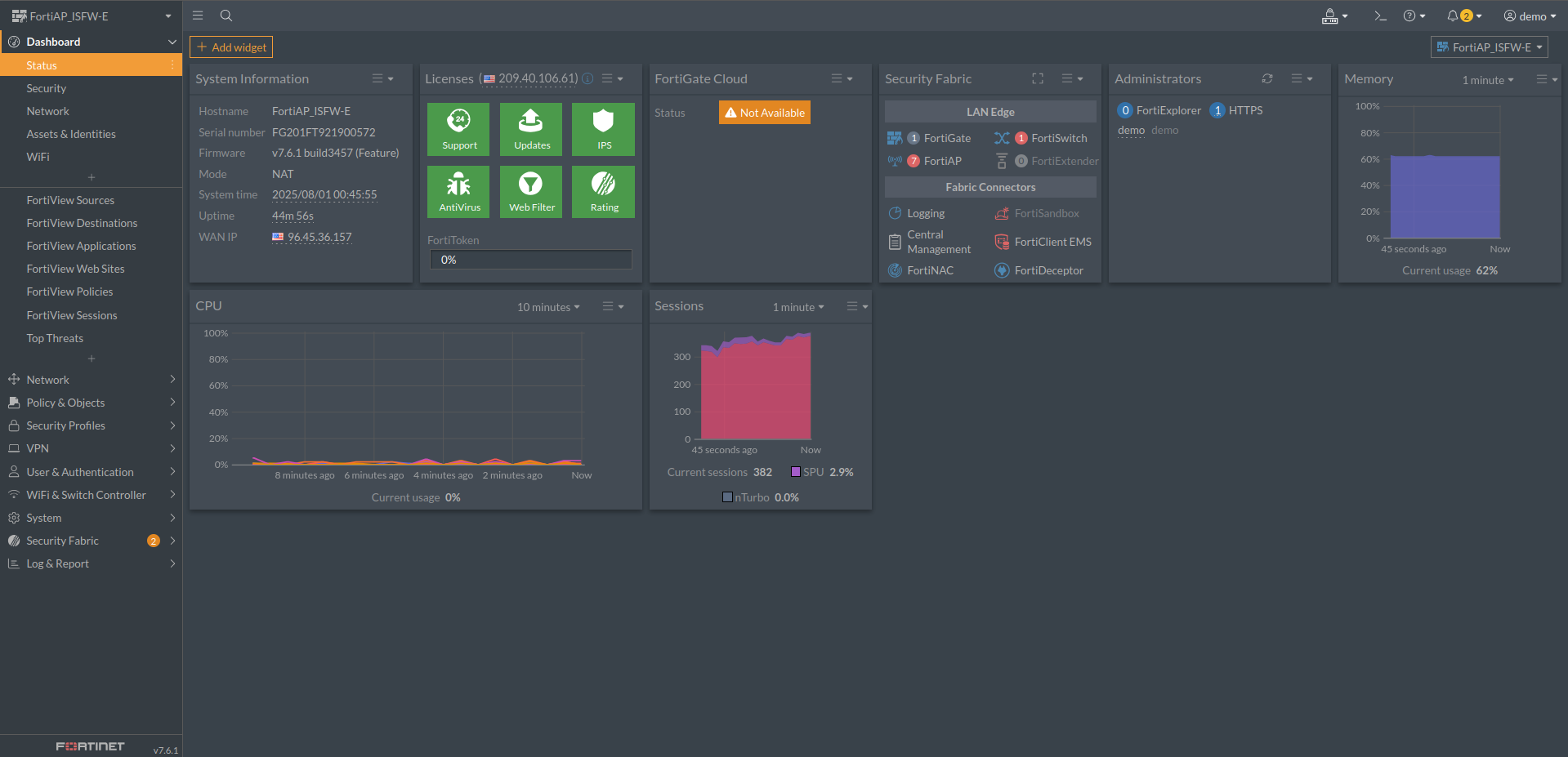
**FortiAP**

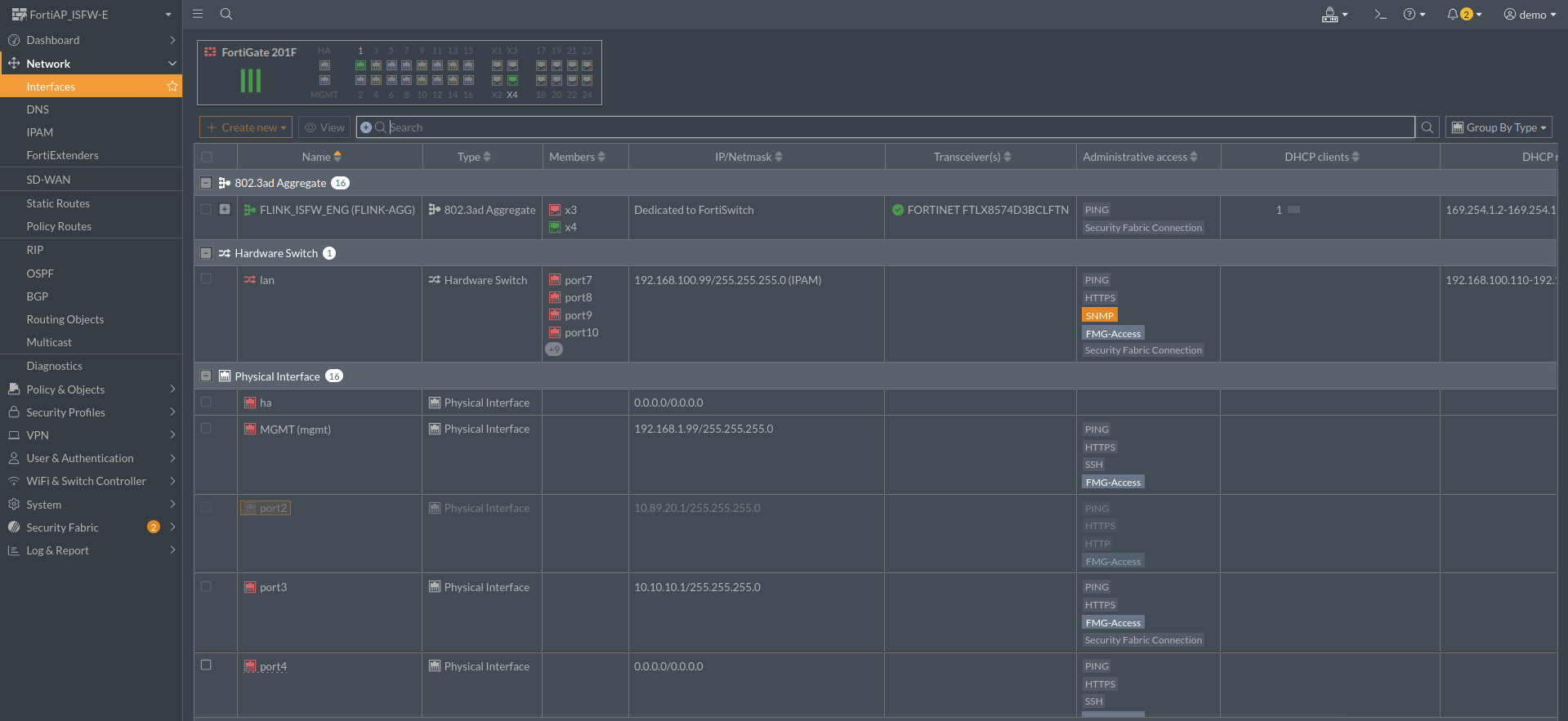
FortiAP, Fortinet firmasının ürettiği bir kablosuz erişim noktası (Wireless Access Point - AP) cihazıdır. Temel olarak, kablosuz ağ (Wi-Fi) sinyali yayınlayarak akıllı telefonlar, tabletler, dizüstü bilgisayarlar gibi kablosuz cihazların internete ve ağ kaynaklarına bağlanmasını sağlar.



