

FortiView

FortiView alanı, cihaz üzerindeki özelliklerin genel durumlarını görüntülemek için kullanılmaktadır. Varsayılanda pek çok sekme geldiği gibi “+” (Add Monitor) seçeneğiyle Fortigate üzerindeki farklı özelliklerin durumunu görüntülemeye yönelik özelleştirmeler (ekleme/çıkarma) yapılabilmektedir. Bu sekmelerin birkaçına bakıldığında;

- **Source Tab**, kullanıcı paketlerinin kaynak adres yönündeki bilgilerin detaylı olarak görüntülenebildiği sekmedir.
 - 1- İP adresi gibi daha birçok özelliğe göre (ip address, MAC address, application, policy etc.) filtreleme işlemi yapılabiliyor.
 - 2- “Sources” kısmında hangi zaman aralığına dair bilgilerin görüntüleneceği filtrelenebiliyor.
 - 3- “Settings” kısmında ekranın ne sıklıkla güncelleneceğinin ayarlaması yapılıyor.
 - 4- Satırların üzerine gelindiğinde ip adresine sahip cihaz hakkında bilgiler görüntülenebiliyor. Burada seçilen ip adresi için ban tanımı gibi işlemler de yapılabiliyor (Sanırım okuma moduna açıldığı için görünmüyor. Detaylar – <https://docs.fortinet.com/document/fortigate/7.0.7/administration-guide/142456/fortiview-sources>).

Source	10.88.2.21	Sessions	Bandwidth
10.88.12.99	Detected Device	29	275.33 Kbps
10.88.101.99	Status	19	101.36 Kbps
10.88.103.99	MAC Address	16	205.32 Kbps
10.88.23.8	IP Address	21	180.31 Kbps
10.88.210.50	Interface	21	2.84 kbps
10.88.41.10	Online Interfaces	62	35.71 kbps
10.89.101.1	Hardware	62	2.72 kbps
10.88.210.62	OS	3	0 bps
10.89.101.3	FortiGate	2	168 bps
10.88.2.21	Connected FortiSwitch / FortiAP	18	11.63 kbps
10.88.210.101	Detected by FortiGuard IoT service	6	2.22 kbps
10.88.210.31	70:4ca5:68:4f:6e	4	22.78 kbps
10.88.210.253	70:4ca5:68:4f:6e	12	37.46 kbps
10.89.101.4	80:80:2ceb:7d:3a	42	62.97 kbps
10.89.101.5	80:80:2ceb:7d:3a	61	1.12 kbps

- o Herhangi bir cihazın üzerine tıklandığında cihazın kullandığı uygulamaları, hedef adresleri ve uygulanan politikalar, gidilen web siteler gibi daha pek çok detay görüntülenebiliyor. Örnek olarak herhangi bir adrese erişim sorunu yaşayan kullanıcının ip adresi “Source” sekmesi altında filtrelandikten sonra “Policies” kısmından hangi politikaların uygulandığı takip edilebiliyor.

Application	Category	Risk	Bytes	Sessions	Bandwidth
Syslog	Network.Service	Low	618.94 MB	3	222.12 Kbps
TCP/541	Network.Service	Low	6.66 MB	1	0 bps
SSL_TLSv1.3	Network.Service	Low	1.55 MB	4	0 bps
FortiGuard.Search	Cloud.IT	Low	716.89 KB	9	288 bps
SSL_TLSv1.2	Network.Service	Low	37.47 KB	4	0 bps
Microsoft.Authentication	Collaboration	Low	26.43 KB	5	0 bps
DNS	Network.Service	Low	1.07 KB	4	0 bps
LDAP	Network.Service	Low	353 B	1	0 bps
UDP/53	Network.Service	Low	174 B	1	0 bps

- **Destinations Tab**, kullanıcı paketlerinin hedef adres yönündeki bilgilerin detaylı olarak görüntülenebildiği sekmedir.
 - o Sources sekmesinde olan özellikler bu sekmede de sağlanmaktadır. Ek olarak listelene ip adreslerin üzerine gelindiğinde Whois bilgileri görüntülenebiliyor.

FortiView Destinations by Bytes

Destination Address	Application	Bytes	Sessions	Bandwidth
10.88.210.50	IP Address 12.34.56.78 Known and verified safe site		3	36.55 kbps
172.30.72.98	Popularity ★★★★★		1	26.71 kbps
172.30.72.55	Owner Fortinet		1	26.23 kbps
10.88.210.62	Location Ashburn, Virginia, United States		4	17.42 kbps
10.88.210.253	Coordinates 39.04°N / -77.48°W		2	536 bps
10.88.101.99	Running Services Fortinet-FortiGuard, Fortinet-Web, Fortinet-ICMP, Fortinet-DNS, Fortinet-SSH, Fortinet-SSL			
96.15.11.11				
service.fortiguard.net (208.184.23.1)				
service.fortiguard.net (12.34.56.78)				
service.fortiguard.net (173.243.1.1)				
us-atl-anx-r007.router.teamviewer.com (10.88.23.8)				
us-njc-anx-r018.router.teamviewer.com (10.88.210.100)				
192.168.100.255				
192.168.59.255				
10.89.20.255				
10.10.10.255				

