

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 filtrelenabiliyor.
 - 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>).

FortiView Sources by Bytes

Drill down

Search filterable columns

Source

10.88.2.21

10.88.12.99

10.88.101.99

10.88.103.99

10.88.23.8

10.88.210.50

10.88.41.10

10.89.101.1

10.88.210.62

10.89.101.3

10.88.2.21

10.88.210.101

10.88.210.31

10.88.210.253

10.89.101.4

10.89.101.5

Detected Device

Status

MAC Address

IP Address

Interface

Online Interfaces

Hardware

OS

FortiGate

Connected FortiSwitch / FortiAP

70:4ca5:68:4f:6e

70:4ca5:68:4f:6e

70:4ca5:68:4f:6e

80:80:2ceb:7d:3a

80:80:2ceb:7d:3a

10.88.2.21

Online

70:4ca5:68:4f:6e

10.88.2.21

DCFW (DCFW)

DCFW (DCFW)

Network / Fortinet / Firewall / FortiGate-2000E

FortiOS

NGFW_PRI

S448ENTF21001605:port7

Detected by FortiGuard IoT service

Sessions

29

19

16

21

21

62

62

3

2

18

6

4

12

42

61

Bandwidth

275.33 K...

101.36 K...

205.32 K...

180.31 K...

2.84 kbps

35.71 kbps

2.72 kbps

0 bps

168 bps

11.63 kbps

2.22 kbps

22.78 kbps

37.46 kbps

62.97 kbps

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 filtrelendikten sonra “Policies” kısmından hangi politikaların uygulandığı takip edilebiliyor.

| Application | Category | Risk | Bytes | Sessions | Bandwidth |
|--------------------------|-----------------|------|-----------|----------|-------------|
| Syslog | Network.Service | Low | 618.94 MB | 3 | 222.12 K... |
| 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 | | | |
| service.fortiguard.net (208.184.130.25) | Resolve | | | |
| service.fortiguard.net (12.34.56.78) | | | | |
| service.fortiguard.net (173.243.10.10) | | | | |
| us-atl-anx-r007.router.teamviewer.com | | | | |
| us-njc-anx-r018.router.teamviewer.com | | | | |
| 10.88.23.8 | | | | |
| 10.88.210.100 | | | | |
| 192.168.100.255 | | | | |
| 192.168.59.255 | | | | |
| 10.89.20.255 | | | | |
| 10.10.10.255 | | | | |

FortiView Destinations by Bytes (Detailed View)

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. Ek olarak uygulamaların oluşturduğu risk miktarı kategorize ediliyor. Uygulamalara yönelik politikalar belirlenirken buradaki risk değerleri de göz önünde bulundurulmalıdır.

FortiView Applications by Bytes

| Application | Category | Risk | Bytes | Sessions | Bandwidth |
|-------------|---|------|-----------|----------|-------------|
| Syslog | Network.Service | | 1.18 GB | 8 | 362.38 k... |
| UDP/514 | | | 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 |
| Fortigu | | | 1.06 MB | 151 | 17.54 kbps |
| TeamV | | | 383.18 kB | 2 | 32 bps |
| UDP/8014 | | | 315.22 kB | 5 | 72 bps |
| Root.C | | | 150.88 kB | 15 | 1.1 kbps |
| Micros | Category Network.Service | | 145.9 kB | 7 | 6.65 kbps |
| SSL_TLS | Risk | | 85.3 kB | 10 | 252.19 k... |
| Google | Popularity ★★★★★ | | 66.52 kB | 1 | 16 bps |
| Micros | Protocol UDP | | 51.47 kB | 10 | 60.78 kbps |
| Micros | Ports UDP/514 | | 44.71 kB | 2 | 49.24 kbps |
| Micros | Technology Network-Protocol | | | | |
| Micros | Vendor Other | | | | |
| SNMP_V2 | Category Network.Service | | 28.14 kB | 1 | 0 bps |
| DHCP | Category Network.Service | | 11.07 kB | 2 | 336 bps |

FortiView Applications by Bytes (Detailed View)

Application: Syslog

Category: Network.Service

Risk:

Popularity: ★★★★★

Protocol: UDP

Ports: UDP/514

Technology: Network-Protocol

Vendor: Other

Summary: This indicates an attempt to use the syslog protocol.

The syslog protocol is used to send event notification messages. The protocol is designed to transport the messages to the collector. The collector does not need to acknowledge the messages.

