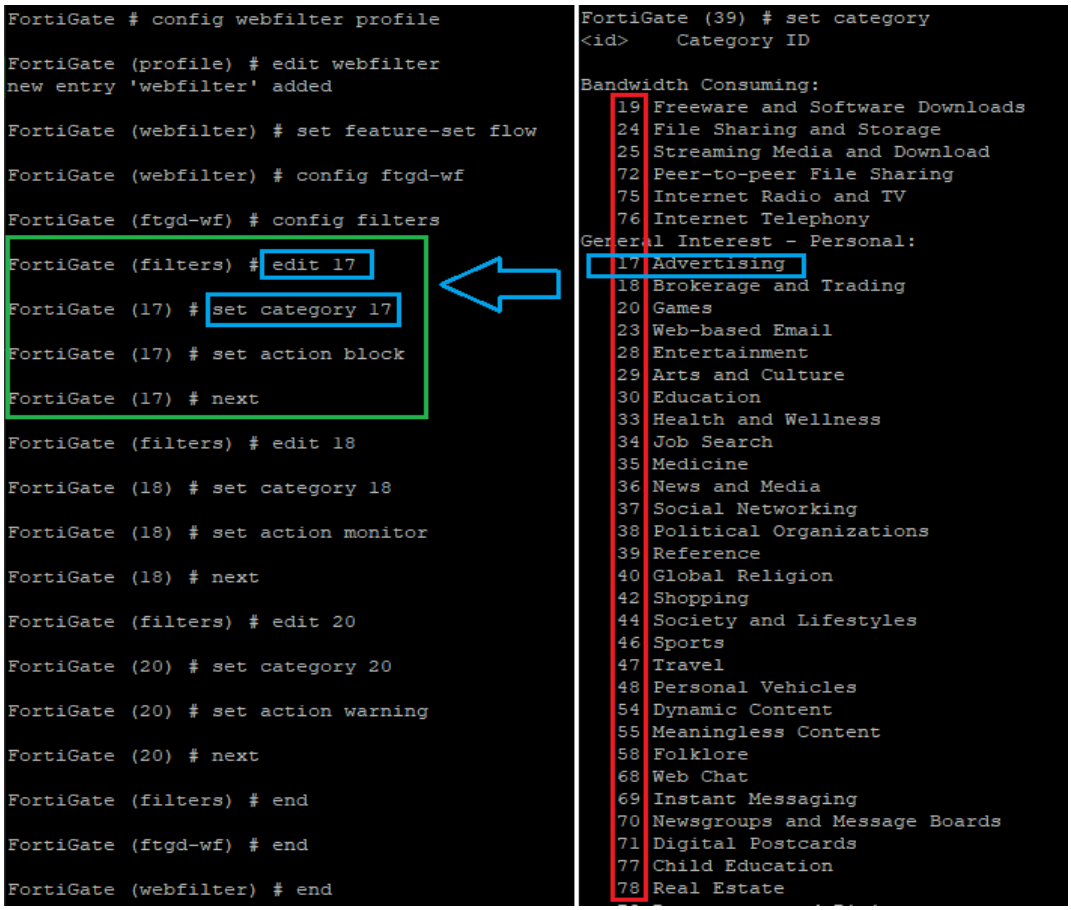
Web Filter and App Control Configuration

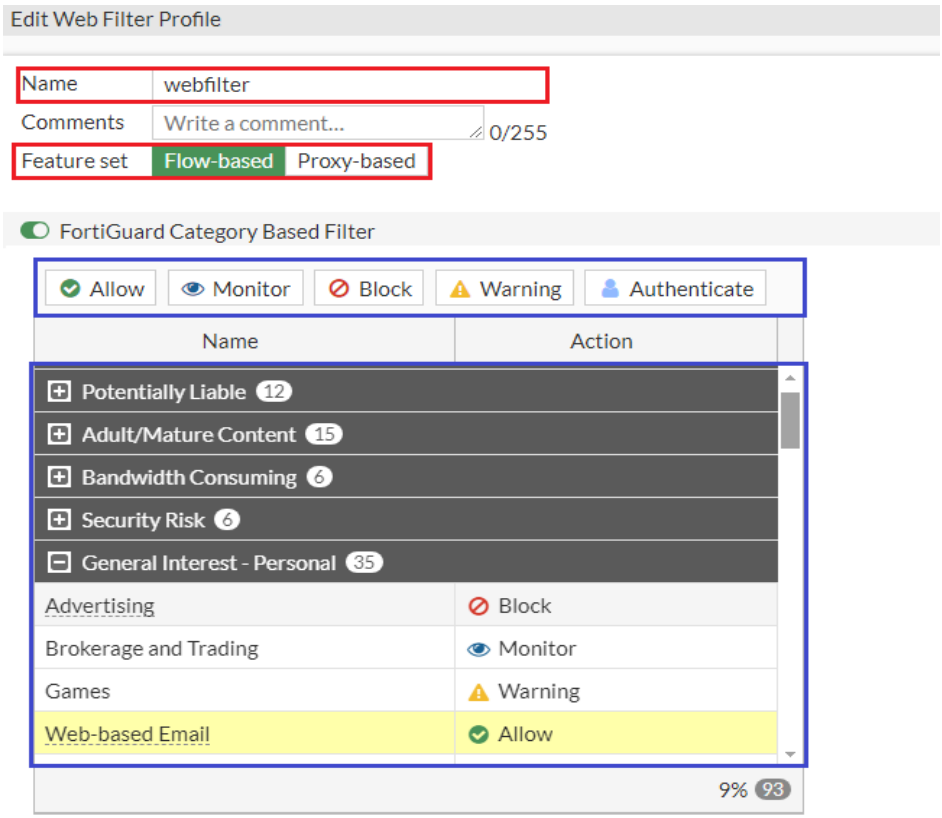
Networke bağlı istemcilerin internete çıkışlarını kısıtlamak veya daha güvenli çıkış yapabilmelerini sağlamak için istemci trafikleri üzerinde çeşitli özellikler devreye alınabiliyor. Bu yazıda bu özelliklerden Web Filter ve Application Control özellikleri açıklanmaya çalışılacaktır.

