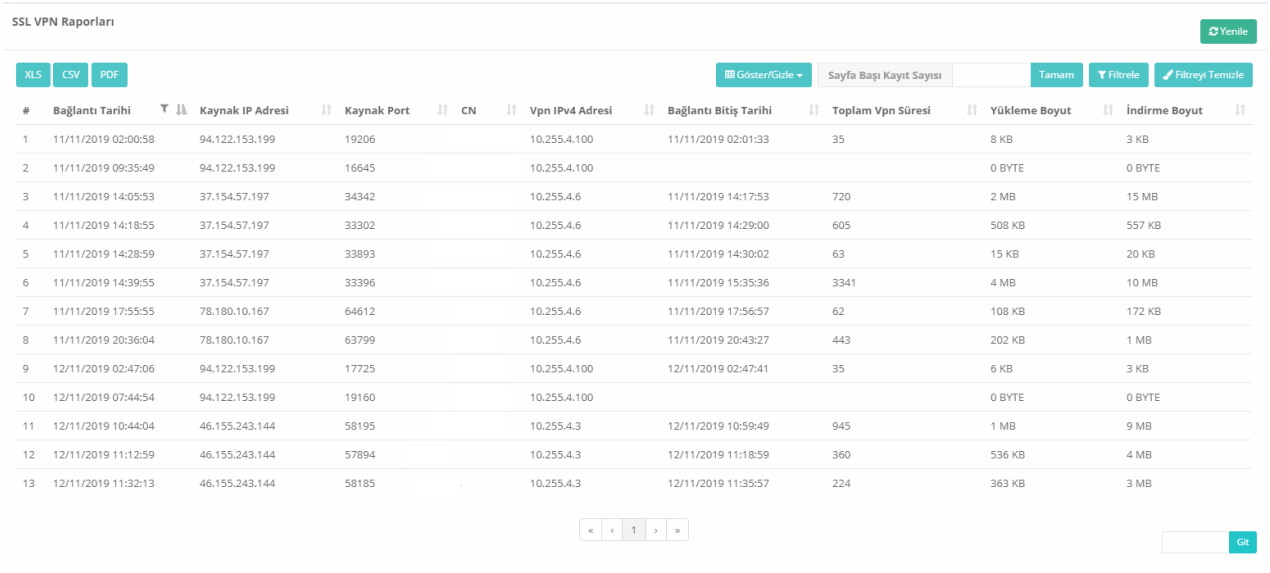
SSH Koruma Raporları

SSH koruma raporları, yetkisiz veya şüpheli SSH bağlantı girişimlerini tespit edip engelleyen güvenlik önlemlerini kayıt altına alan raporlardır.

Alan	Açıklama
`Zaman Damgası`	SSH işleminin gerçekleştiği tarih ve saat bilgisidir.
`İşlem`	Sistem tarafından alınan güvenlik aksiyonunu belirtir; örneğin IP engellendi, erişim reddedildi gibi.
`IP Adresi`	Kısıtlanan veya engellenen kaynak cihazın IP adresidir.

SSL VPN Logları

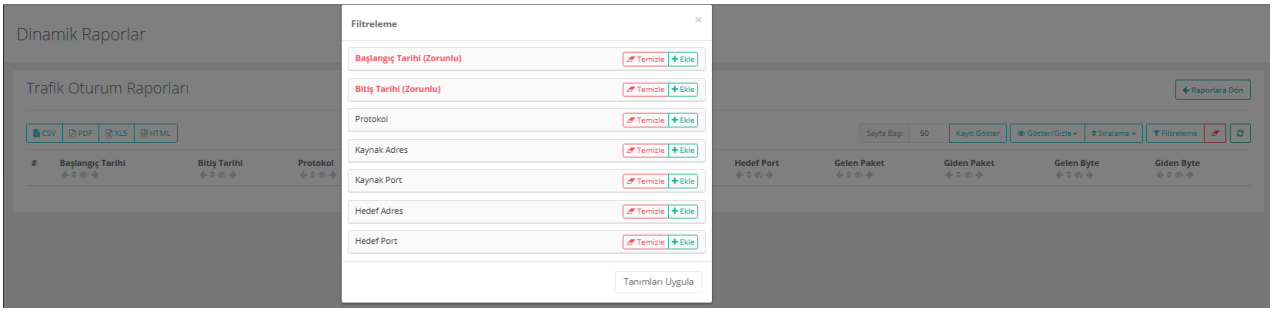
Kullanıcılar için tanımlanmış SSL VPN bağlantılarına ait oturum kayıtları sistem tarafından detaylı şekilde tutulmaktadır. Bu kayıtlar; bağlantı zamanı, kullanıcı bilgileri, IP adresi, bağlantı süresi ve veri trafiği gibi bilgileri içermektedir. Bu sayede hem güvenlik takibi yapılabilir hem de kullanıcı aktiviteleri denetlenebilir.



ALAN	AÇIKLAMA
Bağlantı Tarihi	SSL VPN bağlantısının ne zaman bağlandığını gösterilmektedir.
Kaynak IP Adresi	Hangi IP adresi ile VPN bağlantısı oluşturduğu gösterilmektedir.
Kaynak Port	Hangi port ile bağlantı kurulduğu gösterilmektedir.
CN	Sertifika adı gösterilmektedir.
Vpn IPv4 Adresi	Bağlantı esnasında kullanılan IP adresi gösterilmektedir.
Bağlantı Bitiş Tarihi	SSL VPN bağlantısının ne zaman sonlandığı gösterilmektedir.
Toplam Vpn Süresi	Bağlantı boyunca geçen toplam süre(saniye cinsinden) gösterilmektedir.
Yükleme Boyutu	SSL VPN bağlantısı esnasında ne kadar yükleme yapıldığı gösterilmektedir.
İndirme Boyutu	SSL VPN bağlantısı esnasında ne kadar indirme yapıldığı gösterilmektedir.

Trafik Oturum Logları

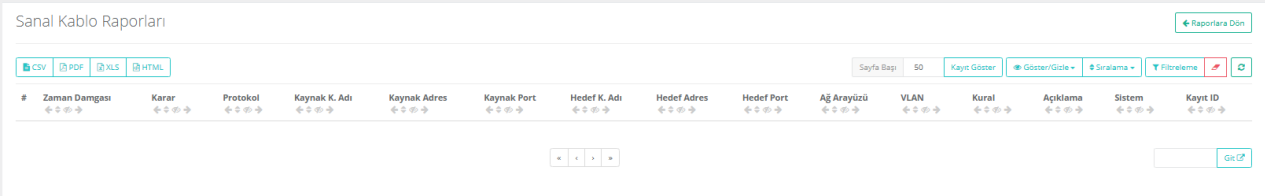
Trafik Oturum Logları, belirli bir zaman aralığında ağ üzerinde gerçekleşen kaynak ve hedef IP'ler arasında kurulan oturumları ve protokol bazlı iletişim bilgilerini incelemek için kullanılan bir rapordur. Bu rapor sayesinde, sistem yöneticileri ağ trafiğini detaylı şekilde analiz edebilir, güvenlik ya da performans açısından olağandışı davranışları tespit edebilir.



Alan	Açıklama
Başlangıç Tarihi	Trafik oturumlarının izlenmeye başlanacağı ilk tarih ve saat bilgisidir (zorunlu olarak girilmelidir).
Bitiş Tarihi	Oturum kayıtlarının alınacağı son tarih ve saat bilgisidir (zorunlu olarak tanımlanmalıdır).
Protokol	İzlenen oturumun gerçekleştiği iletişim protokolüdür (örneğin TCP, UDP, ICMP).
Kaynak Adres	Oturumu başlatan cihazın IP adresidir.
Kaynak Port	Oturumu başlatan cihazın kullandığı port numarasıdır.
Hedef Adres	Oturumun yöneldiği hedef sistemin IP adresidir.
Hedef Port	Hedef cihazda kullanılan servis port numarasıdır.

