Remote Access

Normal şartlarda kurumlarda bulunan FW gibi çeşitli güvenlik ürünleri üzerindeki Web Filter gibi özellikler sayesinde kullanıcıların kurum networkünü olumsuz etkileyecek sitelere erişimi kısıtlanabiliyor. Ne yazık ki kullanıcılar Leptop, tablet gibi taşınabilir cihazlarını farklı networklere bağlayarak kullandıklarında cihazlar kurum çeşitli güvenlik riskleri doğurabiliyor.

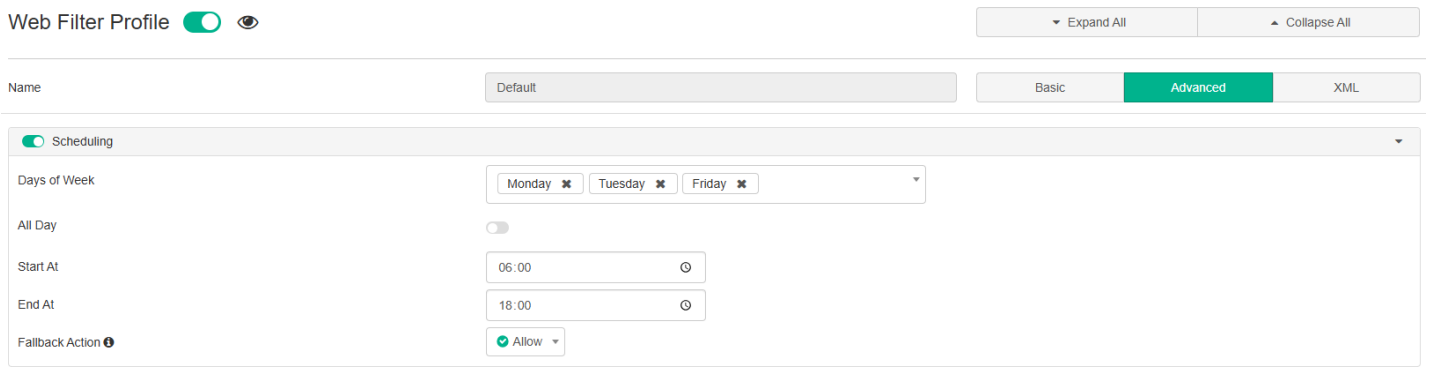
FortiClient yüklü istemcilerin On-Fabric veya Off-Fabric olsalar dahi cihazların kurum networküne dahil olduklarında kurum networkünün zarar vermemeleri için web tarayıcıları üzerinden eriştikleri adreslerin kontrol altında tutulması gerekmektedir. Bu kontrolü sağlayabilmek için Forti EMS uygulamasındaki Web Filter Profile tanımı kullanılmaktadır. Bu uygulamayı ihtiyaçlar doğrultusunda konfigüre edebilmek için "Endpoint Profiles" sekmesi altında bulunan güvenlik özelliklerinin ne için kullanıldığı ve nasıl ayarlandığının bilinmesi gerekiyor. Bu yazıda Endpoint Profiles sekmesi altındaki Web Filter Profile güvenlik özelliğinin kullanım amacını ve nasıl konfigüre edildiği açıklanmaya çalışılacaktır.

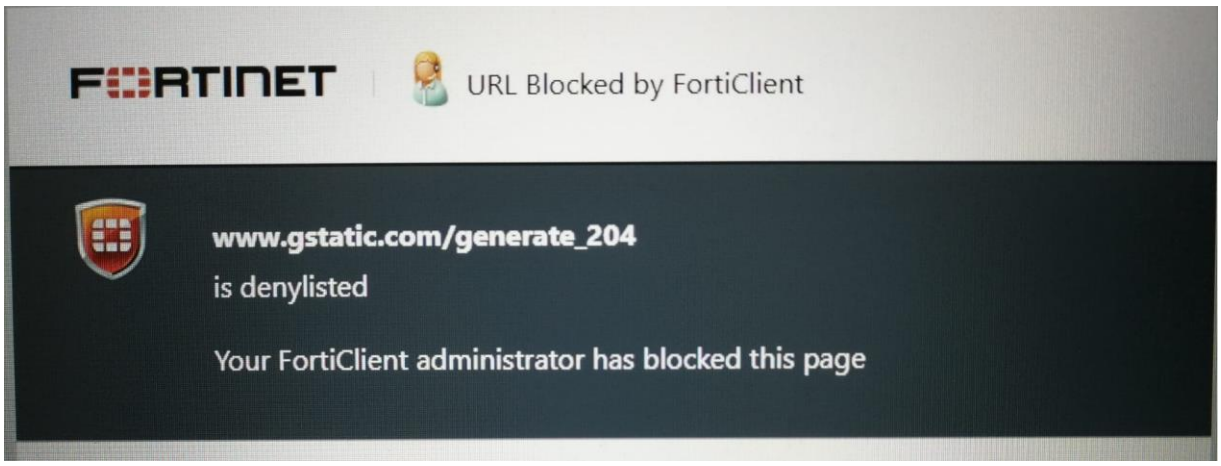
Forti EMS uygulamasındaki Web Filter özelliği ile FortiClient yüklü cihazların nerede ve hangi networke bağlı olduğu fark edilmeksizin (on-Fabric veya off-Fabric olacak şekilde farklı filtrelemeler sağlanabiliyor) cihazların tarayıcı üzerinden erişilmesi istenilmeyen sayfalara erişimi filtrelenebiliyor. Web Filter konfigürasyonu için;