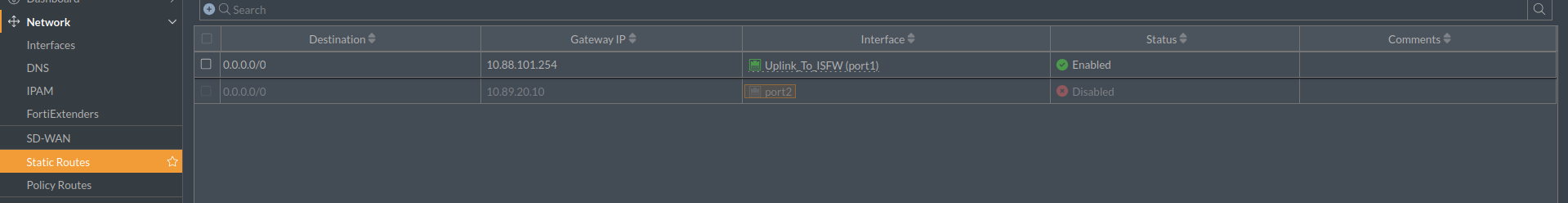
* **Dashboard:** Bu size FortiAP'nin durumu, bağlı istemciler ve genel performansı hakkında bir genel bakış sunacaktır. Hızlı bir anlayış için genellikle bakılacak ilk yerdir.
* **Network:** Bu bölüm, FortiAP'nin ağ yapılandırmasını (IP adresleri, arayüzler ve VLAN'lar dahil) detaylandıracaktır, bunlar ağınızda nasıl bağlandığı ve çalıştığı için temeldir.
* **Policy & Objects:** FortiAP'ler öncelikli olarak erişim noktaları olsa da, bazı politika uygulama yeteneklerine sahip olabilir veya bir FortiGate üzerinde tanımlanmış politikalarla etkileşime girebilirler. Bunu anlamak, AP düzeyinde uygulanan erişim kontrolü veya güvenlik kuralları hakkında size fikir verecektir.
* **Security Profiles:** Bu, FortiAP tarafından kullanılan WPA2/3 gibi kablosuz güvenlik ayarlarını, şifreleme yöntemlerini ve kimlik doğrulama protokollerini anlamak için çok önemlidir.
* **WiFi & Switch Controller:** Bu, bir FortiAP'yi anlamak için belki de *en önemli* bölümdür. SSID'ler, radyo ayarları, kanal yönetimi ve AP'nin nasıl yönetildiği (örneğin, bir kontrolör olarak hareket eden bir FortiGate tarafından) dahil olmak üzere Wi-Fi ile ilgili temel işlevleri kapsayacaktır.
* **System:** Bu, FortiAP'nin genel sistem ayarlarını (donanım yazılımı sürümü, saat ayarları, yönetim erişimi ve potansiyel olarak yüksek kullanılabilirlik yapılandırmaları gibi) kapsayacaktır.
* **Log & Report:** Bu bölümü anlamak, FortiAP'deki olayları, hataları ve etkinliği görmenizi sağlayacaktır; bu da sorun giderme ve izleme için hayati önem taşır.

**Network**

* **Interfaces:** Bu, FortiAP'nin fiziksel veya sanal ağ bağlantı noktalarını yapılandırdığınız yerdir. Her bir arayüzün IP adresi, alt ağ maskesi, VLAN ID'leri (varsa) ve bağlantı durumu gibi ayarlarını içerir. AP'nin ağa nasıl bağlandığının temelini oluşturur.



