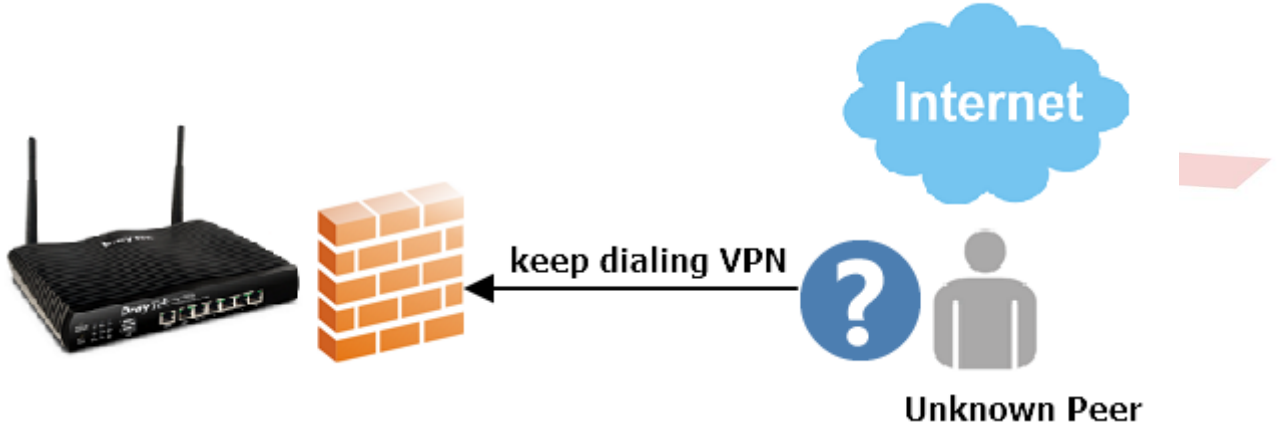


## VPN'i VigorRouter'a çevirmeyi sağlayan bilinmeyen bir IP adresi nasıl engellenir

VPN Server olarak VigorRouter, internetten VPN bağlantısını kabul etmek için her zaman VPN Ports dinler. Bazen, bazı Unknown IP adreslerinin Syslog'daki Vigor Router'a VPN isteği göndermeye devam ettiğini görebiliriz, ancak Remote Peer'in(Karşı Eş) kim olduğunu bulamayabiliriz. Bu durum can sıkıcı ve güvenlik açısından riskli olabilir. Bu belge, VPN'i VigorRouter'a çevirmeyi sürdüren Unknown IP adresinin nasıl engelleneceğini gösterecektir.



1. DrayOS Router'ı VPN sunucusu olarak kullanırken
2. Firewall >> Defense Setup'a git ve DoS Defense enable yap.

### Firewall >> Defense Setup

DoS Defense		Spoofing Defense	
<b>DoS defense</b>			
<input checked="" type="checkbox"/> Enable DoS Defense	Select All	White/Black List Option	Log: Enable
<input type="checkbox"/> Enable SYN flood defense	Threshold	2000	packets / sec
	Timeout	10	sec
<input type="checkbox"/> Enable UDP flood defense	Threshold	2000	packets / sec
	Timeout	10	sec
<input type="checkbox"/> Enable ICMP flood defense	Threshold	250	packets / sec
	Timeout	10	sec
<input type="checkbox"/> Enable Port Scan detection	Threshold	2000	packets / sec
<input type="checkbox"/> Block IP options	<input type="checkbox"/> Block TCP flag scan		
<input type="checkbox"/> Block Land	<input type="checkbox"/> Block Tear Drop		
<input type="checkbox"/> Block Smurf	<input type="checkbox"/> Block Ping of Death		
<input type="checkbox"/> Block trace route	<input type="checkbox"/> Block ICMP fragment		
<input type="checkbox"/> Block SYN fragment	<input type="checkbox"/> Block Unassigned Numbers		
<input type="checkbox"/> Block Fraggle Attack			

Defend ICMP flood attack to make the server resource available for legitimate users.

OK Clear All Cancel

2. White / Black IP List Option'a tıklayın. Unknown peer's IP adresini girin ve IP'yi Black IP List'e eklemek için Add'e tıklayın ve Syslog Explorer'de görmek istiyorsanız günlüğü seçin.