- İlk adımda Web Filter Profile özelliği devreye alınarak bir isim tanımlanaması gerekiyor.

Scheduling, Web Filter özelliğinin belirli zaman aralıklarında çalışması gerektiği durumlarda devreye alınan özelliktir.

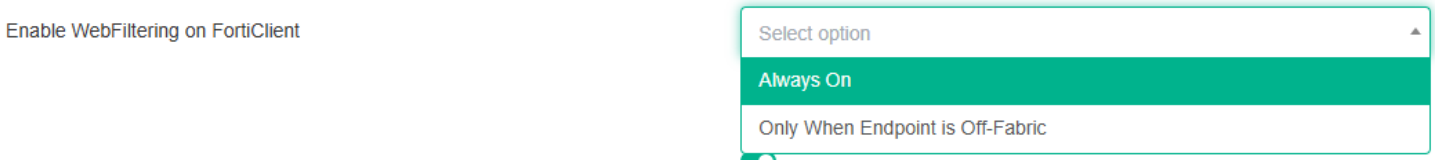
- **Fallback Action** -> Schulading özelliği devreye alınarak Web Filter özelliğinin belirli zaman aralıklarında çalışacağı durumda, özelliğin çalışmadığı zaman aralığında tarayıcı trafiklerinin durumunu belirlemek için kullanılmaktadır (Scheduling dışında Web Filter özelliğini için; Allow, bütün tarayıcı trafiklerine izin verecektir. Block, Web filter özelliğinde **Exclusion List** kısmında izin verilen adresler dışındaki bütün tarayıcı trafiklerini bloklayacaktır).





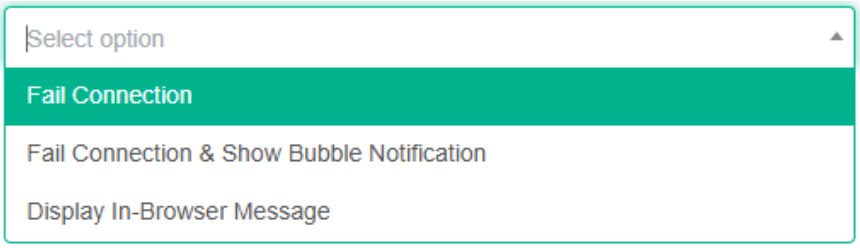
General, Web Filter özelliğinin genel ayarlamalarını yapmak için kullanılan alandır.

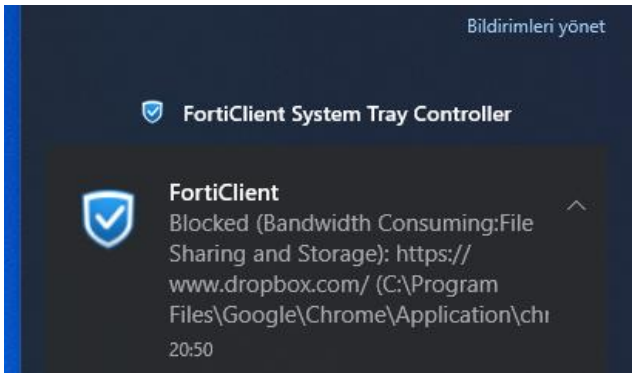
- **Request Timeout** ->
- **Enable WebFiltering on FortiClient** -> cihazların sadece On-Fabric veya sadece Off-Fabric durumda olduklarında Web Filter özelliğinin devreye alınması istendiği durumlarda devreye alınıyor.



