

DrayTek

DrayOS5

Beheer vanaf het Internet



Inhoudsopgave

Beheer vanaf het Internet	3
WAN IP adres controleren	4
Management.....	5
WAN Access Control	6
Brute Force Protection	7

Beheer vanaf het Internet

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

Belangrijk: Wanneer u beheer op afstand inschakelt, moet u er rekening mee houden dat dit toegankelijk is voor iedereen. Het advies is om altijd het volgende te doen:

- Maak gebruik van een sterk admin wachtwoord.
- Wijzig de managementpoort(en).
- Maak gebruik van een Access List om toegang te beperken tot enkele IP-adressen.
- Schakel Brute Force Protection in.
- Gebruik twee-factorauthenticatie (2FA)

Voor de 2FA feature is een handleiding te vinden op www.draytek.nl.



WAN IP adres controleren

Navigeer in de DrayTek naar het Dashboard en controleer onder WAN STATUS of een Public IP adres wordt weergegeven. Dit IP-adres moet overeenkomen met een controle op www.watismijnip.nl.

Wanneer u een private IP adres ontvangt is het niet mogelijk om (direct) toegang tot de router toe te staan. In dat geval dient u eerst poorten open te zetten in de router/modem welke voor de DrayTek staat.

The screenshot shows the DrayTek dashboard with two main sections: PORT STATUS and WAN STATUS.

PORT STATUS: A diagram of the router's ports. The WAN port is highlighted in blue and labeled '2.5G'. The LAN ports are labeled P1, P2, P3, and P4, with P1 and P2 also labeled '2.5G'. There are two USB ports labeled '1' and '2'.

WAN STATUS: A table showing the WAN configuration. The 'IPv4' tab is selected. The table has columns for Name, MAC Address, Connection Type, IP Address, Gateway, Primary DNS, Secondary DNS, and Uptime.

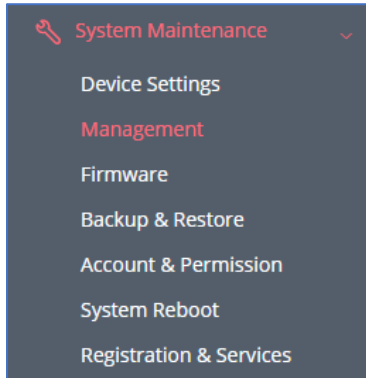
Name	MAC Address	Connection Type	IP Address	Gateway	Primary DNS	Secondary DNS	Uptime
[WAN] WAN1	14:49:BC:6E:14:29	Static IP	80. <input type="text"/>	80. <input type="text"/>	8.8.8.8	8.8.4.4	04:20:34

Belangrijk: 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

Management

Beheer vanaf het internet toestaan is mogelijk in het menu System Maintenance > Management.



Hier ziet u de standaard management services die actief zijn op een DrayTek, voor de LAN interface staan deze default reeds ingeschakeld. Voor de IPv4 en IPv6 WAN interface niet, per management protocol kunt u deze inschakelen. Daarnaast kun u de management poorten wijzigen.

System Maintenance / Management

Service Control TR-069

General

Auto Logout

Management Services

Enforce HTTPS Access

	Port	(default)	LAN Access	IPv4 WAN Access	IPv6 WAN Access
HTTP	<input type="text" value="80"/>	(80)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
HTTPS	<input type="text" value="443"/>	(443)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SSH	<input type="text" value="22"/>	(22)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Telnet	<input type="text" value="23"/>	(23)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SNMP	<input type="text" value="161"/>	(161)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	LAN Access	IPv4 WAN Access	IPv6 WAN Access
Ping	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Klik vervolgens op **Apply** om de instellingen op te slaan.

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

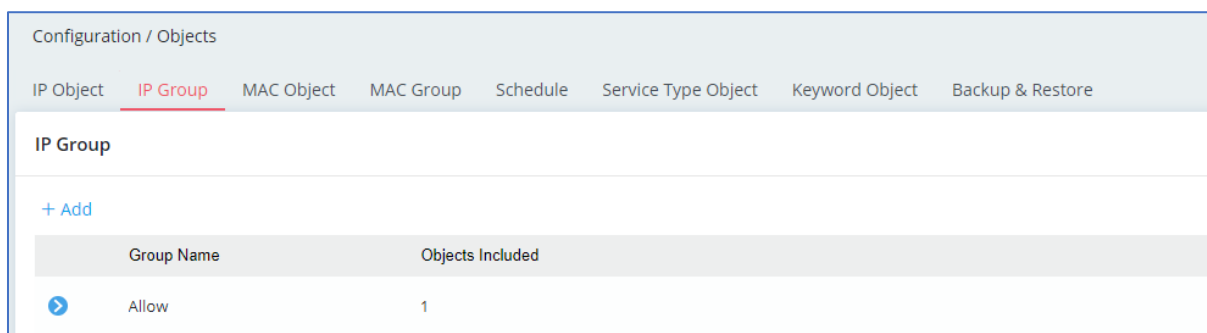
http://{Het WAN IP van de DrayTek} *zonder de {}*