Firewall >> Defense Setup

IP White/Black List Log: All

IPv4 Address

IP Whitelist(Limit:16 entries)

Add
Remove
Clear All

IP Blacklist(Limit:16 entries)

192.168.39.236

192.168.39.236

Add
Remove
Clear All

IPv6 Address

IP Whitelist(Limit:16 entries)

Add
Remove
Clear All

IP Blacklist(Limit:16 entries)

Add
Remove
Clear All

OK

1. Bilinmeyen IP isteği uyarı günlüklerini alma
2. Unknown IP isteği hakkında syslog uyarısı almak için, Syslog Access ayarlamak için System Maintenance >> Syslog / Mail Alert bölümüne gidin.
  - a. Enable durumunu kontrol edin.
  - b. Server Ip adresini girin.
  - c. Firewall Log. Etkinleştir.
  - d. Ayarları uygulamak için OK' a tıklayın.

System Maintenance >> SysLog / Mail Alert Setup

SysLog / Mail Alert Setup

SysLog Access Setup

Enable

Syslog Save to:

Syslog Server

USB Disk

Maximum Syslog folder space 1 GB

When Syslog folder is full: Overwrite oldest logs

Router Name: DrayTek

Server IP/Hostname: 192.168.23.10

Destination Port: 514

Mail Syslog:  Enable

Enable syslog message:

Firewall Log

VPN Log

User Access Log / Hotspot User Information

WAN Log

Router/DSL information

WLAN Log

Mail Alert Setup

Enable Send a test e-mail

SMTP Server:

SMTP Port: 25

Mail To:

Return-Path:

Use SSL

Authentication

Username:

Password:

Enable E-Mail Alert:

DoS Attack

APPE

VPN LOG

APPE Signature

Debug Log

Note:

1. USB Syslog space is available from 256-1024 MB or 1-16 GB.
2. Mail Syslog cannot be activated unless USB Disk is ticked for "Syslog Save to".
3. Mail Syslog feature will send the Syslog when it is full.
4. We only support secured SMTP connection on port 465.

OK

Clear

2. Draytek Syslog Utility'deki Firewall Syslog List'i kontrol edin. Blacklist'deki IP erişmeye çalıştığında Network Administrator, Router'den bir uyarı alır.

The screenshot shows the DrayTek Syslog Utility interface. The main window displays a table of log entries under the 'Defense Log' tab. The first entry is highlighted with a red box:

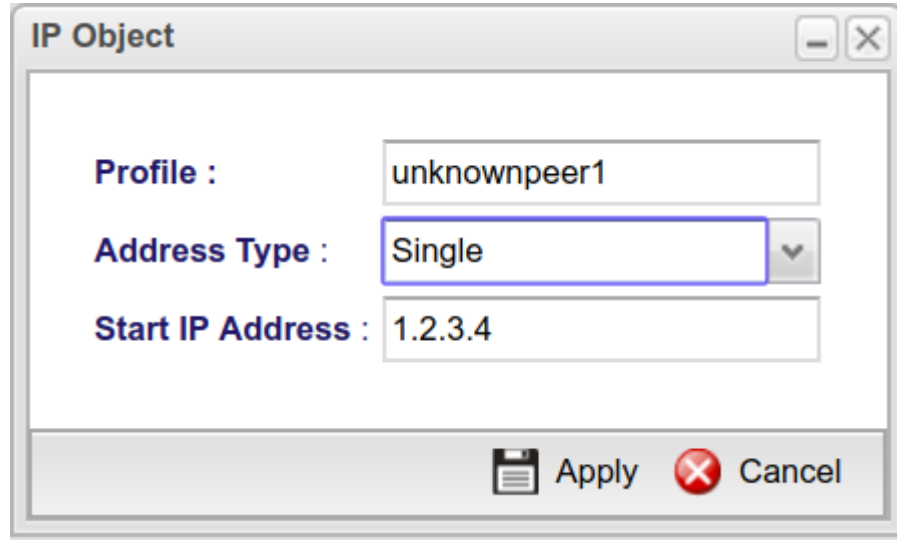
System Time	Router Time	Host	Message
2019-06-28 14:13:02	Jun 28 14:13:00	DrayTek	[DOS][Block][Blocking List][192.168.39.236->192.168.39.11]

The interface also shows various configuration options like Log Filter, WAN Information, and LAN Information.

Ardından Router ayar sayfasından Diagnostics >> Syslog Explorer bölümüne gidin, IP'nin engellenmiş olduğunu da göreceksiniz.

