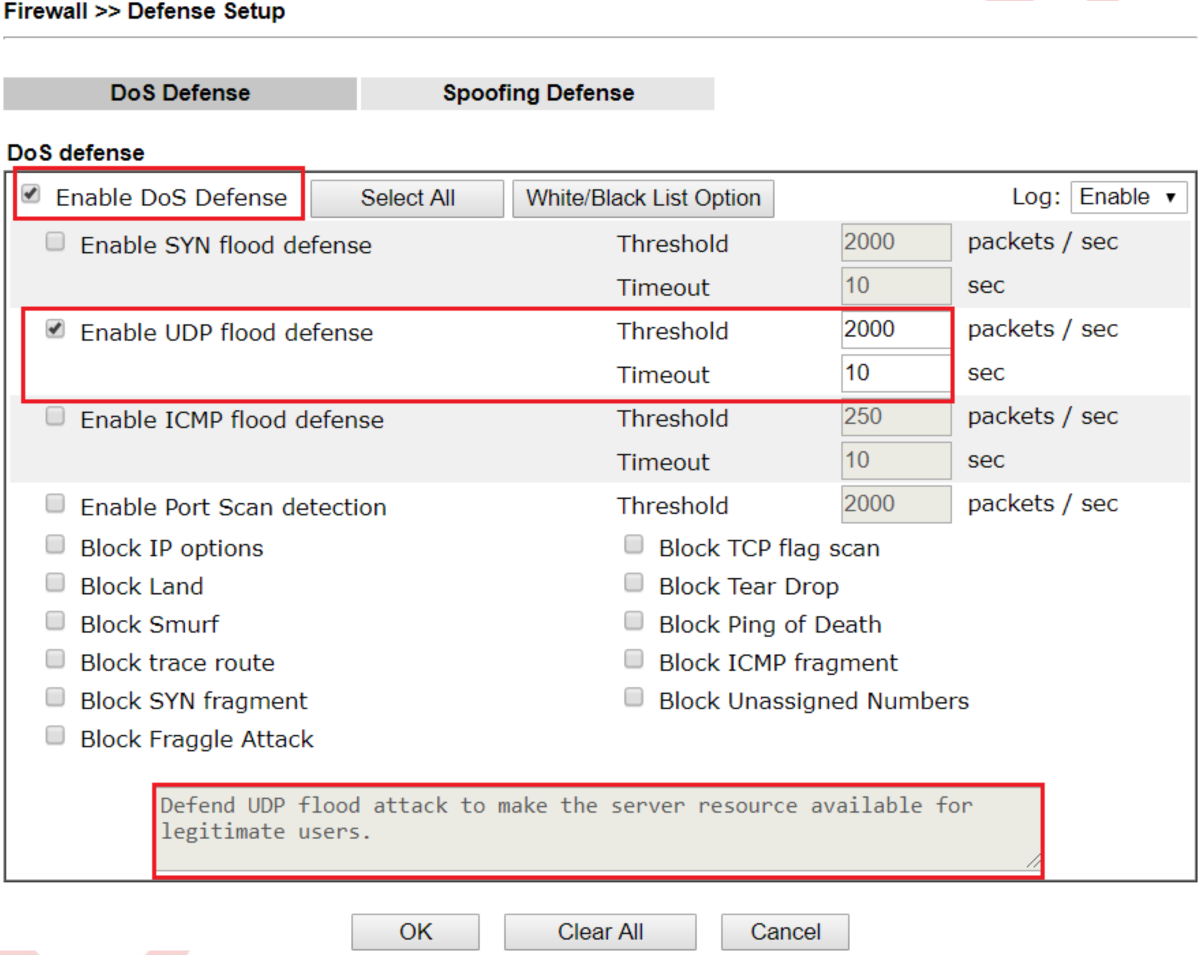
Hizmet Reddi (DoS) Savunmasına Giriş

Vigor Router, kullanıcıyı bilinmeyen kaynak saldırılarından korumak için Denial of Service (DoS) Defense özelliğini sunar. Bu notta, UDP savunmasını ve blacklisti örnek olarak kullanıyoruz; router UDP saldırısını veya IP'yi blacklistte algıladığında, sırasıyla Internet erişimini,zaman aşımı süresini veya IP erişimini engeller. Kullanıcı,Draytek Syslog yardımcı program yazılımından bir alert log alabilir.