Sanal Kablo Logları

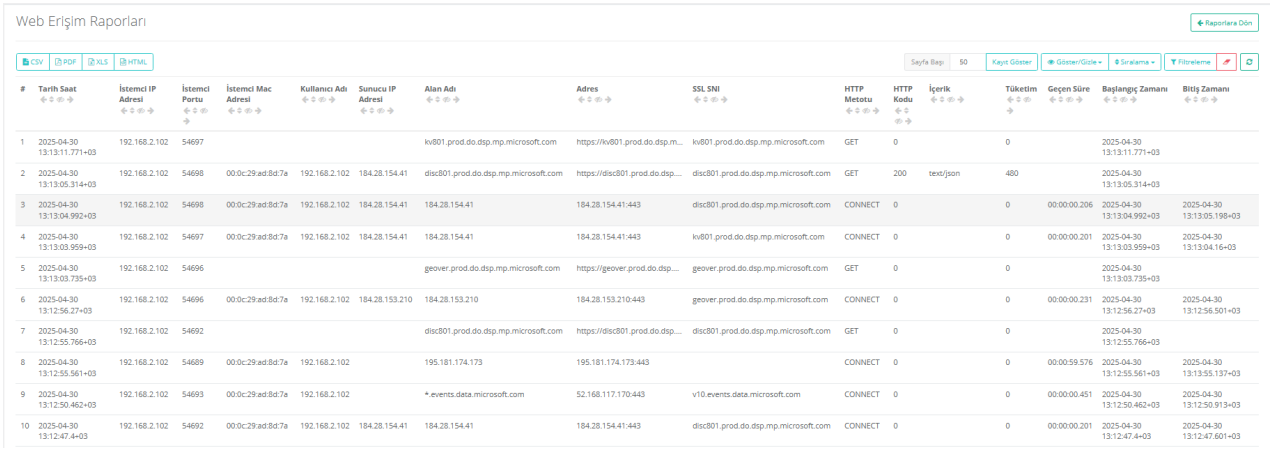
Sanal Kablo Logları sistem üzerinde sanal bağlantı üzerinden geçen ağ trafiğini izleyip, hangi cihazlar ve kullanıcılar arasında nasıl bir iletişim kurulduğunu gösteren ayrıntılı kayıtlardır.



Alan	Açıklama
Zaman Damgası	Sanal kablo olayının veya trafiğinin gerçekleştiği tarih ve saat bilgisidir.
Karar	Trafik için verilen izin (allow) veya engelleme (deny) gibi sistemin uyguladığı karardır.
Protokol	Sanal kablo üzerinden taşınan verinin iletişim protokolüdür (örnek: TCP, UDP).
Kaynak K. Adı	Trafiği başlatan uçta yer alan kullanıcının adıdır.
Kaynak Adres	Bağlantıyı başlatan cihazın IP adresidir.
Kaynak Port	Kaynak cihazın kullandığı port numarasıdır.
Hedef K. Adı	Trafiğin yönlendirildiği uçtaki kullanıcı adıdır.
Hedef Adres	Trafiğin ulaştığı hedef sistemin IP adresidir.
Hedef Port	Hedefteki servisin çalıştığı port numarasıdır.
Ağ Arayüzü	Trafiğin geçtiği fiziksel veya sanal ağ bağlantı noktasıdır.
VLAN	Bağlantının geçtiği sanal yerel ağ (Virtual LAN) kimliğidir.
Kural	Trafiğe uygulanan güvenlik veya yönlendirme politikasının adıdır.
Açıklama	Olay hakkında sistemin oluşturduğu özet veya açıklayıcı bilgidir.
Sistem	Olayı kaydeden veya işleyen güvenlik modülü ya da sistem bileşenidir.
Kayıt ID	Her olay için oluşturulmuş benzersiz tanımlayıcı numaradır.

Web Erişim Logları

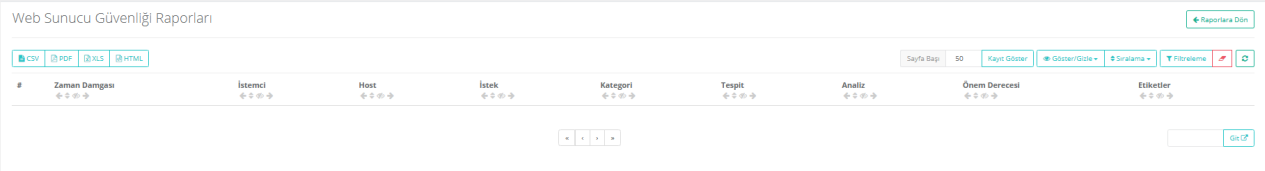
Web erişim Logları, kullanıcıların ağ üzerinden internete yaptıkları web isteklerinin detaylarını kayıt altına alan loglardır. Bu raporlar, kim hangi internet adresine, ne zaman ve ne kadar veri kullanarak erişti sorularını yanıtlamaya yardımcı olur.



Alan	Açıklama
`Tarih Saat`	Web erişiminin gerçekleştiği gün ve saat bilgisidir.
`İstemci IP Adresi`	Web isteğini başlatan cihazın IP adresidir.
`İstemci Portu`	İstemci cihazın web erişimi için kullandığı port numarasıdır.
`İstemci Mac Adresi`	Web erişimini gerçekleştiren cihazın donanımsal MAC adresidir.
`Kullanıcı Adı`	Web erişimini yapan kullanıcı hesabıdır.
`Sunucu IP Adresi`	Erişim sağlanan internet sitesinin IP adresidir.
`Alan Adı`	Bağlantı kurulan web sitesinin alan adı (örnek: google.com) bilgisidir.
`Adres`	Tam erişilen URL ya da web sayfası adresidir.
`SSL SNI`	HTTPS bağlantılarında belirtilen Sunucu Adı Göstergesi (Server Name Indication) bilgisidir.
`HTTP Metotu`	Yapılan web isteğinin türünü gösterir; örneğin GET, POST gibi.
`HTTP Kodu`	Web sunucusunun verdiği yanıt durum kodudur.
`İçerik`	Erişilen web içeriğinin türüdür.
`Tüketim`	Web erişimi sırasında kullanılan toplam veri miktarıdır.
`Geçen Süre`	Web bağlantısının ne kadar süre aktif kaldığını gösterir.
`Başlangıç Zamanı`	Web oturumunun başladığı ilk zaman damgasıdır.
`Bitiş Zamanı`	Web oturumunun bittiği zaman damgasıdır.

Web Sunucu Güvenliği Logları

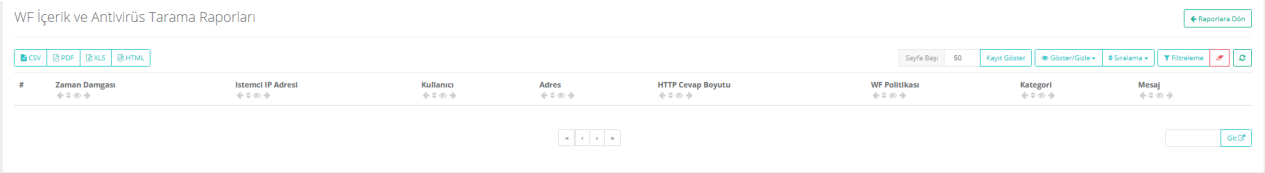
Web Sunucu Güvenliği Logları, kurum içinden veya dışından gelen web isteklerinin sunucu üzerinde oluşturabileceği potansiyel tehditleri ve güvenlik açıklarını analiz eden loglardır.



