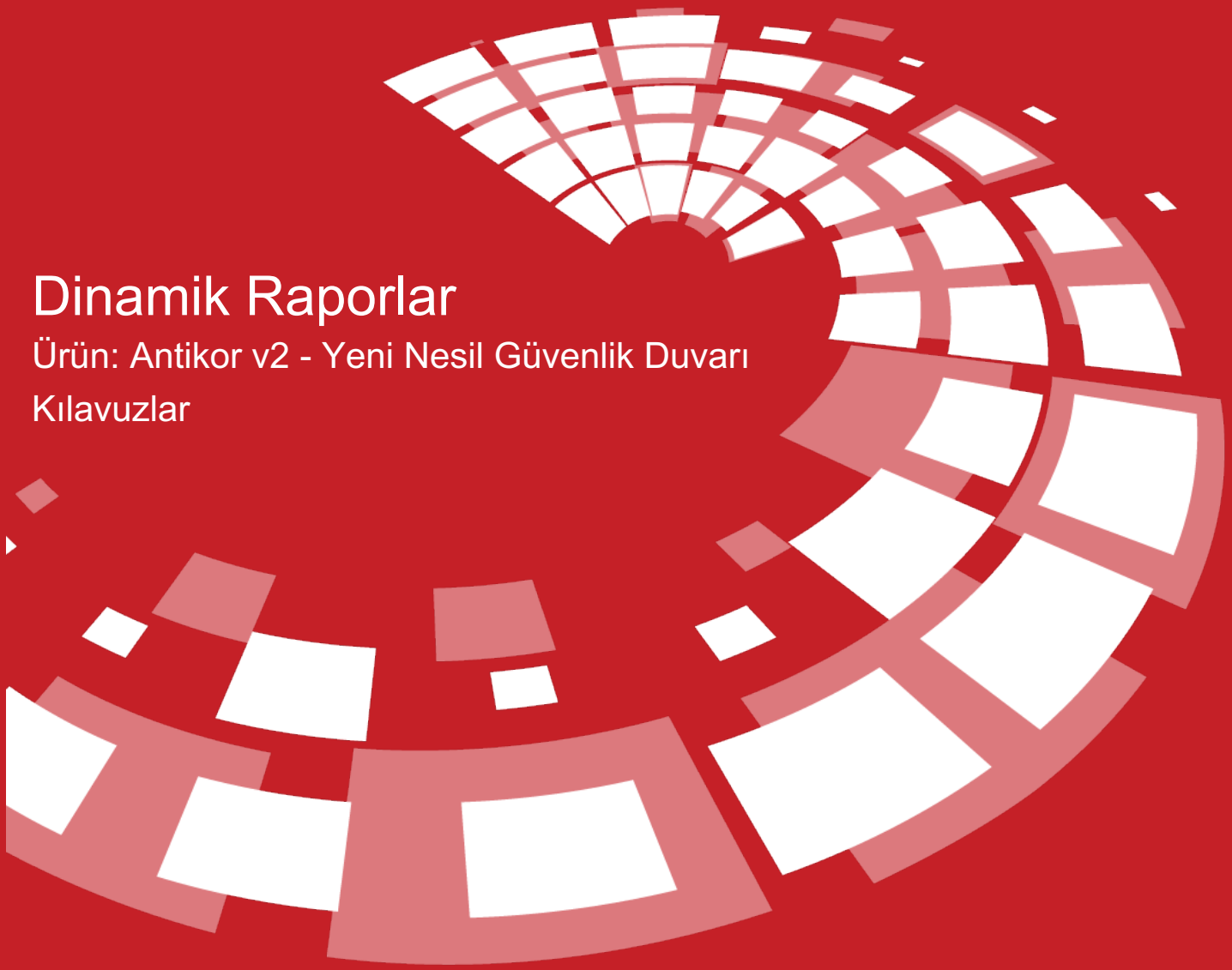
epati

Dinamik Raporlar

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı

Kılavuzlar



www.epati.com.tr

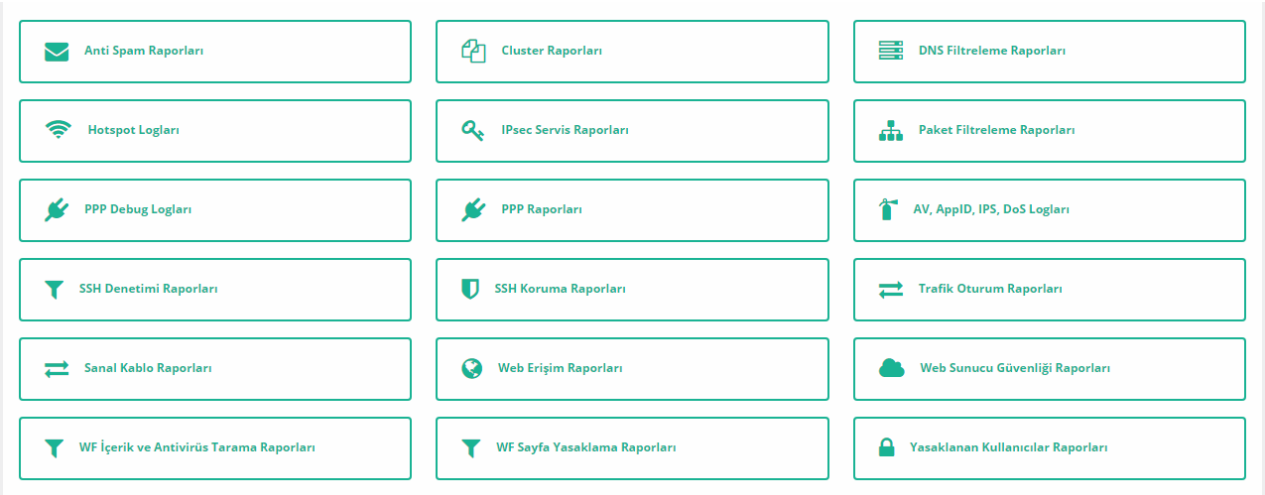
epati

antikor v2
Tümleşik Siber Güvenlik Sistemi

Dinamik Raporlar

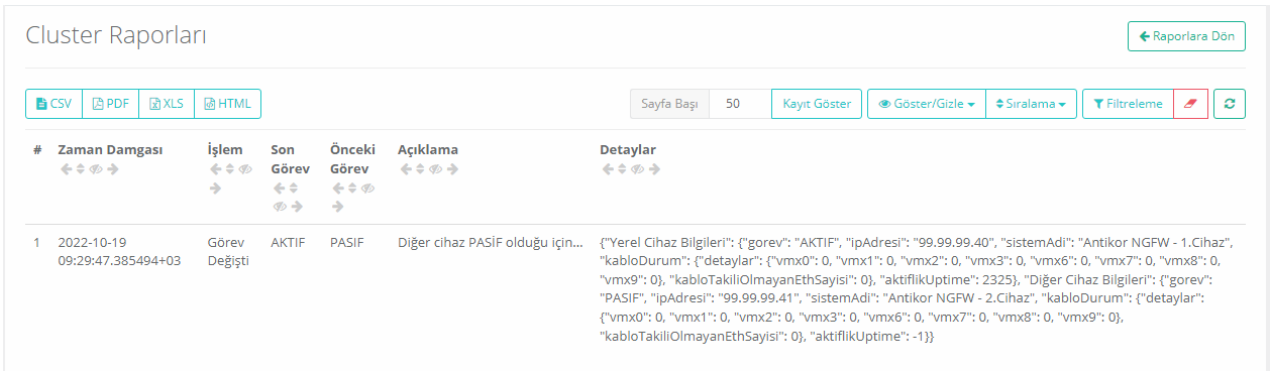
18 farklı rapor çeşidi dinamik olarak buradan görüntülenmekte ve listelenmektedir.

- Anti Spam Raporları
- Cluster Raporları
- DNS Filtreleme Raporları
- Hotspot Logları
- IPsec Servis Raporları
- Paket Filtreleme Raporları
- PPP Debug Logları
- PPP Raporları
- AV, AppID, IPS, DoS Logları
- SSH Denetimi Raporları
- SSH Koruma Raporları
- Trafik Oturum Raporları
- Sanal Kablo Raporları
- Web Erişim Raporları
- Web Sunucu Güvenliği Raporları
- WF (Web Filtreleme) İçerik ve Antivirüs Tarama Raporları
- WF (Web Filtreleme) Sayfa Yasaklama Raporları
- Yasaklanan Kullanıcılar Raporları