1. **UDP Flood savunmasıyla DoS Defence'yi yapılandırma**
2. Firewall >> DoS Defense git.
   a. DoS Defense enable işaretle.
   b. UDP flood Defense enable işaretle
   c. Threshold number gir.



Firewall >> Defense Setup

DoS defense

☑ Enable DoS Defense [Select All] [White/Black List Option] Log: Enable

☐ Enable SYN flood defense	Threshold	2000	packets / sec
	Timeout	10	sec
☑ Enable UDP flood defense	Threshold	2000	packets / sec
	Timeout	10	sec
☐ Enable ICMP flood defense	Threshold	250	packets / sec
	Timeout	10	sec
☐ Enable Port Scan detection	Threshold	2000	packets / sec

☐ Block IP options
☐ Block Land
☐ Block Smurf
☐ Block trace route
☐ Block SYN fragment
☐ Block Fraggle Attack
☐ Block TCP flag scan
☐ Block Tear Drop
☐ Block Ping of Death
☐ Block ICMP fragment
☐ Block Unassigned Numbers

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

Threshold Hakkında

Threshold aralığı, kullanıcının Internet Bandwidth'ine göre ayarlamanız gerektiğini unutmayın. Örneğin, Router'deki maksimum MTU 1500 Bytes ve örnek olarak 2000 Threshold Number değerini alalım.

(Packet number) * (MTU) * (Byte transfer to bits) / 1,000,000 = Data flow (Mbps).
Packet number = Data flow (Mbps) * 1,000,000 / 8 / (MTU).
2,000 = 24 (Mbps) * 1,000,000 / 8 / 1,500.

UDP Flood saldırısının iletim için maksimum MTU sayısını kullanması muhtemel olmadığından, Threshold sayısı 2000 paket / sn, 20 Mbps bandwidth kullanıcı için öneridir. Aşağıda çeşitli bandwidth kullanıcı referansı için bir öneri listesi bulunmaktadır. Kullanıcıların UDP aktarımına özel bir ihtiyacı varsa, lütfen Threshold'u daha bilinçli bir şekilde ayarlayın.

20M Bandwidth: 2,000 (packets/sec).
60M Bandwidth: 5,000 (packets/sec)
100M Bandwidth: 8,000 (packets/sec)
300M Bandwidth: 25,000 (packets/sec)
500M Bandwidth: 42,000 (packets/sec)