Alan	Açıklama
Zaman Damgası	Güvenlik olayının veya tehdidin tespit edildiği tarih ve saat bilgisidir.
İstemci	Web sunucusuna istekte bulunan kaynak cihazın IP adresidir.
Host	İsteğin gönderildiği web sunucusunun alan adı veya IP adresidir.
İstek	İstemciden gelen HTTP isteğinin tam URI veya yöntem bilgisidir.
Kategori	Tespit edilen güvenlik olayının sınıflandırıldığı tehdit türüdür.
Tespit	Güvenlik sisteminin algıladığı şüpheli veya zararlı davranış bilgisidir.
Analiz	Olayla ilgili yapılan teknik inceleme ve açıklayıcı yorumlardır.
Önem Derecesi	Tespit edilen tehdidin ciddiyet seviyesini belirtir.
Etiketler	Olayla ilişkilendirilen anahtar kelimeler veya sınıflandırıcı ifadelerdir.

WF WF İçerik ve Antivirüs Tarama Logları

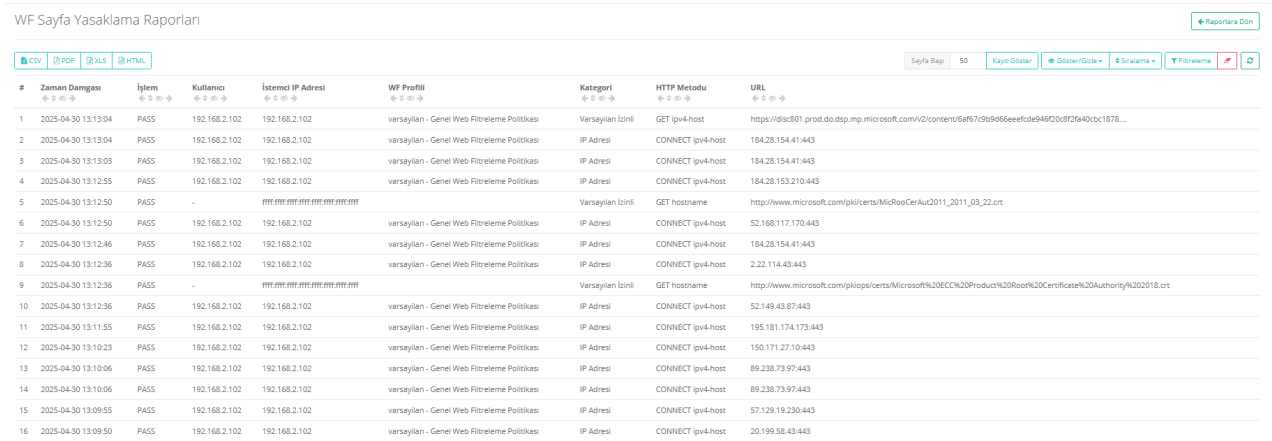
Bu log, Web Filtreleme (WF) ve Antivirüs motoru tarafından taranan içeriklerin kayıtlarını içerir; kullanıcıların erişmeye çalıştığı adreslerde zararlı içerik, uygunsuz kategori ya da politika ihlali olup olmadığını analiz eder.



Alan	Açıklama
Zaman Damgası	Tarama olayının gerçekleştiği tarih ve saat bilgisidir.
İstemci IP Adresi	Web erişimini yapan istemci cihazın IP adresidir.
Kullanıcı	İçeriğe erişim girişiminde bulunan kullanıcı hesabıdır.
Adres	Tarama yapılan web adresi ya da dosya URL'sidir.
HTTP Cevap Boyutu	Web sunucusundan gelen içeriğin boyutudur.
WF Politikası	Uygulanan Web Filtreleme kural veya politikasıdır.
Kategori	Erişilen içeriğin WF sistemi tarafından sınıflandırıldığı içerik türüdür.
Mesaj	Tarama sonucunda oluşan bilgilendirici veya uyarı mesajıdır.

WF Sayfa Yasaklama Logları

WF (Web Filtreleme) Sayfa Yasaklama Logları, kullanıcıların erişmeye çalıştığı ancak filtre politikaları nedeniyle engellenen web sayfalarını kaydeder. Bu rapor, yasaklanan içeriklerin ne zaman, kim tarafından ve hangi kategoriye göre engellendiğini göstererek içerik denetimi ve kullanıcı kontrolü sağlar.



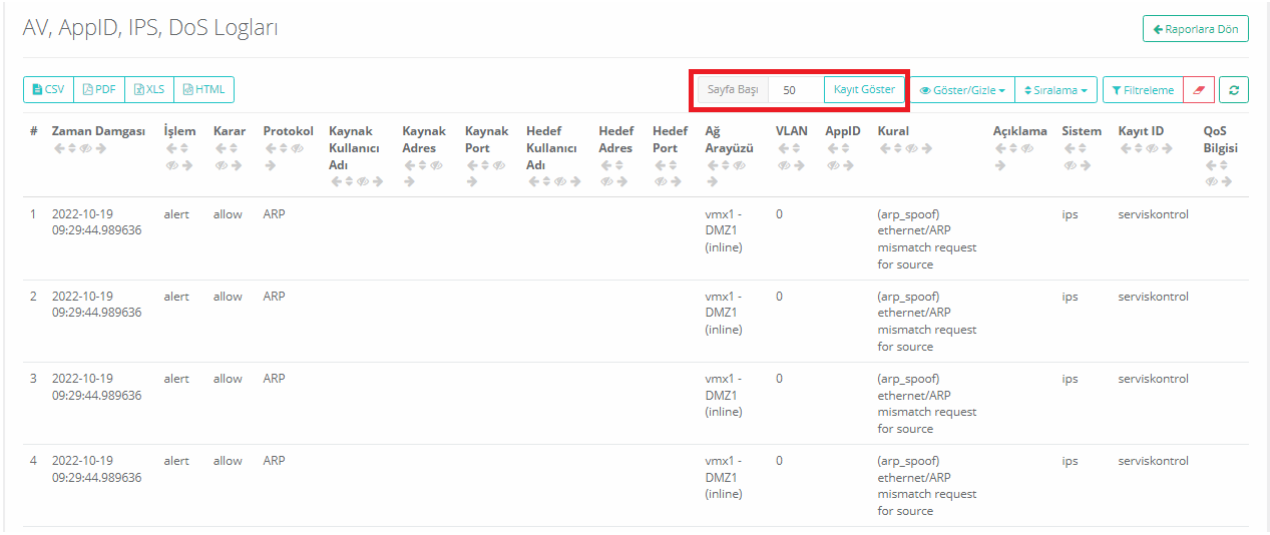
Alan	Açıklama
`Zaman Damgası`	Erişim engelleme olayının gerçekleştiği tarih ve saat bilgisidir.
`İşlem`	Sistem tarafından uygulanan işlemdir.
`Kullanıcı`	Engellenen web sayfasına erişmek isteyen kullanıcı hesabıdır.
`İstemci IP Adresi`	Erişim isteğinde bulunan cihazın IP adresidir.
`WF Profili`	O kullanıcıya uygulanan web filtreleme profilidir.
`Kategori`	Engellenen sayfanın içerik türüdür.
`HTTP Metodu`	Kullanıcının yaptığı web isteğinin HTTP türüdür (örnek: GET, POST).
`URL`	Erişilmek istenen tam web adresidir.

