

Router'i İnternette Yönetin

VigorRouter uzaktan yönetim erişimi sunar; Ancak, güvenlik nedeniyle devre dışı bırakılmıştır. Router'i internette yönetmek istiyorsanız, aşağıdaki adımları izleyin.

DrayOS

1. İnternete bağlanın

WAN Interface'nin çevrimiçi olduğundan ve Router'in internette erişilebilecek ortak bir IP adresine sahip olduğundan emin olun. WAN IP'sini yazın.

Online Status

Physical Connection			System Uptime: 0day 0:11:28		
IPv4		IPv6			
LAN Status	Primary DNS: 168.95.1.1		Secondary DNS: 168.95.192.1		
IP Address	TX Packets	RX Packets			
192.168.60.1	5,950	6,130			
WAN 1 Status >> Drop PPPoE					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:11:23	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
192.168.60.1	168.95.1.1	5,041	215	5,689	393

2. İnternette erişime izin ver

System Maintenance >> Management sayfasına gidin, internetteyete yonetime izin ver secenegini isaretleyin ve internetteyete erismek istediginiz yonetim arayuzu icin etkinlestirin. (CLI icin SSH, Web UI'ya HTTPS erisimi). Yukaridaki konfigurasyonla, Router'in web yonetim sayfasina internetteyete https:// [Router'in WAN IP'si] erisebilirsiniz.

System Maintenance >> Management

IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup
Router Name: DrayTek		
<input type="checkbox"/> Default: Disable Auto-Logout <input type="checkbox"/> Enable Validation Code in Internet/LAN Access		
Internet Access Control		
<input checked="" type="checkbox"/> Allow management from the Internet Domain name allowed:		
<input type="checkbox"/> FTP Server <input type="checkbox"/> HTTP Server <input type="checkbox"/> Enforce HTTPS Access <input checked="" type="checkbox"/> HTTPS Server <input type="checkbox"/> Telnet Server <input type="checkbox"/> TR069 Server <input type="checkbox"/> SSH Server <input type="checkbox"/> SNMP Server <input checked="" type="checkbox"/> Disable PING from the Internet		
Management Port Setup		
<input checked="" type="radio"/> User Define Ports <input type="radio"/> 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)		
Brute Force Protection		
<input type="checkbox"/> Enable brute force login protection <input type="checkbox"/> FTP Server <input type="checkbox"/> HTTP Server <input type="checkbox"/> HTTPS Server		

3. (Önerilen) Erişim Listesini Ayarla

Uzaktan erişimi yalnızca belirli bir IP ile sınırlamak için, Access List'i etkinleştirin, ardından remote host public IP'sini IP Listesine ekleyin. (Remote Access statik bir public IP yoksa, seçenek devre dışı bırakılmalıdır.)

Access List from the Internet		
List	IP	Subnet Mask
1	100.100.100.100	255.255.255.255 / 32
2		
3		

4. (Önerilen) Değişim yönetimi bağlantı noktası

Daha yüksek güvenlik için, yönetim portunu değiştirebilirsiniz. Yönetim portunu değiştirirseniz, IP adresinden sonra port numarasını belirtmeniz gerekecektir. Örneğin, aşağıdaki yapılandırma ile Router'ın yönetim sayfasına [https:// \[Yönlendiricinin WAN IP'si\]:4433](https://[Yönlendiricinin WAN IP'si]:4433) üzerinden erişebilirsiniz.

System Maintenance >> Management

IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup
Router Name: DrayTek		
<input type="checkbox"/> Default: Disable Auto-Logout <input type="checkbox"/> Enable Validation Code in Internet/LAN Access Internet Access Control <input checked="" type="checkbox"/> Allow management from the Internet Domain name allowed: <input type="text"/> <input type="checkbox"/> FTP Server <input type="checkbox"/> HTTP Server <input type="checkbox"/> Enforce HTTPS Access <input checked="" type="checkbox"/> HTTPS Server <input type="checkbox"/> Telnet Server <input type="checkbox"/> TR069 Server <input type="checkbox"/> SSH Server <input type="checkbox"/> SNMP Server <input checked="" type="checkbox"/> Disable PING from the Internet	Management Port Setup <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports Telnet Port: 23 (Default: 23) HTTP Port: 80 (Default: 80) HTTPS Port: 4433 (Default: 443) FTP Port: 21 (Default: 21) TR069 Port: 8069 (Default: 8069) SSH Port: 22 (Default: 22)	
Brute Force Protection <input type="checkbox"/> Enable brute force login protection <input type="checkbox"/> FTP Server <input type="checkbox"/> HTTP Server <input type="checkbox"/> HTTPS Server		

