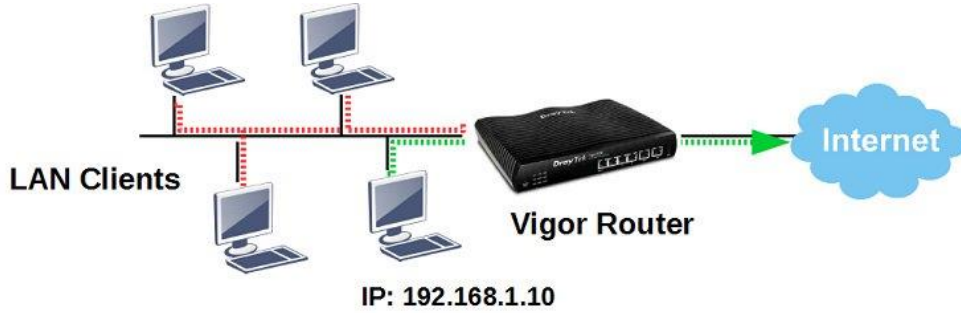


Yalnızca Belirli LAN İstemcileri için İnternet Erişimine İzin Ver

Bu belge, LAN kullanıcılarının çoğunu internetten engellemek ve yalnızca bazı IP'lerin geçmesine izin vermek için Firewall Filter Rule'nin nasıl ayarlanacağını tanıtmaktadır. Bunu yapmak için iki Firewall Filter Rule gerekir: biri tüm LAN istemcisini internetten engellemek, diğeri İnternet erişimi için bazı IP'leri geçirmek. (TIPS: DHCP clientine statik bir IP vermek için [Bind-IP-to-MAC](#) özelliğini de kullanın.)



1. Firewall >> Filter Setup >> Set 2'ye (Default Data Filter) gidin, yeni Filtre Kuralı eklemek için mevcut bir dizin numarasına tıklayın.

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 2

Comments : Default Data Filter

Filter Rule	Active	Comments	Move Up	Move Down
1	<input checked="" type="checkbox"/>	xNetBios -> DNS		Down
2	<input type="checkbox"/>		UP	Down
3	<input type="checkbox"/>		UP	Down
4	<input type="checkbox"/>		UP	Down

2. Tüm LAN kullanıcılarını internetten engelleyen bir Firewall Rule oluşturun:

- Filter Rule'i etkinleştirin
- Yönlendirmeyi "LAN / DMZ / RT / VPN → WAN" olarak ayarlayın, böylece bu kural giden paketleri filtreler.
- Kaynak / Hedef IP, Source Type ve Fragments "Any" olarak bırakın; bu kural, tüm giden paketler için geçerlidir.
- Filter Actionu "Block If No Further Match" olarak ayarlayın, bu, diğeri Filter Rule'ye uymuyorsa Router'in paketleri bırakacağı anlamına gelir.
- Kaydetmek için OK'a tıklayın.

Filter Set 2 Rule 2

Check to enable the Filter Rule

Comments: block_all

Index(1-15) in **Schedule** Setup: [], [], [], []

Clear sessions when schedule ON: Enable

Direction: LAN/DMZ/RT/VPN -> WAN

Source IP: Any

Destination IP: Any

Service Type: Any

Fragments: Don't Care

Application Filter: **Block If No Further Match**

Branch to Other Filter Set: None

Syslog

3. Belirli bir IP adresinin Internet'e girmesini sağlayan bir Firewall Rule oluşturun:

- Filter Rule'yi etkinleştir.
- Directionu "LAN / DMZ / RT / VPN → WAN" olarak ayarlayın.
- Source IP'yi girmek için Edit'e tıklayın. Açılan pencerede, bir Address Type seçin ve bu örnekte 192.168.1.10 ila 192.168.1.15 olan Internet erişimine izin vermek istediğiniz IP adresini girin.
- Destination IP ve Service Type'ı "Any" olarak bırakın.
- Filter Action'u "Pass Immediately" olarak ayarlayın, böylece tanımlanan IP adresinden gelen trafik kaynağı derhal kabul edilir ve Internet'e iletilir, eşleşen başka Filter Rule olup olmadığını kontrol etmenize gerek yoktur.
- Kaydetmek için OK'a tıkla.

Filter Set 2 Rule 3

Check to enable the Filter Rule
 Comments: pass
 Index(1-15) in **Schedule Setup**:
 Clear sessions when schedule ON: Enable

Direction: LAN/DMZ/RT/VPN -> WAN
 Source IP: Any **Edit**
 Destination IP: Any **Edit**
 Service Type: Any **Edit**
 Fragments: Don't Care

Application **Action/Profile**
 Filter: **Pass Immediately**

IP Address Edit

Address Type: Range Address
 Start IP Address: 192.168.1.10
 End IP Address: 192.168.1.15
 Subnet Mask: 0.0.0.0
 Invert Selection:
 IP_Group: None
 or IP_Group: None
 or IP_Object: None
 or IP_Object: None
 IPv6_Group: None
 or IPv6_Object: None
 or IPv6_Object: None
 or IPv6_Object: None

OK Close

Şimdi iki tane Filter Rule'miz var. Paketlerin çoğu, Filter Rule 2 tarafından engellenecektir, çünkü Filter Rule 3'deki filtreleme koşullarına uymuyor ve Filter Rule 3, belirli IP aralığından gelen paketleri filtreleyecek ve Internet'e geçirecektir.

Filter Set 2

Comments : Default Data Filter

Filter Rule	Active	Comments	Move Up	Move Down
1	<input checked="" type="checkbox"/>	xNetBios -> DNS		Down
2	<input checked="" type="checkbox"/>	block_all	UP	Down
3	<input checked="" type="checkbox"/>	pass	UP	Down
4	<input type="checkbox"/>		UP	Down
5	<input type="checkbox"/>		UP	Down
6	<input type="checkbox"/>		UP	Down
7	<input type="checkbox"/>		UP	

Next Filter Set: None