Web Filter

Web Filter özelliği istemcilerin web tarayıcıları üzerinde erişilmesi istenmeyen çeşitli kategorilerdeki web sayfalarına, fidye yazılımı, kimlik avı ve diğer web kaynaklı saldırılar gibi tehditlere karşı tehdit barındıran sitelere erişimleri kısıtlamak için kullanılan özelliktir. Konfigürasyonu için "**Security Profiles -> Web Filter -> Create New**" yolu takip edilerek;

- **Name** :Tanımlanacak Web Filter Profile'a isim tanımı yapılmalıdır.
- Web Filter tanımının Prox şekilde mi Flow şekilde mi çalışacağı belirtilmelidir.
- Tarayıcı üzerindeki sitelerin kategori bazında filtre uygulanmak isteniyorsa "**FortiGuard Category Based Filter**" kısmı devreye alınarak burada bulunan kategorilere 5 farklı aksiyon (Allow, Monitor, Block, Warning, Authenticate) tipinden birisinin uygulanması gerekiyor.
    - Kategorilerin varsayılanda gelen aksiyon tiplerinde değişiklik yapılmak istendiğinde komut satırında bir "**edit <Edit Value>**" tanımı altında "set categoriy <Categoriy Number>" komutuyla ilgili kategori seçilip "**set action <Action Type>**" komutuyla aksiyon tipi değiştiriliyor.





- Belirli bir kullanıcı veya kullanıcı grubunun bir zaman arağında farklı bir Web Filter Policy tanımı uygulanması isteniyorsa "**Allow users to override blocked categories**" kısmı devreye alınabiliyor. Bu özelliğin nasıl devreye alınacağı farklı bir yazının konusu olacaktır.
- Kategori temelli filtrelerin yanında ek tanımlar da eklenmek güvenlik özelliklerini de devreye alabilmek için "**Static URL Filter**" kısmında;
    - **Block invalid URLs** :SSL sertifikasın CN alanı geçerli bir alan adı içermediğinde web sitelerini engellemek için etkinleştirilebilir.

```
FortiGate # config webfilter profile

FortiGate (profile) # edit "webfilter"

FortiGate (webfilter) # set options block-invalid-url

FortiGate (webfilter) # end
```

    - **Block malicious URLs discovered by FortiSandbox** :FortiSandbox tarafından keşfedilen kötü amaçlı URL'leri engellemek için devreye alınabilen özelliktir.

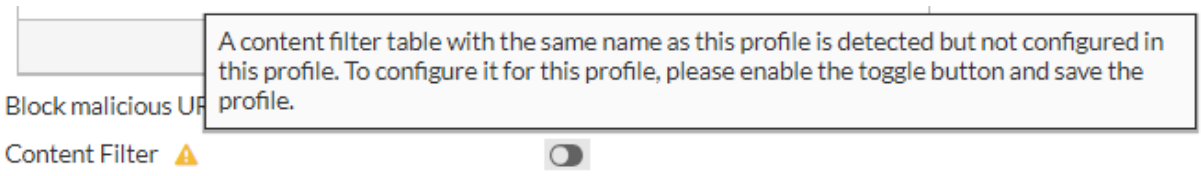
```
FortiGate # config webfilter profile

FortiGate (profile) # edit webfilter
                      Web Filter Profile Name
FortiGate (webfilter) # config web

FortiGate (web) # set blocklist enable

FortiGate (web) # end

FortiGate (webfilter) # end
```