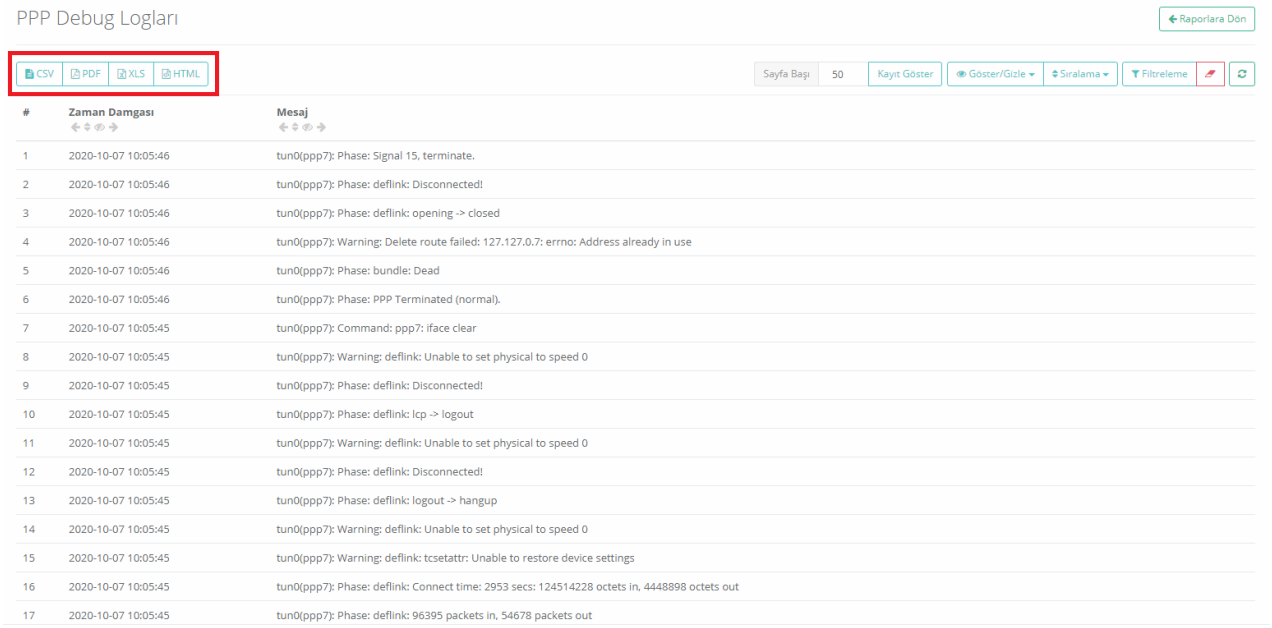


Cluster Raporları

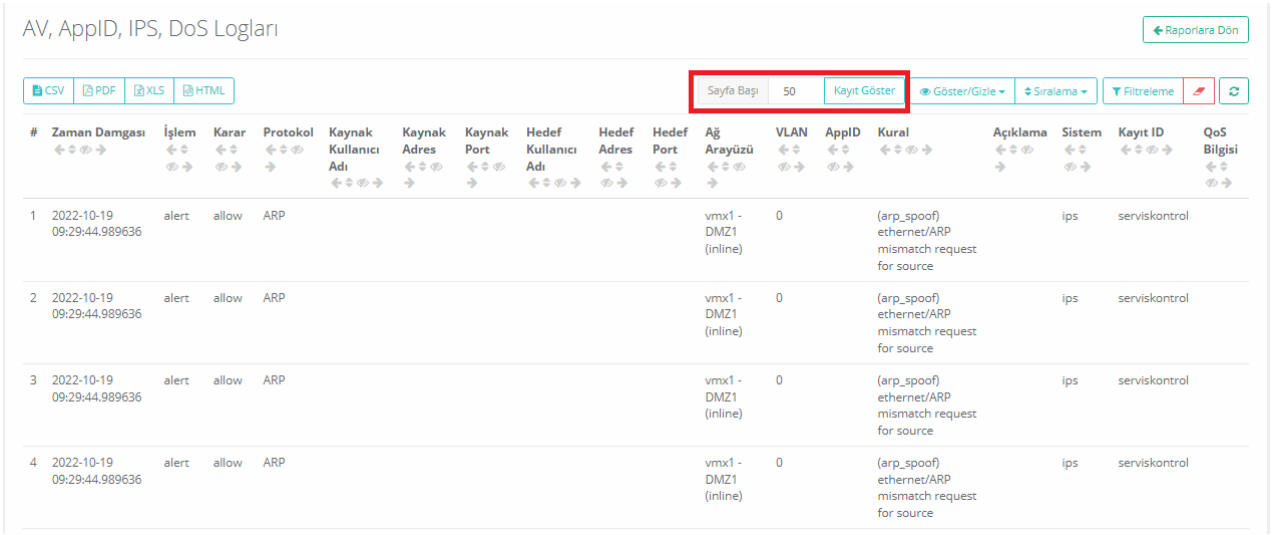
Cluster ile ilgili oluşan durumları ve durumların gerçekleştiği arayüzleri tarihe göre raporlamaktadır.



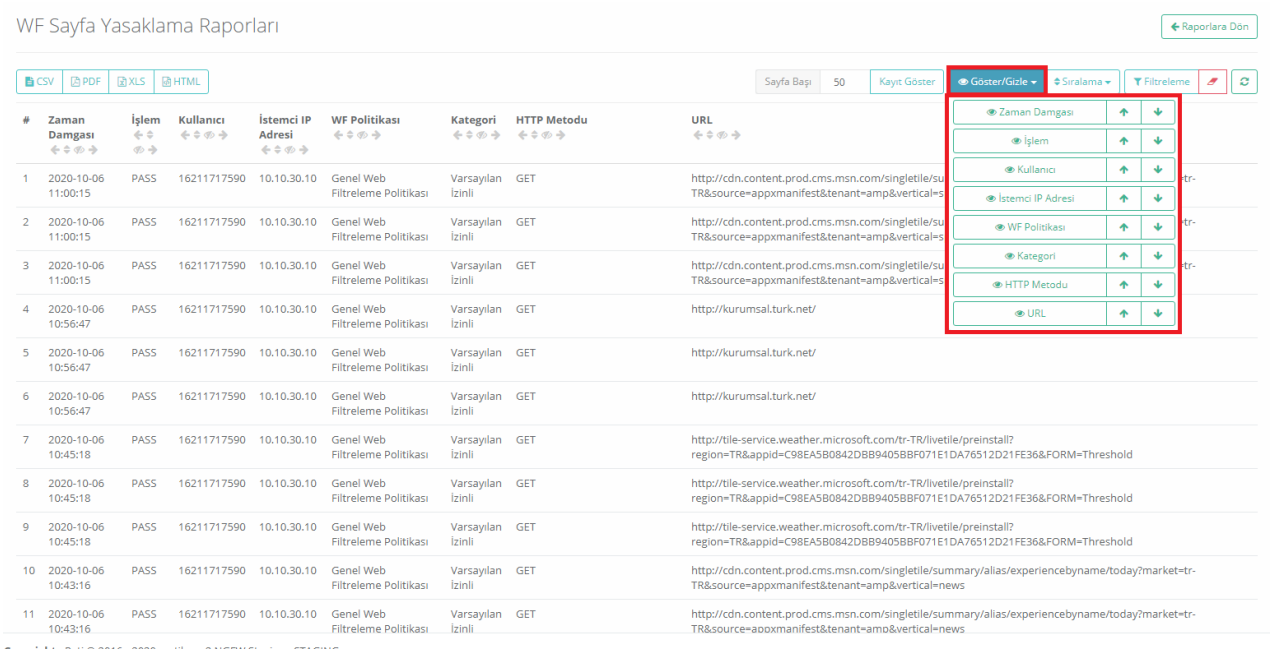
Kullanıcılar bu raporları `csv, pdf, xls ve html` formatlarında indirebilmektedir.



