DrayTek

DrayOS5

IKEv2 EAP - macOS

Inhoudsopgave

IKEv2 EAP

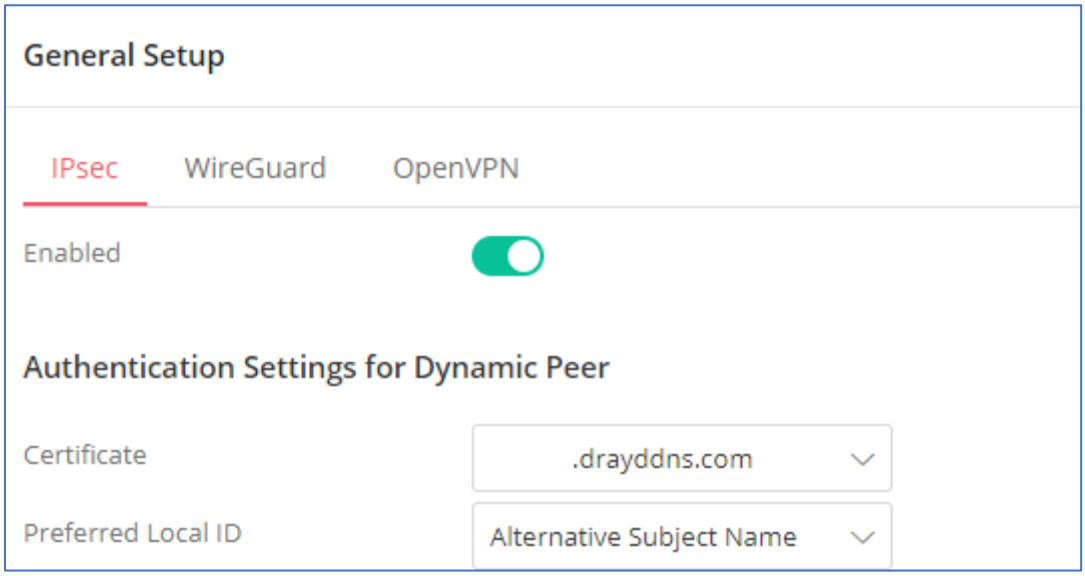
IKEv2 staat voor Internet Key Exchange version 2 en is een protocol dat wordt gebruikt voor het opzetten van Virtual Private Network (VPN) tunnels voor veilige communicatie over internet. Het is een belangrijk onderdeel van IPsec (Internet Protocol Security), dat wordt gebruikt voor het versleutelen en authenticeren van gegevens die over een netwerk worden verzonden. EAP is een flexibel authenticatieframework dat verschillende methoden ondersteunt voor het verifiëren van de identiteit van gebruikers of apparaten die verbinding maken met een netwerk. Met IKEv2 EAP kunnen apparaten een veilige communicatieverbinding tot stand brengen en kunnen ze EAP gebruiken voor de authenticatie van de gebruiker.

Voor het gebruik van IKEv2 EAP is het noodzakelijk een Let's Encrypt certificaat te hebben, deze kunt u gratis aanvragen icm een DrayDDNS account. De configuratie stappen kunt u terug vinden in de DrayDDNS handleiding op onze website.

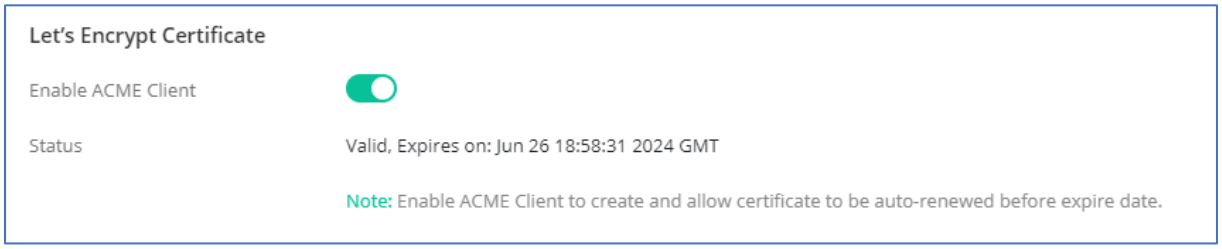
Dit artikel demonstreert hoe je een DrayOS 5 Vigor Router configureert als een VPN-server voor IKEv2 EAP-clients, en welke configuratie vereist is op macOS om de VPN op te zetten. In het voorbeeld wordt de Vigor2136 router gebruikt icm de Smart VPN applicatie van DrayTek.

IPsec General Setup

Belangrijk is dat u IPsec op enable zet zodat dit VPN protocol gebruikt kan worden.