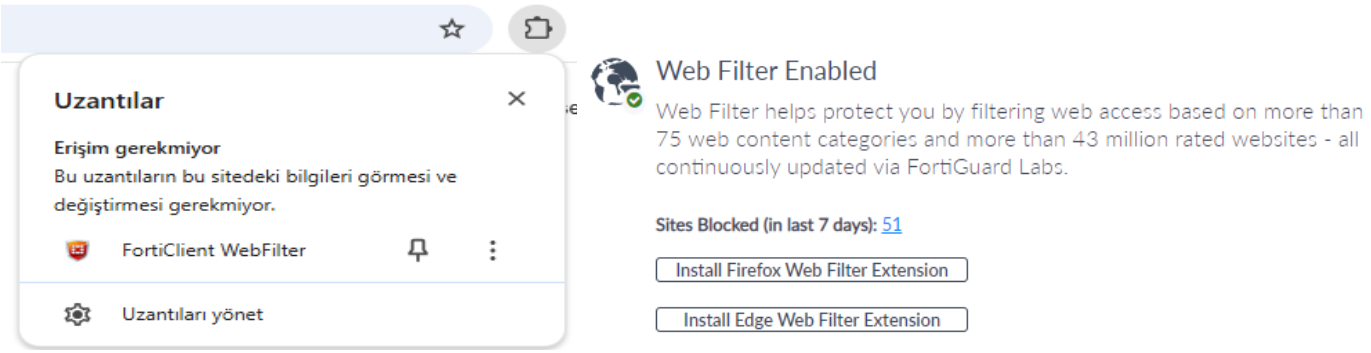
- **Log All URLs** -> FortiClient üzerinde Web Filter özelliği kapsamında oluşan bütün URL'lerin loglanılması istendiğinde devreye alınan özelliktir. Bu özellik devre dışı bırakıldığında FortiClient istemcisi sadece Web Filter kapsamında kategori olarak veya URL olarak belirlenen URL'leri loglar.
- **Log User Initiated Traffic** -> kullanıcının başlattığı trafiklerin loglanması istendiği durumda devreye alınan özelliktir.

- **Action On HTTPS Site Blocking** -> Web Filter özelliğiyle erişimi engellenen sitelere giriş yapılmak istendiğinde kullanıcıya nasıl bir bildiri gönderileceğini belirlemek için kullanılan seçenektir. Bu süreçte uygulanabilecek 3 seçenek bulunuyor.
    - **Fail Connection**, erişilesi istenmeyen bir sayfaya erişilmeye çalışılması durumunda kullanıcıya herhangi bir bildiri yapılmamasını sağlamak için kullanılıyor. Varsayılanda seçili gelen seçenektir.
    - **Fail Connection & Show Bubble Notification**, erişilesi istenmeyen bir sayfaya erişilmeye çalışılması durumunda erişilmeye çalışılan sitenin engellendiğine dair kullanıcıya bildirim gönderilmesi istendiğinde tercih edilen seçenektir.
    - **Display In-Browser Message**, erişilesi istenmeyen bir sayfaya erişilmeye çalışılması durumunda erişilmeye çalışılan sitenin engellendiğine dair sadece tarayıcı üzerinden kullanıcıya bildirim gönderilmesi istendiğinde tercih edilen seçenektir.