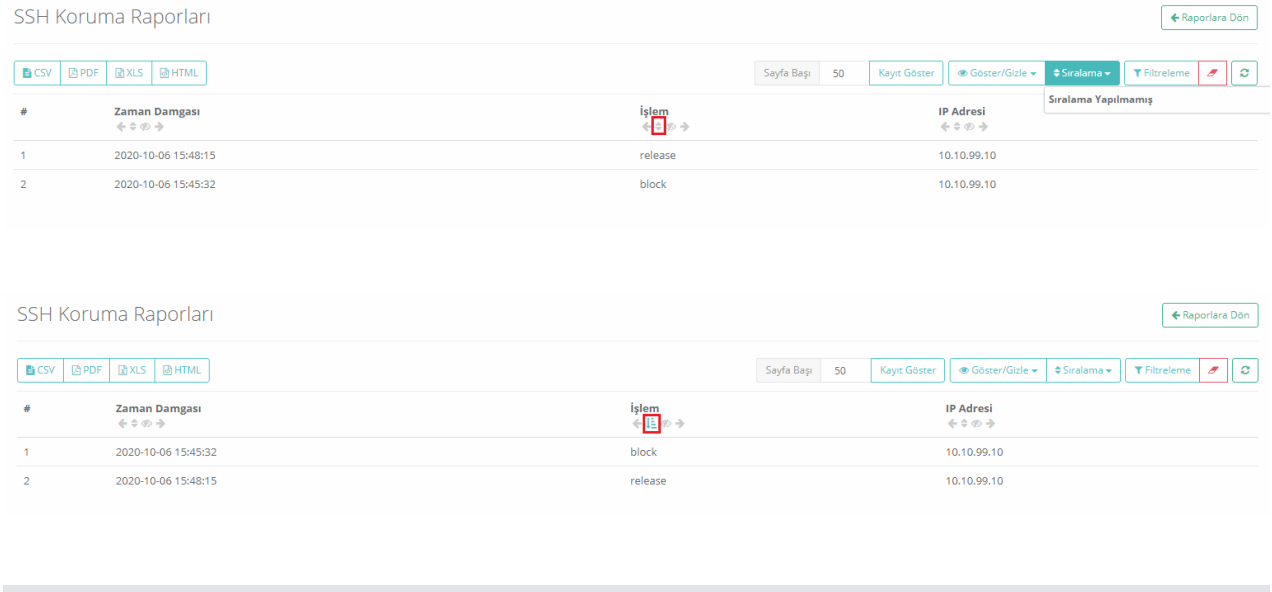
Her sayfada kaç kayıt gösterileceği `Sayfa Başından` sonra değer girilip, kayıt göster butonuna basıldığında; sayfa başı kullanıcının girdiği değer kadar veri gösterilir. (Varsayılan 50 olarak gelmektedir.)



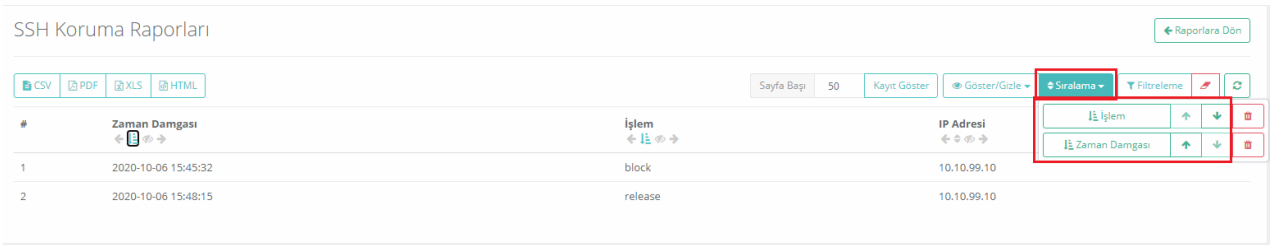
Göster/Gizle butonu ile sütunlar gizlenip, gizlenen sütunlar tekrar gösterilebilmektedir. Yukarı aşağı ok butonları ile aynı zamanda sütunların yeri de değiştirilebilmektedir.



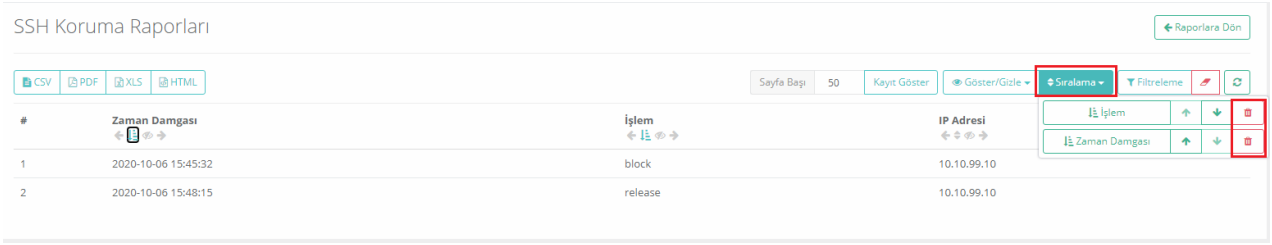
Aşağıdaki ekran görüntüsünde sırala simgesine tıkladığımızda sütundaki değerlere göre tüm tablo sıralanmış olacaktır.