Yasaklanan Kullanıcılar Logları

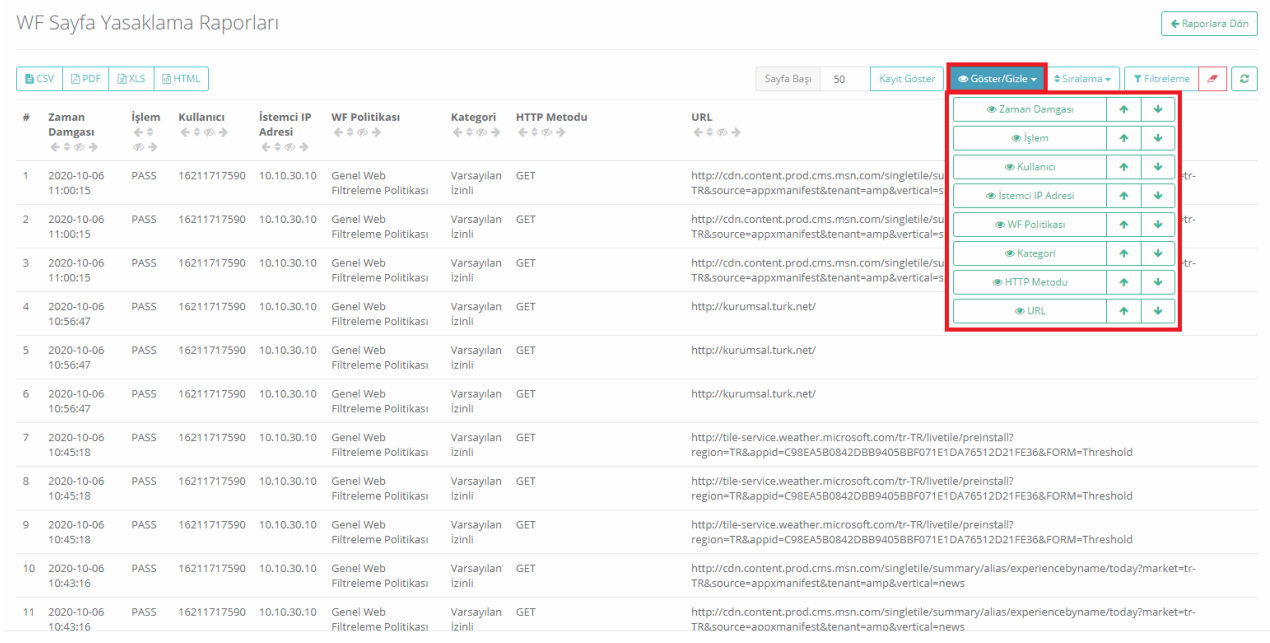
Alan	Açıklama
`Zaman Damgası`	Kullanıcının yaptığı işlemin sistem tarafından tutulan tarih ve saat bilgisidir.
`İşlem`	Uygulanan güvenlik politikası sonucunda gerçekleşen bilgilendirme işlemidir.
`Açıklama`	Kullanıcının yaptığı işlemlere ait bilgilendirici kısa nottur.
`Kullanıcı Adı`	Yasaklama işlemine tabi tutulan kullanıcı hesabıdır.
`IP Adresi`	Yasaklanan kullanıcıya ait istemci cihazın IP adresidir.

Rapor Özellikleri

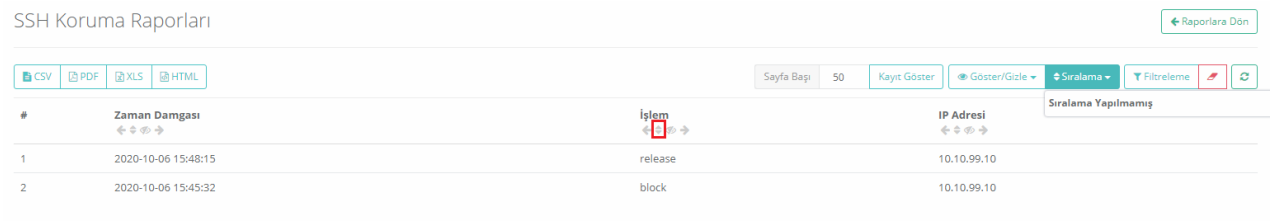
Her sayfada kaç kayıt gösterileceği `Sayfa Başından` sonra değer girilip, kayıt göster butonuna basıldığında; sayfa başı kullanıcının girdiği değer kadar veri gösterilir. (Varsayılan 50 olarak gelmektedir.)

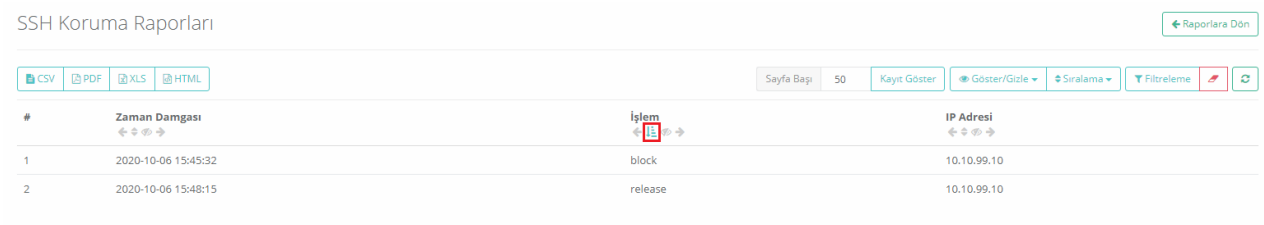


Göster/Gizle butonu ile sütunlar gizlenip, gizlenen sütunlar tekrar gösterilebilmektedir. Yukarı aşağı ok butonları ile aynı zamanda sütunların yeri de değiştirilebilmektedir.

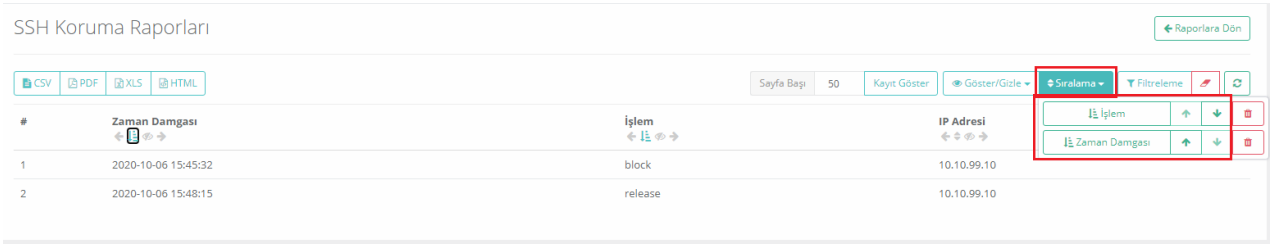


Aşağıdaki ekran görüntüsünde sırala simgesine tıkladığımızda sütundaki değerlere göre tüm tablo sıralanmış olacaktır.