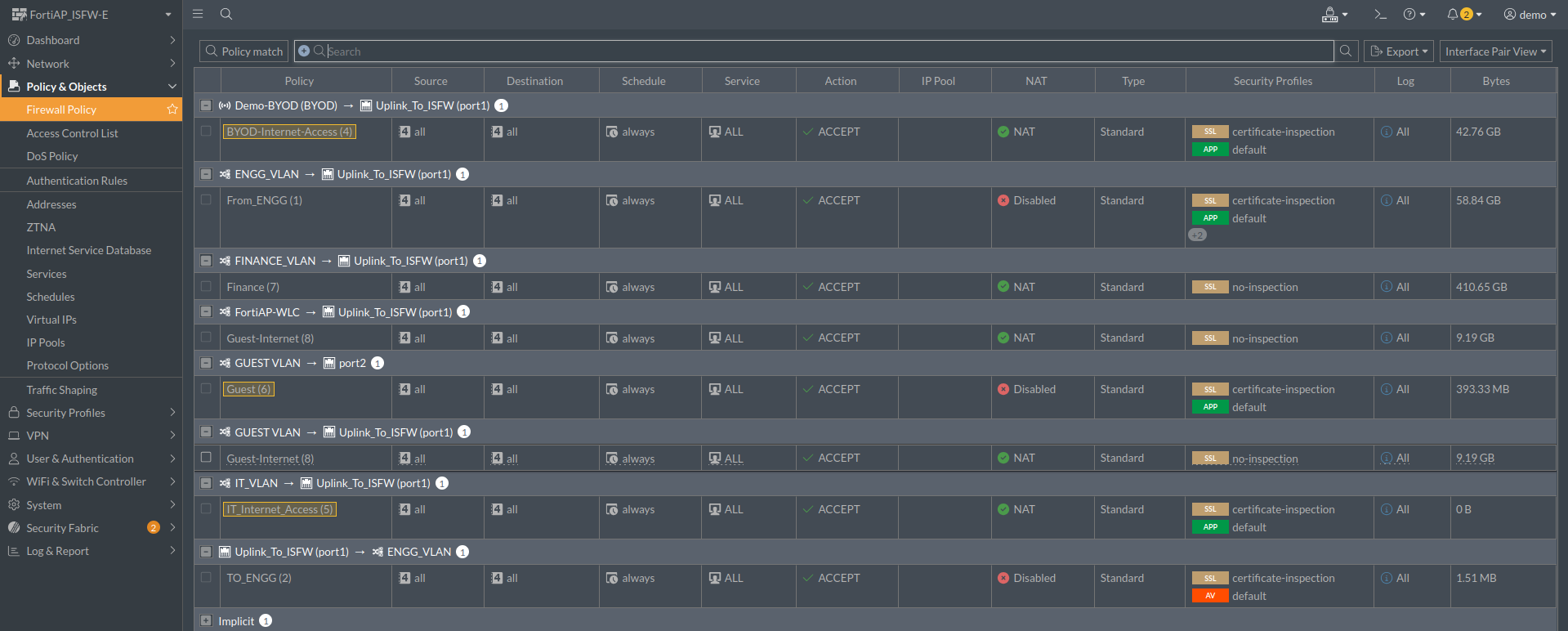
* **DNS**: FortiAP'nin alan adlarını IP adreslerine çözümlemek için kullandığı DNS sunucularını yapılandırdığınız yerdir. Cihazın internete veya yerel ağdaki kaynaklara isimle erişebilmesi için önemlidir.
* **IPAM**: Genellikle daha büyük ağlarda IP adresi atamasını ve yönetimini kolaylaştırmak için kullanılır. FortiAP'nin kendisi için veya bağlı cihazlara DHCP aracılığıyla IP dağıtımıyla ilgili ayarları içerebilir.
* **FortiExtenders**: Eğer FortiAP, FortiExtender cihazları (kablosuz veya kablolu genişleticiler) ile birlikte çalışıyorsa, bu bölüm onların yönetimini ve bağlantısını gösterir. FortiExtender'lar, FortiGate'in WAN veya LAN bağlantısını genişletmek için kullanılır. Ancak bir FortiAP'nin direkt olarak bu bölümde olması, FortiAP'nin bir FortiGate tarafından yönetildiği ve FortiExtender'ların da aynı FortiGate tarafından yönetildiği anlamına gelebilir. FortiAP'nin kendi başına FortiExtender olmadığını unutmayın.
* **SD-WAN**: Bu, birden fazla WAN bağlantısını (örneğin, birden fazla internet servis sağlayıcısı) tek bir mantıksal bağlantı olarak yönetmek ve trafiği en iyi yol üzerinden yönlendirmek için kullanılır. Bir FortiAP'nin kendisi doğrudan SD-WAN kontrolcüsü olmasa da, bağlı olduğu FortiGate'in SD-WAN yapılandırmasının bir parçası olarak trafiği bu kurallara göre yönlendirmesine yardımcı olabilir veya bu bağlantı türlerini kullanabilir.
* **Static Routes:** Bu, belirli ağlara ulaşmak için manuel olarak tanımlanmış yollardır. FortiAP'nin bilmediği veya doğrudan bağlı olmadığı ağlara nasıl ulaşacağını belirtir. Küçük veya sabit ağ yapıları için kullanışlıdır.



