

***DrayTek***

*DrayTek*  
***Beheren vanaf het Internet***



## Inhoudsopgave

DrayTek beheren vanaf het Internet .....	3
WAN IP adres controleren .....	4
Toegang vanaf het Internet .....	5
Access List .....	6
Brute Force Protectie .....	7

## DrayTek beheren vanaf het Internet

Om de DrayTek te beheren dient u normaal gesproken met hetzelfde netwerk verbonden te zijn als de DrayTek. De DrayTek ondersteund ook beheer op afstand zodat u waar dan ook ter wereld toegang kunt krijgen tot uw DrayTek router/modem. In deze handleiding leggen we uit hoe u de DrayTek op afstand kan benaderen.



## WAN IP adres controleren

Navigeer in de DrayTek naar **Online Status >> Physical Connection** en controleer onder **WAN Status IP** of een Public IP adres wordt weergegeven. Wanneer u een private IP adres ontvangt is het niet mogelijk om toegang tot de router toe te staan. In dat geval dient eerst poorten open te zetten in de router/modem die voor de DrayTek staat.

Noteer het onderstaande weergegeven IP adres.

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)
192.168.158.95	168.95.192.1	5,041	215	5,689	393

**Informatie:** De onderstaande IP adressen zijn private IP adressen:

10.0.0.0      t/m    10.255.255.255  
172.16.0.0    t/m    172.31.255.255  
192.168.0.0   t/m    192.168.255.255

## Toegang vanaf het Internet

Navigeer naar “**System Maintenance >> Management**” en zet een vinkje bij “**Allow management from the Internet**” gevolgd door **HTTP** en/of **HTTPS Server** aan te vinken.

Op basis van de onderstaande configuratie zal de router toegankelijk worden via HTTP poort 80 en HTTPS poort 443.

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  
**Note:** IE8 and below version does NOT support DrayOS CAPTCHA auth code.

**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

**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

Klik vervolgens op **OK** en herstart de router.

Controleer of de DrayTek benaderbaar is door in een browser het volgende in te typen:

http://{Het WAN IP van de DrayTek}    *zonder de {}*

https://{Het WAN IP van de DrayTek}    *zonder de {}*

**Opmerking:** Wanneer de poorten niet default zijn (http=80 https=443) dient u achter het WAN IP ook het betreffende poort nummer in te vullen. Voorbeeld: http://80.78.468.46:**8080**

## Access List

Om te voorkomen dat iedereen toegang kan krijgen tot uw DrayTek kunt u gebruik maken van een access list zodat alléén specifieke IP adressen toegang krijgen tot uw router.

Klik onder **Access List from the Internet** op **IP Object** waarna u verschillende objecten(Index regels) aan kunt maken voor de IP adressen die u toegang wilt geven tot de DrayTek. Onthoud de aangemaakte Index nummer(s) en vul deze onder de Access List in.

**Access List from the Internet**

Apply Access List to PING

List	index in IP Object	IP / Mask
1	1	79.99.134.3/255.255.255.255
2	2	79.99.134.5/255.255.255.255
3		
4		
5		
6		
7		
8		
9		
10		

Klik op **OK** om de instellingen op te slaan.

## Brute Force Protectie

Om te voorkomen dat hackers het wachtwoord van de router proberen te raden kunt u de optie Brute Force Protection inschakelen op basis van HTTP of HTTPS.

In het onderstaande voorbeeld zal een gebruiker worden geblokkeerd zodra hij of zij drie keer achter elkaar foutieve inloggegevens heeft ingevoerd. De blokkade zal in dit geval 900 seconden(15 minuten) lang duren.

**Brute Force Protection**

Enable brute force login protection

FTP Server

HTTP Server

HTTPS Server

Telnet Server

TR069 Server

SSH Server

Maximum login failures  times

Penalty period  seconds

**Blocked IP List**



### **Voorbehoud**

We behouden ons het recht voor om deze en andere documentatie te wijzigen zonder de verplichting gebruikers hiervan op de hoogte te stellen. Afbeeldingen en screenshots kunnen afwijken.

### **Copyright verklaring**

© 2020 DrayTek

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand en/of openbaar gemaakt in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of op enige andere manier zonder voorafgaande schriftelijke toestemming van de uitgever.

Ondanks alle aan de samenstelling van deze handleiding bestede zorg kan noch de fabrikant, noch de auteur, noch de distributeur aansprakelijkheid aanvaarden voor schade die het gevolg is van enige fout uit deze uitgave.

### **Trademarks**

Alle merken en geregistreerde merken zijn eigendom van hun respectievelijke eigenaren.