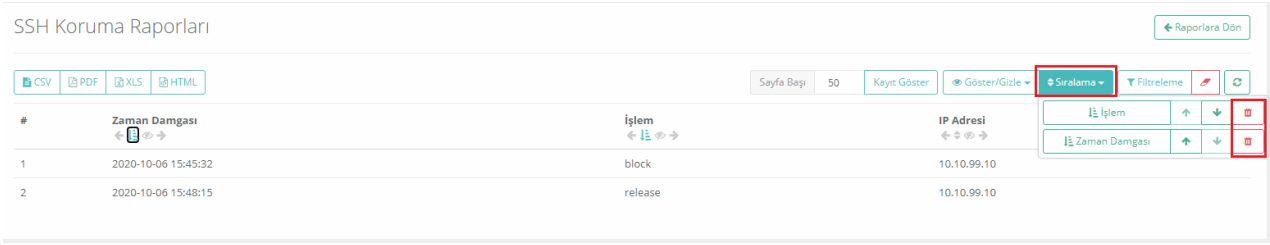




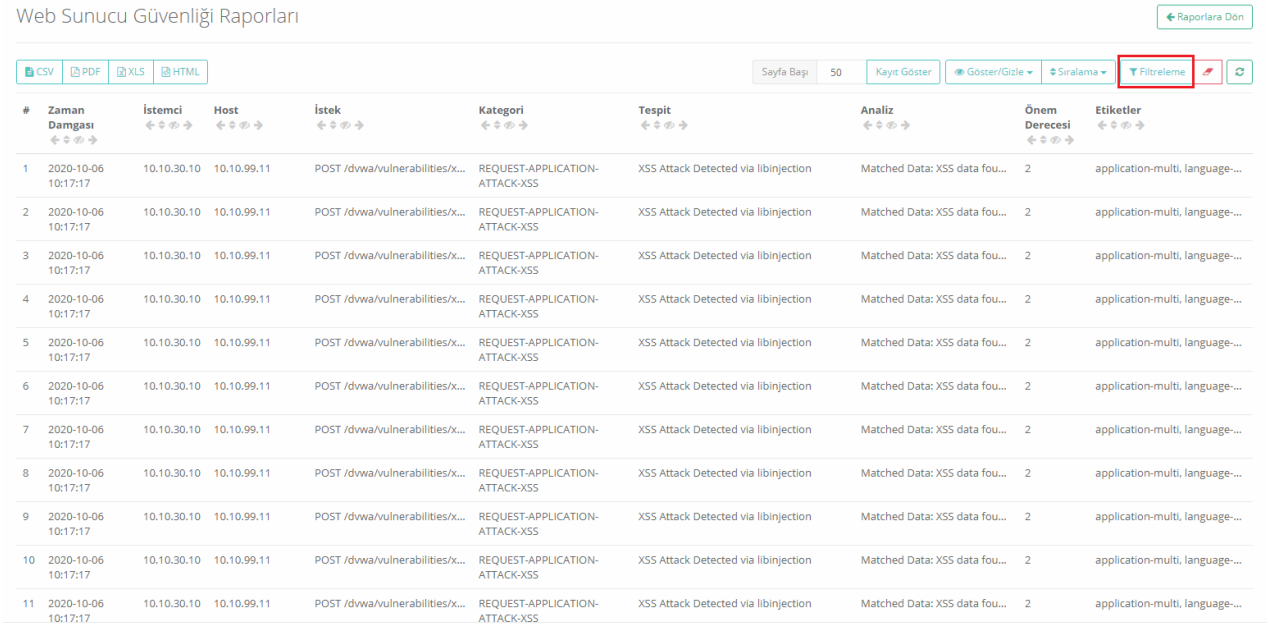
Sıralamada bulunan yukarı aşağı ok butonları ile sütun sıralama önceliğini değiştirebilirsiniz.

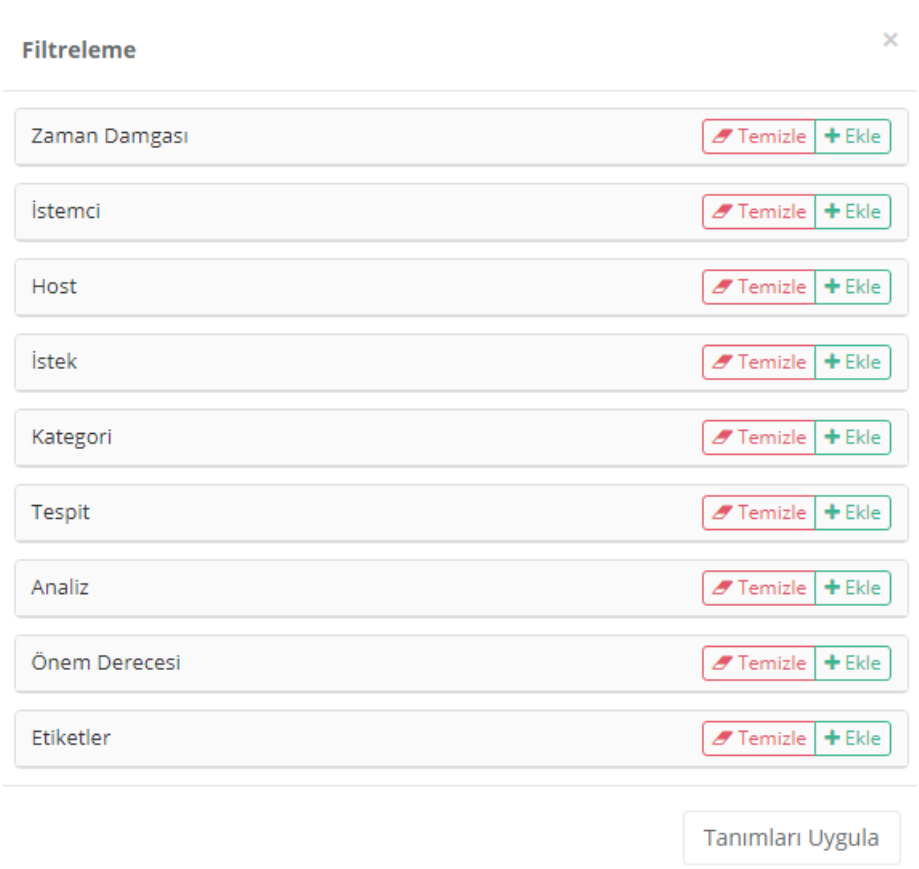


Sıralamada bulunan çöp simgesine sahip butonlar ile sütuna ait sıralama filtresini kaldırabilirsiniz.