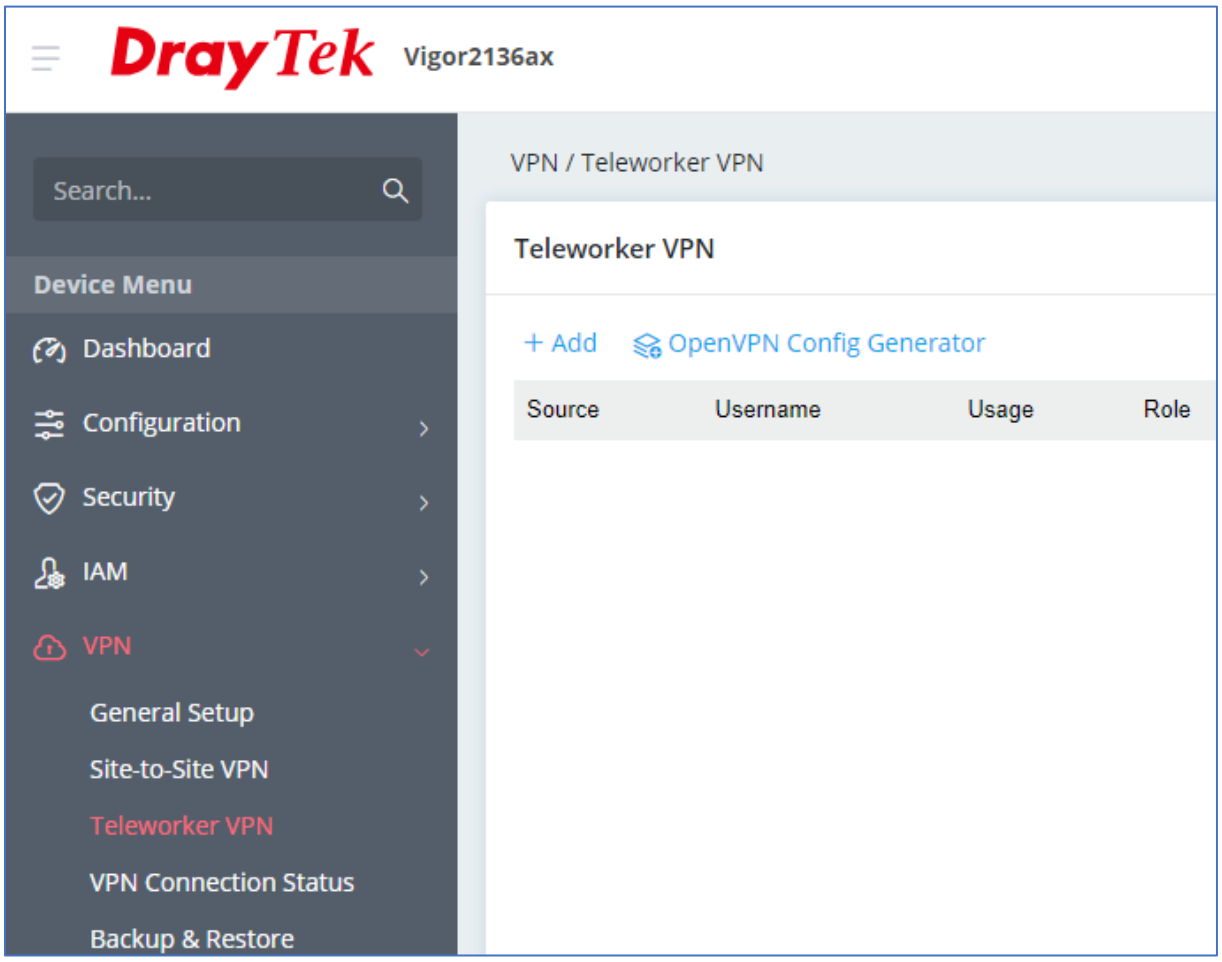


Daarnaast dient u bij Certificate het DrayDDNS certificaat te selecteren, op dit DrayDDNS account dient u de Let's Encrypt te activeren.

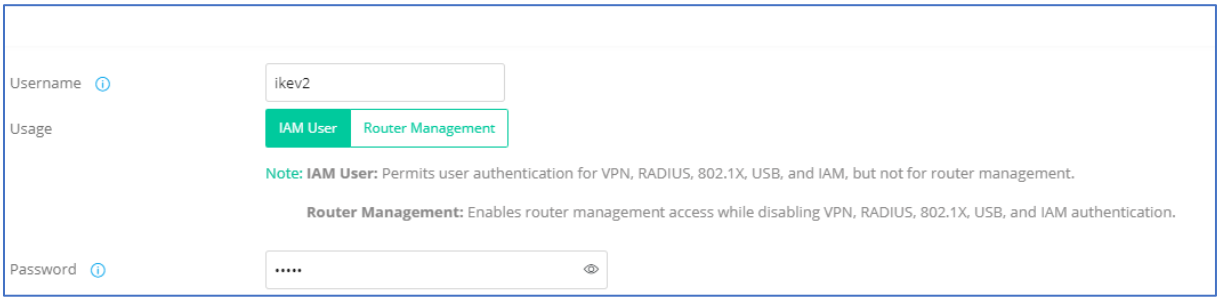


Teleworker VPN instellingen

Voor het aanmaken van een VPN account kunt u bij Teleworker VPN een nieuw account toevoegen om op + Add te klikken.