Drill down Search filterable columns

FortiView Destinations by Bytes

Destination Address service.fortiguard.net (12.34.56.78)

Application Fortiguard.Search

Bytes 262.24 kB

Sessions 12

Bandwidth 80 bps

View sessions

Source Applications Policies

Source	Device	Bytes	Sessions
10.88.106.153	LAN-E_U431F_46110	87.02 kB	1
10.88.106.152	LAN-E_U431F_39379_SpectrumAnalyzer	86.9 kB	1
10.88.106.151	LAN-E_U431F_4373	86.9 kB	1

- **Application Tab**, kullanıcıların oluşturduğu trafik üzerinden hangi uygulamaların ne kadar kullandığı görüntülenebiliyor.

FortiView Applications by Bytes

Application	Category	Risk	Bytes	Sessions	Bandwidth
Syslog	Network.Service		1.18 GB	8	362.38 k...
UDP/514	Syslog		47.55 MB	2	17.42 kbps
SSL_TLS			11.2 MB	20	188.13 k...
TCP/541	ID 16283		7.58 MB	1	1.34 kbps
TCP/514	Summary This indicates an attempt to use the syslog protocol.		7.89 MB	3	13.33 kbps
FortiGuard			1.06 MB	151	17.54 kbps
TeamViewer			383.18 kB	2	32 bps
UDP/8014			315.22 kB	5	72 bps
Root.C			150.88 kB	15	1.1 kbps
Microsoft			145.9 kB	7	6.65 kbps
SSL_TLS			85.3 kB	10	252.19 k...
Google			66.52 kB	1	16 bps
Microsoft			51.47 kB	10	60.78 kbps
Microsoft			44.71 kB	2	49.24 kbps
SNMP_V2			28.14 kB	1	0 bps
DHCP			11.07 kB	2	336 bps