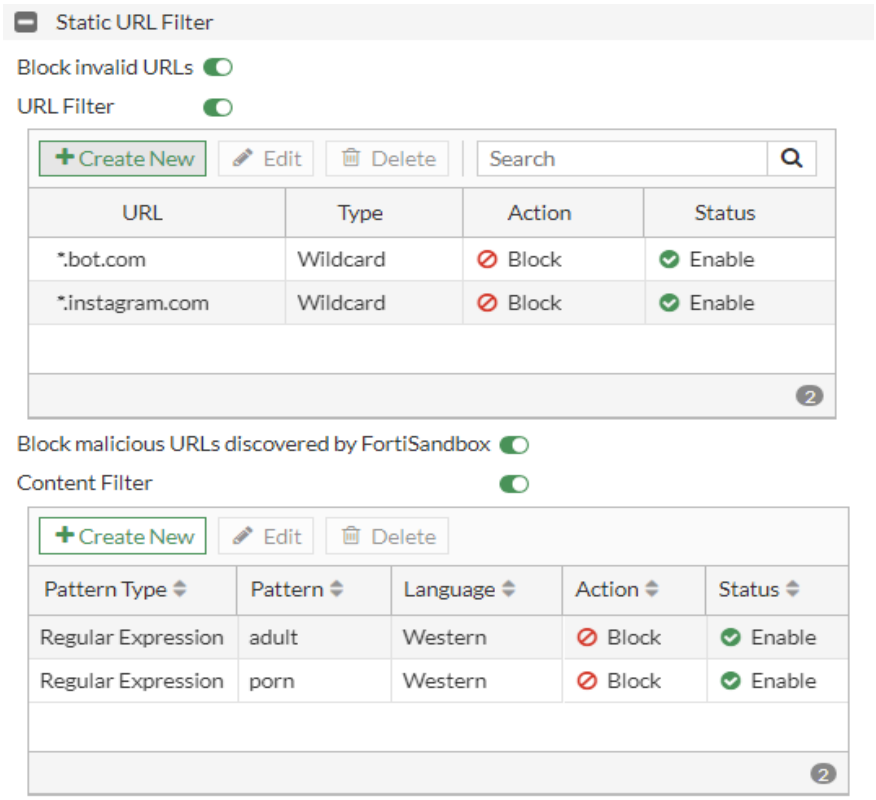
- **URL Filter** :Belirli/spesifik bir URL için Statik/Manuel bir URL tanımı yapılarak bu URL'e erişilmek istendiğinde uygulanması istenen aksiyon belirtilebiliyor. Kullanımına örnek olarak belirli bir kategoriye ait sitelerin tamamının değil de bu kategorideki sadece spesifik birkaç sitenin filtrelenmesi için kullanılabilir.
- **Content Filter** :Belirtilen kalıpları/örüntüleri/metinleri içeren web sayfalarına erişimleri filtrelemek için kullanılan bir özelliktir.

```
FortiGate # config webfilter urlfilter

FortiGate (urlfilter) # edit 1
new entry '1' added

FortiGate (1) # set name webfilter
                Web Filter Profile Name
FortiGate (1) # config entries

FortiGate (entries) # edit 1
new entry '1' added

FortiGate (1) # set url "*.bot.com"

FortiGate (1) # set type wildcard

FortiGate (1) # set action block

FortiGate (1) # set status enable

FortiGate (1) # next

FortiGate (entries) # edit 2
new entry '2' added

FortiGate (2) # set url "*.instagram.com"

FortiGate (2) # set type wildcard

FortiGate (2) # set action block

FortiGate (2) # set status enable

FortiGate (2) # next

FortiGate (entries) # end

FortiGate (1) # next

FortiGate (urlfilter) # end
```

```
FortiGate # config webfilter content

FortiGate (content) # edit 1
new entry '1' added

FortiGate (1) # set name webfilter
                Web Filter Profile Name
FortiGate (1) # config entries

FortiGate (entries) # edit adult
new entry 'adult' added
Web sayfalarında eşlenecek Pattern tanımı
FortiGate (adult) # set pattern-type regexp

FortiGate (adult) # set status enable

FortiGate (adult) # set lang western

FortiGate (adult) # set score 10

FortiGate (adult) # set action block

FortiGate (adult) # next

FortiGate (entries) # edit porn
new entry 'porn' added

FortiGate (porn) # set pattern-type regexp

FortiGate (porn) # set status enable

FortiGate (porn) # set lang western

FortiGate (porn) # set score 10

FortiGate (porn) # set action block

FortiGate (porn) # next

FortiGate (entries) # end

FortiGate (1) # end
```

- **URL Filter** ve **Content Filter** özellikleri web arayüzü üzerinden doğrudan tanımlanabiliyor. Eğer ki bu tanımlamalar komut satırı üzerinden gerçekleştiriliyorsa tanım sonrasında web arayüzüne giriş yapılarak bu özelliklerin ayrıca devreye alınması (Toggle Button yardımıyla) gerekiyor (Komut satırı üzerinde tanım yapıldıktan sonra web arayüzünde kullanıcıyı aşağıdaki gibi bir uyarı karşılayacaktır).



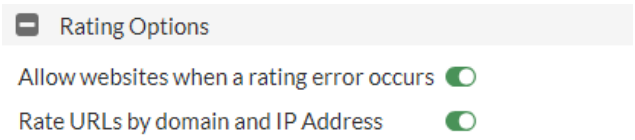


- **Allow websites when a rating error occurs** :Fortigate'in geçici olarak FortiGuard hizmetiyle iletişim kuramaması durumunda bu ayar, bağlantı yeniden sağlanana kadar ünitenin üzerinde bulunan kayıtlar üzerinden hangi erişime izin vereceğini belirler. **FortiGuard hizmetine erişim kesildiğinde bu hizmet etkinleştirilirse,** URL'nin derecesi önbellekteyse, FortiGate önbelleğe alınan o derece için eşleşen profil eylemini uygular (Block, Warning, Monitor, Allow …). URL'nin derecesi önbellekte yoksa, FortiGate varsayılan olarak "Allow" seçeneğine ayarlanacak ve trafiğe izin verecektir. Devre dışı bırakılırsa kullanıcıların hiçbir web sitesine erişmesine izin verilmeyecektir (Web Filter özelliğinin FortiGuard hizmeti üzerinden filtreleme veritabanını güncelleyemediği durumlarda kullanılabiliyor).

FortiGuard hizmetinden Web Filter veritabanını çekemediğini kontrol etmek için "System -> FortiGuard -> Filter" yolu izlenebilir.