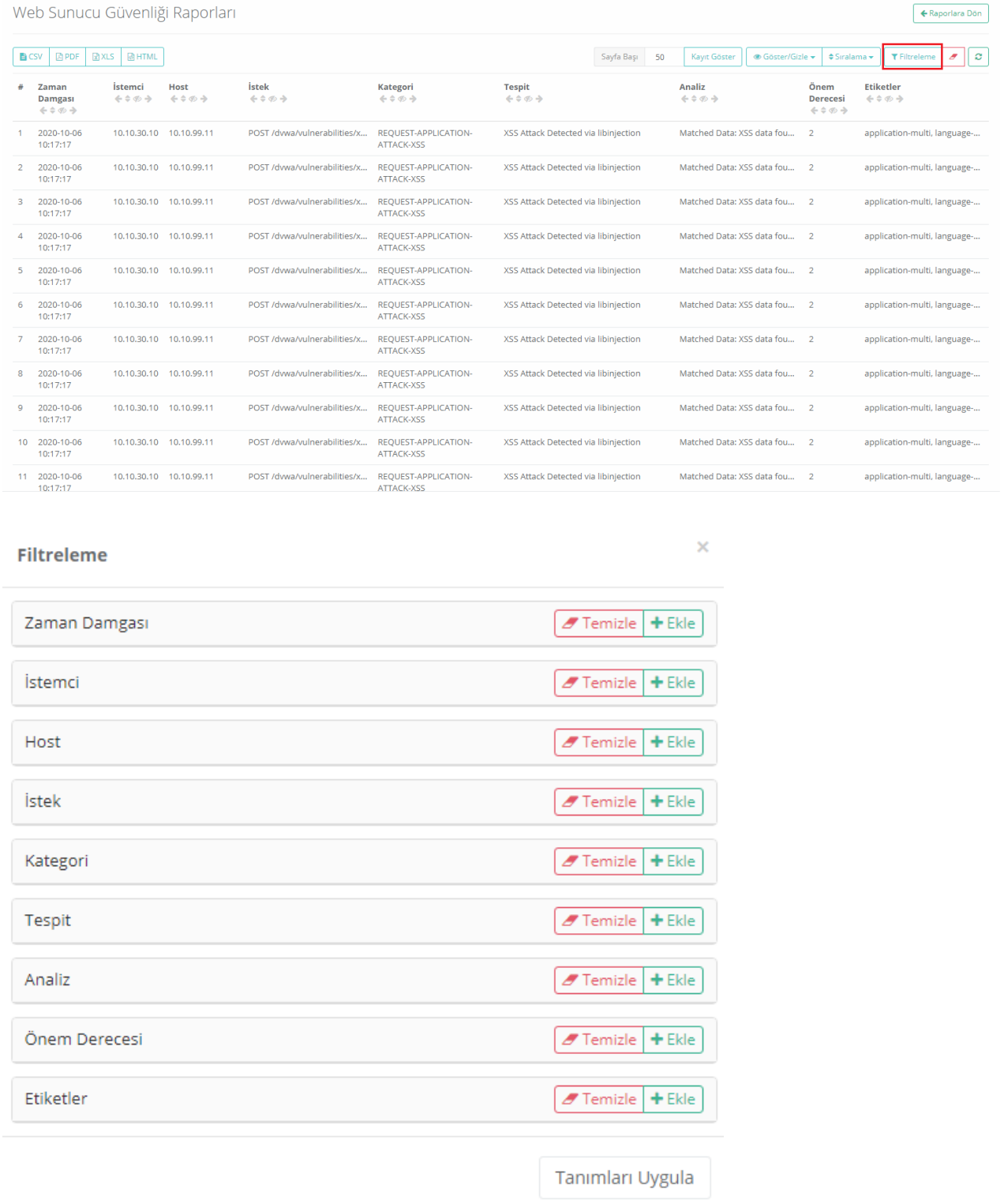
Sıralamada bulunan yukarı aşağı ok butonları ile sütun sıralama önceliğini değiştirebilirsiniz.



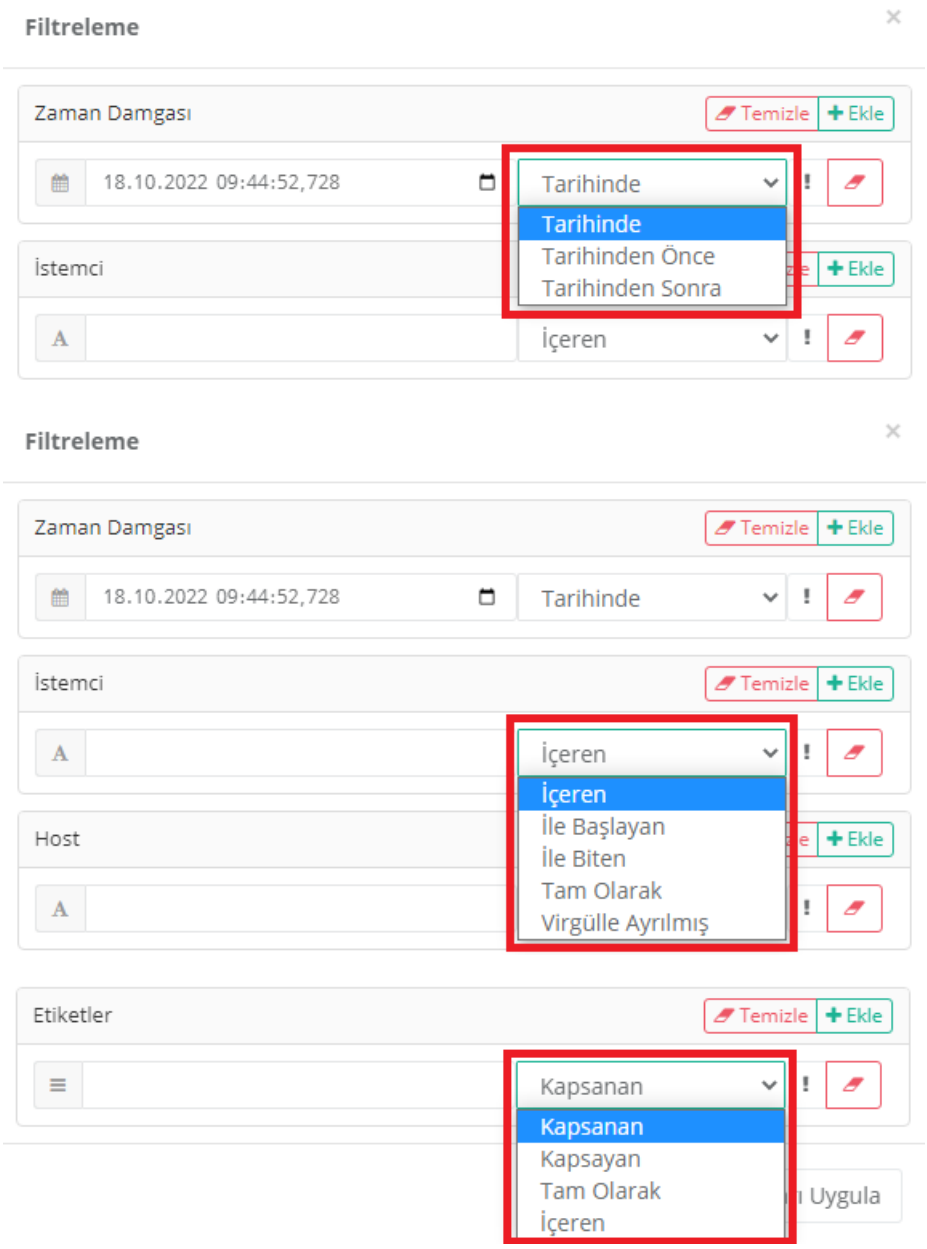
Sıralamada bulunan çöp simgesine sahip butonlar ile sütuna ait sıralama filtresini kaldırabilirsiniz.



