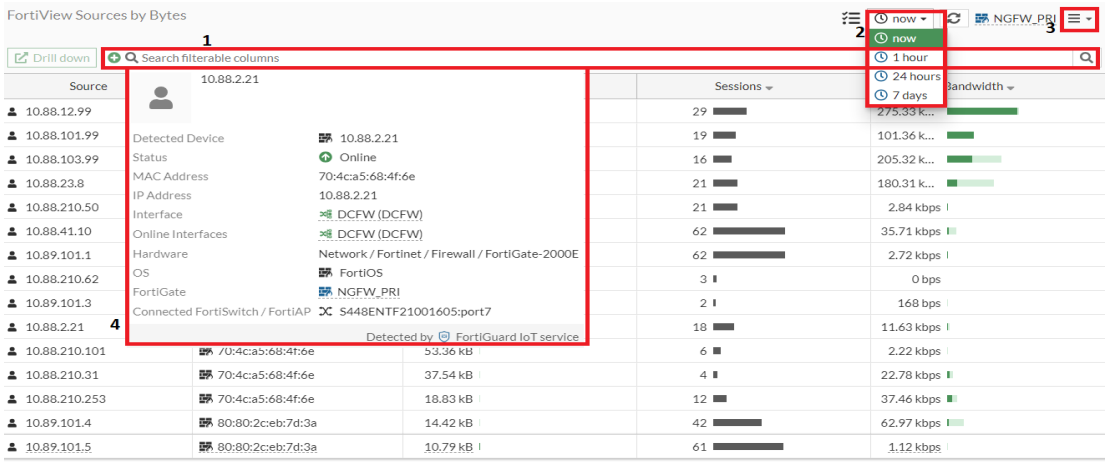
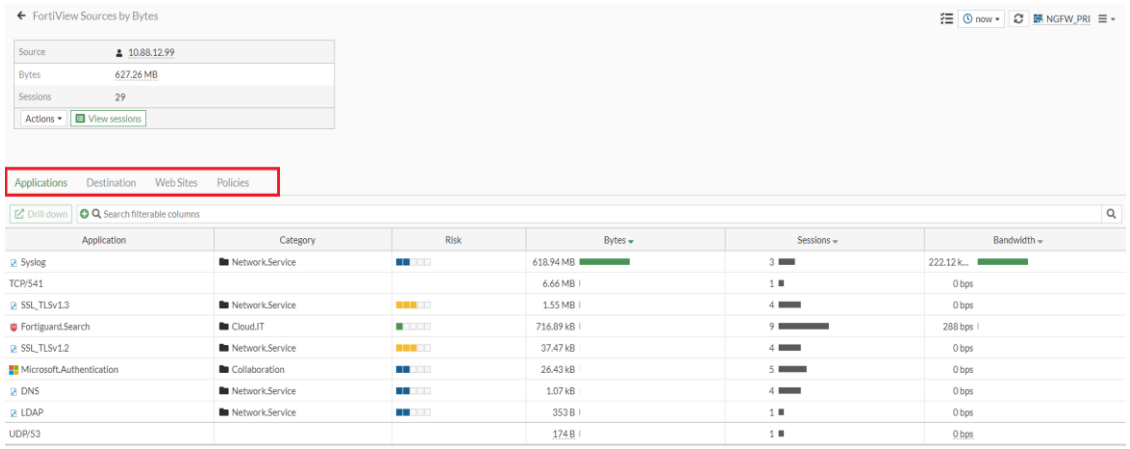
FortiView

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;