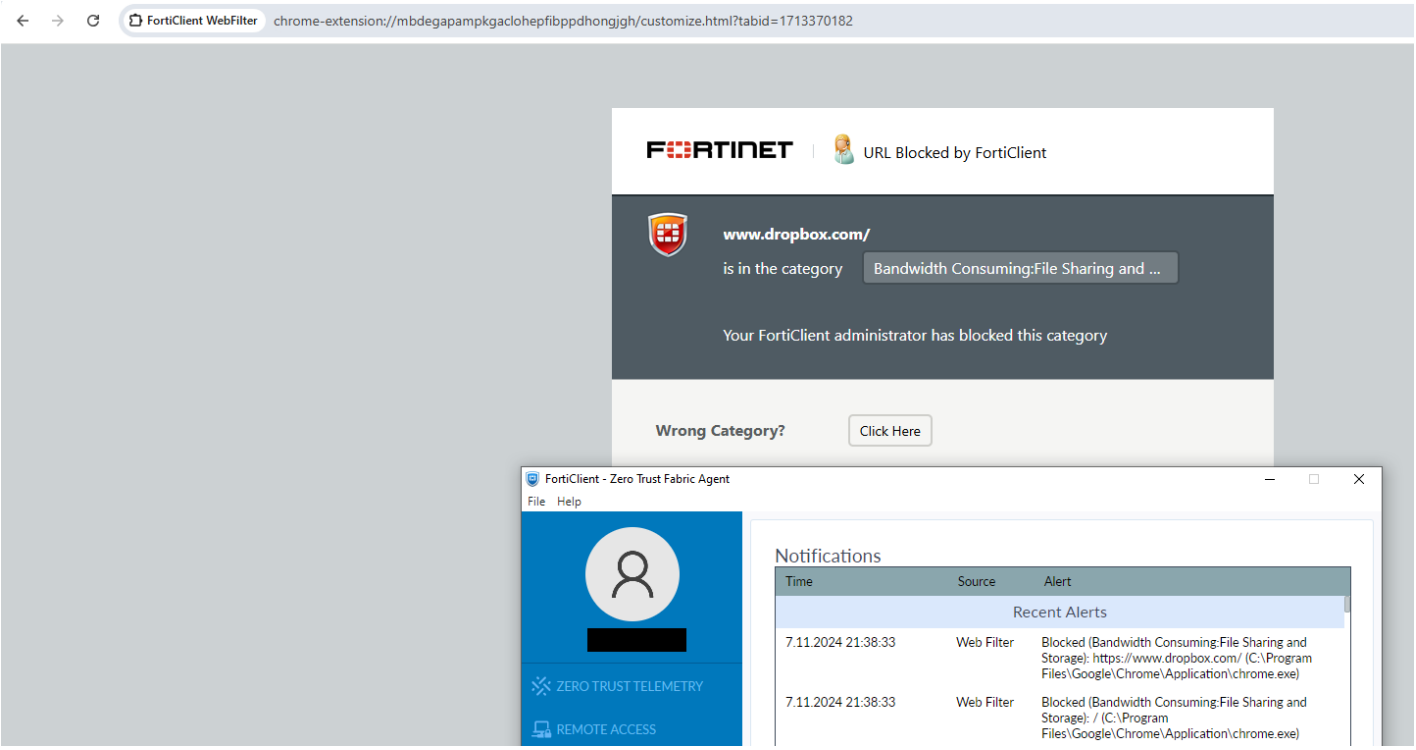




- **Enable Web Browser Plugin for Web Filtering** -> HTTPS protokolü kullanan sitelerde Web Filter özelliğiyle belirlenen filter tanımlarının daha sağlıklı çalışabilmesi için devreye alınmaktadır. Bu özellik devreye alındığında Google Chrome, Mozilla Firefox ve Microsoft Edge tarayıcılarında Web Filter eklentisi otomatik olarak eklenir.



  - **Sync Mode** -> web tarayıcısı başka bir HTTPS isteği göndermeden önce bir HTTPS isteğinden yanıtının beklenmesi için devreye alınan özelliktir.
  - **Check User Initiated Traffic Only** -> Web tarayıcısı eklentisini yalnızca kullanıcı tarafından başlatılan trafik için kullanın. Bu özellik devreye alındığında daha az işlem yapılacağı için daha hızlı çalışılmasını sağlar. Bu özellik devre dışı bırakıldığında, eklenti tüm URL isteklerini kontrol eder.

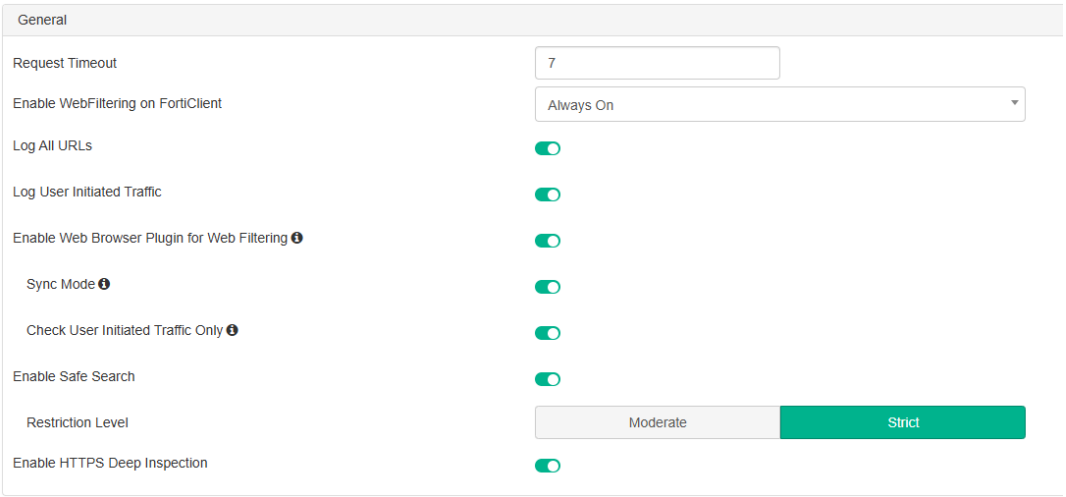


- **Enable Safe Search** -> Windows işletim sistemi kullanan cihazlar ve Chromebook'lar için bu özellik etkinleştirilerek Kısıtlama Düzeyini Strict veya Moderate olarak yapılandırılabiliyor. Bu özellikle son kullanıcıların YouTube, Google ve Bing dahil olmak üzere arama motoru üzerinden erişebileceği içeriği etkiler. Chromebook'lar için YouTube erişimini kısıtlanmamış olarak ayarlamak için Safe Search özelliği devre dışı bırakabilir. Google Arama ve YouTube erişimini FortiClient EMS yerine Google Yönetici Konsolu ile yapılandırılabilir.