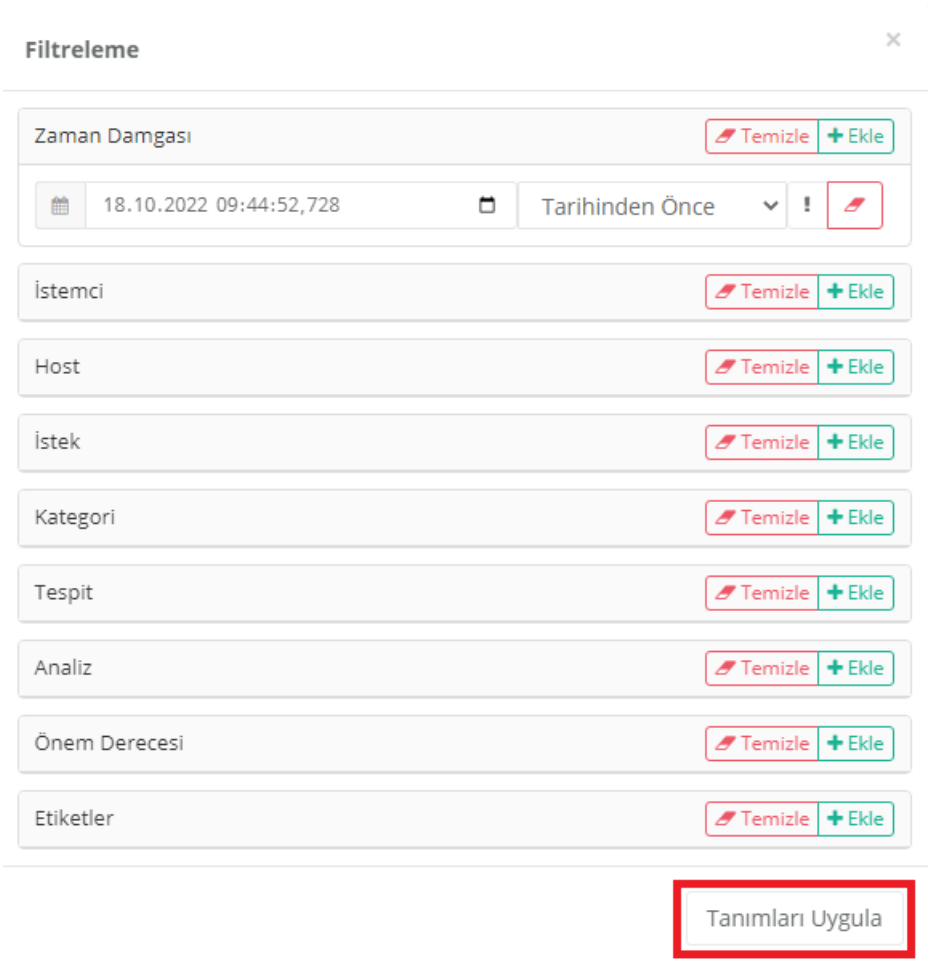
Filtreleme butonu ile tabloda bulunan verileri belirlenen kriterlere göre filtreleyebilirsiniz.



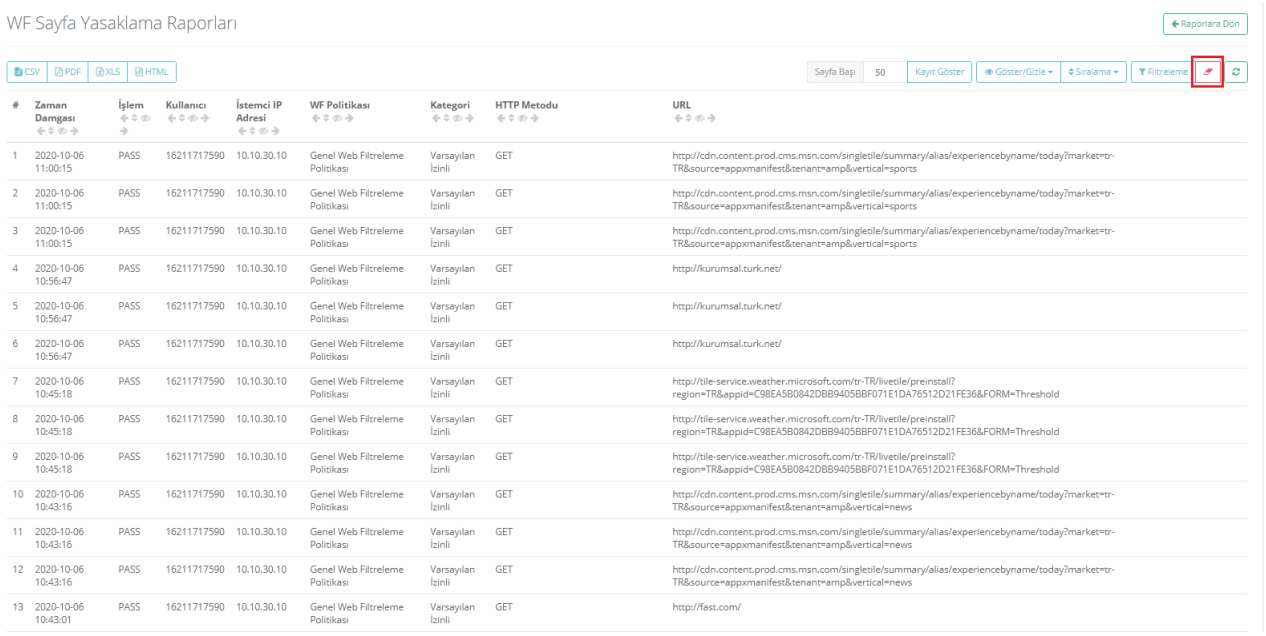
Kriterleri girerken yanında bulunan açılır listeye göre filtreleyeceğinden, azami dikkat etmeniz gerekmektedir.