* **Policy Routes:** Trafiği belirli koşullara (kaynak IP, hedef IP, servis vb.) göre yönlendiren rotalardır. Statik rotalardan farklı olarak, bu rotalar daha esnek ve kural tabanlıdır.
* **RIP, OSPF ve BGP:** Bunlar dinamik yönlendirme protokolleridir. FortiAP genellikle bu protokolleri kendi başına çalıştırmaz, ancak bağlı olduğu FortiGate veya ana yönlendirici bu protokolleri kullanarak ağdaki rota bilgilerini FortiAP'ye aktarabilir veya FortiAP bu protokollerin çalıştığı bir ağda konumlanmış olabilir. Eğer FortiAP'nin kendi başına daha gelişmiş yönlendirme yetenekleri varsa (ki bu bir AP için nadirdir), bu protokoller üzerinden rota öğrenebilir veya ilan edebilir. Genellikle bir FortiGate cihazının menüsünde bulunur ve AP'lerin bu protokollere doğrudan katılımı sınırlıdır.
* **Routing Objects:** Yönlendirme kurallarında (statik, politika, dinamik) kullanılacak ağ adresleri, adres grupları veya diğer nesnelerin tanımlandığı yerdir. Yönlendirme yapılandırmalarını daha düzenli ve tekrar kullanılabilir hale getirir.
* **Multicast:** Bu, tek bir veri paketinin birden fazla alıcıya aynı anda gönderilmesi için kullanılır (örneğin, video akışları veya bazı kurumsal uygulamalar için). FortiAP'nin çoklu yayın trafiğini ağında nasıl işlediği ve yönlendirdiği ile ilgili ayarları içerir.
* **Diagnostics:** Ağ bağlantısı sorunlarını gidermek veya performansını test etmek için kullanılan araçları (ping, traceroute, paket yakalama vb.) içerir. Herhangi bir ağ sorunu yaşadığınızda bakmanız gereken ilk yerlerden biridir.