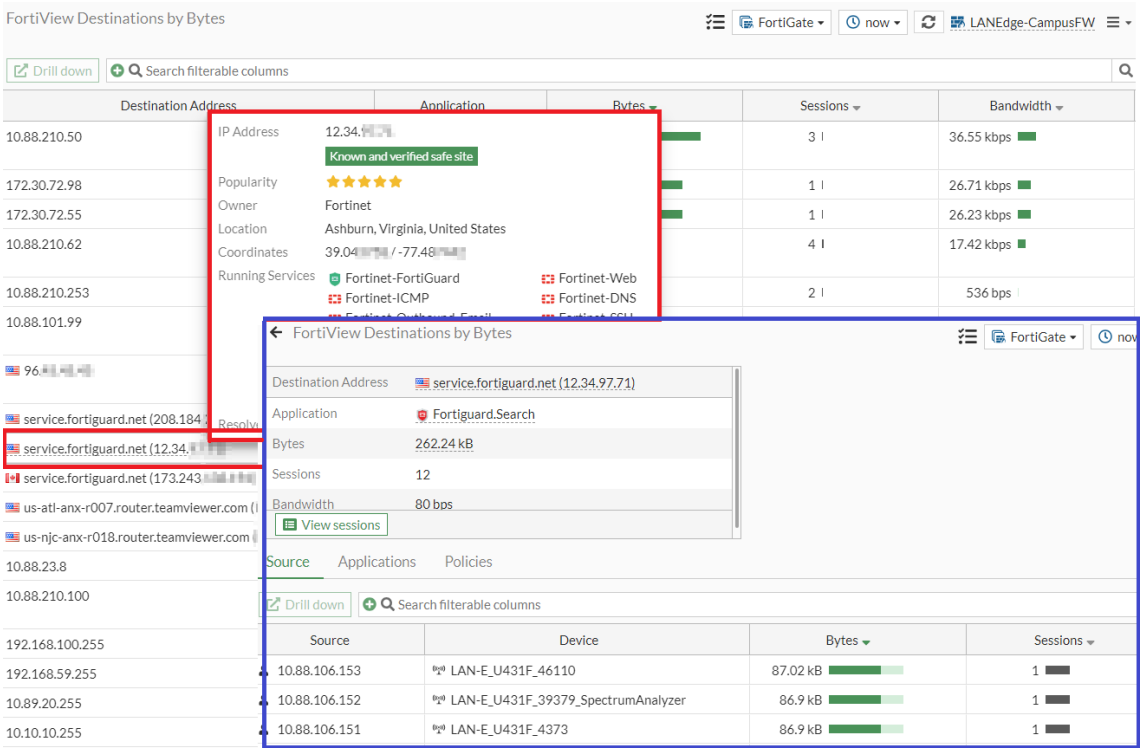
- **Source Tab**, kullanıcı paketlerinin kaynak adres yönündeki bilgilerin detaylı olarak görüntülenebildiği sekmedir.
    1- İP adresi gibi daha birçok özelliğe göre (ip address, MAC address, aplication, policy etc.) filtreleme işlemi yapılabiliyor.
    2- "Sources" kısmında hangi zaman aralığına dair 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).



