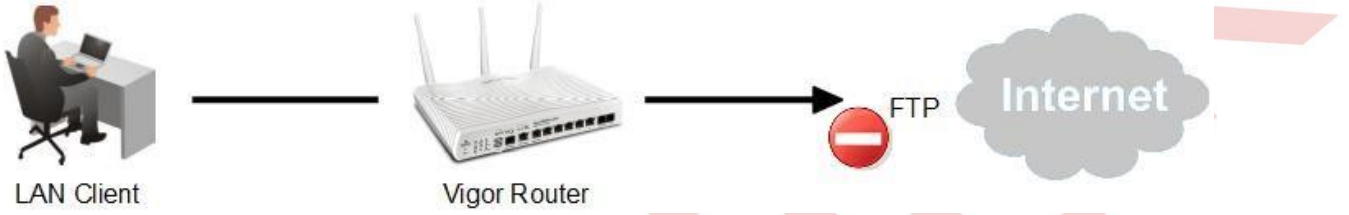


Firewall ile FTP Hizmeti'ni Engelleyin

Bu makalede, TCP port 21'deki trafiği engellemek için Firewall işlevini kullanarak FTP servisinin LAN kullanıcılarının nasıl kısıtlanacağı anlatılmaktadır. Bu örnekte, tüm LAN kullanıcıları için bir firewall kuralı oluşturmak istiyoruz. Gerekli konfigürasyon aşağıda gösterilmiştir.

Not: Router zaten gelen tüm trafiği varsayılan olarak engellediğinden, yalnızca giden trafik için (LAN'dan WAN'a) firewall kuralları oluşturmamız gerekir.

DrayOS



1. Aşağıdaki gibi bir profil oluşturmak için Object Setting >> Services Type Object'e gidin:

- Profile name "FTP" olarak yazın
- Protokolü "TCP" olarak ayarlayın
- Destination Port 'u "= 21 - 21" olarak ayarlayın

Profile Index : 2

Name	FTP
Protocol	TCP 6
Source Port	= 1 ~ 65535
Destination Port	= 21 ~ 21

2. Firewall >> Filter Setup >> Filter Set 2'ye gidin, boş bir kurala tıklayın ve aşağıdaki gibi düzenleyin:

- "Enable" yi işaretleyin
- (İsteğe bağlı) Bazı yorumlar girin (isteğe bağlı)
- (İsteğe bağlı) Source IP'de Edit'e tıklayın ve bu Policy'e uyması gereken IP'yi girin. Belirtilmezse, bu kural tüm LAN hostuna uygulanır.
- Service Type 'de Edit'e tıklayın ve 1. adımda oluşturulan profili seçin.
- Filter için " Block Immediately " seçeneğini seçin. Router'in bu kural hakkında log oluşturmasını istiyorsanız, Syslog'u da kontrol edebilirsiniz.
- Profili kaydetmek için OK'a tıklayın.

Filter Set 2 Rule 2

Check to enable the Filter Rule

Comments:

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

Clear sessions when schedule ON: Enable

Direction:

Source IP:

Destination IP:

Service Type:

Fragments:

Application	Action/Profile	Syslog
Filter:	Block Immediately	<input checked="" type="checkbox"/>
Branch to Other Filter Set:	None	<input type="checkbox"/>
Sessions Control	0 / 60000	<input type="checkbox"/>
MAC Bind IP	Non-Strict	<input type="checkbox"/>
Quality of Service	None	<input type="checkbox"/>
User Management	None	<input type="checkbox"/>
APP Enforcement:	None	<input type="checkbox"/>
URL Content Filter:	None	<input type="checkbox"/>
Web Content Filter:	None	<input checked="" type="checkbox"/>
DNS Filter	None	<input type="checkbox"/>

Advance Setting

1. Firewall Rule enable olduğu sürece aktif olacaktır .Diagnostics >> Syslog Explorer'dan , Router'in 21 numaralı TCP portuna bağlanma girişimlerini engellediğini görebiliriz.

