

Web Filter and App Control Configuration

Network'e bağılı 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 tanımlanmalıdır.
- 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.
 - o Kategorilerin varsayılanda gelen aksiyon tiplerinde değişiklik yapılmak istendiğinde komut satırında bir "**edit <Edit Value>**" tanımı altında "**set category <Kategori Number>**" komutuyla ilgili kategori seçilip "**set action <Action Type>**" komutuyla aksiyon tipi değiştiriliyor.

```
FortiGate # config webfilter profile
FortiGate (profile) # edit webfilter
new entry 'webfilter' added
FortiGate (webfilter) # set feature-set flow
FortiGate (webfilter) # config ftdg-wf
FortiGate (ftgd-wf) # config filters
FortiGate (filters) # edit 17
FortiGate (17) # set category 17
FortiGate (17) # set action block
FortiGate (17) # next
FortiGate (filters) # edit 18
FortiGate (18) # set category 18
FortiGate (18) # set action monitor
FortiGate (18) # next
FortiGate (filters) # edit 20
FortiGate (20) # set category 20
FortiGate (20) # set action warning
FortiGate (20) # next
FortiGate (filters) # end
FortiGate (ftgd-wf) # end
FortiGate (webfilter) # end
```

```
FortiGate (39) # set category
<id>      Category ID
Bandwidth Consuming:
19 Freeware and Software Downloads
24 File Sharing and Storage
25 Streaming Media and Download
72 Peer-to-peer File Sharing
75 Internet Radio and TV
76 Internet Telephony
General Interest - Personal:
17 Advertising
18 Brokerage and Trading
20 Games
23 Web-based Email
28 Entertainment
29 Arts and Culture
30 Education
33 Health and Wellness
34 Job Search
35 Medicine
36 News and Media
37 Social Networking
38 Political Organizations
39 Reference
40 Global Religion
42 Shopping
44 Society and Lifestyles
46 Sports
47 Travel
48 Personal Vehicles
54 Dynamic Content
55 Meaningless Content
58 Folklore
68 Web Chat
69 Instant Messaging
70 Newsgroups and Message Boards
71 Digital Postcards
77 Child Education
78 Real Estate
```

Edit Web Filter Profile

Name	webfilter
Comments	Write a comment... 0/255
Feature set	Flow-based Proxy-based

☒ FortiGuard Category Based Filter

<input checked="" type="radio"/> Allow	<input type="radio"/> Monitor	<input type="radio"/> Block	<input type="radio"/> Warning	<input type="radio"/> Authenticate
Name	Action			
<input checked="" type="checkbox"/> Potentially Liabile 12				
<input checked="" type="checkbox"/> Adult/Mature Content 15				
<input checked="" type="checkbox"/> Bandwidth Consuming 6				
<input checked="" type="checkbox"/> Security Risk 6				
<input checked="" type="checkbox"/> General Interest - Personal 35				
Advertising	<input type="radio"/> Block			
Brokerage and Trading	<input type="radio"/> Monitor			
Games	<input type="radio"/> Warning			
Web-based Email	<input checked="" type="radio"/> Allow			

9% 93

- Belirli bir kullanıcı veya kullanıcı grubunun bir zaman aralığında farklı bir Web Filter Policy tanımlı 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;

- o **Block invalid URLs** :SSL sertifikasının 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
```

- o **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
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

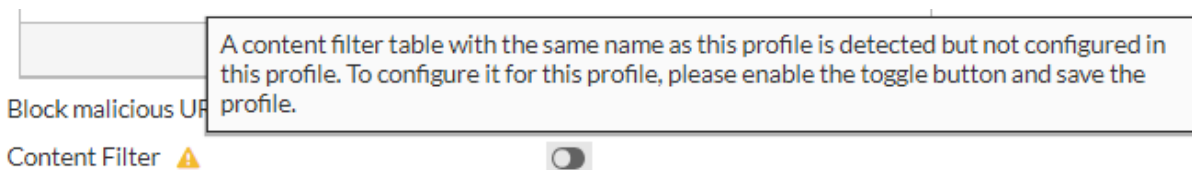
FortiGate (porn) # next

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).



Static URL Filter

Block invalid URLs ☒
URL Filter ☒

+ Create New

Edit

Delete

Search

Q

URL	Type	Action	Status
*.bot.com	Wildcard	Block	Enable
*.instagram.com	Wildcard	Block	Enable
2			

Block malicious URLs discovered by FortiSandbox ☒
Content Filter ☒

+ Create New

Edit

Delete

Pattern Type	Pattern	Language	Action	Status
Regular Expression	adult	Western	Block	Enable
Regular Expression	porn	Western	Block	Enable
2				

- **Allow websites when a rating error occurs** :Fortigate'in geçici olarak FortiGuard hizmetiyle iletişim kuramaması durumunda bu ayar, bağlantı yeniden sağlanana kadar ünitenin hangi erişime izin vereceğini belirler. Etkinleştirilirse, kullanıcılar tüm web sitelerine filtresiz tam erişime sahip olacaktır. Devre dışı bırakılırsa kullanıcıların hiçbir web sitesine erişmesine izin verilmeyecektir.
- **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