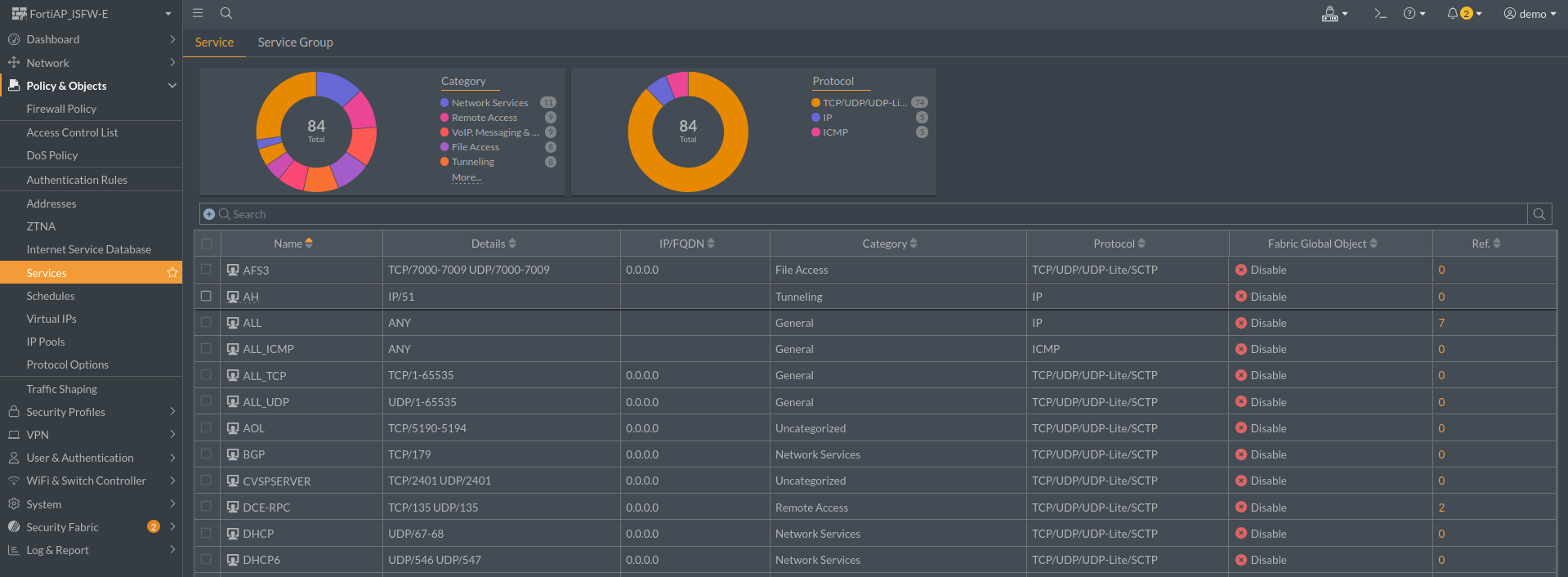
**Policy & Objects:**

* **Firewall Policy:** Ağ trafiğinin bir arayüzden diğerine (örneğin, dahili ağdan internete veya farklı VLAN'lar arasında) geçişine izin veren veya engelleyen kurallar setidir. Hangi kaynak IP'lerin, hangi hedeflere, hangi servisleri kullanarak erişebileceğini ve bu trafik üzerinde hangi güvenlik profillerinin uygulanacağını burada belirlersiniz.



Üstüne tıklayıp view dedikten sonra kuralın detaylarını inceleyebiliriz.

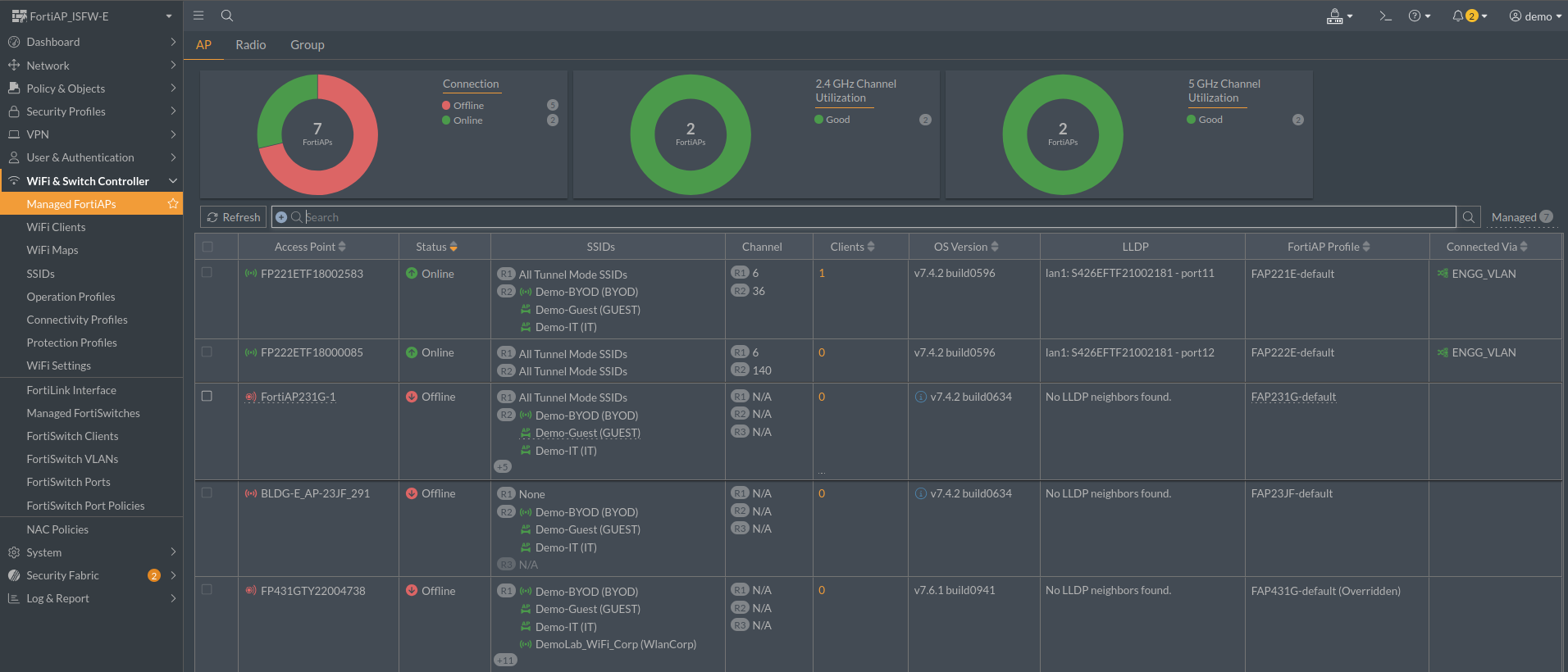
* **Access Control List:** Belirli ağ segmentlerine veya kaynaklara erişimi kontrol etmek için kullanılan daha basit veya daha spesifik kurallar listesidir. Genellikle daha detaylı trafik filtrelemesi için kullanılır.
* **DoS Policy:** Denial of Service (Hizmet Reddi) saldırılarına karşı koruma sağlamak için kullanılan politikalardır. Belirli trafik tiplerine veya hedeflere yönelik anormal trafik akışlarını algılayıp engelleyerek hizmet kesintilerini önlemeye yardımcı olur.