Savunma uyarı günlüklerini alma

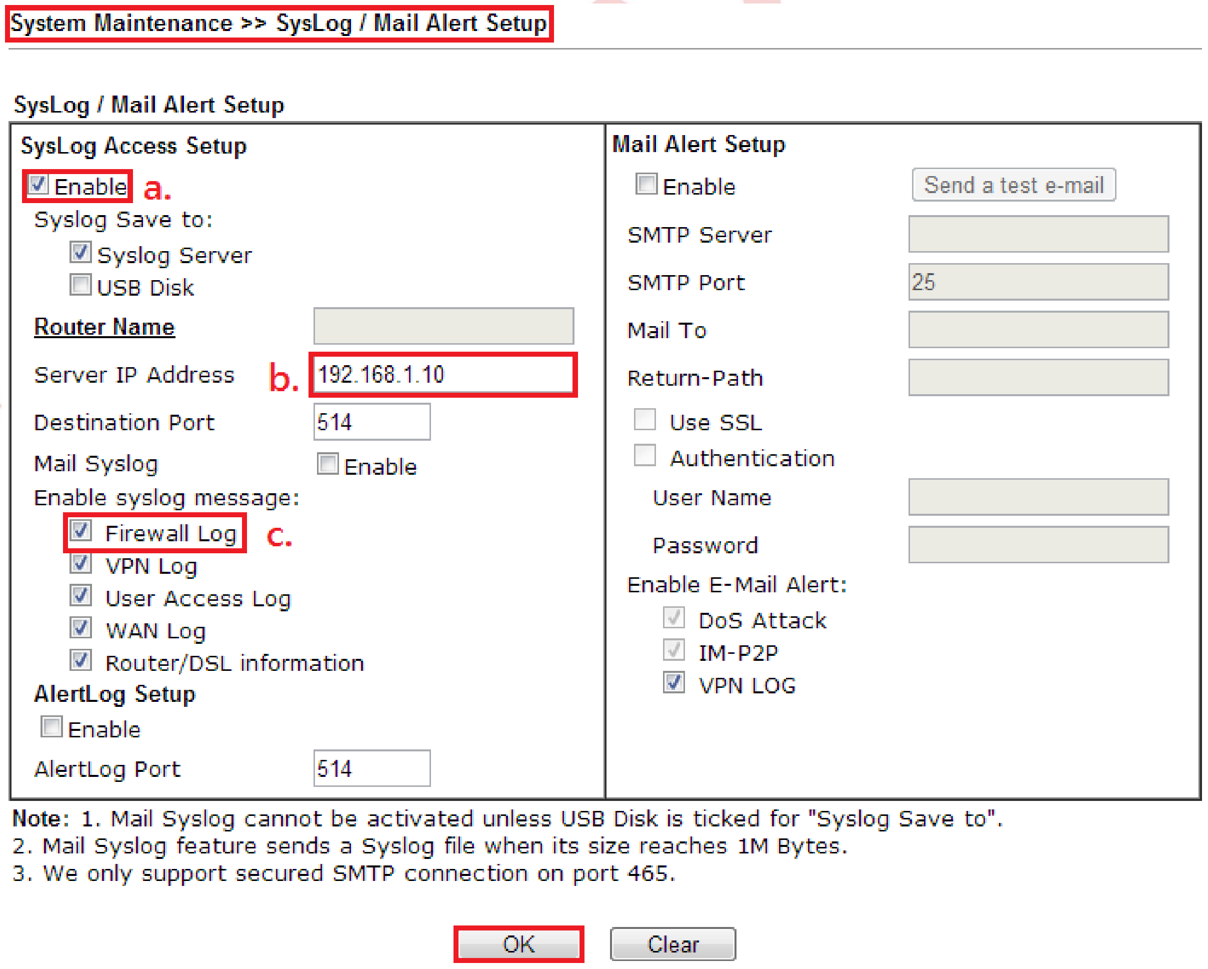
1. DoS hakkında Syslog uyarısı almak için, Syslog Access ayarlamak üzere System Maintenance >> Syslog / Mail Alert bölümüne gidin.

a. Enable durumunu kontrol edin.

b. Server IP girin.

c. Firewall Log State kontrol edin.

d. Ayarları uygulamak için OK'a tıklayın.