```

Rating Options

Allow websites when a rating error occurs ☒
Rate URLs by domain and IP Address ☒

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 tanımlanmalıdır.
- **Categories** :Burada kategorize edilen trafik türleri için uygulanması istenen üç aksiyon tipinden biri seçilmelidir.
 - o Bu tanımları komut satırında yaparken “**set category <Category Number>**” komutunda kategori numarası belirtilmediği takdirde sonraki satırında belirtilen aksiyon tanımları 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
```

Edit Application Sensor

Name

Comments 0/255

Categories

▼ All Categories

- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Business (179, ☁ 6) | <input checked="" type="checkbox"/> Cloud.IT (31) | <input checked="" type="checkbox"/> Collaboration (293, ☁ 6) |
| <input checked="" type="checkbox"/> Email (87, ☁ 12) | <input checked="" type="checkbox"/> Game (124) | <input checked="" type="checkbox"/> General.Interest (241, ☁ 9) |
| <input checked="" type="checkbox"/> Mobile (3) | <input checked="" type="checkbox"/> Network.Service (332) | <input checked="" type="checkbox"/> P2P (85) |
| <input checked="" type="checkbox"/> Proxy (106) | <input checked="" type="checkbox"/> Remote.Access (91) | <input checked="" type="checkbox"/> Social.Media (150, ☁ 31) |
| <input checked="" type="checkbox"/> Storage.Backup (296, ☁ 16) | <input checked="" type="checkbox"/> Update (48) | <input checked="" type="checkbox"/> Video/Audio (206, ☁ 13) |
| <input checked="" type="checkbox"/> VoIP (31) | <input checked="" type="checkbox"/> Web.Client (18) | <input checked="" type="checkbox"/> Unknown Applications |

- **Network Protocol Enforcement** :Uygulama trafiklerinde port/protokol bazlı filtreleme işlemi yapabilmeyi sağlama özelliğidir. 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-services) # 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-services) # 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
```

Network Protocol Enforcement		
+ Create New	Edit	Delete
<input type="text" value="Search"/>		
Port	Enforce Protocols	Violation Action
Port 80	PROT HTTP	Block
Port 53	PROT DNS	Monitor
2		

- **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).

```
FortiGate # config application list
FortiGate (list) # edit AppControlList1
FortiGate (AppControlList1) # config entries
FortiGate (entries) # edit 11
FortiGate (11) # set application 15832 23813 17735 29210 40934
FortiGate (11) # set action block
FortiGate (11) # next
FortiGate (entries) # edit 12
new entry '12' added
FortiGate (12) # set application 39164
FortiGate (12) # set action block
FortiGate (12) # end
FortiGate (AppControlList1) # end
```

Application Codes

AnyDesk App Code

```
FortiGate (11) # set application
ID          Select application ID
38614       1kxun
29025       lundl.Mail
36322       2Safe
36324       2Safe_File.Download
36323       2Safe_File.Upload
17534       2ch
17535       2ch_Post
31236       2shared_File.Download
31237       2shared_File.Upload
16284       3PC
35703       4Sync
35740       4Sync_File.Upload
16616       4shared
35760       4shared_File.Download
34742       4shared_File.Upload
35096       6cn_Search.Music
38923       8tracks
17045       9PFS
39431       9gag
26378       24im
28325       51.Com_BBS
28426       51.Com_Games
--More--
```

Edit Application Sensor

VoIP (31) WebClient (18)

Network Protocol Enforcement

Create New Edit Delete Search

Port	Enforce Protocols	Violation Action
Port 80	HTTP	Block
Port 53	DNS	Monitor

Application and Filter Overrides

Create New Edit Delete

Priority	Details	Type	Action
1	Facebook.App_Name Facebook.App Facebook.Like.Button Facebook.Messenger.Image.Transfer	Application	Block
2	AnyDesk	Application	Block