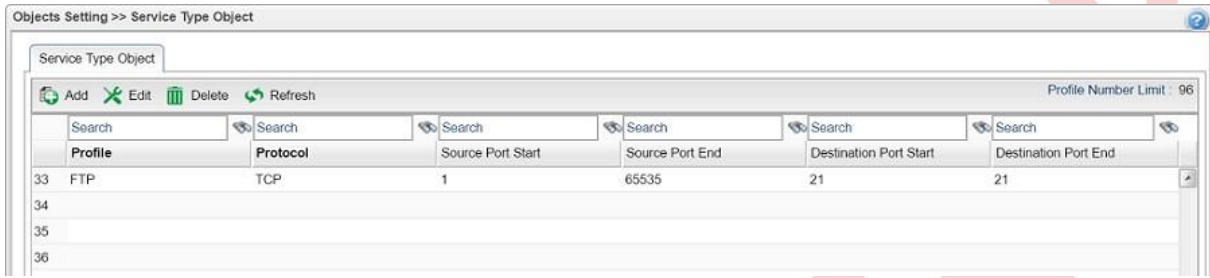
Diagnostics >> Syslog Explorer

Web Syslog		USB Syslog	
<input checked="" type="checkbox"/> Enable Web Syslog		Export Refresh Clear	
Syslog Type <input type="text" value="Firewall"/>		Display Mode <input type="text" value="Always record the new event"/>	
Time	Message		
2017-05-16 10:07:18	[FILTER][Block][LAN/RT/VPN->WAN, 25:14:02][@S:R=2:2, 192.168.66.111:7134->41.73.111.21:21][TCP][HLen=20, TLen=52, Flag=S, Seq=1973572910, Ack=0, Win=8192]		
2017-05-16 10:07:13	[FILTER][Block][LAN/RT/VPN->WAN, 25:13:57][@S:R=2:2, 192.168.66.111:7126->41.73.111.21:21][TCP][HLen=20, TLen=48, Flag=S, Seq=1909807500, Ack=0, Win=8192]		
2017-05-16 10:07:07	[FILTER][Block][LAN/RT/VPN->WAN, 25:13:51][@S:R=2:2, 192.168.66.111:7126->85.236.41.61:21][TCP][HLen=20, TLen=52, Flag=S, Seq=1909807500, Ack=0, Win=8192]		
2017-05-16 10:07:04	[FILTER][Block][LAN/RT/VPN->WAN, 25:13:48][@S:R=2:2, 192.168.66.111:7126->85.236.41.61:21][TCP][HLen=20, TLen=52, Flag=S, Seq=1909807500, Ack=0, Win=8192]		