Drill down Search filterable columns

Syslog

Category Network.Service

Risk

Popularity ★★★★★

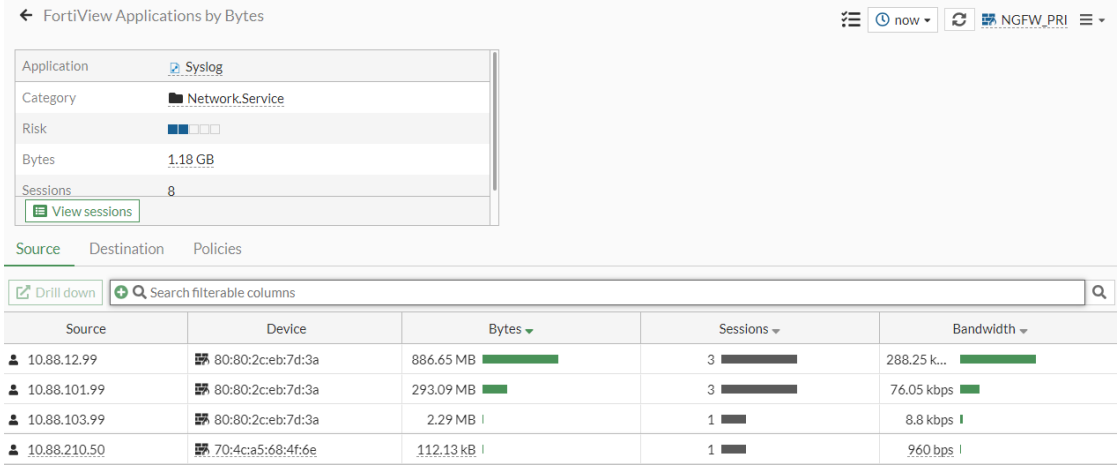
Protocol UDP

Ports UDP/514

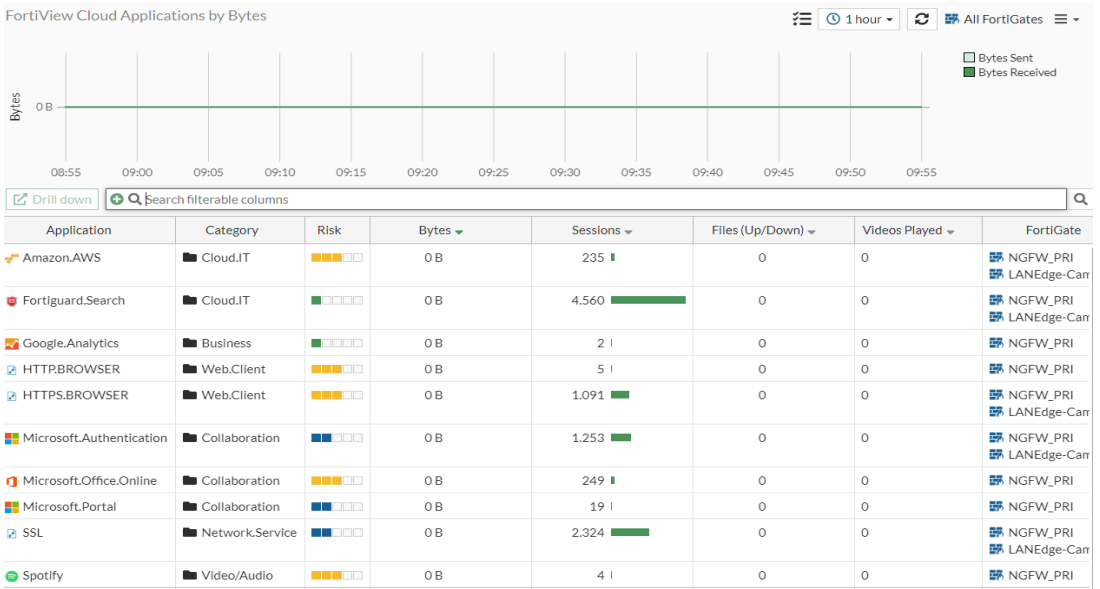
Technology Network-Protocol

Vendor Other

- o Satırlara tıklanarak uygulamayı kullanan istemciler ve bu istemciler hakkında detaylar görüntülenebiliyor. Her tabloda olduğu gibi burada da sütun kısmı fare ile sağ tuşuyla özelleştirilebiliyor.



- **Cloud Application Tab**, kullanılan bulut tabanlı uygulamaların kullanımı hakkında detayları görüntülemek için kullanılıyor. Application sekmesi altında olduğu gibi burada da uygulamaların üzerine gelinerek ön bilgi alınabilirken üzerine tıklandığında detaylı bilgi edinilebiliyor.



- **Web Sites Tab**, kullanıcıların gittiği web siteleri hakkında detaylar görüntülenebiliyor. Bu sekmede kayıtların görüntülenebilmesi için Web Filter lisansına sahip olunması ve kural yazılan IPv4 politikalarında loglama özelliğinin devreye alınması gerekiyor.
- **Threat Tab**, cihaza yönelik gerçekleştirilen saldırıları görüntülemek için kullanılıyor. Burada saldırıların önem seviyesi, denenen oturum sayısı gibi daha birçok niteliği görüntülenebiliyor.
- **Compromised Hosts Tab**, herhangi bir nedenden dolayı bloke edilen istemcilerin listelendiği sekmedir.
- **Wifi Clients Tab**, Wifi kullanıcılarına ilişkin bilgilerin görüntülendiği sekmedir.
- **Traffic Shaping Tab**, traffic shaper tarafından toplanan en yüksek trafik oturumlarının görüntülendiği sekmedir.
- **Servers Tab**, sunucular hakkında bilgilerin görüntülendiği sekmedir.
- **System Events**, sistem olaylarının görüntülendiği sekmedir.
- **VPN Tab**, kurulan VPN bağlantılarına yönelik durumların görüntülenebildiği sekmedir.

- **Endpoint Vulnerability**, istemciler üzerinde bulunan/tespit edilen zafiyetlerle ilgili bilgilerin listelendiği sekmedir. İlgili zafiyetlerin üzerine tıklanarak detaylı bilgi elde edilebiliyor.
- **Policy Tab**, hangi politikanın ne kadar trafik harcadığı gibi özelliklerin görüntülendiği sekmedir. İlgili politikaların üzerine tıklanarak detaylı bilgi elde edilebiliyor.
- **Interfaces Tab**, cihaz üzerindeki arayüzlerin durumu hakkında bilgilerin görüntülendiği sekmedir. Arayüzün üzerine tıklandığında, o arayüze bağlı cihazlar hakkında detaylı bilgiler de elde edilebiliyor.
- **Sandbox Tab**, Sandbox üzerine bir ayarlama yapılmışsa durumu hakkında bilgiler bu sekme altında görüntülenebiliyor.
- **All Sessions Tab**, cihaz üzerinden gerçekleştirilen bütün oturumların görüntülenebildiği sekmedir.

NOTLAR:

- Fortigate FW cihazlarda loglama işlemlerinin sağlıklı yapılabilmesi için “**Log & Report -> Log Settings**” alanından loglama ayarlarının düzenlenmesi gerekiyor (kayıt alınacak disk seçimi, local traffic veya olay günlüklerinin kayıt edilip edilmeyeceği gibi bazı seçimler).
- Grafikler üzerinde tablolarda istenen belirli zaman aralığı seçilerek bu zaman diliminde oluşan kayıtların listelenmesi sağlanabiliyor.

