



Internet

TP

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



LAN Client

Vigor Router

- 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 T
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:	File Sharing	
Index(1-15) in <u>Schedule</u> Setup:		
Clear sessions when schedule ON:	Enable	
Direction:	LAN/DMZ/RT/VPN -> WAN	T
Course ID:	Any	
Source IP:	Edit	
Destination ID:	Any	
Destination IP.	Edit	
Service Type:	FTP	
Service Type.	Edit	
Fragments:	Don't Care 🔻	
Application	Action/Profile	Syslog
Filter:	Block Immediately	
Branch to Other Filter Set:	None 🔻	
Sessions Control	0 / 60000	
MAC Bind IP	Non-Strict v	
Quality of Service	None 🔻	
User Management	None v	
APP Enforcement:	None v	
URL Content Filter:	None 🔻	
Web Content Filter:	None v	1
DNS Filter	None 🔻	

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
Enable Web Syslog	Export Refresh Clear Syslog Type Firewall ▼ Display Mode Always record the new event ▼
Time	Message
2017-05-16 10:07:18	<pre>[FILTER][Block][LAN/RT/VPN->WAN, 25:14:02][@S:R=2:2, 192.168.66.111:7134-> 40.123.101.220:21][TCP][HLen=20, TLen=52, Flag=S, Seq=1973572910, Ack=0, Win=8192]</pre>
2017-05-16 10:07:13	<pre>[FILTER][Block][LAN/RT/VPN->WAN, 25:13:57][@S:R=2:2, 192.168.66.111:7126->#5 736.4 [51:21][TCP][HLen=20, TLen=48, Flag=S, Seq=1909807500, Ack=0, Win=8192]</pre>
2017-05-16 10:07:07	<pre>[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]</pre>
2017-05-16 10:07:04	<pre>[FILTER][Block][LAN/RT/VPN->WAN, 25:13:48][@S:R=2:2, 192.168.66.111:7126-></pre> 5.210 41.01 :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.

Ser	vice Type Object	261										16
Q	Add 🔀 Edit 🔟 Delete	4	Refresh								Profile Number L	imit : 96
	Search	30	Search	8	Search	50	Search	0	Search	1	Search	02
	Profile		Protocol		Source Port Start	1	Source Port End	Í	Destination Port Start	1	Destination Port End	
33	FTP		TCP		1	6	65535	1	21		21	
34												
35												
36												

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.





lule	-								_)×
	Profile :	BlockFTP							
		I Enable							
	Action :	Block	~						
	Next Group :		*						
	SysLog:	🔵 Enable 💿 Disable	•						
1	nput Interface :	Any	*						
OL	tput Interface :	Any	*						
	Advanced Set	tting ol							
4	Service Type	Object							
	Profile	Protocol	Source Port Start	Source Port End	Destination Por	Destination Por	Edit		
	FTP	TCP	1	65535	21	21	×	-	
								The second second second second second second second second second second second second second second second se	
•	Service Type (Group							
-	ncoming Count	try Filter							-
									- 2

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

Sys	slog File Systog Access Setup Mail Alert	
4	🔊 Refresh 📑 Download Log 🏦 Clear Syslog 🛛 Auto Refresh : 10 Seconds 🛩	
_	Search	100
	Log	
1	<135>May 16 10.55:22 Vigor; [IPF-Block-block_file_sharing] BLOCK src ip 192.168.39,77 mac 30:5-6:87 65:57 dst ip 86.298.11.67 proto top DPT=21, skbmark=1	
2	<135>May 16 10.55:17 Vigor: [IPF-Block-block_file_sharing] BLOCK src ip 192.168.39.77 mac 300000000 dst ip 85.203.41 A* proto top DPT=21, skbmark=1	
3	<135>May 16 10.55:14 Vigor; [IPF-Block-block_file_sharing] BLOCK src ip 192.168.39.77 mac 305; 62:57 ds fa to ip in 2.2 e 41 b) proto top DPT=21, skbmark=1	
4	<135>May 16 10:55:13 Vigor: [IPF-Block-block_file_sharing] BLOCK src ip 192.168.39.77 mac 307654er82/56151 dst ip 140.159.104.229 proto top DPT=21, skbmar	
5	<135>May 16 10:55:11 Vigor: IPF-Block-block file sharing) BLOCK src ip 192 168:39.77 mac 30:57 er 87 49:57 dst ip 85 238.11.81 proto top DPT=21, skbmark=1	