

DrayTek

VPN
IPSec XAuth iOS



IPSec XAuth

IPSec XAuth maakt het mogelijk om voor elke gebruiker een eigen VPN account aan te maken, waardoor ze zowel gebruik maken van één algemene XAuth Pre-Shared Key als een username en wachtwoord. In onderstaande FAQ beschrijven wij de stappen die u dient te volgen voor het opzetten van een IPSec XAuth VPN verbinding vanaf een iOS device.

Er zal een algemene IPSec XAuth Pre-shared-key nodig zijn, deze kunt u instellen bij VPN and Remote Access >> IPSec General Setup.

VPN and Remote Access >> IPSec General Setup

VPN IKE/IPsec General Setup
Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

IKE Authentication Method
Certificate for Dial-in: None

General Pre-Shared Key
Pre-Shared Key:

Confirm Pre-Shared Key:

Pre-Shared Key for XAuth User (highlighted with a red box)
Pre-Shared Key:

Confirm Pre-Shared Key:

IPsec Security Method
 Medium (AH)
Data will be authenticated, but will not be encrypted.

High (ESP) DES 3DES AES
Data will be encrypted and authenticated.

OK Cancel

Vervolgens dient u één of meerdere VPN Remote Dial In Users aan te maken, per VPN gebruiker kunt u een eigen account aanmaken zodat iedere gebruiker zijn eigen gebruikersnaam en wachtwoord kan gebruiken.

VPN and Remote Access >> Remote Dial-in User

Index No. 1

User account and Authentication

Enable this account
Idle Timeout second(s)

Allowed Dial-In Type

PPTP
 IPsec Tunnel
 L2TP with IPsec Policy
 SSL Tunnel
 IPsec XAuth
 Specify Remote Node
Remote Client IP
or Peer ID

Username
Password
 Enable Mobile One-Time Passwords(mOTP)
PIN Code
Secret

IKE Authentication Method

Pre-Shared Key
IKE Pre-Shared Key
 Digital Signature(X.509)

IPsec Security Method

Medium(AH)
 High(ESP) DES 3DES AES

Klik op OK om het VPN profiel op te slaan.

VPN configuratie iOS

Via het instellingen menu kunt u naar VPN gaan om hier een nieuwe VPN verbinding aan te maken. Als Type selecteert u IPsec waarbij de volgende instellingen belangrijk zijn:

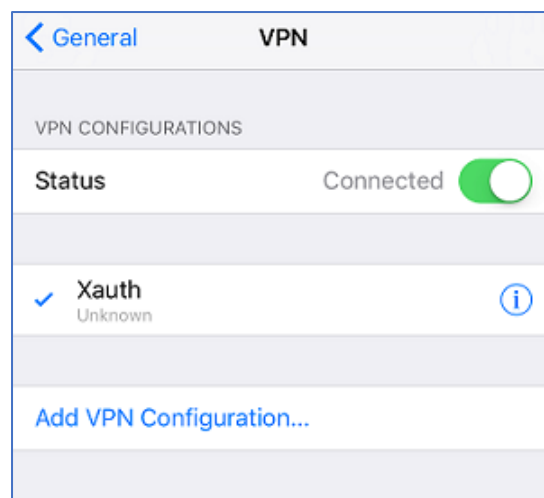
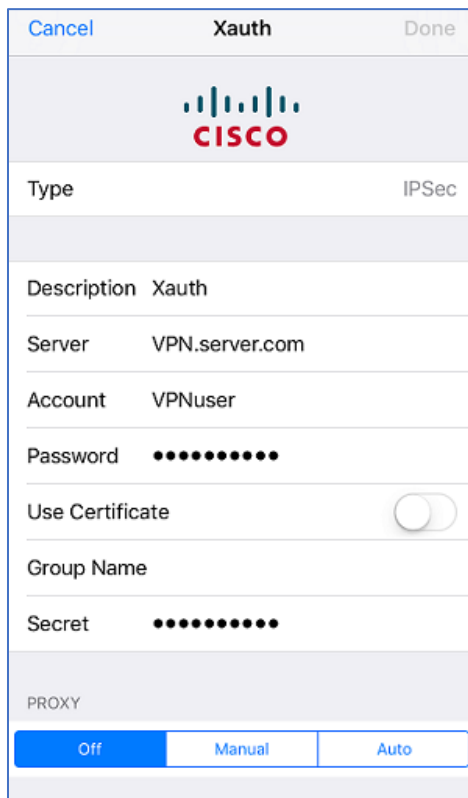
Description: Omschrijving van het VPN profiel welke u aanmaakt.

Server: Publiek IP-adres/DNS naam waar u de VPN tunnel naar op wilt zetten.

Account: Username van de VPN gebruiker

Password: Password van de VPN gebruiker

Secret: IPsec XAuth Pre-Shared Key welke is opgegeven in de configuratie van de DrayTek.



Klik op Gereed om het profiel op te slaan. U kunt vervolgens het VPN profiel selecteren en de VPN verbinding opbouwen.

Wanneer de VPN verbinding succesvol online is gekomen zal dit tevens te zien zijn in de DrayTek onder VPN and Remote Access >> Connection Management.

VPN and Remote Access >> Connection Management

Dial-out Tool | [Refresh](#) |

General Mode: ▼

Backup Mode: ▼

Load Balance Mode: ▼

VPN Connection Status

All VPN Status
LAN-to-LAN VPN Status
Remote Dial-in User Status

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Kbps)	Rx Pkts	Rx Rate(Kbps)	UpTime	
1 (VPNuser)	IPsec Tunnel AES-SHA1 Auth	42.73.98.50 via WAN2	192.168.1.11/32	367	180.34	431	71.85	0:0:3	<input type="button" value="Drop"/>

xxxxxxx : Data is encrypted.
xxxxxxx : Data isn't encrypted.



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.