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

FortiView Applications by Bytes

Application: Syslog
Category: Network.Service
Risk: ■ ■ ■ ■
Bytes: 1.18 GB
Sessions: 8
[View sessions](#)

Source Destination Policies

[Drill down](#) [Search filterable columns](#)

| Source | Device | Bytes | Sessions | Bandwidth |
|--------------|-------------------|-----------|----------|-------------|
| 10.88.12.99 | 80:80:2c:eb:7d:3a | 886.65 MB | 3 | 288.25 k... |
| 10.88.101.99 | 80:80:2c:eb:7d:3a | 293.09 MB | 3 | 76.05 kbps |
| 10.88.103.99 | 80:80:2c:eb:7d:3a | 2.29 MB | 1 | 8.8 kbps |
| 10.88.210.50 | 70:4c:a5:68:4f:6e | 112.13 kB | 1 | 960 bps |

- **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.

FortiView Cloud Applications by Bytes

Bytes Sent Bytes Received

0 B

08:55 09:00 09:05 09:10 09:15 09:20 09:25 09:30 09:35 09:40 09:45 09:50 09:55

[Drill down](#) [Search filterable columns](#)

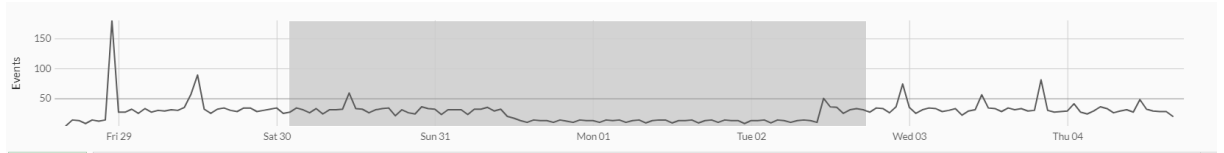
| Application | Category | Risk | Bytes | Sessions | Files (Up/Down) | Videos Played | FortiGate |
|--------------------------|-----------------|---|-------|----------|-----------------|---------------|-------------------------|
| Amazon.AWS | Cloud.IT | ■ ■ ■ ■ | 0 B | 235 | 0 | 0 | NGFW_PRI LANEdge-Car |
| Fortiguard.Search | Cloud.IT | ■ ■ ■ ■ | 0 B | 4.560 | 0 | 0 | NGFW_PRI LANEdge-Car |
| Google.Analytics | Business | ■ ■ ■ ■ | 0 B | 2 | 0 | 0 | NGFW_PRI |
| HTTP.BROWSER | Web.Client | ■ ■ ■ ■ | 0 B | 5 | 0 | 0 | NGFW_PRI |
| HTTPS.BROWSER | Web.Client | ■ ■ ■ ■ | 0 B | 1.091 | 0 | 0 | NGFW_PRI LANEdge-Car |
| Microsoft.Authentication | Collaboration | ■ ■ ■ ■ | 0 B | 1.253 | 0 | 0 | NGFW_PRI LANEdge-Car |
| Microsoft.Office.Online | Collaboration | ■ ■ ■ ■ | 0 B | 249 | 0 | 0 | NGFW_PRI |
| Microsoft.Portals | Collaboration | ■ ■ ■ ■ | 0 B | 19 | 0 | 0 | NGFW_PRI |
| SSL | Network.Service | ■ ■ ■ ■ | 0 B | 2.324 | 0 | 0 | NGFW_PRI LANEdge-Car |
| Spotify | Video/Audio | ■ ■ ■ ■ | 0 B | 4 | 0 | 0 | NGFW_PRI |

- **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 görüntüldüğü 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 görüntüldüğü sekmedir. İlgili politikaların üzerine tıklanarak detaylı bilgi elde edilebiliyor.
- **Interfaces Tab**, cihaz üzerindeki arayüzlerin durumu hakkında bilgilerin görüntüldüğü 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.



- Sekmelerde gösterilen özellikler genel olarak her sekme için aynı veya benzer olduğundan dolayı tekrar tekrar açıklama yapılmadı. Fortiview alanı için Fortigate güvenlik duvarı üzerinde kullanılan özelliklerin görüntülenebilmesi ve detaylandırılmasını sağladığı söylenebilir. Fortigate FW V6.XX sürümlerinde ayrı bir alan olarak karşımıza çıksa da V7.XX için bu alanın “Dashboard” alanı altında alınmıştır.