* **Authentication Rules:** Kullanıcıların belirli ağ kaynaklarına veya internete erişmeden önce kimlik doğrulaması yapmasını gerektiren kurallardır. Bu sayede, ağ erişimi kullanıcı bazında kontrol edilebilir.
* **Addresses:** Ağdaki IP adreslerini veya IP aralıklarını temsil eden nesnelerin tanımlandığı yerdir. Bu nesneler, Firewall Policy'ler gibi diğer kurallarda kaynak veya hedef olarak kullanılabilir, bu da yönetimi kolaylaştırır.
* **ZTNA:** Zero Trust Network Access (Sıfır Güven Ağ Erişimi) ile ilgili ayarların yapıldığı bölümdür. Geleneksel VPN'lere göre daha granüler ve güvenli uygulama erişimi sağlamayı hedefler.
* **Internet Service Database:** Bilinen internet servisleri (örneğin, Microsoft 365, Facebook, Netflix) için Fortinet tarafından sağlanan güncel IP adresi ve port bilgilerini içeren bir veritabanıdır. Bu, politikaları belirli servislere göre kolayca yapılandırmanızı sağlar.
* **Services:** Ağdaki belirli protokol ve port numarası kombinasyonlarını temsil eden özel servis nesnelerinin oluşturulduğu yerdir (örneğin, HTTP, HTTPS, SSH veya özel bir uygulama portu). Bu nesneler Firewall Policy'lerde kullanılabilir.