  MacOS işletim sistemi kullanan son kullanıcılar için Safe Search etkinleştirildiğinde uç noktanın Google aramasını kısıtlanmış moda ve YouTube erişimini sıkı kısıtlanmış erişime ayarlar. Safe Search özelliğini devreye alındığında arama motoru isteklerini yeniden yönlendirmek için Yandex.ru dahil olmak üzere kayıtları istemci cihazının ana bilgisayar dosyasına ekler.

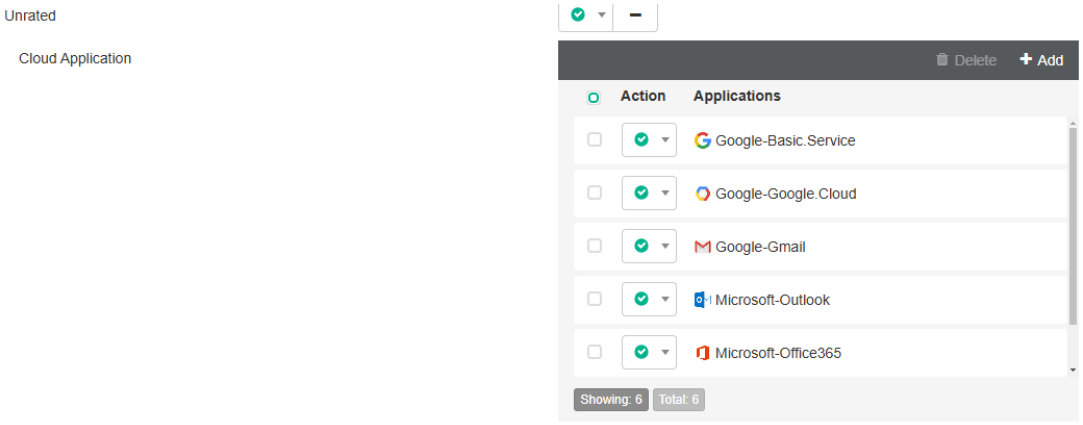
  - Video Filter ve Web Filter özelliklerindeki Safe Search özelliği etkinleştirilebilir. Bu nitelik her iki özellikte de etkinleştirildiğinde, YouTube'a daha kısıtlayıcı ayarlar uygulanır.

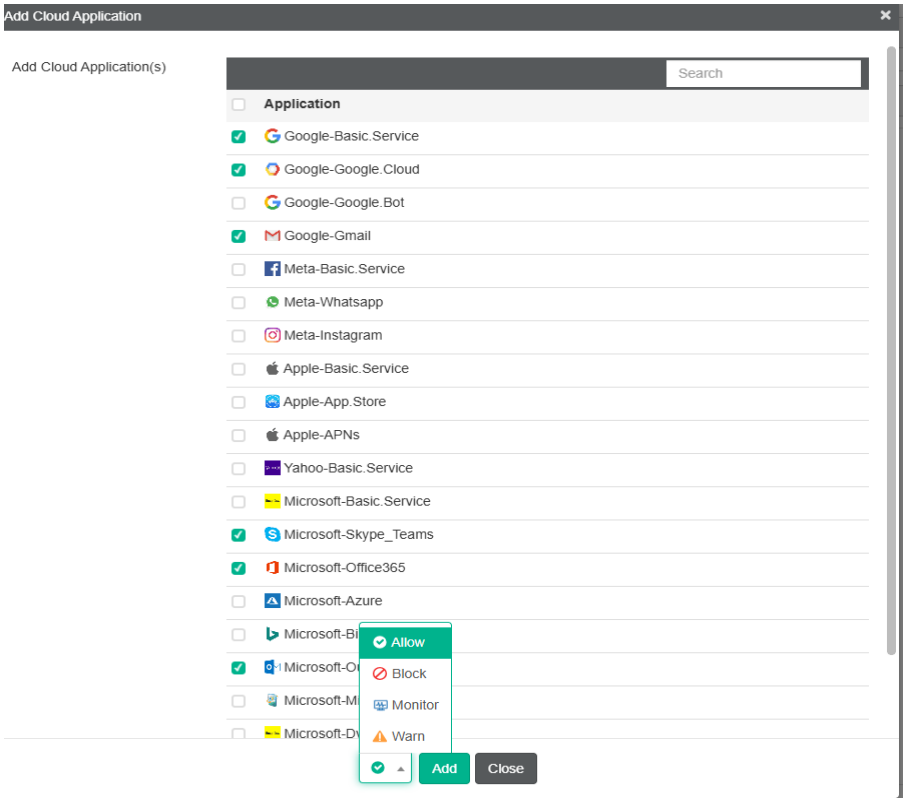
- **Enable HTTPS Deep Inspection** -> SSL/TLS ile şifrelenen (HTTPS protokolü kullanılan) trafiklerinde FortiClient istemcisinin Proxy'lik yapıp paketlerin şifrelerinin çözümlenerke içeriğinin incelenebilmesini ve bu sayede daha sağlıklı filtreleme işleminin yapılabilmesi sağlayabilmek için devreye alınan özelliktir.