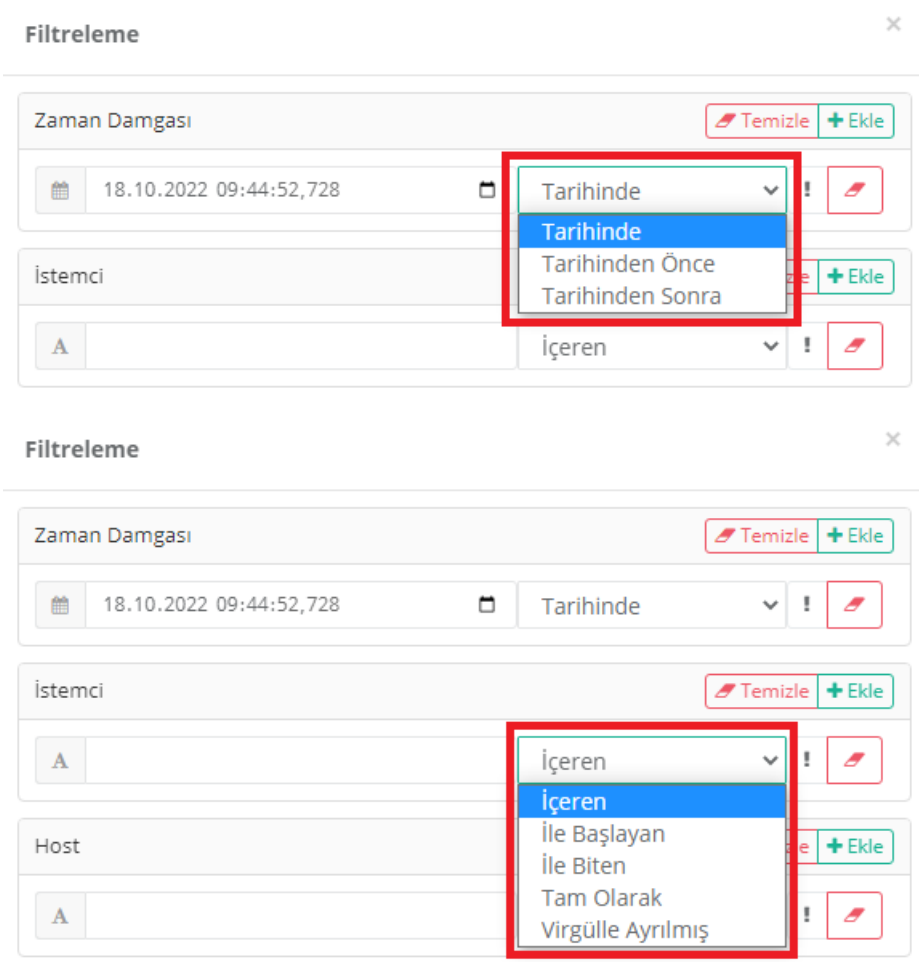


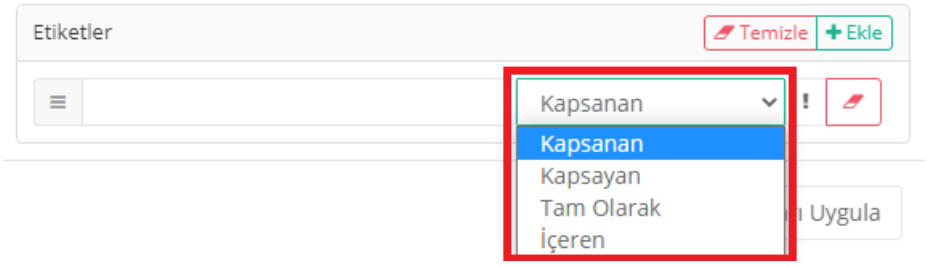
Filtreleme butonu ile tabloda bulunan verileri belirlenen kriterlere göre filtreleyebilirsiniz.



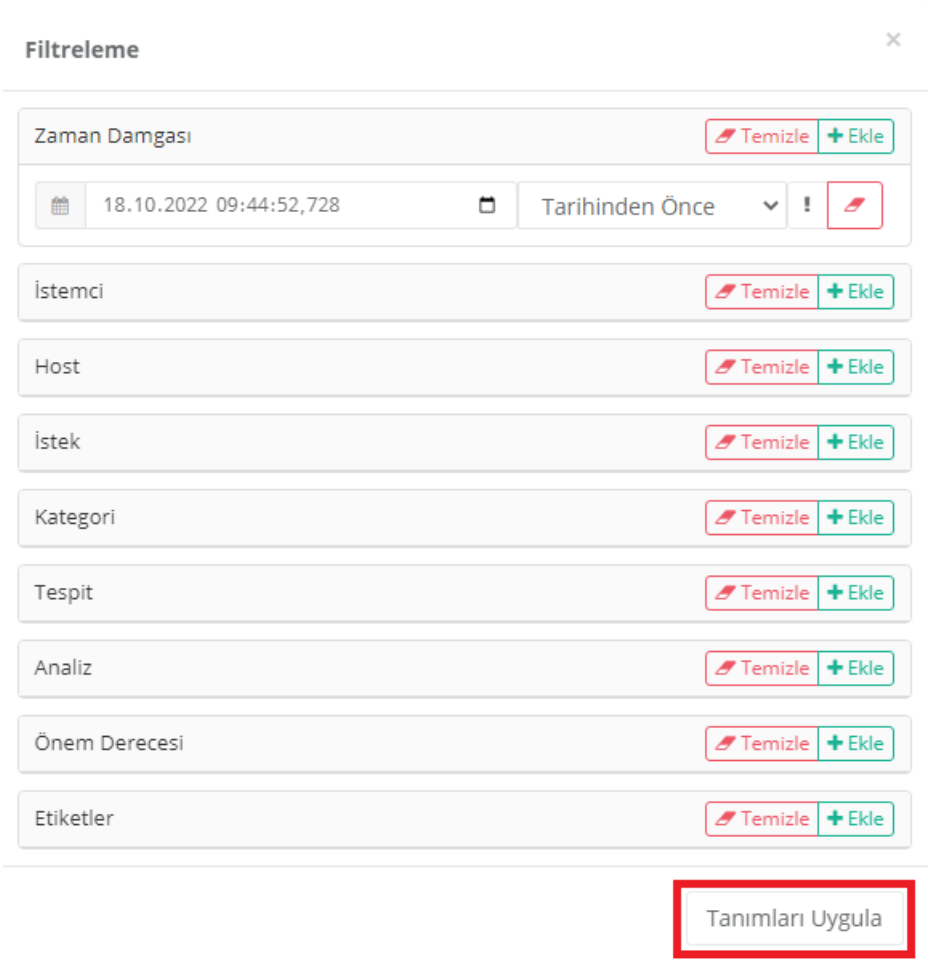


Kriterleri girerken yanında bulunan açılır listeye göre filtreleyeceğinden, azami dikkat etmeniz gerekmektedir.