Geef vervolgens een username en password op, selecteer IAM user om gebruik te kunnen maken van VPN.

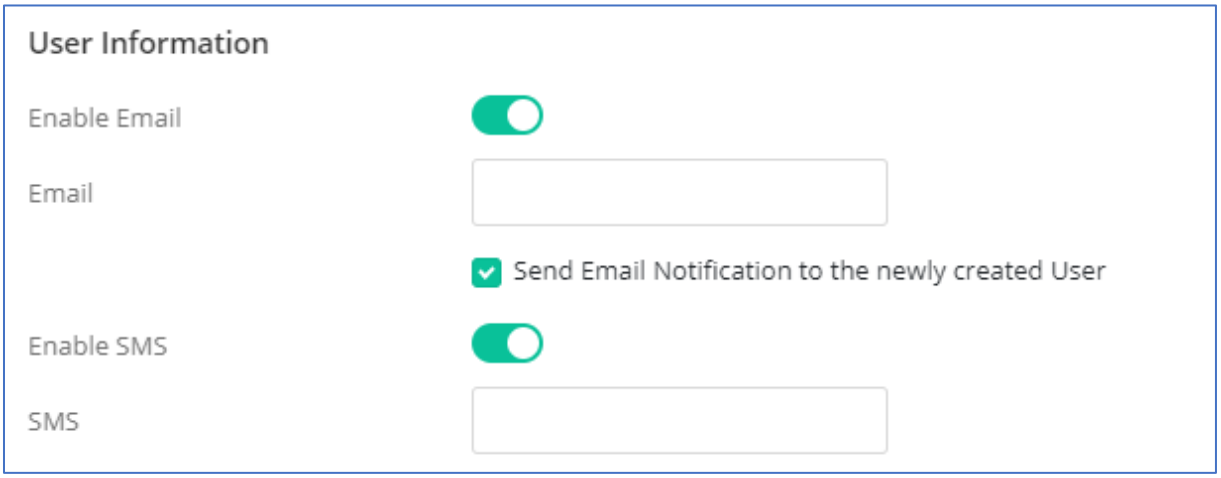


General

Naast het in en uitschakelen van een VPN profiel kunt u hier tevens een group policy koppelen aan het VPN account. Daarnaast kunt u een verval datum koppelen aan het VPN profiel. De Group Policy kunt u verder inrichten in het IAM menu, raadpleeg hiervoor de IAM handleiding op onze website voor meer informatie.

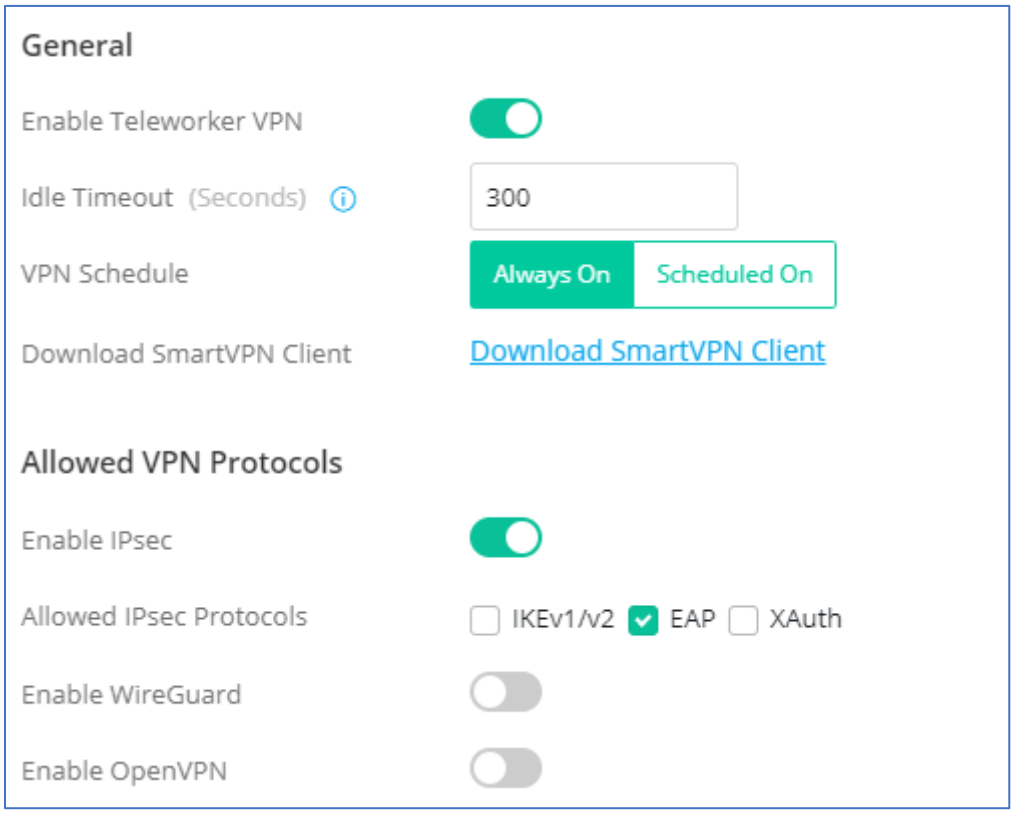
User Information

Per gebruikers account kunt u e-mail adres of 06-nummer achterlaten. Deze informatie kan gebruikt worden wanneer u gebruik maakt van MFA. Indien u hier gebruik van wilt maken dient u een koppeling te hebben met een SMTP server of SMS provider, verder configuratie is mogelijk onder Configuration > Notification Services.