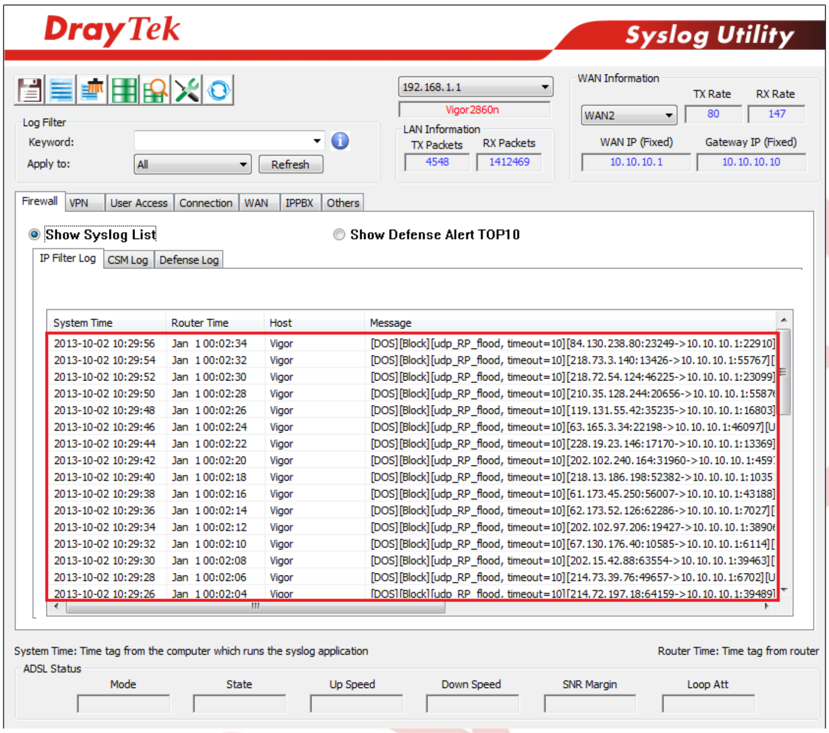
System Maintenance >> SysLog / Mail Alert Setup

SysLog / Mail Alert Setup

SysLog Access Setup		Mail Alert Setup	
☑ Enable a.		☐ Enable	Send a test e-mail
Syslog Save to:		SMTP Server	
☑ Syslog Server		SMTP Port	25
☐ USB Disk		Mail To	
Router Name		Return-Path	
Server IP Address b.	192.168.1.10	☐ Use SSL	
Destination Port	514	☐ Authentication	
Mail Syslog	☐ Enable	User Name	
Enable syslog message:		Password	
☑ Firewall Log c.		Enable E-Mail Alert:	
☑ VPN Log		☑ DoS Attack	
☑ User Access Log		☑ IM-P2P	
☑ WAN Log		☑ VPN LOG	
☑ Router/DSL information			
AlertLog Setup			
☐ Enable			
AlertLog Port	514		

Note: 1. Mail Syslog cannot be activated unless USB Disk is ticked for "Syslog Save to".
2. Mail Syslog feature sends a Syslog file when its size reaches 1M Bytes.
3. We only support secured SMTP connection on port 465.

Draytek Syslog Utility'deki Firewall Syslog List'i kontrol edin. Network Administrator, Router saldırı altında olduğunda Router'den bir uyarı alır.