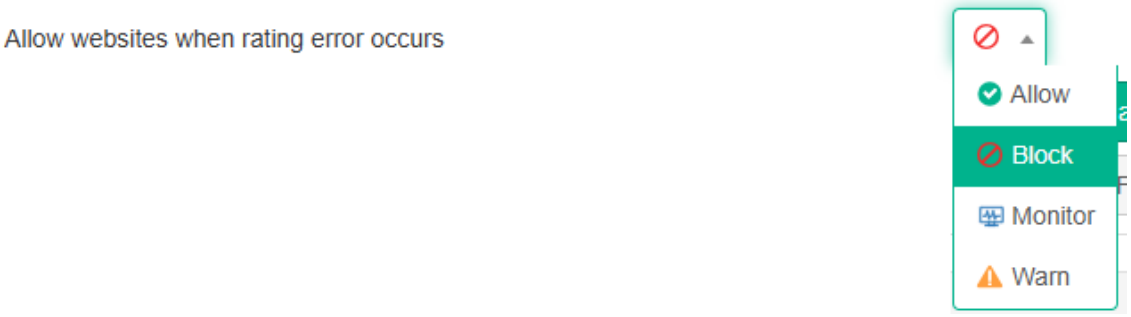
Categories, Fortinet'in Web Filter özelliği kapsamında web sayfalarını değerlendirip kategorize ettiği ve bu kategoriler kapsamında web sayfaların filtrelendiği alandır. Burada kategoriler için **Allow, Block, Monitor** ve **Warning** olmak üzere 4 farklı aksiyon tipi belirlenebiliyor.

- **Unrated** -> FortiGuard servisinin derecelendirilmemiş olarak sınıflandırdığı (herhangi bir kategoriye dahil edilmeyen siteler) sitelerde uygulanacak aksiyon tipini belirlemek için kullanılan alandır.
    - FortiClient, FortiGuard'ın derecelendirilmemiş olarak sınıflandırdığı belirli bulut uygulamaları için derecelendirilmemiş bir IP adresi alırsa, yedek olarak Internet Service DB (ISDB) kullanabilir. Bulut uygulamaları için Derecelendirilmemiş kategorisini genişletebilir ve ISDB'yi kullanarak seçili bulut uygulamaları için bir aksiyon tanımı yapılabilir.