- **Rate URLs by domain and IP Address** :IP adreslerine yönelik Web Filtresi derecelendirmeleri, URL'lere yönelik derecelendirmeler kadar hızlı güncellenmez. Bu farklılık bazen Fortigate'in engellenmesi gereken sitelere erişim izni vermesine veya izin verilmesi gereken siteleri engellemesine neden olabilir. Bu özellik sayesinde erişilmek istenen sitelerin URL ve IP adresine göre ayrı ayrı derecelendirilmesi sağlanarak daha etkili filtreleme işlemine tabi tutulması sağlanabiliyor.

```
FortiGate # config webfilter profile

FortiGate (profile) # edit webfilter

FortiGate (webfilter) # config ftgd-wf

FortiGate (ftgd-wf) # set options error-allow rate-server-ip

FortiGate (ftgd-wf) # end

FortiGate (webfilter) # end
```



Application Control

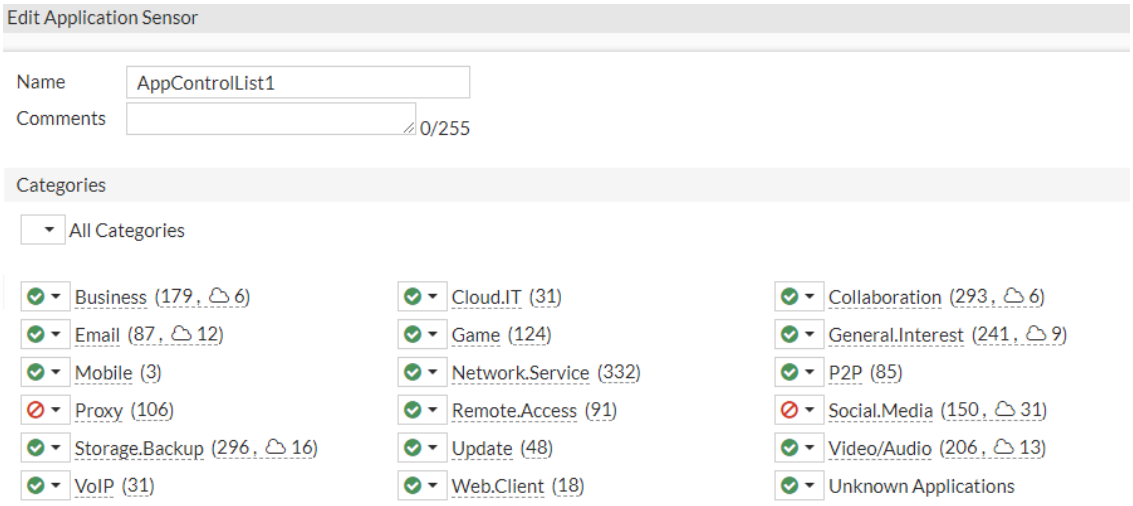
Tarayıcı üzerinden oluşturulan trafiklere üzerinde çeşitli filtreleme işlemleri yapılabildiği gibi istemci üzerinde yüklü uygulamaların trafikleri üzerinde de filtreleme işlemi yapılabiliyor. Konfigürasyonu için "**Security Profiles -> Application Control -> Create New**" yolu takip edilerek;

- **Name** :Tanımlanacak Application Control listesine bir isim tanımı yapılmalıdır.
- **Categories** :Burada kategorize edilen trafik türleri için uygulanması istenen üç aksiyon tipinden biri seçilmelidir.
    - Bu tanımları komut satırında yaparken "**set category <Category Number>**" komutunda kategori numarası belirtilmediği takdirde sonraki satırında belirtilen aksiyon tanımı bütün trafik kategorilerine uygulanıyor. (Örnek olarak 1. tanım altında "**set category 23**" tanımı yerine "**set category**" tanımı yapılmış olsaydı, sonraki satırında belirtilen "**set action block**" komutu bütün kategorilere uygulanacaktı).

```
FortiGate # config application list

FortiGate (list) # edit AppControlList1
new entry 'AppControlList1' added

FortiGate (AppControlList1) # config entries

FortiGate (entries) # edit 1
new entry '1' added

FortiGate (1) # set category 23

FortiGate (1) # set action block

FortiGate (1) # next

FortiGate (entries) # edit 2
new entry '2' added

FortiGate (2) # set category 6

FortiGate (2) # set action block

FortiGate (2) # end

FortiGate (AppControlList1) # end
```

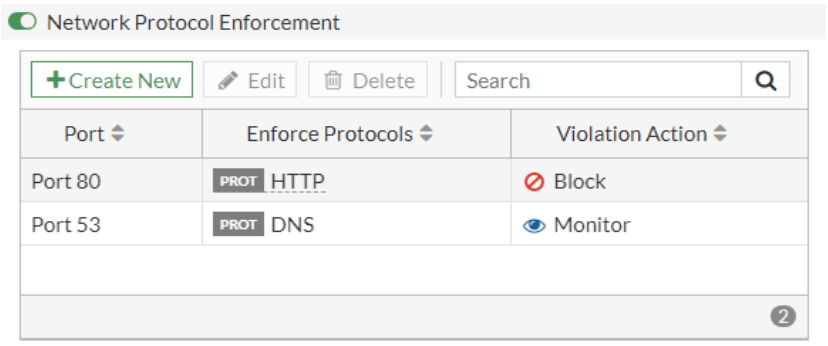
```
FortiGate (1) # set category
ID              Select Category ID
2               P2P
3               VoIP
5               Video/Audio
6               Proxy
7               Remote.Access
8               Game
12              General.Interest
15              Network.Service
17              Update
21              Email
22              Storage.Backup
23              Social.Media
25              Web.Client
26              Industrial
28              Collaboration
29              Business
30              Cloud.IT
31              Mobile
```