192.168.1.1
Vigor2860n

Log Filter
Keyword:
Apply to: All
Refresh

LAN Information

TX Packets	RX Packets
4548	1412469

WAN Information

	TX Rate	RX Rate
WAN2	80	147

WAN IP (Fixed)	Gateway IP (Fixed)
10.10.10.1	10.10.10.10

● Show Syslog List ○ Show Defense Alert TOP10

```
System Time          Router Time       Host    Message
2013-10-02 10:29:56  Jan  1 00:02:34   Vigor   [DOS][Block][udp_RP_flood, timeout=10][84.130.238.80:23249->10.10.10.1:22910]
2013-10-02 10:29:54  Jan  1 00:02:32   Vigor   [DOS][Block][udp_RP_flood, timeout=10][218.73.3.140:13426->10.10.10.1:55767][
2013-10-02 10:29:52  Jan  1 00:02:30   Vigor   [DOS][Block][udp_RP_flood, timeout=10][218.72.54.124:46225->10.10.10.1:23099]
2013-10-02 10:29:50  Jan  1 00:02:28   Vigor   [DOS][Block][udp_RP_flood, timeout=10][210.35.128.244:20656->10.10.10.1:5587
2013-10-02 10:29:48  Jan  1 00:02:26   Vigor   [DOS][Block][udp_RP_flood, timeout=10][119.131.55.42:35235->10.10.10.1:16803]
2013-10-02 10:29:46  Jan  1 00:02:24   Vigor   [DOS][Block][udp_RP_flood, timeout=10][63.165.3.34:22198->10.10.10.1:46097][U
2013-10-02 10:29:44  Jan  1 00:02:22   Vigor   [DOS][Block][udp_RP_flood, timeout=10][228.19.23.146:17170->10.10.10.1:13369]
2013-10-02 10:29:42  Jan  1 00:02:20   Vigor   [DOS][Block][udp_RP_flood, timeout=10][202.102.240.164:31960->10.10.10.1:459
2013-10-02 10:29:40  Jan  1 00:02:18   Vigor   [DOS][Block][udp_RP_flood, timeout=10][218.13.186.198:52382->10.10.10.1:1035
2013-10-02 10:29:38  Jan  1 00:02:16   Vigor   [DOS][Block][udp_RP_flood, timeout=10][61.173.45.250:56007->10.10.10.1:43188]
2013-10-02 10:29:36  Jan  1 00:02:14   Vigor   [DOS][Block][udp_RP_flood, timeout=10][62.173.52.126:62286->10.10.10.1:7027][
2013-10-02 10:29:34  Jan  1 00:02:12   Vigor   [DOS][Block][udp_RP_flood, timeout=10][202.102.97.206:19427->10.10.10.1:3890
2013-10-02 10:29:32  Jan  1 00:02:10   Vigor   [DOS][Block][udp_RP_flood, timeout=10][67.130.176.40:10585->10.10.10.1:6114][
2013-10-02 10:29:30  Jan  1 00:02:08   Vigor   [DOS][Block][udp_RP_flood, timeout=10][202.15.42.88:63554->10.10.10.1:39463][
2013-10-02 10:29:28  Jan  1 00:02:06   Vigor   [DOS][Block][udp_RP_flood, timeout=10][214.73.39.76:49657->10.10.10.1:6702][U
2013-10-02 10:29:26  Jan  1 00:02:04   Vigor   [DOS][Block][udp_RP_flood, timeout=10][214.72.197.18:64159->10.10.10.1:39489]
```

System Time: Time tag from the computer which runs the syslog application

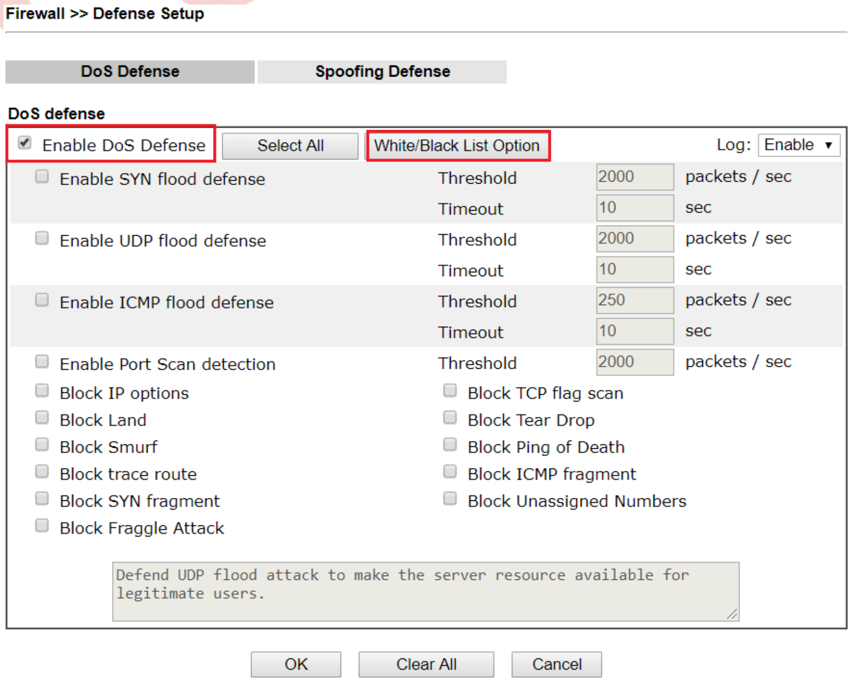
Router Time: Time tag from router

ADSL Status

Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att

DoS Defence'yi White/Black List'e Göre Yapılandırma:

1. Firewall >> DoS Defense git.
   a. DoS Defense enable işaretle.
   b. White/black List Option tıkla.



Firewall >> Defense Setup

DoS defense

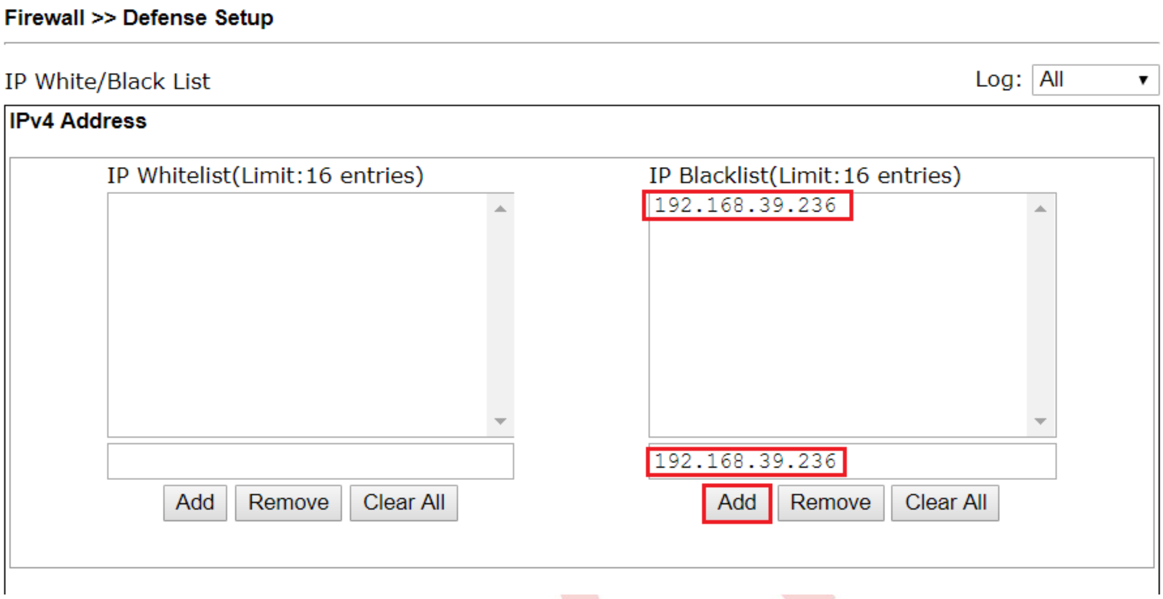
☑ Enable DoS Defense Select All White/Black List Option Log: Enable

□ Enable SYN flood defense	Threshold	2000	packets / sec
	Timeout	10	sec
□ Enable UDP flood defense	Threshold	2000	packets / sec
	Timeout	10	sec
□ Enable ICMP flood defense	Threshold	250	packets / sec
	Timeout	10	sec
□ Enable Port Scan detection	Threshold	2000	packets / sec

□ Block IP options
□ Block Land
□ Block Smurf
□ Block trace route
□ Block SYN fragment
□ Block Fraggle Attack
□ Block TCP flag scan
□ Block Tear Drop
□ Block Ping of Death
□ Block ICMP fragment
□ Block Unassigned Numbers

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

c. Router’inize erişmek için izin verilecek veya engellenecek olan IP'leri IP Whitelist’e veya IP Blacklist’e girin.