Linux

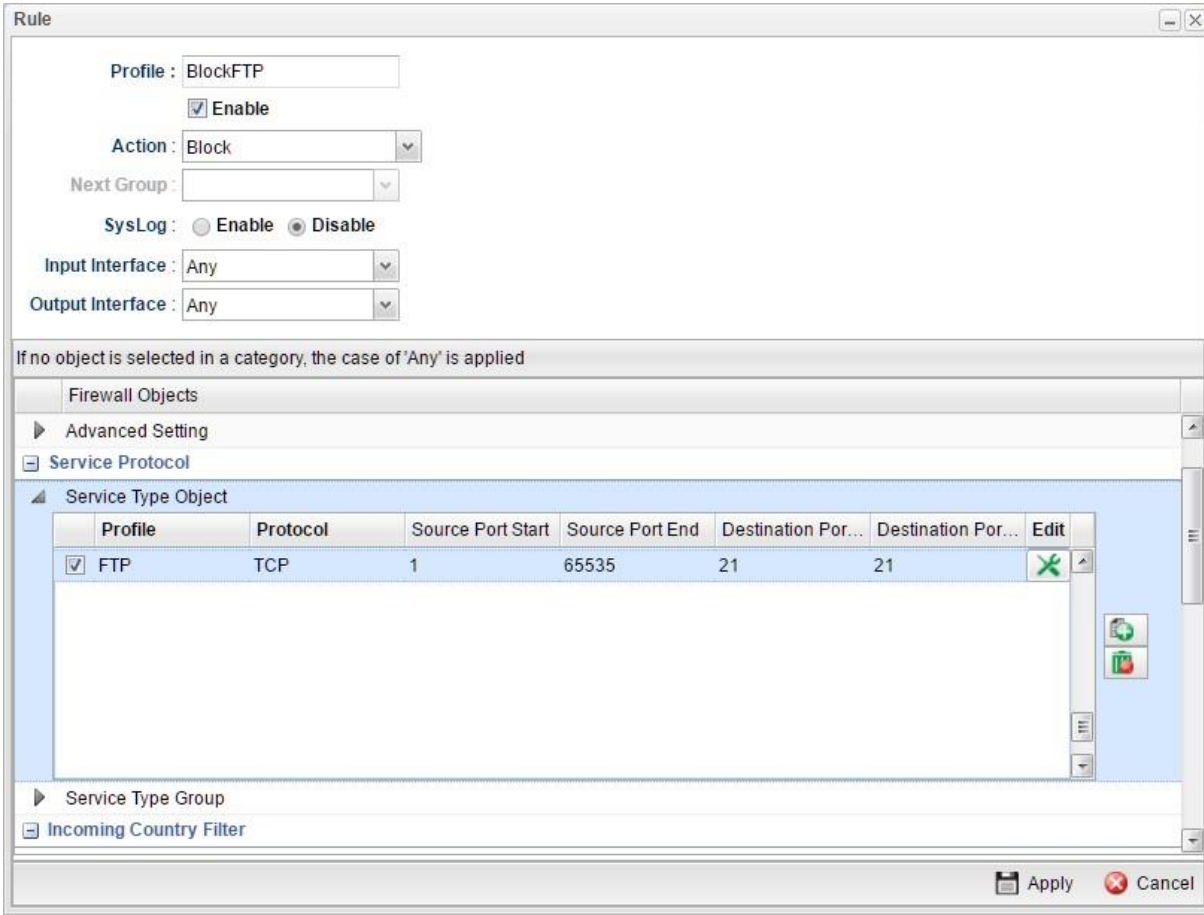
1. Aşağıdaki gibi bir profil oluşturmak için Object Setting >> Services Type Object 'e gidin:

- Profile name "FTP" olarak yazın.
- Protokolü "TCP" olarak ayarlayın
- Source Port 1 ila 65535 arasında bırakın (tüm bağlantı noktaları anlamına gelir).
- Destination Port 'u 21'den 21'e ayarlayın.



2. Firewall >> Filter Setup >> IP Filter'e gidin, bir IP Filter Group oluşturun ve aşağıdaki gibi bir kural ekleyin:

- Etkinleştirmeyi Denetle.
- Action için "Block" u seçin.
- (İsteğe bağlı) Router'in bu kural hakkında log oluşturmasını istiyorsanız, Syslog için "Enable" i seçin.
- Input Interface için "Any" seçeneğini seçin.
- Output Interface için "Any"i seçin
- Services Type Object için 1. adımda "FTP" adlı profili seçin.
- (İsteğe bağlı) Bu kuralı yalnızca bazı hostlara uygulamak istiyorsanız Kaynak IP Object'de IP adresini seçin. Belirtilmezse, tüm LAN hostlarına uygulanır.
- Apply ile ayarları uygulayın.



Filtre Rule enable olduğu sürece etkin olacaktır. Router'ın herhangi bir FTP trafiğini filtrelediğini görmek için System Maintenance >> Syslog / Mail Alert >> Syslog File'a gidebiliriz.