"

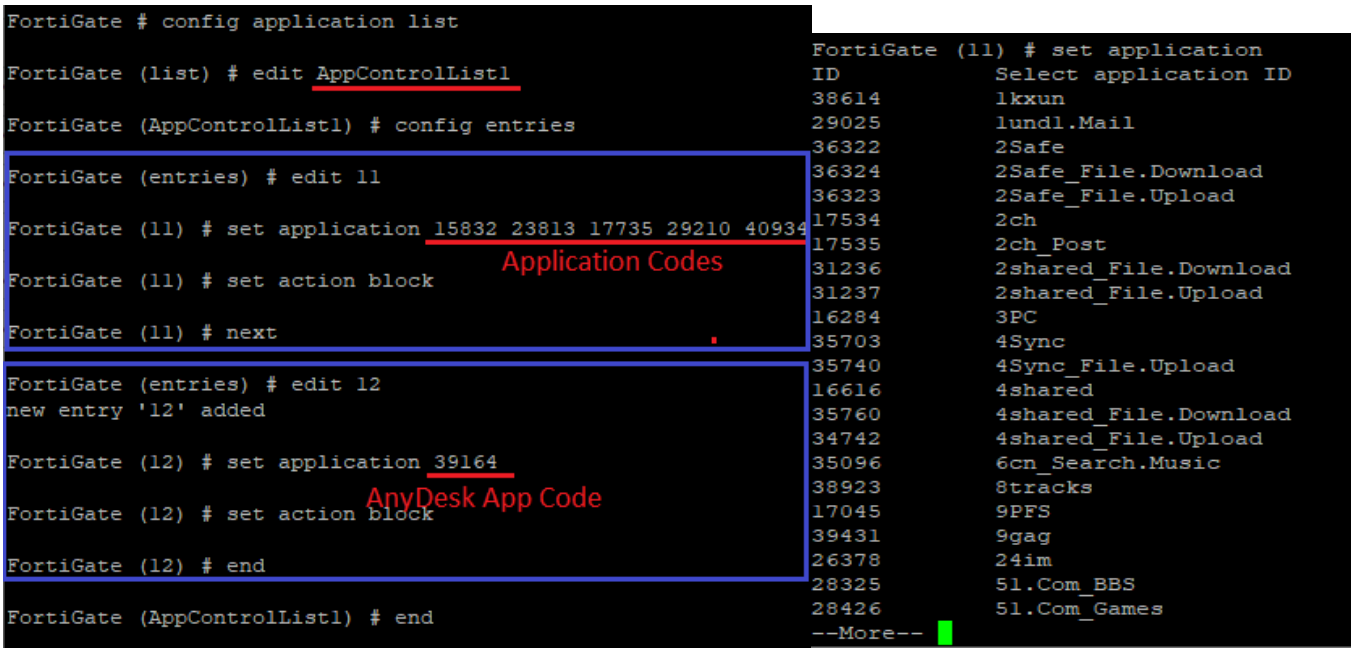


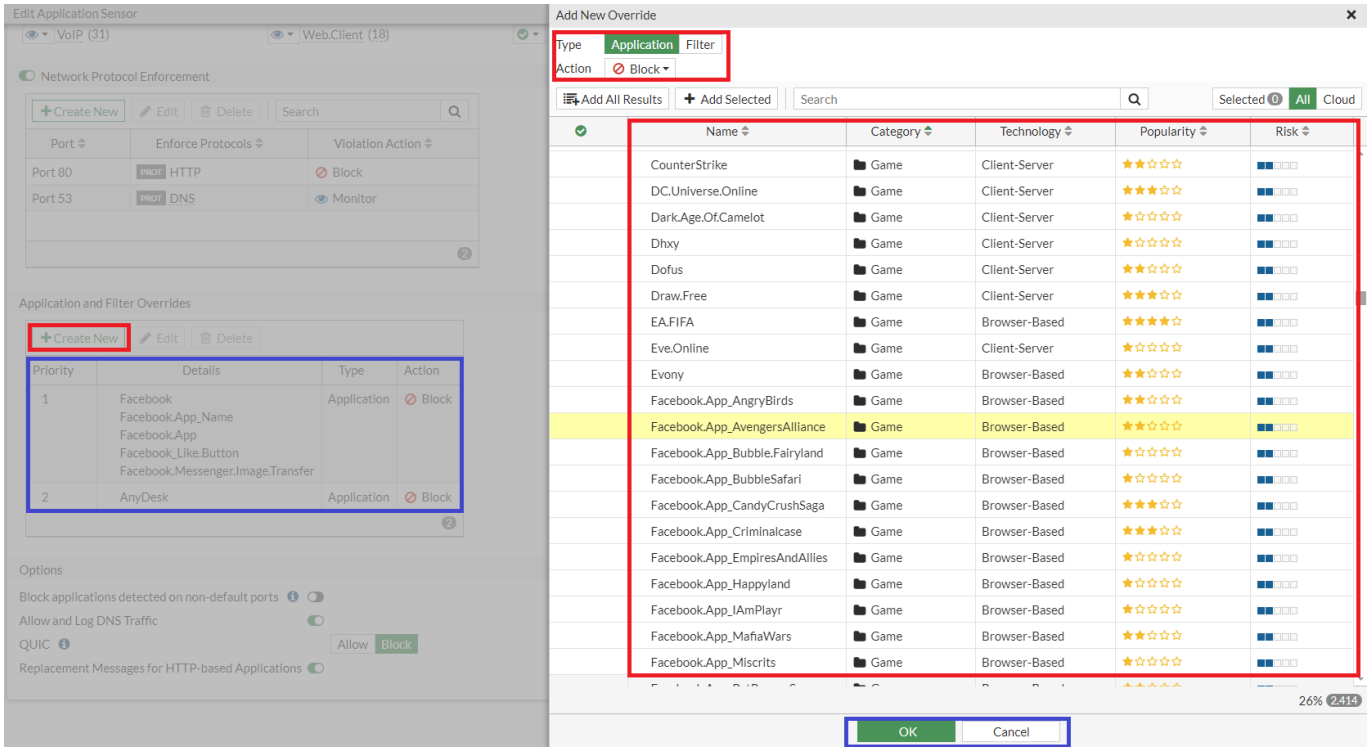
- **Network Protocol Enforcement** :Uygulama trafiklerinde port/protokol bazlı filtreleme işlemi yapabilmeyi sağlana özelliktir. Bu kısımda hangi port için hangi aksiyonun uygulanacağı belirtilmelidir.

```
FortiGate # config application list

FortiGate (list) # edit AppControlList1

FortiGate (AppControlList1) # set other-application-log enable

FortiGate (AppControlList1) # set control-default-network-services enable

FortiGate (AppControlList1) # config default-network-services

FortiGate (default-network-~ces) # edit 1
new entry '1' added

FortiGate (1) # set port 80

FortiGate (1) # set services http

FortiGate (1) # set violation-action block

FortiGate (1) # next

FortiGate (default-network-~ces) # edit 2
new entry '2' added

FortiGate (2) # set port 53

FortiGate (2) # set services dns