Teleworker VPN

Hier activeert u het VPN profiel voor dit account, daarnaast kunt u hier aangeven welke VPN protocollen gebruikt kunnen worden om een VPN tunnel op te bouwen. We selecteren in dit geval enkel EAP.

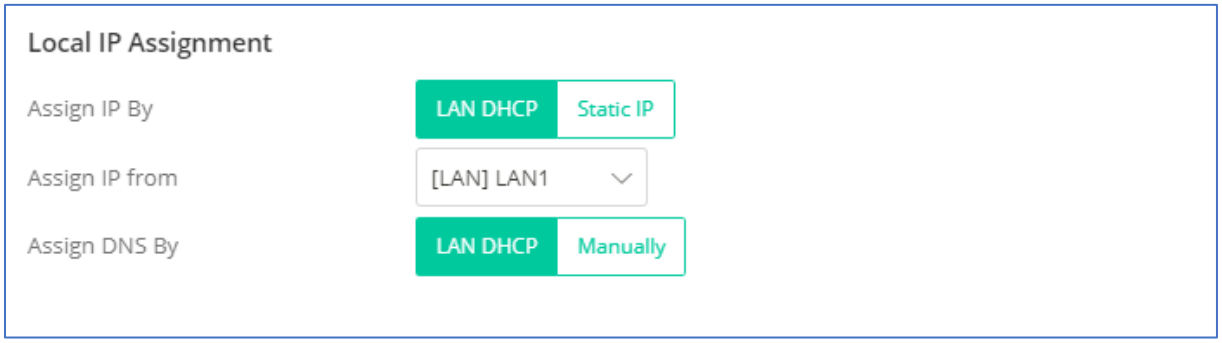


Security

In verband met Zero Trust is het noodzakelijk dat u hier het publieke/Internet IP-adres opgeeft van de VPN client die verbinding wil maken. Het is helaas niet mogelijk om met een Dynamic IP-adres een IKEv2 EAP verbinding op te zetten.

Local IP Assignment

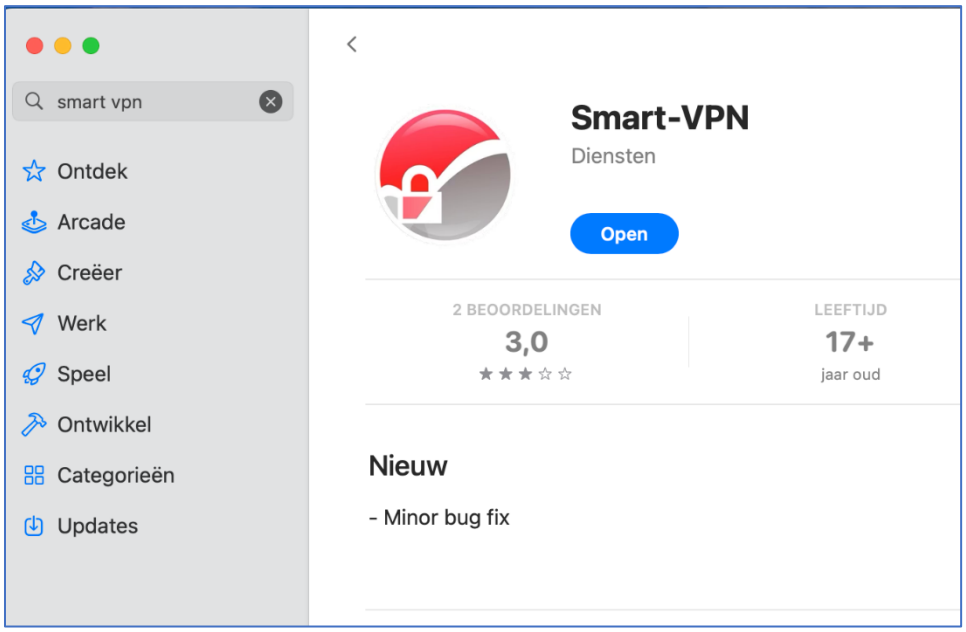
Bij Local IP Assignment kunt u de VPN client een vast IP-adres geven of de keuze op DHCP laten staan, de VPN client zal dan een IP-adres ontvangen van de DHCP server in de DrayTek.