Options

Block applications detected on non-default ports

Allow and Log DNS Traffic

QUIC

Replacement Messages for HTTP-based Applications

Add New Override

Type Application Filter

Action Block

Add All Results Add Selected Search

Name	Category	Technology	Popularity	Risk
CounterStrike	Game	Client-Server	★★★★★	■■■■■
DC.Universe.Online	Game	Client-Server	★★★★★	■■■■■
Dark.Age.Of.Camelot	Game	Client-Server	★★★★★	■■■■■
Dhxy	Game	Client-Server	★★★★★	■■■■■
Dofus	Game	Client-Server	★★★★★	■■■■■
Draw.Free	Game	Client-Server	★★★★★	■■■■■
EA.FIFA	Game	Browser-Based	★★★★★	■■■■■
Eve.Online	Game	Client-Server	★★★★★	■■■■■
Evony	Game	Browser-Based	★★★★★	■■■■■
Facebook.App_AngryBirds	Game	Browser-Based	★★★★★	■■■■■
Facebook.App_AvengersAlliance	Game	Browser-Based	★★★★★	■■■■■
Facebook.App_Bubble.Fairyland	Game	Browser-Based	★★★★★	■■■■■
Facebook.App_BubbleSafari	Game	Browser-Based	★★★★★	■■■■■
Facebook.App_CandyCrushSaga	Game	Browser-Based	★★★★★	■■■■■
Facebook.App_Criminalcase	Game	Browser-Based	★★★★★	■■■■■
Facebook.App_EmpiresAndAllies	Game	Browser-Based	★★★★★	■■■■■
Facebook.App_Happyland	Game	Browser-Based	★★★★★	■■■■■
Facebook.App_IAmPlayr	Game	Browser-Based	★★★★★	■■■■■
Facebook.App_MafiaWars	Game	Browser-Based	★★★★★	■■■■■
Facebook.App_Miscrits	Game	Browser-Based	★★★★★	■■■■■

OK Cancel

- **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).

Security Profiles
AntiVirus ☐
Web Filter ☒ WEB webfilter
DNS Filter ☐
Application Control ☒ APP AppControlList1
IPS ☐
File Filter ☐
SSL Inspection ☐ SSL certificate-inspection

[+ Create New](#) [Edit](#) [Delete](#) [Policy Lookup](#)

Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
Clients-to-Internet	Clients_Ntw (port4)	WAN-Port (port2)	port4 address	all	always	ALL	✓ ACCEPT	✓ Enabled	<div>WEB webfilter APP AppControlList1 SSL certificate-inspection</div>
Internet_to_Client	WAN-Port (port2)	Clients_Ntw (port4)	all	port4 address	always	ALL	✓ ACCEPT	✓ Enabled	<div>WEB webfilter APP AppControlList1 SSL certificate-inspection</div>
Implicit Deny	<input type="checkbox"/> any	<input type="checkbox"/> any	all	all	always	ALL	✗ DENY		

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. Bu sayede ip adresleri üzerinden istemciler için yeni Policy tanımı yapılabilecektir.

DHCP Server
DHCP status ☒ Enabled ☐ Disabled
Address range 192.168.10.2-192.168.10.254
Netmask 255.255.255.0
Default gateway Same as Interface IP Specify
DNS server Same as System DNS Same as Interface IP Specify
Lease time ☒ 604800 second(s)

Advanced

IP Address Assignment Rules

<div> + Create New Edit Delete <input type="text" value="Search"/> Add from DHCP Client List </div>			
Type	Match Criteria	Action	IP
MAC Address	MAC address: AB:E4:23:44:12:35	Reserve IP	192.168.10.40
MAC Address	MAC address: AF:AD:14:32:44:11	Reserve IP	192.168.10.41
Implicit	Unknown MAC Addresses	Assign IP	

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.

<ul style="list-style-type: none"> Network Policy & Objects <ul style="list-style-type: none"> Firewall Policy IPv4 DoS Policy Addresses 	<table> <tr> <th>Name</th><th>Details</th></tr> <tr> <td>IP Range/Subnet 7</td><td></td></tr> <tr> <td>Client-1</td><td>192.168.10.40/32</td></tr> <tr> <td>Client-2</td><td>192.168.10.41/32</td></tr> </table>	Name	Details	IP Range/Subnet 7		Client-1	192.168.10.40/32	Client-2	192.168.10.41/32
Name	Details								
IP Range/Subnet 7									
Client-1	192.168.10.40/32								
Client-2	192.168.10.41/32								

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.

Network										
Policy & Objects										
Firewall Policy										
IPv4 DoS Policy										
Addresses										
Internet Service Database										
Services										
Schedules										
Virtual IPs										
IP Pools										
Protocol Options										
Traffic Shaping										
Security Profiles										
	Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
	PrivClient_to_Internet	Clients_Ntw (port4)	WAN-Port (port2)	Client-1 Client-2	all	always	ALL	ACCEPT	Enabled	Web NewWebFilProf1 App NewAppContList1 SSL certificate-inspection
	Internet_to_PrivClient	WAN-Port (port2)	Clients_Ntw (port4)	all	Client-1 Client-2	always	ALL	ACCEPT	Enabled	Web NewWebFilProf1 App NewAppContList1 SSL certificate-inspection
	Clients-to-Internet	Clients_Ntw (port4)	WAN-Port (port2)	port4 address	all	always	ALL	ACCEPT	Enabled	Web webfilter App AppControlList1 SSL certificate-inspection
	Internet_to_Client	WAN-Port (port2)	Clients_Ntw (port4)	all	port4 address	always	ALL	ACCEPT	Enabled	Web webfilter App AppControlList1 SSL certificate-inspection
	Implicit Deny	any	any	all	all	always	ALL	DENY		

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>