FortiGate (2) # set violation-action monitor

FortiGate (2) # end

FortiGate (AppControlList1) # end
```



- **Application and Filter Overrides** :"**Category**" kısmında kategori olarak filtre uygulanıyordu. Burada ise kategori kapsamına genel olarak filtre uygulamak yerine kategorilere dâhil olan belirli uygulamalar üzerinde kontroller sağlayabilmek için kullanılan alandır (Örnek olarak "**Category**" kısmıyla oyun kategorisine giren bütün uygulamalar zerinde tanımlama yapmak yerin sadece Facebook üzerindeki oyun kategorisine giren uygulama trafiklerini engellemek için bu kısım kullanılmaktadır).

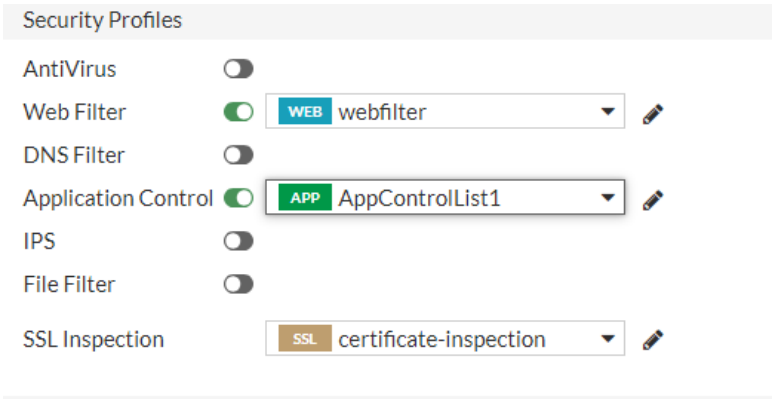


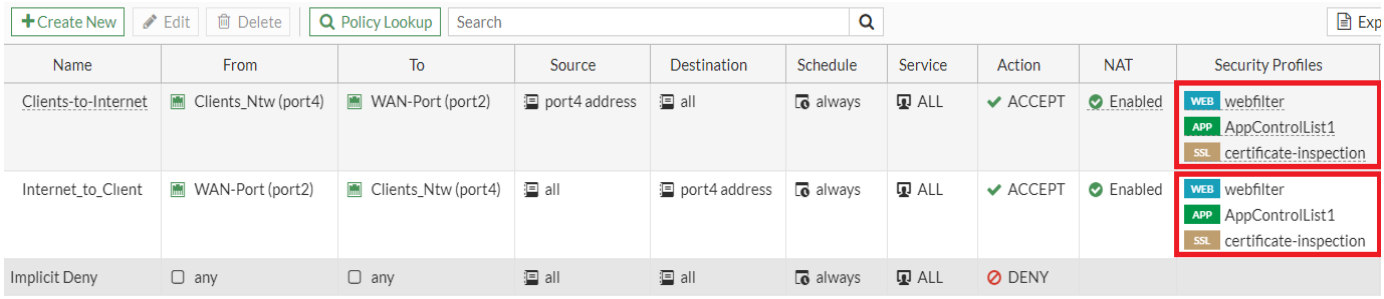


- **Block applications detected on non-default ports** :Uygulamaların oluşturduğu trafiklerde kategori kısmında izin verilmiş olsa dahi varsayılan portu kullanmayan trafiklerin tespit edilerek bloklanmasını sağlayan özelliktir.