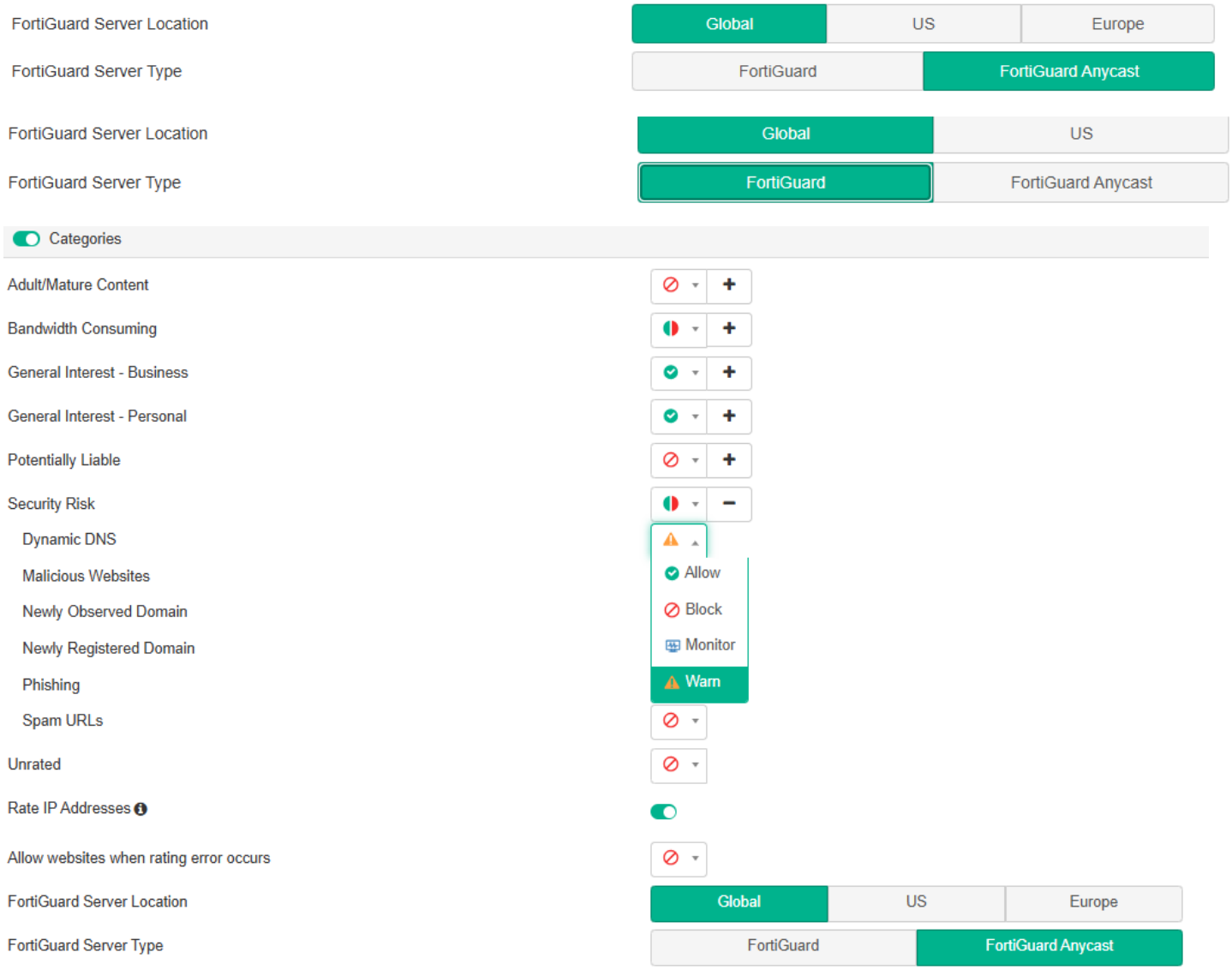


- **Rate IP Addresses** -> Hedef sitelerin URL ve IP adreslerine göre ayrı ayrı derecelendirilmesi istendiği durumlarda devreye alınan özelliktir. Bu sayede FortiGuard hizmetinin Web Filter özelliğinin atlatılmasına karşın ek güvenlik sağlanmış oluyor.
    - Hedef sitenin Alan adı ile IP adresi farklı derecelendirilmesi durumunda karar verme surecinde hedef adres ile ilişkili olan diğer kategorilerin genel durumu göz önünde bulundurulur ve bu kategorilerin geneline uygulanan aksiyon belirlenerek karara varılır.
- **Allow websites when rating error occurs** -> Web Filter özelliğinin geçici olarak FortiGuard hizmetiyle iletişim kuramaması durumunda bu ayar, bağlantı yeniden sağlanana kadar ünitenin üzerinde bulunan kayıtlar üzerinden hangi erişime izin vereceğini belirler. FortiGuard hizmetine erişim kesildiğinde bu hizmet etkinleştirilirse, URL'nin derecesi önbellekteyse, Web Filter özelliği önbelleğe alınan o derece için eşleşen profil eylemini uygular (Block, Warning, Monitor, Allow …). URL'nin derecesi önbellekte yoksa burada belirlenen aksiyon tipini uygulayacaktır;
    - **Block** -> Önbellekte bulunmayan herhangi bir web sitesine erişimi engeller. Bu, uç noktaların tutsak portallara erişmesini önleyebilir.
    - **Warn**-> Önbellekte bulunmayan herhangi bir web sitesine devam etmek istendiğinde kullanıcıya uyarı sayfası çıkarılmasını sağlar.
    - **Allow**-> Önbellekte bulunmayan tüm web sitelerine erişim izin verir.
    - **Monitor**-> Site erişimmlerini loglar.