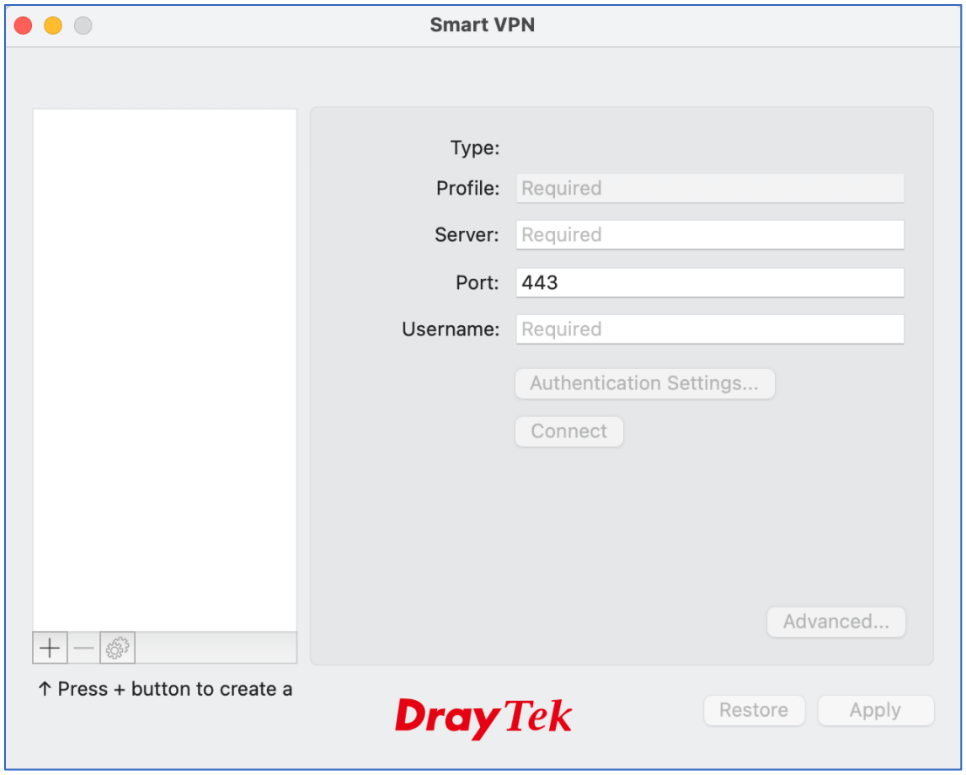
macOS setup

Smart-VPN setup

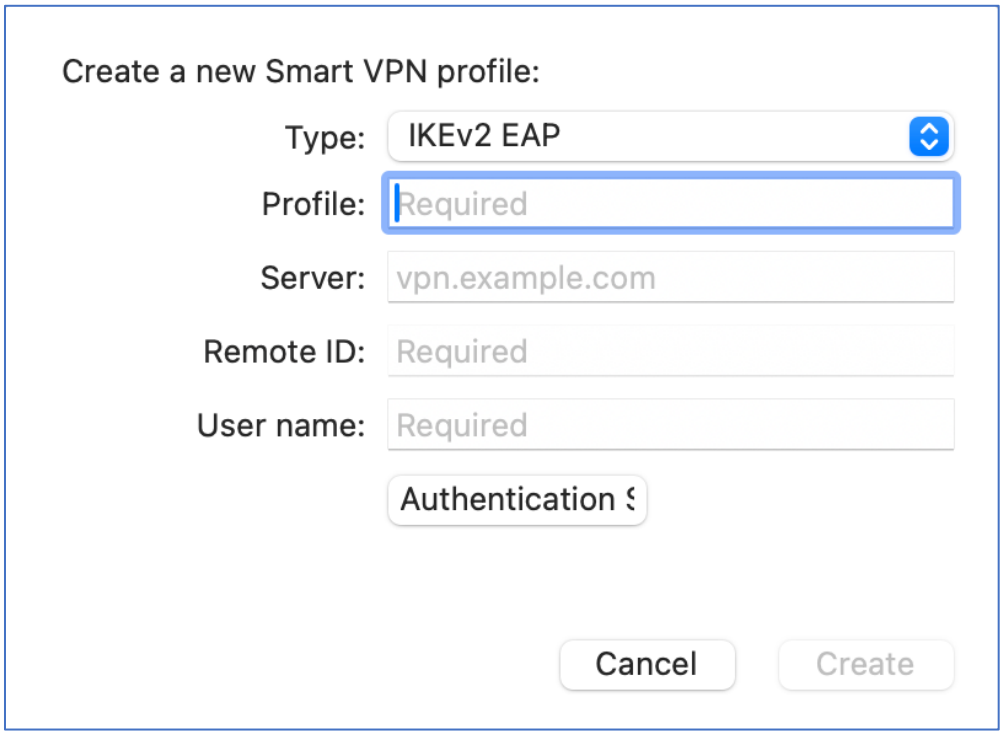
DrayTek heeft tevens een eigen VPN client beschikbaar voor macOS gebruikers, deze VPN client app kunt u gratis downloaden in de App Store op uw Apple device. Deze tool is beschikbaar voor zowel macOS als iOS.