Firewall >> Defense Setup

IP White/Black List — Log: All

IPv4 Address

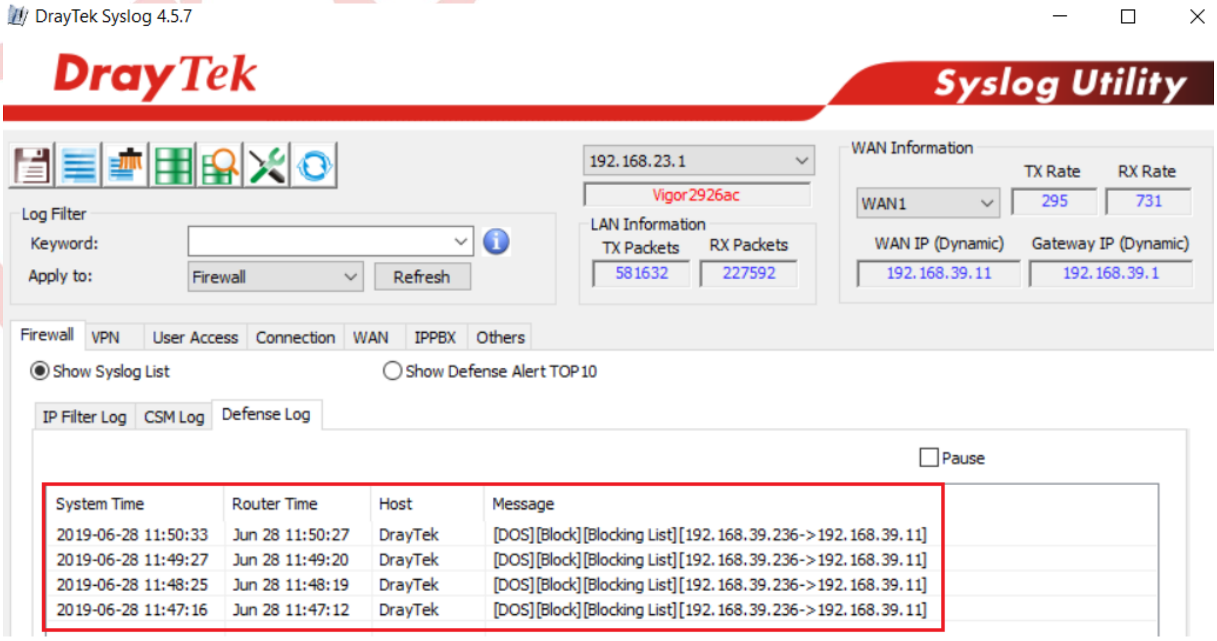
IP Whitelist(Limit:16 entries)

IP Blacklist(Limit:16 entries): 192.168.39.236

192.168.39.236

Defense alert günlüklerini alma:

Draytek Syslog Utility’de Firewall Syslog List’i kontrol edin. Blacklist’deki IP erişmeye çalıştığında Network Administrator Router’den uyarı alır.