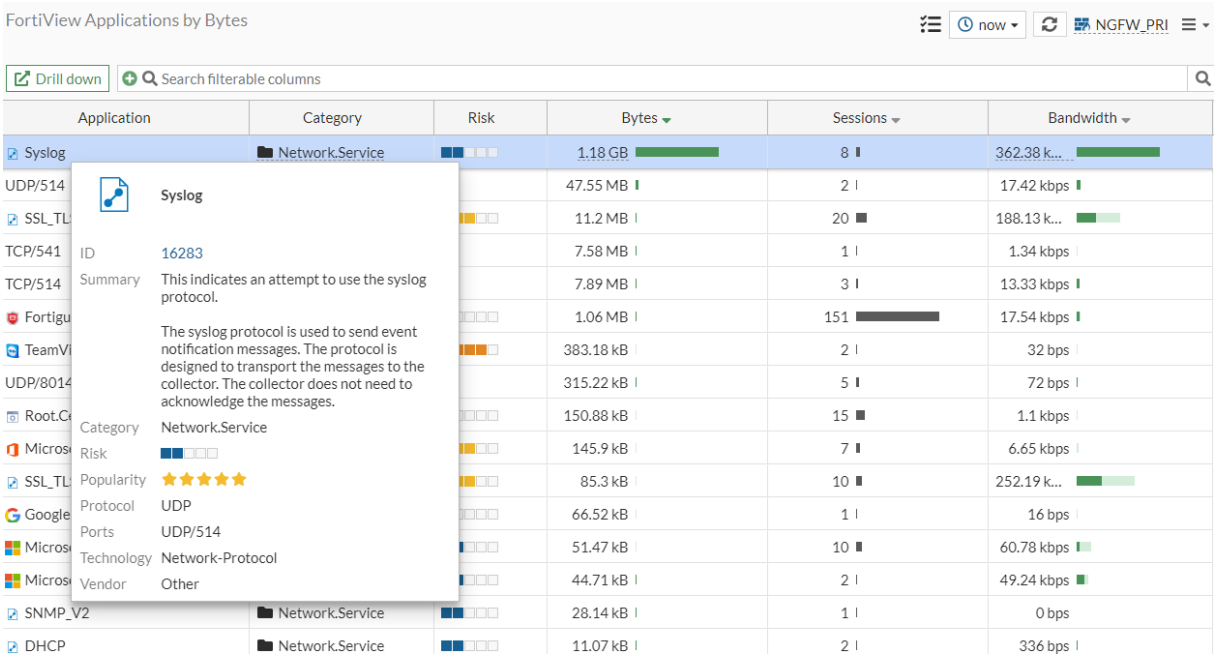
    - Herhangi bir cihazın üzerine tıklandığında cihazın kullandığı uygulamaları, hedef adresleri ve uygulanan politikalar, gidilen web siteler gibi daha pek çok detay görüntülenebiliyor. Örnek olarak herhangi bir adrese erişim sorunu yaşayan kullanıcının ip adresi "Source" sekmesi altında filtrelendikten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



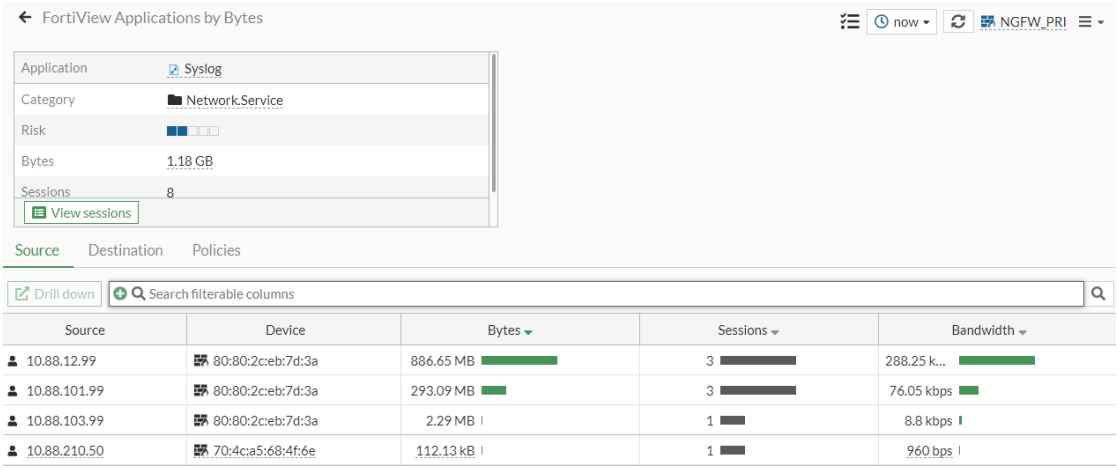
- **Destinations Tab**, kullanıcı paketlerinin hedef adres yönündeki bilgilerin detaylı olarak görüntülenebildiği sekmedir.
    - Sources sekmesinde olan özellikler bu sekmede de sağlanmaktadır. Ek olarak listelene ip adreslerin üzerine gelindiğinde Whois bilgileri görüntülenebiliyor.