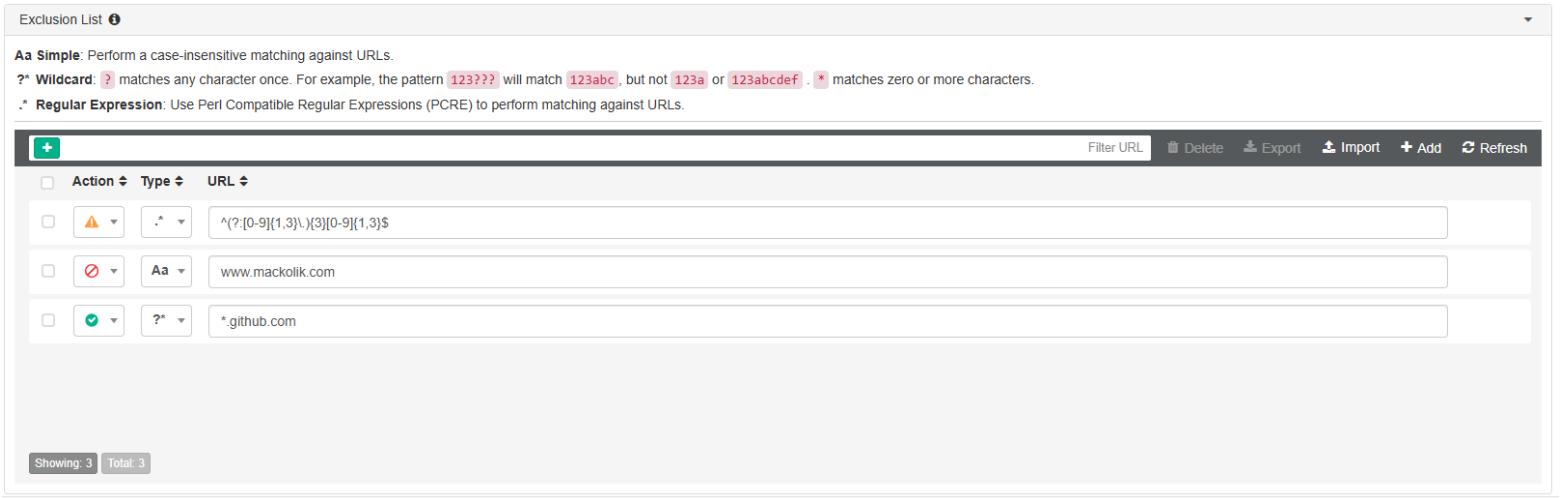
- **Use HTTPS Rating Server** -> Varsayılanda Web Filtresi URL derecelendirme istekleri UDP protokolü kullanılarak FortiGuard derecelendirme sunucusuna gönderir. Bu isteklerin TCP protokolü aracılığıyla göndermek için bu özellik etkinleştirilebiliyor.
- **FortiGuard Server Location / FortiGuard Server Type** -> Dünya üzerinde hangi lokasyondaki FortiGuard sunucusuna nasıl bağlanacağını belirlemek için kullanılan alandır.

- FortiGuard sunucu alanı için FortiGuard Anycast seçiliyse, Global, ABD veya Avrupa arasından seçim yapılabiliyor.
  - Global: fctguard.fortinet.net
  - U.S.: fctusguard.fortinet.net
  - Europe: fcteuguard.fortinet.net
- FortiGuard sunucu seçimi için FortiGuard seçiliyse, Global veya ABD arasından seçim yapılabiliyor.
  - Global: fgd1.fortigate.com
  - U.S.: usfgd1.fortigate.com



Exclusion List, FortiGuard sunucusu tarafından derecelendirilerek kategorize edilen hedef adresler arasında istisnai durumları tanımlamak için kullanılan alandır. Temel anlamda ilk kısımda uygulanacak aksiyon tipi belirlenmelidir. İkinci kısımda ise giriş yapılacak hedef adresin tipi belirlenmelidir. Son olarak hedef adres tanımı yapılmalıdır.

- Exclusion List kısmının sağlıklı çalışabilmesi için burada 1000 ‘den fazla tanım yapılması önerilmiyor.



- İsteğe bağlı olarak Fortigate FW üzerinde tanımlı Exclusion List tanımları Export edilip buraya doğrudan import edilebiliyor.

Notlar

- Kullanıcılar erişmek istediği bir siteye erişememesi durumunda FortiClient istemcisi üzerinde “Notifications” kısmında erişimin engellenmesine dair kayıtlar görüntüleniyor.
- Fortigate FW Forti EMS ürünü ile FortiGuard üzerinden bağlandığı takdirde Fortigate üzerinde halihazırda kullanılan Web Filter tanımları EMS ‘e doğrudan çekilebiliyor (https[:]//docs.fortinet.com/document/forticlient/6.2.0/new-features/96529/automated-syncing-of-the-fortigate-web-filter-profile).

Kaynaklar

- https[:]//fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/f49d7ea5-afe9-11ea-8b7d-00505692583a/FortiClient_EMS_6.4.1_Administration_Guide.pdf
- https[:]//docs.fortinet.com/document/forticlient/7.4.0/ems-administration-guide/68075/web-filter
- https[:]//docs.fortinet.com/document/forticlient/6.2.0/new-features/96529/automated-syncing-of-the-fortigate-web-filter-profile