

## Uygulama Katmanı Gateway Etkinleştirin

SIP, RTSP ve FTP gibi protokoller NAT-T'nin kısa olması nedeniyle, servis sunucusu NAT'ın arkasında olduğunda, bağlantı başarısız olabilir. Application Layer Gateway (ALG) bu sorunun çözümüdür. ALG etkin durumdayken, Router istemciden anlaşılan paketindeki private IP'yi public IP ile değiştirecek ve bağlantı için gereken dinamik TCP / UDP bağlantı noktalarını açacaktır.

### SIP ALG ve RTSP ALG'yi etkinleştir

Firmware versiyonu 3.8.5'ten itibaren, ALG özelliği için geçerli bir sayfa hazırladık. Etkinleştirmek için şu adrese gidin **NAT >> ALG**,

- Enable ALG** Kontrolü
- SIP / RTSP ALG Enable**, ve input **SIP / RTSP Listen port** server ayarları kontrolü, TCP ve UDP yapılandırılabilir.

#### NAT >> ALG

##### ALG (Application Layer Gateway)

[Set to Factory Default](#)

<input checked="" type="checkbox"/> Enable ALG				
<input checked="" type="checkbox"/> Enable	Protocol	Listen Port	TCP	UDP
<input checked="" type="checkbox"/>	SIP	5060	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	RTSP	554	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

### PPTP, IPsec ve FTP ALG'yi Etkinleştir

VigorRouter, eğer bu local servisler devre dışı bırakılmışsa ve servis portları sunucuyu bir LAN üzerinden yönlendirmek üzere ayarlanmışsa, PPTP, IPsec veya FTP ALG'yi etkinleştirecektir.

- Local servisi disable yapın. PPTP / IPsec için. VPN ve Remote Access >> Remote Access Control'e gidin ve PPTP / IPsec VPN Service Enable işaretini kaldırın.

#### VPN and Remote Access >> Remote Access Control Setup

##### Remote Access Control Setup

<input type="checkbox"/> Enable PPTP VPN Service
<input type="checkbox"/> Enable IPsec VPN Service
<input checked="" type="checkbox"/> Enable L2TP VPN Service
<input checked="" type="checkbox"/> Enable SSL VPN Service

#### Note:

To allow VPN pass-through to a separate VPN server on the LAN, disable any services above that use the same protocol and ensure that NAT **Open Ports** or **Port Redirection** is also configured.

FTP için, System Maintenance >> Management'e gidin ve Internet Access Control altında FTP sunucusunu devre dışı bırakın.

System Maintenance >> Management

**IPv4 Management Setup**

Router Name: DrayTek

Default:Disable Auto-Logout  
 Enable Validation Code in Internet/LAN Access

**Internet Access Control**

Allow management from the Internet  
 Domain name allowed:

**FTP Server**  
 HTTP Server  
 HTTPS Server  
 Telnet Server  
 TR069 Server  
 SSH Server  
 Disable PING from the Internet

**IPv6 Management Setup**

**Management Port Setup**

User Define Ports  Default Ports

Telnet Port:  (Default: 23)  
 HTTP Port:  (Default: 80)  
 HTTPS Port:  (Default: 443)  
 FTP Port:  (Default: 21)  
 TR069 Port:  (Default: 8069)  
 SSH Port:  (Default: 22)

**Brute Force Protection**

Enable brute force login protection

FTP Server  
 HTTP Server  
 HTTPS Server

2. Servis için Open Ports'u ayarlayın, NAT **Open Ports** 'a gidin ve düzenlemek için uygun herhangi bir dizini tıklayın.

- **Open Ports'u enable yapınız.**
- **WAN interface'yi seçin.**
- **Private IP'ye local server ip'yi girin.**
- Protocol, Start ve End portunu servisin Service Port'una ayarlayın. (lütfen aşağıdaki tablodaki bilgilere bakınız)

Service	Service Port (Required manual configuration)	ALG (Opened by the router automatically)
PPTP	TCP 1723	GRE IP47
IPsec	UDP 500, 4500	ESP IP50
FTP	TCP 21	FTP data port

NAT >> Open Ports >> Edit Open Ports

Index No. 1

Enable Open Ports

Comment: Passthrough

WAN Interface: ALL

Source IP: Any **IP Object**

Private IP: 192.168.86.150

	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	TCP	20	21	2.	UDP	500	500
3.	TCP	1723	1723	4.	UDP	4500	4500
5.	----	0	0	6.	----	0	0
7.	----	0	0	8.	----	0	0
9.	----	0	0	10.	----	0	0