Apply Firewall Policy

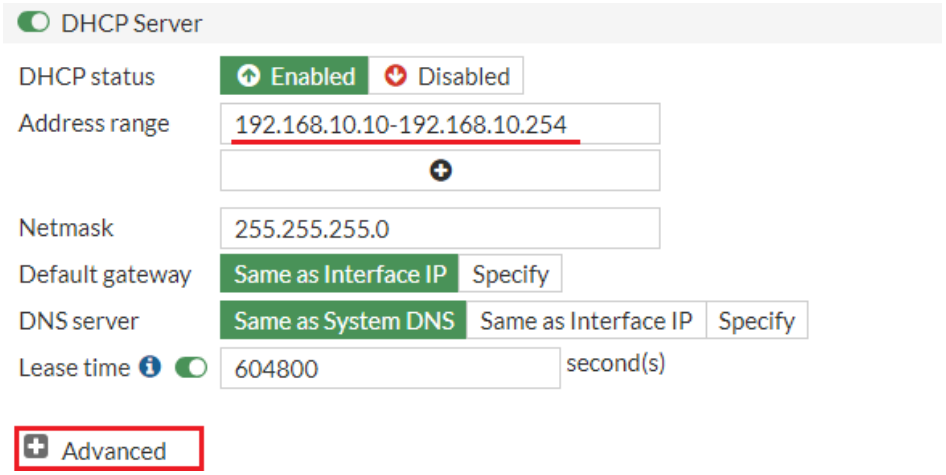
Web Filter ve Application Control tanımları yapıldıktan sonra “**Firewall & Objects –> Firewall Policy**” yolu takip edilerek trafiğine uygulanmak istenen networklerin Policy tanımları altında “” kısmında Web filter ve Application Control kısımları devreye alınarak bu tanımlar çift yönlü olacak şekilde (giden trafik tanımı için de gelen trafik tanımı için de) uygulanmalıdır (Genelde bu tanımlar internet trafiğine yönelik yapıldığı için networklerin internete çıkışı için oluşturulan politika altına tanımlanır).



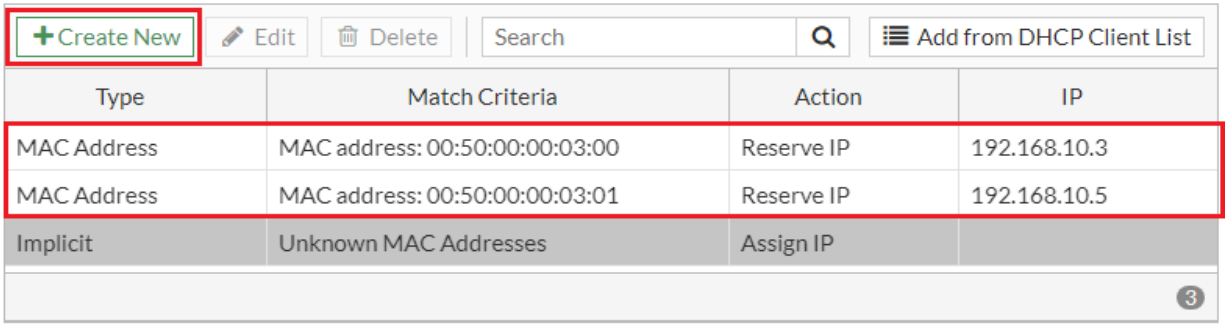


For Privileged User

Eğer ki network geneli için kullanılan politika altında uygulanan bir Web Filter profili ve Application Control listesi varsa ve belirli kullanıcılara farklı politikalar uygulanmak isteniyorsa bu durumda öncelikle bu tanımların dışında tutulacak istemcilerin ip adresleri belirlenerek bu adreslerin istemcilere Bind edilmesi gerekiyor (Bind edilen adresleri IP Pool dışında tutmayı unutma). Bu sayede ip adresleri üzerinden istemciler için yeni Policy tanımı yapılabilecektir.