2019-06-28 14:13:03	WAN4_Status:[GW_IP4=--- BBandMode4=--- BBandIp4=--- BBandTxPkt4=0 BBandTxRate4=0 BBandRxPkt4=0 BBandRxRate4=0 BBandUpTime4=00:00:00
2019-06-28 14:13:03	WAN3_Status:[GW_IP3=--- BBandMode3=--- BBandIp3=--- BBandTxPkt3=0 BBandTxRate3=0 BBandRxPkt3=0 BBandRxRate3=0 BBandUpTime3=00:00:00
2019-06-28 14:13:03	WAN2_Status:[GW_IP2=--- BBandMode2=--- BBandIp2=--- BBandTxPkt2=0 BBandTxRate2=0 BBandRxPkt2=0 BBandRxRate2=0 BBandUpTime2=00:00:00
2019-06-28 14:13:03	LAN_Status:[Tx=689749 Rx=259094 ] WAN_Status:[GW_IP=192.168.39.1 BBandMode=DHCP Client BBandIp=192.168.39.11 BBandTxPkt=152634 BBandTxRate=31 BBandRxPkt=272318 BBandRxRate=436 BBandUpTime=20:34:02 ] Model:[Style=0 ModelName=Vigor2926ac]
2019-06-28 14:13:00	[DOS][Block][Blocking List][192.168.39.236->192.168.39.11]

1. Vigor3900 veya Vigor2960'ı VPN Server olarak kullanırken
2. Objects Setting >> IP Object sayfasına gidin ve unknown IP'yi IP Address olarak ekleyin.
  - e. Bir profil adı girin.
  - f. Address Type olarak Single seçin.
  - g. Unknown peer IP adresini Start IP Address olarak girin.



IP Object

Profile : unknownpeer1

Address Type : Single

Start IP Address : 1.2.3.4

Apply Cancel

3. Objects Setting >> Time Object sayfasına gidin ve Time Object ekleyin.
  - a. Bir profil ismi verin.
  - b. Frequency olarak Weekdays seçin.
  - c. Start Time,,End Time ve Weekdays girin.

**Not:** Lütfen daha sonra fakat geçerli saate kapalı olan Start Time girin ve End Time , Start Time'den biraz daha önde olmalıdır. Örneğin, geçerli saat 15:55 ise ve Start Time 16:00:00, End Time 15:59:59 olarak girebiliriz. Firewall kuralı etkinleştikten sonra, bu Time Object kaldırılabilir.

3. Firewall >> Filter Setup sayfasına gidin, bir IP Filter Group oluşturun, ardından Unknown Peer IP'yi engellemek için bir IP Filter Rule oluşturmak için Add'e tıklayın.
  - a. Enable'yi işaretleyin.
  - b. Action olarak Block seçin.
  - c. Time Schedule >> Time Object'de önceki adımda oluşturulan Time Object seçin.
  - d. Time Schedule >> Advanced Setting'de Scheduler açıkken Clear Session'i seçin.
  - e. Source IP'de önceki adımda oluşturulan IP Object seçin.
  - f. Ayarları uygulayın.

Rule

Profile : Block\_Unknown  
 Enable  
Action : Block  
Next Group :  
SysLog :  Enable  Disable  
Input Interface : Any  
Output Interface : Any

If no object is selected in a category, the case of 'Any' is applied

Firewall Objects

Time Schedule

Time Object

Profile	Frequency	Start Date	Start Time	End Date	End Time	Weekdays	Edit
<input checked="" type="checkbox"/> Block_VPN	Weekdays	2018-01-16	16:00:00	2018-01-16	15:59:59	Mon, Tue, Wed, ...	

Time Group

Advanced Setting

Clear Session when Scheduler on

Apply Cancel

Firewall Objects

Source IP Object

Profile	Address Type	Start IP Address	End IP Address	Subnet Mask	Edit
<input checked="" type="checkbox"/> unknownpeer1	Single	1.2.3.4			

Source IP Group

Source User Profile

Source User Group

Source LDAP Group

Apply Cancel

Bundan sonra, VPN Log yerine böyle bir Firewall Log göreceğiz:

```
<13>Dec 27 17:13:02 Vigor: [Clear Session] Delete conntrack by ip_filter_set_rule : unknown  
<135>Dec 27 17:13:07 Vigor: [IPF-unknown] BLOCK src ip 1.2.3.4 mac 00:1d:aa:xx:xx:xx dst ip 172.17.5.92 proto  
udp DPT=500, skbmark=10000002/0
```