5. (Önerilen) Brute Force Attack'i etkinleştirin

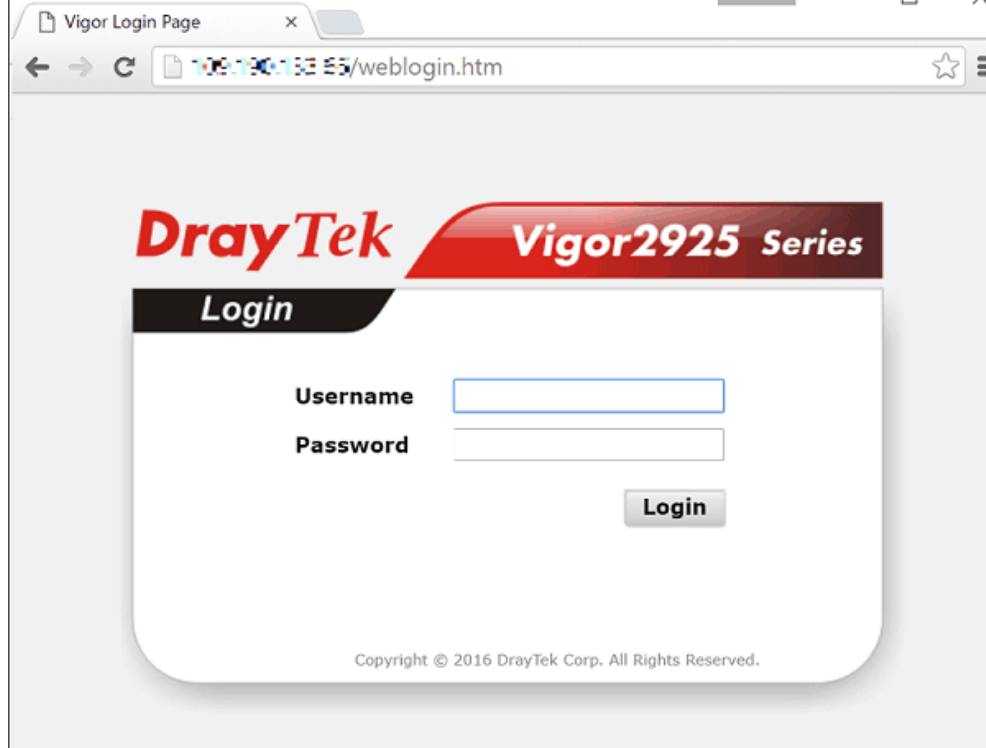
Router'ı saldırınlardan korumak için yönetim şifresini tahmin ediyorum.