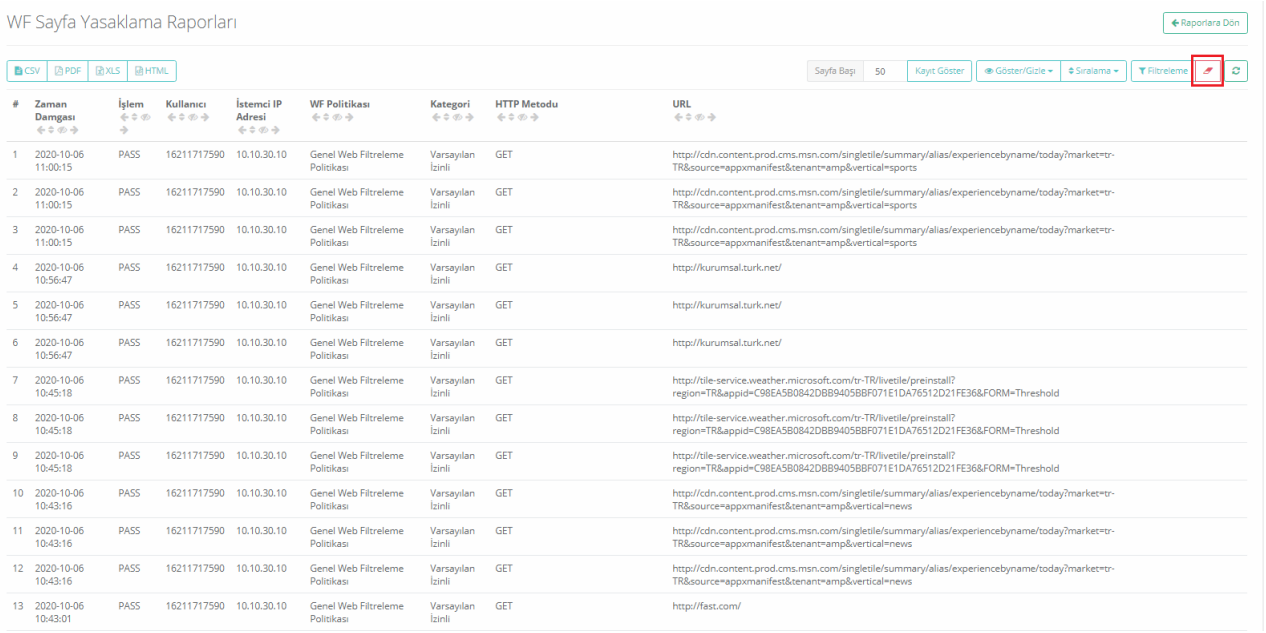




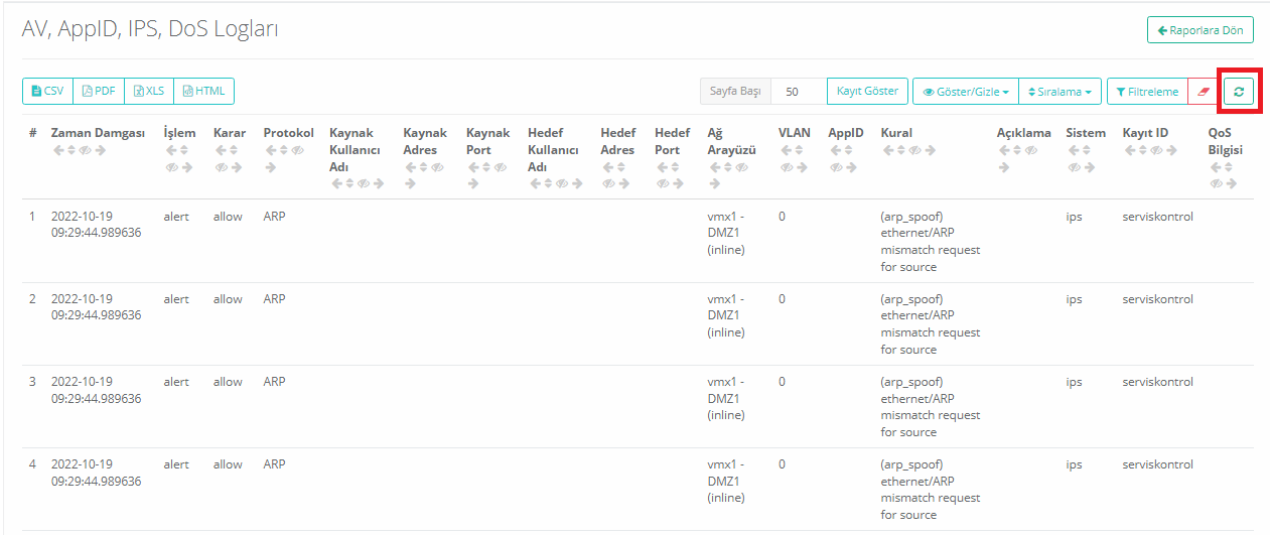
Tablo için gereken filtreler girildikten sonra `Tanımları Uygula` butonuna basılmalıdır.



Tablo için yapılan filtrelemeleri kaldırmak için silgi simgesi olan butona tıklamanız yeterli olacaktır.

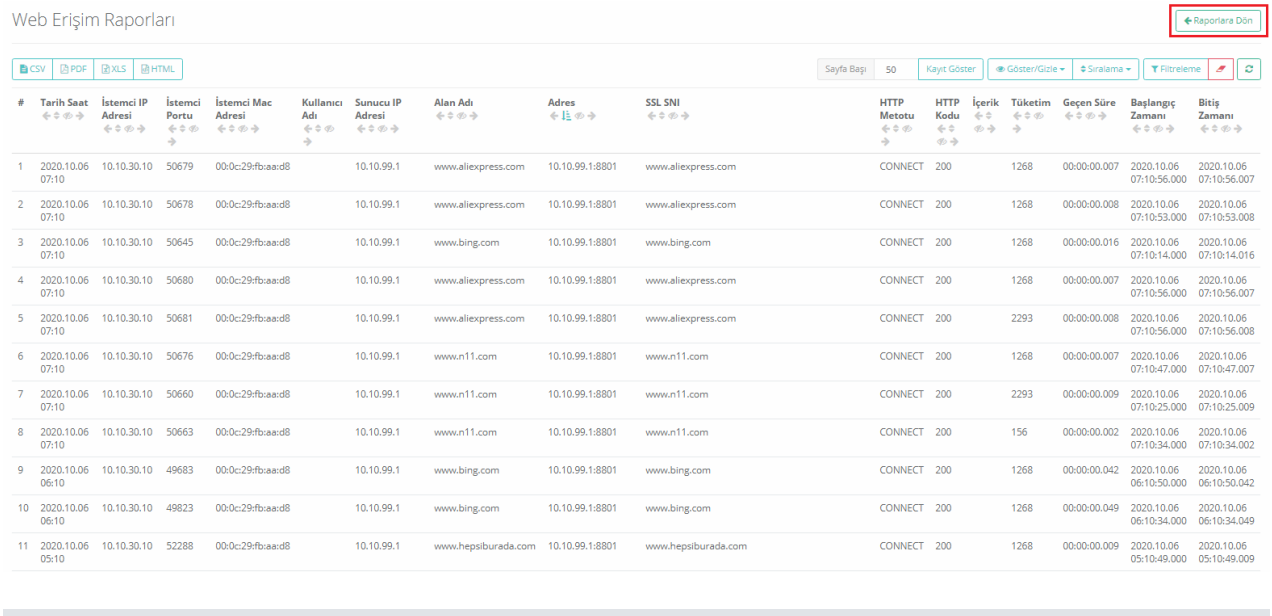


Tabloya yeni gelen değerleri görmek için yenile butonuna butonuna basılmalıdır.



#	Zaman Damgası	İşlem	Karar	Protokol	Kaynak Kullanıcı Adı	Kaynak Adres	Kaynak Port	Hedef Kullanıcı Adı	Hedef Adres	Hedef Port	Ağ Arayüzü	VLAN	AppID	Kural	Açıklama	Sistem	Kayıt ID	QoS Bilgisi
1	2022-10-19 09:29:44.989636	alert	allow	ARP							vmx1 - DMZ1 (inline)	0		(arp_spoof) ethernet/ARP mismatch request for source		ips	serviskontrol	
2	2022-10-19 09:29:44.989636	alert	allow	ARP							vmx1 - DMZ1 (inline)	0		(arp_spoof) ethernet/ARP mismatch request for source		ips	serviskontrol	
3	2022-10-19 09:29:44.989636	alert	allow	ARP							vmx1 - DMZ1 (inline)	0		(arp_spoof) ethernet/ARP mismatch request for source		ips	serviskontrol	
4	2022-10-19 09:29:44.989636	alert	allow	ARP							vmx1 - DMZ1 (inline)	0		(arp_spoof) ethernet/ARP mismatch request for source		ips	serviskontrol	

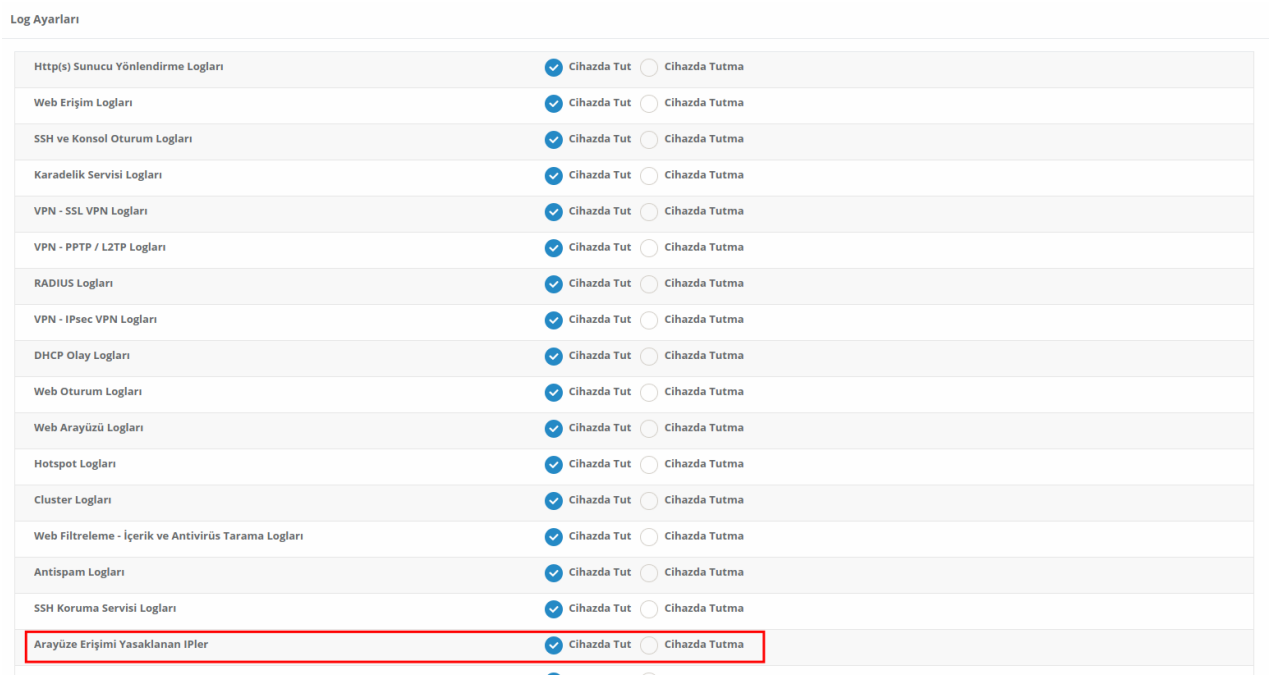
Raporlara Dön butonu ile dinamik raporlar menüsüne geri dönebilir, başka raporlara göz atabilirsiniz.