DrayTek Syslog 4.5.7

DrayTek Syslog Utility

192.168.23.1 — Vigor2926ac

Log Filter — Keyword: — Apply to: Firewall

LAN Information — TX Packets: 581632 — RX Packets: 227592

WAN Information — WAN1 — TX Rate: 295 — RX Rate: 731

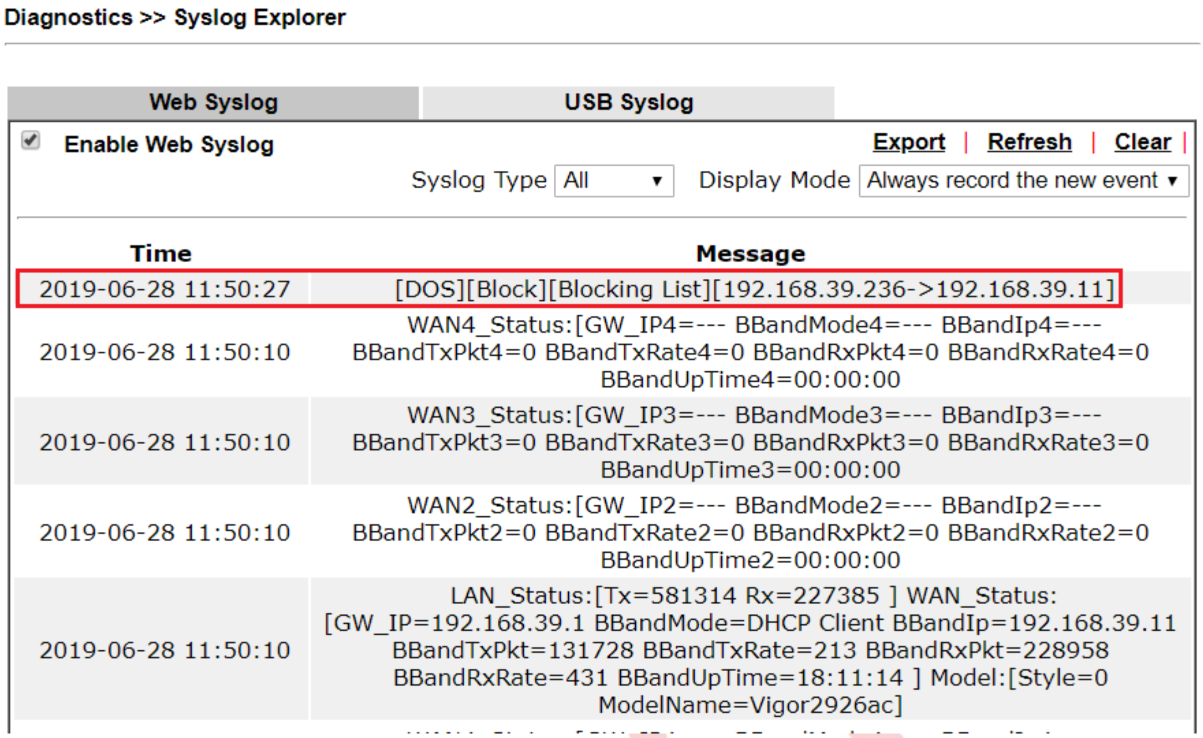
WAN IP (Dynamic): 192.168.39.11 — Gateway IP (Dynamic): 192.168.39.1

● Show Syslog List ○ Show Defense Alert TOP10

□ Pause

System Time	Router Time	Host	Message
2019-06-28 11:50:33	Jun 28 11:50:27	DrayTek	[DOS][Block][Blocking List][192.168.39.236->192.168.39.11]
2019-06-28 11:49:27	Jun 28 11:49:20	DrayTek	[DOS][Block][Blocking List][192.168.39.236->192.168.39.11]
2019-06-28 11:48:25	Jun 28 11:48:19	DrayTek	[DOS][Block][Blocking List][192.168.39.236->192.168.39.11]
2019-06-28 11:47:16	Jun 28 11:47:12	DrayTek	[DOS][Block][Blocking List][192.168.39.236->192.168.39.11]

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



Diagnostics >> Syslog Explorer

☑ Enable Web Syslog

Syslog Type All ▾ Display Mode Always record the new event ▾

Time	Message
2019-06-28 11:50:27	[DOS][Block][Blocking List][192.168.39.236->192.168.39.11]
2019-06-28 11:50:10	WAN4_Status:[GW_IP4=--- BBandMode4=--- BBandIp4=--- BBandTxPkt4=0 BBandTxRate4=0 BBandRxPkt4=0 BBandRxRate4=0 BBandUpTime4=00:00:00
2019-06-28 11:50:10	WAN3_Status:[GW_IP3=--- BBandMode3=--- BBandIp3=--- BBandTxPkt3=0 BBandTxRate3=0 BBandRxPkt3=0 BBandRxRate3=0 BBandUpTime3=00:00:00
2019-06-28 11:50:10	WAN2_Status:[GW_IP2=--- BBandMode2=--- BBandIp2=--- BBandTxPkt2=0 BBandTxRate2=0 BBandRxPkt2=0 BBandRxRate2=0 BBandUpTime2=00:00:00
2019-06-28 11:50:10	LAN_Status:[Tx=581314 Rx=227385] WAN_Status:[GW_IP=192.168.39.1 BBandMode=DHCP Client BBandIp=192.168.39.11 BBandTxPkt=131728 BBandTxRate=213 BBandRxPkt=228958 BBandRxRate=431 BBandUpTime=18:11:14] Model:[Style=0 ModelName=Vigor2926ac]

]