System Maintenance >> Management

IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup															
Router Name: DrayTek																	
<input type="checkbox"/> Default: Disable Auto-Logout <input type="checkbox"/> Enable Validation Code in Internet/LAN Access Internet Access Control <input checked="" type="checkbox"/> Allow management from the Internet Domain name allowed: <input type="text"/> <input type="checkbox"/> FTP Server <input type="checkbox"/> HTTP Server <input type="checkbox"/> Enforce HTTPS Access <input checked="" type="checkbox"/> HTTPS Server <input type="checkbox"/> Telnet Server <input type="checkbox"/> TR069 Server <input type="checkbox"/> SSH Server <input type="checkbox"/> SNMP Server <input checked="" type="checkbox"/> Disable PING from the Internet	Management Port Setup <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports Telnet Port: 23 (Default: 23) HTTP Port: 80 (Default: 80) HTTPS Port: 4433 (Default: 443) FTP Port: 21 (Default: 21) TR069 Port: 8069 (Default: 8069) SSH Port: 22 (Default: 22)																
Brute Force Protection <input checked="" type="checkbox"/> Enable brute force login protection <input type="checkbox"/> FTP Server <input checked="" type="checkbox"/> HTTPS Server <input type="checkbox"/> Telnet Server <input type="checkbox"/> TR069 Server <input type="checkbox"/> SSH Server Maximum login failures: 0 times Penalty period: 0 seconds																	
Access List from the Internet <table border="1"> <thead> <tr> <th>List</th> <th>index in IP Object</th> <th>IP / Mask</th> </tr> </thead> <tbody> <tr> <td>1</td> <td></td> <td></td> </tr> <tr> <td>2</td> <td></td> <td></td> </tr> <tr> <td>3</td> <td></td> <td></td> </tr> <tr> <td>4</td> <td></td> <td></td> </tr> </tbody> </table>			List	index in IP Object	IP / Mask	1			2			3			4		
List	index in IP Object	IP / Mask															
1																	
2																	
3																	
4																	
Blocked IP List																	

6. Router'e İnternette'nden Erişim

Bir tarayıcı açın, adres çubuğuna [https:// \[Router'in WAN IP\]](https://[Router'in WAN IP]) yazın ve Enter tuşuna basın. Router'in Web-based UI giriş sayfasını görmelisiniz. (NOT: Router'in HTTPS portunu değiştirdiyse'niz, IP adresinden sonraki port numarasını belirtin.)



LINUX

1. İnternete bağlanın

WAN Interface'nin çevrimiçi olduğundan ve Router'in public bir IP adresine sahip olduğundan emin olun.

2. İnternette'nden erişime izin ver

System Maintenance >> Access Control'e gidin. Internet Access Control'de, internette'nden erişmek istediğiniz yönetim arayüzü için "Enable" i seçin. (CLI için SSH, Web UI HTTPS erişimi). Yukarıdaki yapılandırma ile, Router'in web yönetim sayfasına internette'nden [https:// \[Vigor3900'ün WAN IP\]](https://[Vigor3900'ün WAN IP]) adresini kullanarak erişebilirsiniz.

System Maintenance >> Access Control >> Access Control

Access Control | Fail to Ban | Access Barrier

Default: Disable Auto-Logout : Enable Disable

Use Validation Code : Enable Disable

Customized Login Image : Enable Disable

Internet Access Control

Apply to WAN Interface : wan1, wan2, usb1,...

Web Allow : Enable Disable

Telnet Allow : Enable Disable

SSH Allow : Enable Disable

HTTPS Allow : Enable Disable

FTP Allow : Enable Disable

SAMBA Allow : Enable Disable

Server Certificate : Default

3. (Önerilen) Erişim Listesini Ayarla

Uzaktan erişimi yalnızca belirli bir IP ile sınırlamak için, Access List'i etkinleştirin, ardından remote hostun public IP'sini IP List'e ekleyin. Aşağıdaki yapılandırma sadece IP 1.2.3.4'teki hostun Router'e WAN'dan erişebileceği anlamına gelir. (Remote Access peer de statik bir public IP yoksa, seçenek devre dışı bırakılmalıdır.)

Access List : Enable Disable

Add Save Profile Number Limit : 16

IP	Subnet Mask
1.2.3.4	255.255.255.255

4. (Önerilen) Değişim yönetimi bağlantı noktası

Daha yüksek güvenlik için, management(yönetim) portunu değiştirebilirsiniz. Yönetim portunu değiştirirseniz, IP adresinden sonra port numarasını belirtmeniz gerekecektir. Örneğin, aşağıdaki yapılandırma ile Router'in yönetim sayfasına https:// [Vigor3900'un WAN IP]: 4433 üzerinden erişebilirsiniz.

Management Port Setup

Web Port : 80 Default:80

Telnet Port : 23 Default:23

SSH Port : 2222 Default:22

HTTPS Port : 4433 Default:443

SSL VPN Port : 443 Default:443

FTP Port : 21 Default:21