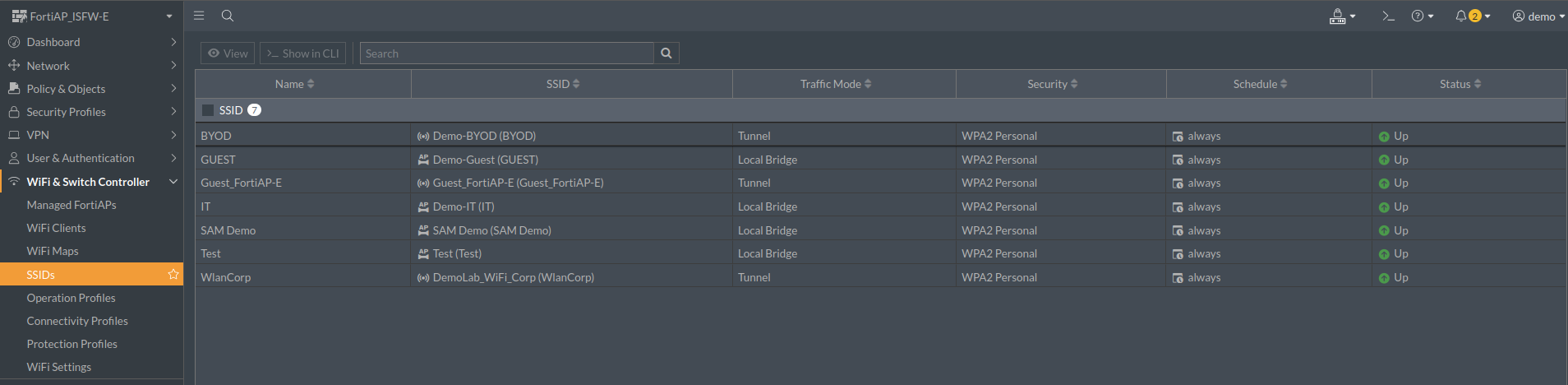
* **Schedules:** Güvenlik politikalarının veya diğer kuralların belirli zaman dilimlerinde veya tarihlerde etkin olmasını sağlayan zamanlama nesnelerinin oluşturulduğu yerdir.
* **Virtual IPs:** Dahili ağdaki sunuculara dışarıdan erişim sağlamak için kullanılan sanal IP adreslerinin (genellikle NAT kuralları için) tanımlandığı bölümdür. Dış IP adresini belirli bir dahili sunucunun IP adresine eşler.
* **IP Pools:** Outbound NAT (kaynak NAT) için kullanılan IP adres havuzlarının tanımlandığı yerdir. Birden fazla dahili kullanıcının tek bir veya bir grup dış IP adresi üzerinden internete çıkmasını sağlar.
* **Protocol Options:** Belirli uygulama protokolleri (HTTP, FTP, SIP vb.) için derinlemesine inceleme (deep inspection) ve güvenlik ayarlarının yapıldığı bölümdür. Uygulama katmanı güvenlik kontrolleri için kullanılır.