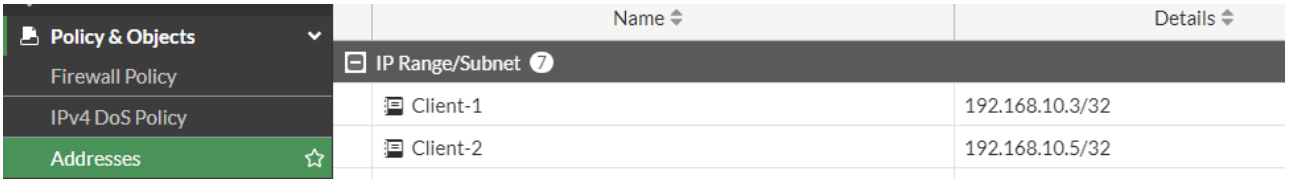


IP Address Assignment Rules



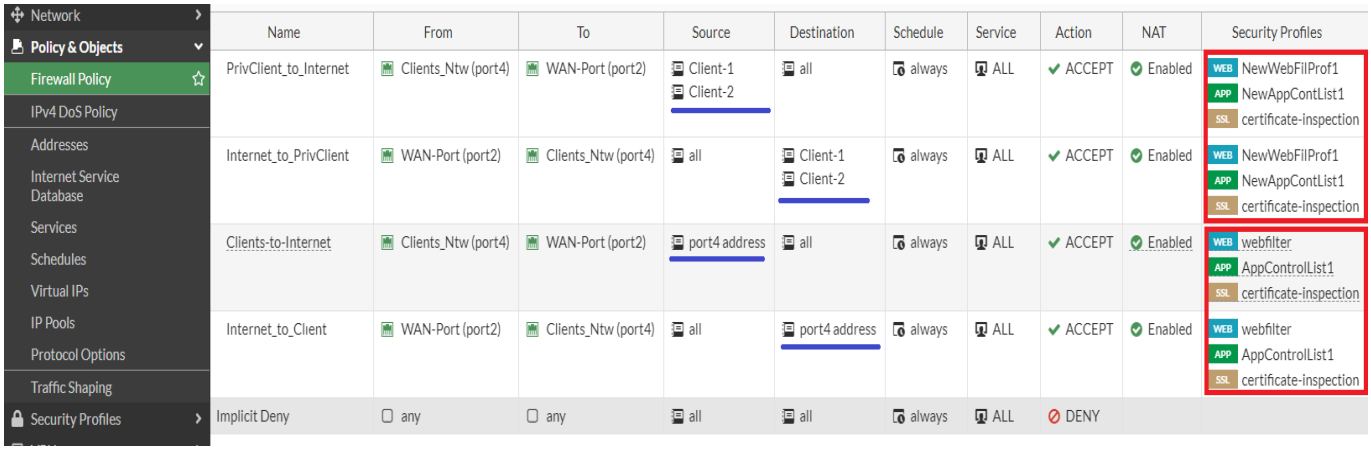
Ip adresleri istemcilere Bind edildikten sonra istemcilere uygulanmak üzere yeni bir Web Filter Profile ve Application Control List tanımı oluşturmak gerekecek.

Web Filter Profile ve Application Control tanımları yapıldıktan sonra Policy tanımında kullanılmak üzere "**Addresses**" kısmında ip adresi Bind edilen istemcilerin ip adreslerinin oluşturulması gerekiyor (isteğe bağlı olarak oluşturulan adresler tek bir adres grubu oluşturularak buraya dâhil edilebilir). Adres tanımları oluşturulduktan sonra artık ayrı politikaları uygulanması istenen istemciler için Policy tanımına geçilebilir.



Policy tanımında network geneline uygulanan Policy tanımından farklı olarak "**Source Address**" kısmında network adresini değil de Ip adresi Bind edilen istemciler için oluşturulan adres /adres grubu tanımı eklenmelidir. Ek olarak Web Filter Profile ve Application Control List kısımlarında yeni oluşturulan tanımlar uygulanmalıdır.

Dikkat edilmesi gereken son kısım ise ayrı politika uygulamak için belirli ip adreslerine yönelik oluşturulan Policy tanımının genel network için oluşturulan Policy tanımından yukarıda bir yerde olmasıdır. Unutulmamalıdır ki trafikler Firewall Policy kısmında bulunan tanımları sırasıyla yukarıdan aşağıya doğru kontrol etmektedir. Trafiğin ilk eşleştiği satırı kabul ederek trafiğe yön vermektedir. Eğer ki trafik ilk olarak network geneli için oluşturulan Policy tanımıyla eşleşirse alt kısımdaki Policy tanımlarını kontrol etmeden trafiğe network geneli için tanımlanan politikaları uygulayacaktır.



Kaynaklar

- https[:]//docs.fortinet.com/document/fortigate/7.4.4/administration-guide/108890/configuring-web-filter-profiles-to-block-ai-and-cryptocurrency
- https[:]//docs.fortinet.com/document/fortigate/7.4.4/administration-guide/931220/configuring-web-filter-profiles-with-hebrew-domain-names
- https[:]//docs.fortinet.com/document/fortigate/6.4.0/new-features/304324/configure-web-filter-profiles-in-ngfw-policy-mode-6-4-2
- https[:]//docs.fortinet.com/document/fortigate/7.4.4/administration-guide/833698/web-filter
- https[:]//community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-configure-a-web-rating-override-to/ta-p/276489
- https[:]//docs.fortinet.com/document/fortigate/6.2.16/cookbook/615462/url-filter
- https[:]//help.fortinet.com/fortiproxy/10/Content/Admin%20Guides/FPX-AdminGuide/700_Security-Profiles/702_Web-filter.htm
- https[:]//docs.fortinet.com/document/fortigate/7.4.4/administration-guide/371670/static-url-filter#:~:text=in%20the%20GUI%3A-,Go%20to%20Security%20Profiles%20%3E%20Web%20Filter%20and%20click%20Create%20New,Click%20OK.
- https[:]//docs.fortinet.com/document/fortigate/6.2.16/cookbook/371670/advanced-filters-1#:~:text=Web%20Filter%20service.-,To%20enable%20this%20feature%20in%20the%20GUI%3A,when%20a%20rating%20error%20occurs.
- https[:]//docs.fortinet.com/document/fortigate/7.4.4/administration-guide/410638/protocol-enforcement
- https[:]//docs.fortinet.com/document/fortigate/6.2.16/cookbook/019814/basic-category-filters-and-overrides
- https[:]//docs.fortinet.com/document/fortigate/7.4.4/administration-guide/19814/basic-category-filters-and-overrides
- https[:]//docs.fortinet.com/document/fortigate/6.4.0/new-features/304324/configure-web-filter-profiles-in-ngfw-policy-mode-6-4-2