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

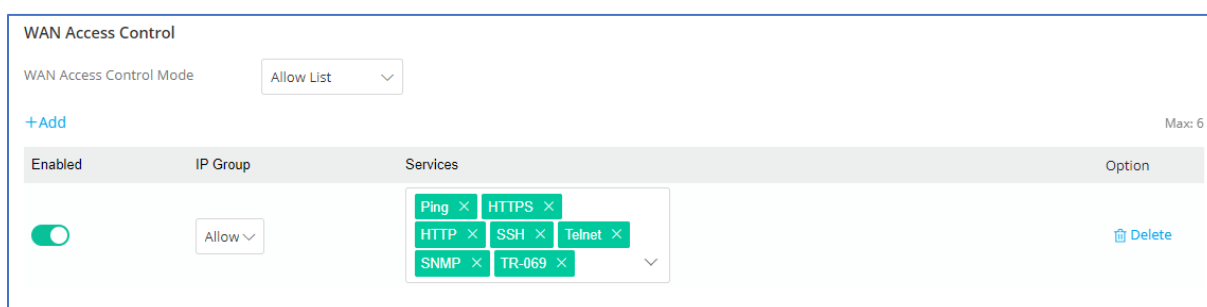
Opmerking: Wanneer de poorten niet default zijn ($http=80$ $https=443$) dient u achter het WAN IP ook het betreffende poort nummer in te vullen. Voorbeeld: $https://80.90.100.200:4433$

WAN Access Control

Om te voorkomen dat de router voor iedereen toegankelijk wordt, kunt u gebruik maken van een allow list zodat alléén specifieke IP adressen toegang krijgen tot uw router. Hiervoor dient u één of meerdere IP-objecten aan te maken welke u vervolgens in een IP Group plaatst.



Vervolgens kunt u bij WAN Access Control een Allow List aanmaken en hier de IP Group selecteren met daarin de management services die u wilt toestaan voor de geselecteerde IP Group.

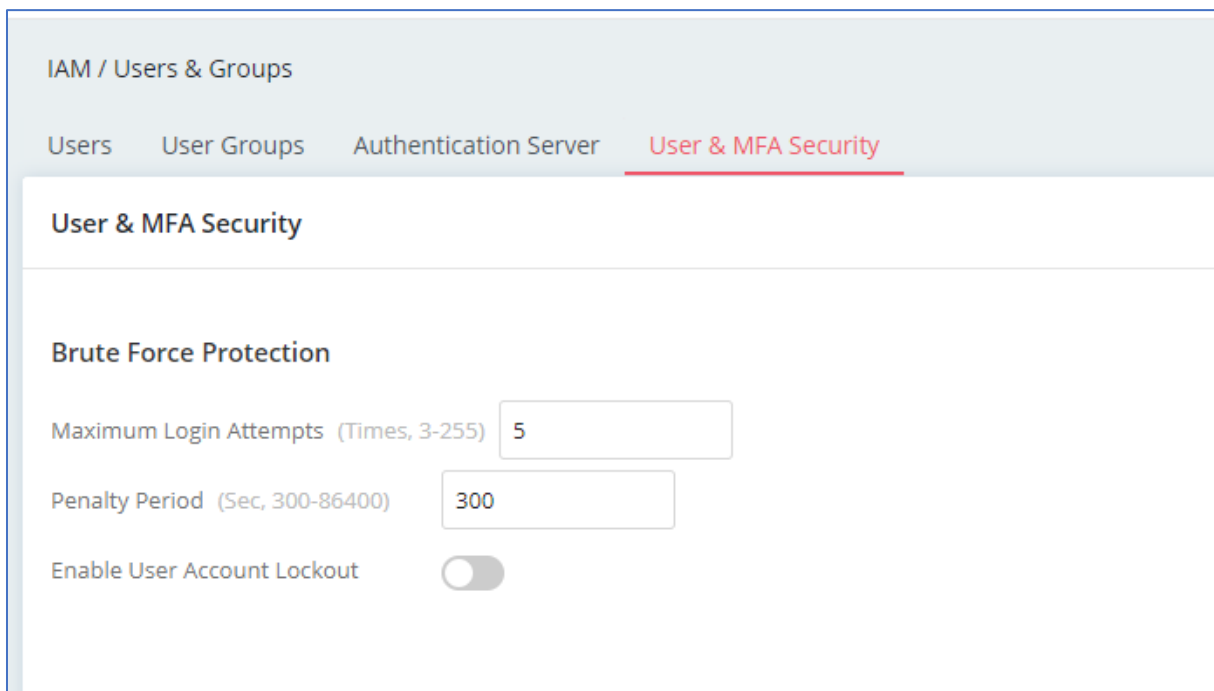


Klik op **Apply** om de instellingen op te slaan.

Let op! Standaardgebruikersaccounts hebben geen toestemming om vanaf het internet in te loggen. Zorg ervoor dat de optie "Allow Login from WAN" voor het betreffende account is ingeschakeld (te vinden onder System Maintenance / Account & Permission).

Brute Force Protection

Brute Force Protection staat standaard ingeschakeld en zorgt ervoor dat clients vanaf het internet niet onbeperkt een login poging kunnen uitvoeren. Standaard kan een client (publiek IP) 5 keer een login poging wagen, na deze 5 keer zal dit IP-adres voor 300 seconden op de blocklist worden gezet.



The screenshot shows the 'User & MFA Security' settings page in the Azure AD portal. The breadcrumb trail is 'IAM / Users & Groups' > 'Users' > 'User Groups' > 'Authentication Server' > 'User & MFA Security'. The 'User & MFA Security' section is expanded to show the 'Brute Force Protection' settings. The 'Maximum Login Attempts' is set to 5, the 'Penalty Period' is set to 300 seconds, and the 'Enable User Account Lockout' toggle is turned on.

Setting	Value
Maximum Login Attempts (Times, 3-255)	5
Penalty Period (Sec, 300-86400)	300
Enable User Account Lockout	On

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

© 2024 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.