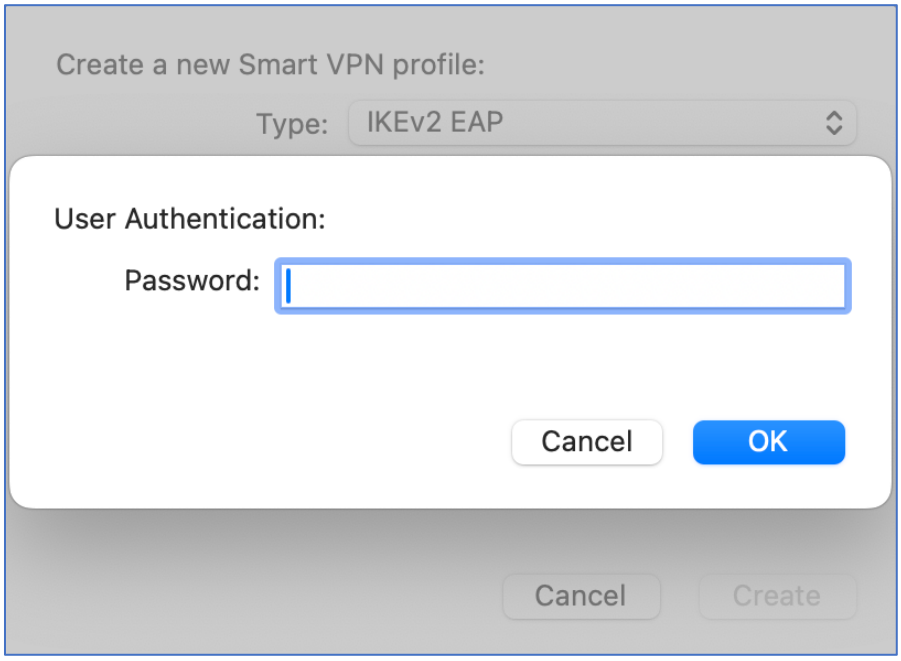
Door op het + teken te klikken kunt u een nieuw VPN profiel inrichten.



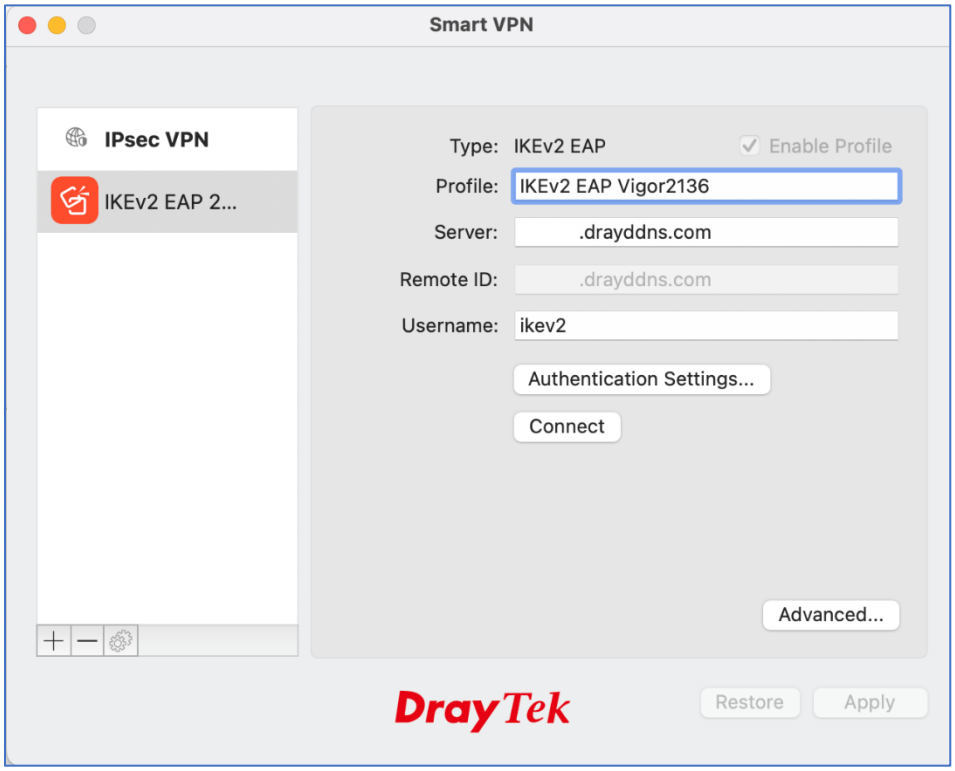
Selecteer bij Type IKEv2 EAP, vervolgens kunt u het profiel een naam geven. Bij Server geeft u het DrayDDNS account in van de DrayTek. Het Remote ID wordt automatisch ingevuld op basis van uw DrayDDNS account. Bij User name kunt u de gebruikersnaam opgeven van de VPN Teleworker die u hebt aangemaakt.