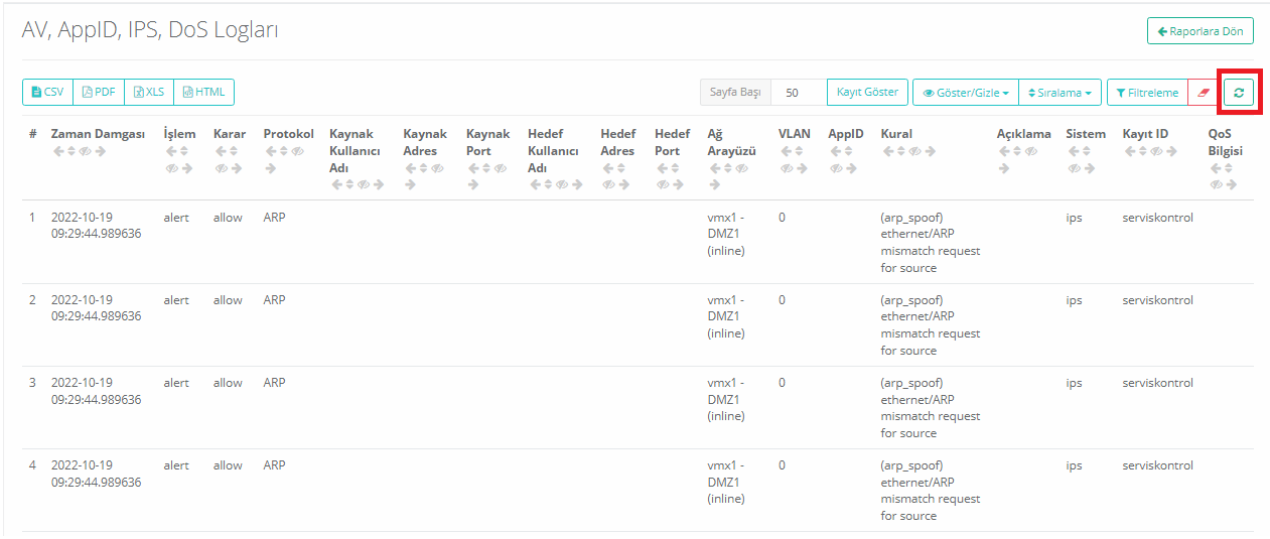
Tablo için gereken filtreler girildikten sonra `Tanımları Uygula` butonuna basılmalıdır.



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

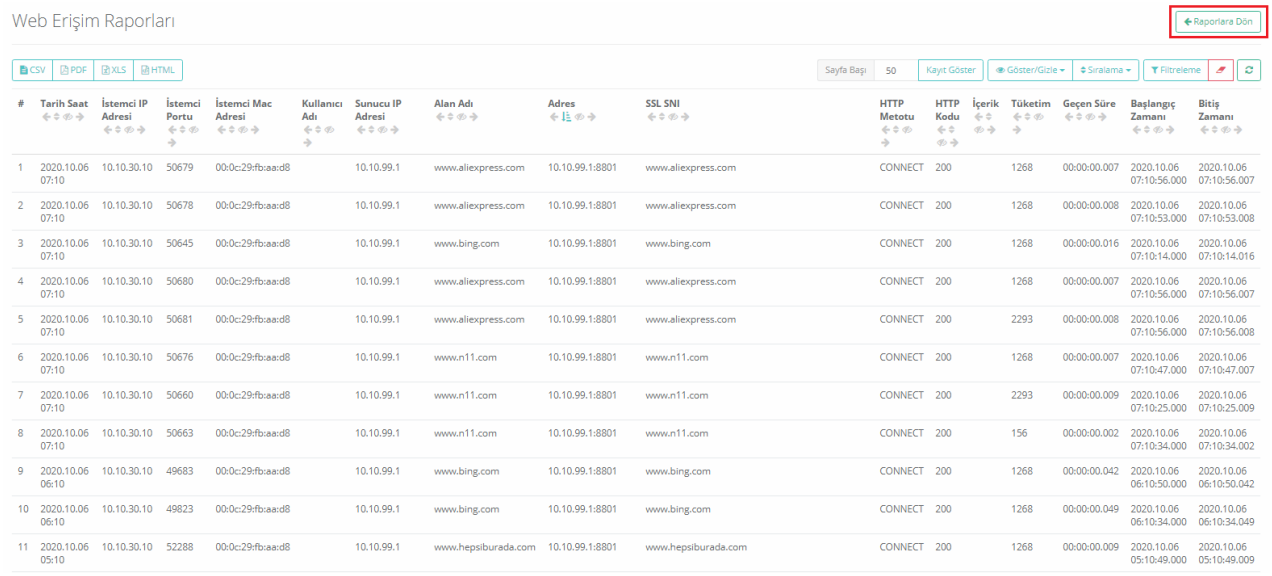


Tabloya yeni gelen değerleri görmek için yenile butonuna butonuna basılmalıdır.