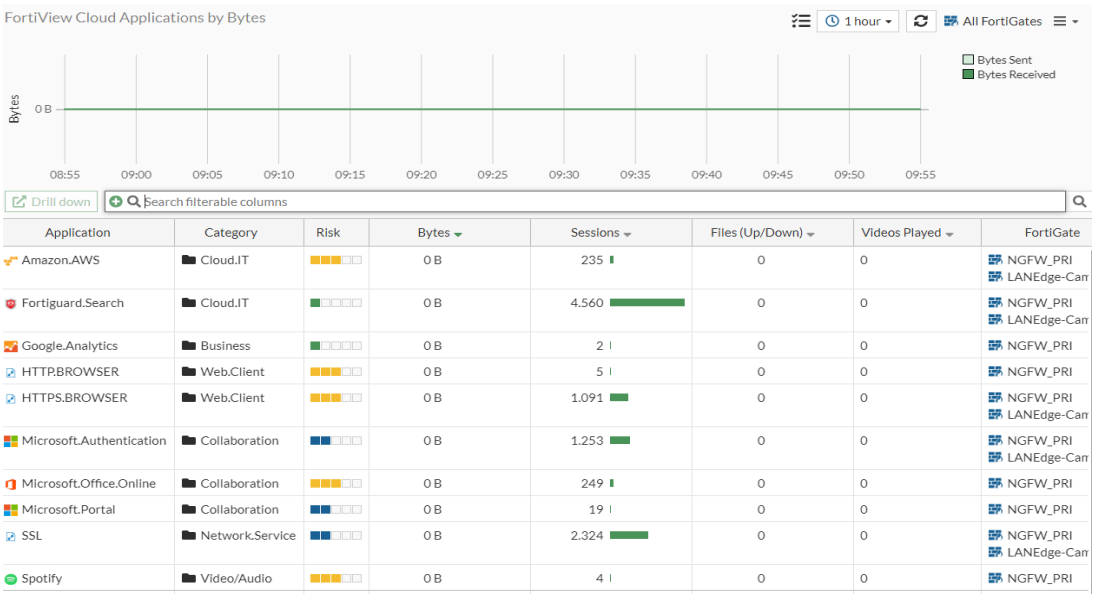
- **Application Tab**, kullanıcıların oluşturduğu trafik üzerinden hangi uygulamaların ne kadar kullandığı görüntülenebiliyor. Ek olarak uygulamaların oluşturduğu risk miktarı kategorize ediliyor. Uygulamalara yönelik politikalar belirlenirken buradaki risk değerleri de göz önünde buiundurulmalıdır.



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

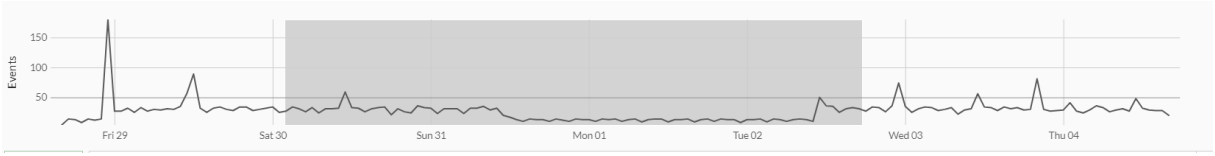


- **Web Sites Tab**, kullanıcıların gittiği web siteleri hakkında detaylar görüntülenebiliyor. Bu sekmede kayıtların görüntülenebilmesi için Web Filter lisansına sahip olunması ve kural yazılan IPv4 politikalarında loglama özelliğinin devreye alınması gerekiyor.
- **Threat Tab**, cihaza yönelik gerçekleştirilen saldırıları görüntülemek için kullanılıyor. Burada saldırıların önem seviyesi, denenen oturum sayısı gibi daha birçok niteliği görüntülenebiliyor.
- **Compromised Hosts Tab**, herhangi bir deneden 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.



- 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.