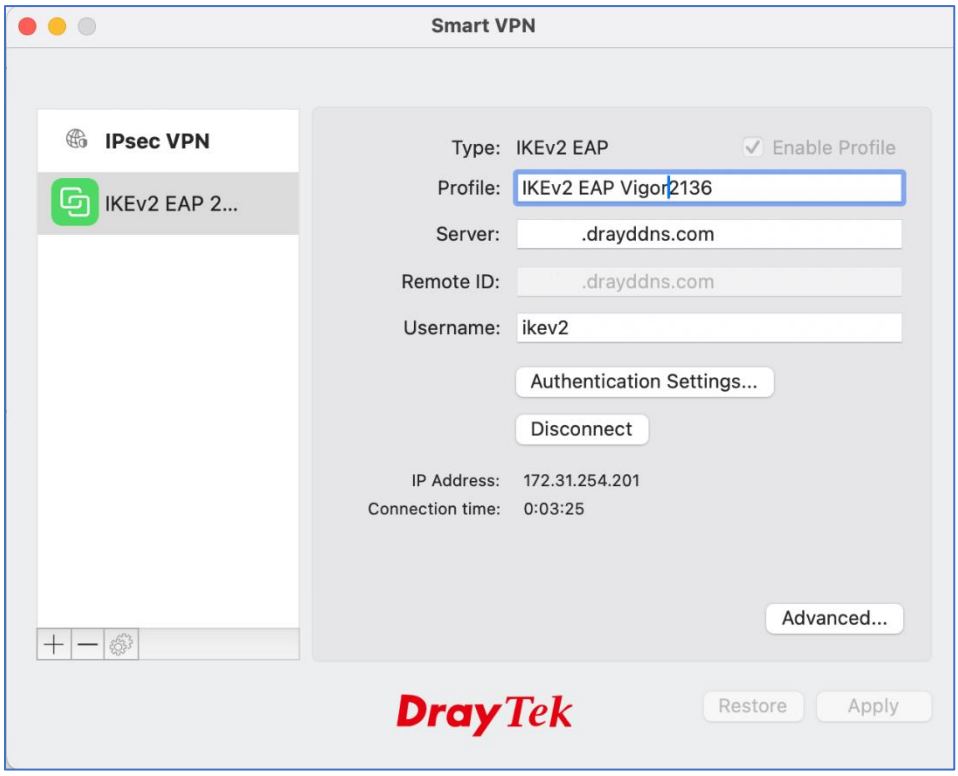


Klik vervolgens op Authentication om het wachtwoord en de XAuth pre-shared key in te vullen. Klik hierna op OK en op Create om het VPN profiel op te slaan.



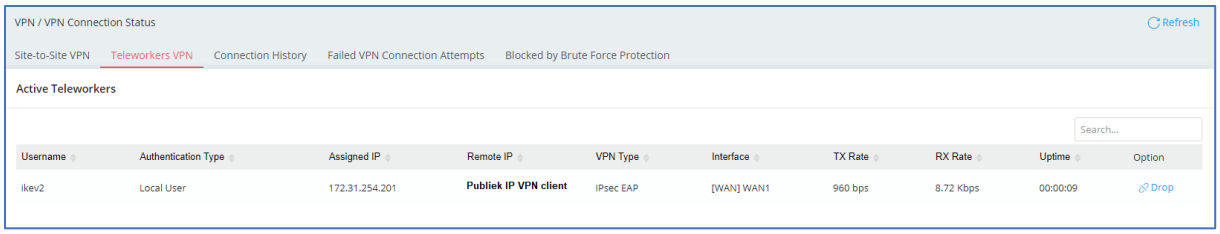
Activeer het profiel door Enable Profile aan te vinken, vervolgens kunt u op Connect klikken om de VPN tunnel op te bouwen.





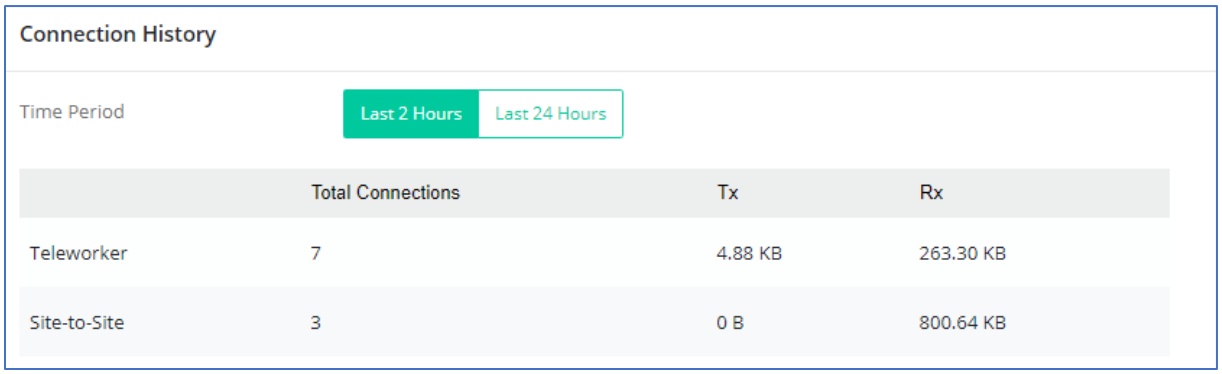
VPN Connection Status

In de DrayTek kunt u onder VPN Connection Status de verbinding informatie terug vinden.