#	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	

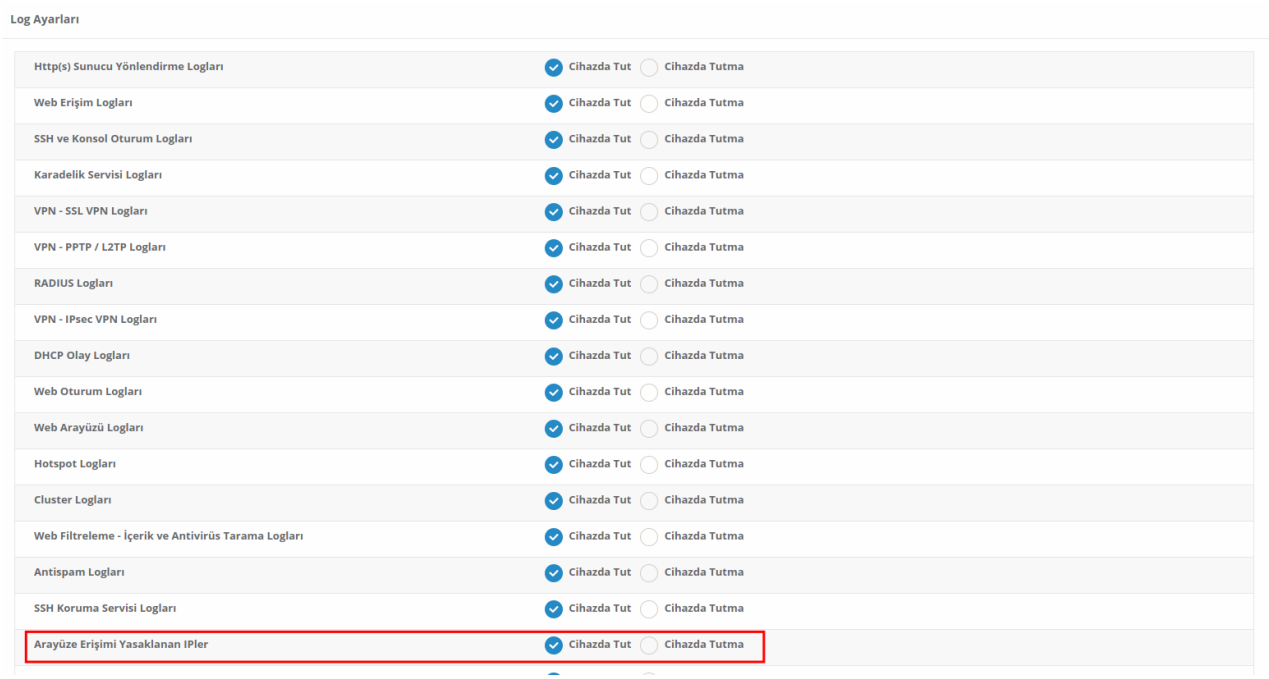
Raporlara Dön butonu ile dinamik raporlar menüsüne geri dönebilir, başka raporlara göz atabilirsiniz.



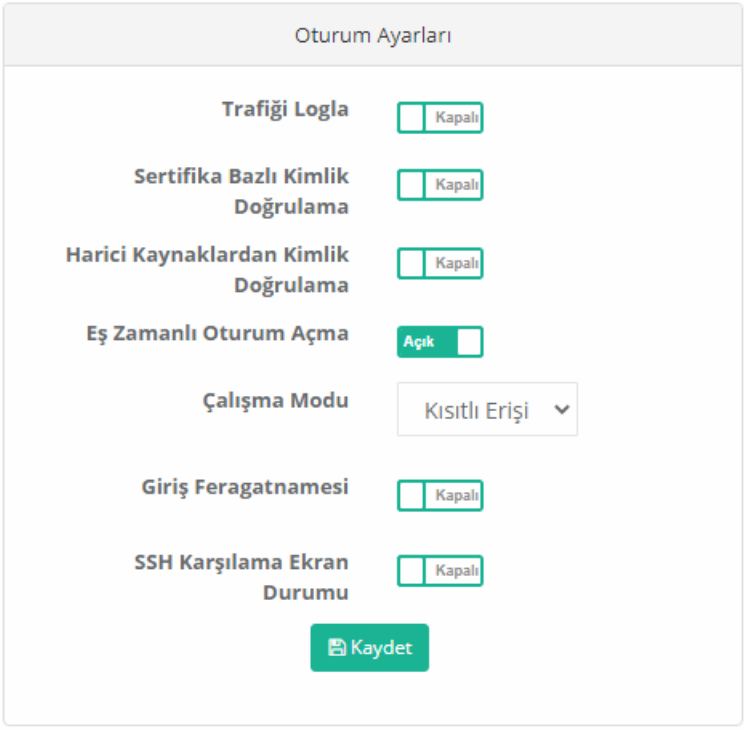
#	Tarih Saat	İstemci IP Adresi	İstemci Portu	İstemci Mac Adresi	Kullanıcı Adı	Sunucu IP Adresi	Alan Adı	Adres	SSL SNI	HTTP Metotu	HTTP Kodu	İçerik	Tüketim	Geçen Süre	Başlangıç Zamanı	Bitiş Zamanı
1	2020.10.06 07:10	10.10.30.10	50679	00:0c:29:fb:aa:d8		10.10.99.1	www.aliexpress.com	10.10.99.1:8801	www.aliexpress.com	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 Kullanıcı Raporlarına log 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.