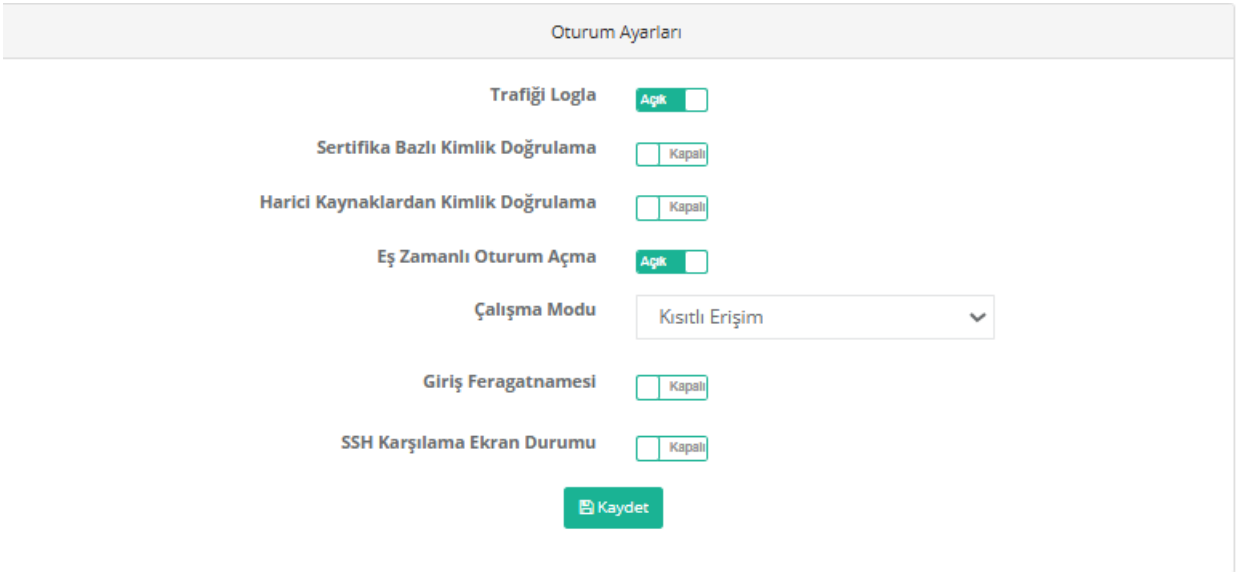
#	Tarih Saat	İstemci IP Adresi	İstemci Portu	İstemci Mac Adresi	Kullanıcı Adı	Sunucu IP Adresi	Alan Adı	Adres	SSL SNI	HTTP Metotu	HTTP Kodu	İçerik	Tüketim	Geçen Süre	Başlangıç Zamanı	Bitiş Zamanı
1	2020.10.06 07:10	10.10.30.10	50679	00:0c:29:fb:aa:d8		10.10.99.1	www.aliexpress.com	10.10.99.1:8801	www.aliexpress.com	CONNECT	200		1268	00:00:00.007	2020.10.06 07:10:56.000	2020.10.06 07:10:56.007
2	2020.10.06 07:10	10.10.30.10	50678	00:0c:29:fb:aa:d8		10.10.99.1	www.aliexpress.com	10.10.99.1:8801	www.aliexpress.com	CONNECT	200		1268	00:00:00.008	2020.10.06 07:10:53.000	2020.10.06 07:10:53.008
3	2020.10.06 07:10	10.10.30.10	50645	00:0c:29:fb:aa:d8		10.10.99.1	www.bing.com	10.10.99.1:8801	www.bing.com	CONNECT	200		1268	00:00:00.016	2020.10.06 07:10:14.000	2020.10.06 07:10:14.016
4	2020.10.06 07:10	10.10.30.10	50680	00:0c:29:fb:aa:d8		10.10.99.1	www.aliexpress.com	10.10.99.1:8801	www.aliexpress.com	CONNECT	200		1268	00:00:00.007	2020.10.06 07:10:56.000	2020.10.06 07:10:56.007
5	2020.10.06 07:10	10.10.30.10	50681	00:0c:29:fb:aa:d8		10.10.99.1	www.aliexpress.com	10.10.99.1:8801	www.aliexpress.com	CONNECT	200		2293	00:00:00.008	2020.10.06 07:10:56.000	2020.10.06 07:10:56.008
6	2020.10.06 07:10	10.10.30.10	50676	00:0c:29:fb:aa:d8		10.10.99.1	www.n11.com	10.10.99.1:8801	www.n11.com	CONNECT	200		1268	00:00:00.007	2020.10.06 07:10:47.000	2020.10.06 07:10:47.007
7	2020.10.06 07:10	10.10.30.10	50660	00:0c:29:fb:aa:d8		10.10.99.1	www.n11.com	10.10.99.1:8801	www.n11.com	CONNECT	200		2293	00:00:00.009	2020.10.06 07:10:25.000	2020.10.06 07:10:25.009
8	2020.10.06 07:10	10.10.30.10	50663	00:0c:29:fb:aa:d8		10.10.99.1	www.n11.com	10.10.99.1:8801	www.n11.com	CONNECT	200		156	00:00:00.002	2020.10.06 07:10:34.000	2020.10.06 07:10:34.002
9	2020.10.06 06:10	10.10.30.10	49683	00:0c:29:fb:aa:d8		10.10.99.1	www.bing.com	10.10.99.1:8801	www.bing.com	CONNECT	200		1268	00:00:00.042	2020.10.06 06:10:50.000	2020.10.06 06:10:50.042
10	2020.10.06 06:10	10.10.30.10	49823	00:0c:29:fb:aa:d8		10.10.99.1	www.bing.com	10.10.99.1:8801	www.bing.com	CONNECT	200		1268	00:00:00.049	2020.10.06 06:10:34.000	2020.10.06 06:10:34.049
11	2020.10.06 05:10	10.10.30.10	52288	00:0c:29:fb:aa:d8		10.10.99.1	www.hepsiburada.com	10.10.99.1:8801	www.hepsiburada.com	CONNECT	200		1268	00:00:00.009	2020.10.06 05:10:49.000	2020.10.06 05:10:49.009

`Not:` Yasaklanan Kullanıcılar Loglarına düşmesi için;

- `Log Ayarları`nda Arayüze Erişimi Yasaklanan IPler Log çeşidinin `Cihazda Tut` seçili olması gerekir.



- Erişim / Oturum Ayarları'nda Trafiği Logla seçeneğinin aktifleştirilmesi gerekir.



- Bu ayarların yapılmadığı durumda ürün Common Criteria EAL4+ sertifika kapsamından çıkmaktadır.