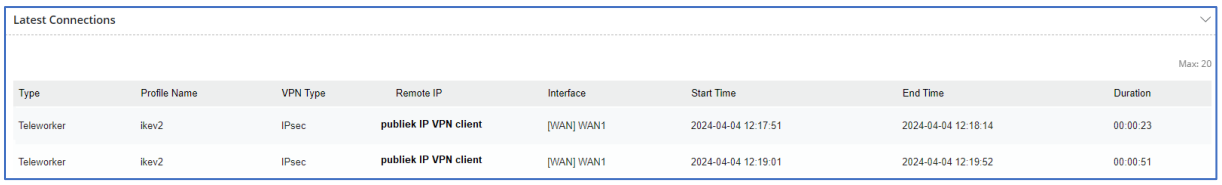


Connection History

Op basis van de laatste 2 uur of laatste 24 uur kunt u bij Connection History informatie terug vinden over de hoeveelheid clients (Teleworkers) of Site-to-Site (LAN-to-LAN) VPN verbindingen er actief zijn geweest.

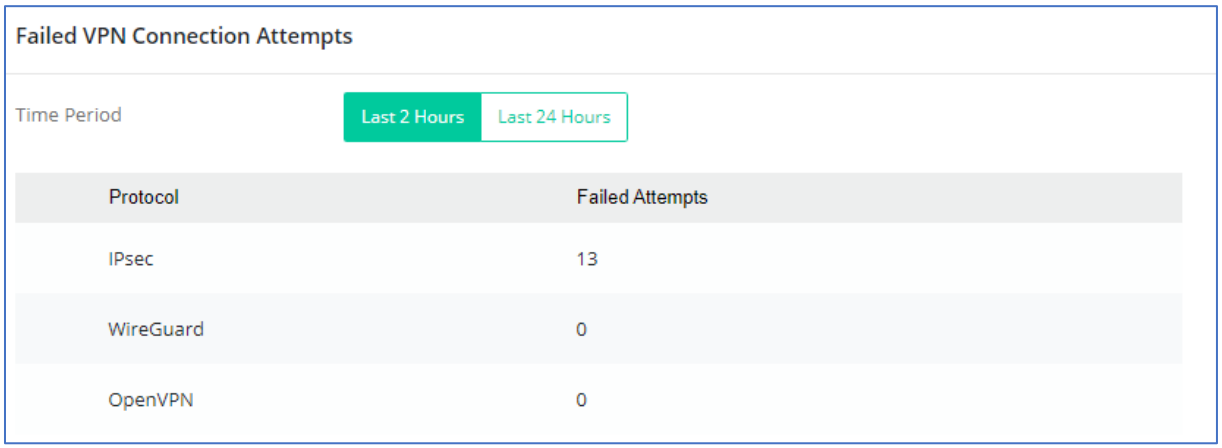


Bij Latest Connections kunt u zien vanaf welk IP-adres deze client verbonden is geweest, op welk moment deze online is gekomen en voor welke duur de tunnel online is geweest.



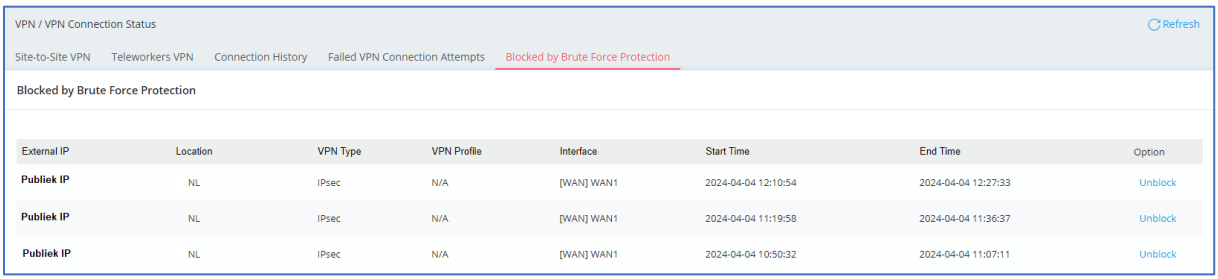
Failed VPN Connection Attemps

Indien de VPN tunnel niet online komt zal deze informatie terug te vinden zijn bij het tabblad Failed VPN Connection Attempts. Op basis van de laatste 2 uur of 24 uur kunt u deze informatie inzien.



Blocked by Brute Force Protection

Indien u Brute Force Protection hebt aangezet onder VPN > General Setup kunt u hier informatie vinden over IP-adressen die zijn geblokkeerd vanwege Brute Force Protection. Dit kan gebeuren als gevolg van onjuiste VPN-inloggegevens, zoals een verkeerd wachtwoord. Het kan echter ook een onbekend IP-adres zijn dat probeert een tunnel op te zetten via een specifiek VPN-protocol.



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.