

Vigor2760, Vigor2860 , Vigor2912, Vigor2922, Vigor2952, and Vigor2120

1. Cihazı son versiyonuna güncelleyin .
2. DoS defense özelliğini aktif edin (UDP defense check'i kaldırın)

3. Cihazınızı mümkünse internet üzerinden erişime kapatın.

4. Eğer internet üzerinden cihazınıza erişmek zorundaysanız Telnet ve TR069 servisini kapatın . http ve HTTPS portlarını değiştirin . Brute Force Protection özelliğini aktif edin ve tüm özellikleri seçin . max login hatasını 3 ve bloklama süresini 21600 sn (6 saat) olarak ayarlayın .

System Maintenance >> Management

IPv4 Management Setup IPv6 Management Setup LAN Access 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 ☒ Enforce HTTPS Access
☒ HTTPS Server
☐ Telnet Server
☐ TR069 Server
☐ SSH Server
☐ SNMP Server
☒ Disable PING from the Internet

Access List from the Internet

List Type	Index	Description
1	[IP Object] None	
2	[IP Object] None	
3	[IP Object] None	
4	[IP Object] None	
5	[IP Object] None	
6	[IP Object] None	
7	[IP Object] None	
8	[IP Object] None	
9	[IP Object] None	
10	[IP Object] None	

Note: Access list time, hostname, china ID address supported for

Management Port Setup

☒ User Define Ports ☐ Default Ports

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

Note: Ports 8001 and 8043 are used for Hotspot Web Portal.

Brute Force Protection

☒ Enable brute force login protection

☒ FTP Server
☒ HTTP Server
☒ HTTPS Server
☒ Telnet Server
☒ TR069 Server
☒ SSH Server
☒ VPN Server

Maximum login failures: 3 times
Penalty period: 21600 seconds

Blocked IP List

TLS/SSL Encryption Setup

☒ Enable TLS 1.3
☒ Enable TLS 1.2
☐ Enable TLS 1.1
☐ Enable TLS 1.0

5. Eğer mümkünse SSL vpn servisini kapatın ve yerine PPTP vpn servisini kullanın. SSL vpn servisini kullanacaksanız portu değiştirin .

VPN and Remote Access >> Remote Access Control

Remote Access Control Setup Bind to WAN

☐ Enable PPTP VPN Service
☐ Enable IPsec VPN Service
☐ Enable L2TP VPN Service
☐ Enable SSL VPN Service
☐ Enable OpenVPN Service
☐ Enable WireGuard VPN Service

Note:

1. To allow VPN pass-through to a separate VPN server on the LAN, disable the services listed above that use the same protocol and ensure that NAT Open Ports or Port Redirection is well-configured.
2. Disable unused VPN services, enable Brute Force Protection, and block unknown IP access to the used VPN services to reduce Cyberattacks.

OK Clear Cancel

VPN and Remote Access >> SSL General Setup

SSL General Setup Bind to WAN

☒ WAN1
☒ WAN2
☒ WAN3

Port: 443 (Default: 443)
Server Certificate: Default Certificate

Note: Server Certificate follow the Default Certificate now Default Certificate can be configured at Certificate >> Local Services List

OK Cancel