**WiFi & Switch Controller**

* **Managed FortiAPs:** Bu bölümde, FortiGate tarafından keşfedilen ve yönetilen tüm FortiAP cihazlarının bir listesini görürsünüz. Her bir AP'nin durumu (online/offline), IP adresi, modeli, seri numarası ve atanan profil gibi detayları buradan izleyebilir ve FortiAP'leri yetkilendirme (authorize) işlemlerini yapabilirsiniz.



* **WiFi Clients:** FortiAP'ler aracılığıyla kablosuz ağınıza bağlı olan tüm Wi-Fi istemcilerinin (telefonlar, dizüstü bilgisayarlar vb.) bir listesidir. Bağlı olan her istemcinin MAC adresi, IP adresi, bağlı olduğu AP, kullanılan SSID ve bağlantı durumu gibi bilgileri buradan gözlemleyebilirsiniz.
* **WiFi Maps:** Büyük alanlarda veya birden fazla FortiAP'nin olduğu yerlerde, AP'lerin fiziksel konumunu bir harita veya kat planı üzerinde işaretlemenizi sağlar. Bu, sinyal kapsama alanını görselleştirmeye ve sorun gidermeye yardımcı olur.
* **SSIDs:** Kablosuz ağ tanımlayıcılarının (Service Set Identifier - SSID) oluşturulduğu ve yapılandırıldığı yerdir. Örneğin, "Kurumsal-Wi-Fi", "Misafir-Wi-Fi" gibi farklı kablosuz ağ adlarını burada tanımlar ve her bir SSID için güvenlik ayarları (WPA2/3, şifreleme), VLAN ataması, misafir portalı gibi özelliklerini belirlersiniz.



* **Operation Profiles:** FortiAP'lerin çalışma özelliklerini tanımlayan profillerdir. Bu profiller, FortiAP'lerin hangi Wi-Fi standartlarını (802.11a/b/g/n/ac/ax), hangi frekansları (2.4GHz, 5GHz), kanal seçimini, güç ayarlarını ve radyo ayarlarını kullanacağını belirler. Birden fazla FortiAP'ye aynı ayarları toplu olarak uygulamak için kullanılır.
* **Connectivity Profiles:** FortiAP'lerin FortiGate ile nasıl iletişim kuracağını ve ağa nasıl bağlanacağını tanımlayan profillerdir. Bu profillerde FortiAP'nin IP adresi alma yöntemi (DHCP/Statik), yönetim VLAN'ı gibi ayarlar bulunur.
* **Protection Profiles:** Kablosuz ağdaki güvenlik tehditlerine karşı koruma sağlayan profillerdir. Bu profil, kablosuz IPS (Intrusion Prevention System), rogue AP algılama (yetkisiz AP'leri tespit etme), kablosuz atak engelleme gibi gelişmiş kablosuz güvenlik özelliklerini içerir.
* **WiFi Settings:** Genel Wi-Fi sistemiyle ilgili global ayarların yapıldığı bölümdür. Örneğin, genel AP discovery (AP keşfetme) ayarları, CAPWAP (Control and Provisioning of Wireless Access Points) tüneli ayarları gibi seçenekleri içerebilir.

**System (Sistem):** Bu, FortiAP'nin genel sistem ayarlarını (donanım yazılımı sürümü, saat ayarları, yönetim erişimi ve potansiyel olarak yüksek kullanılabilirlik yapılandırmaları gibi) kapsayacaktır.

**Log & Report (Günlük ve Rapor):** Bu bölümü anlamak, FortiAP'deki olayları, hataları ve etkinliği görmenizi sağlayacaktır; bu da sorun giderme ve izleme için hayati önem taşır.