

İOS'TAN VIGOR ROUTER'A IPsec XAUTH

IPsec çok güvenlidir ve mükemmel performans sunar. Ayrıca 2018'den beri IPsec Xauth sağlamaktadır. Her VPN istemcisiyle aynı pre-shared key kullanırken rahatsız hissediyorsanız onun yerine IPsec Xauth kullanabilirsiniz. IPsec Xauth VPN istemcileri yalnızca pre-shared key ile değil aynı zamanda özgün bir kullanıcı adı ve parola ile doğrulanır. Bu makale Vigor Router'ın IPsec Xauth istemcileri için VPN server olarak nasıl ayarlanacağını ve VPN'i kurmak için iOS cihazında gerekli olan konfigürasyonu gösterir.

Vigor Router Üzerinde Kurulum

1. DrayOS

1. **VPN and Remote Access >> IPsec General Setup** sayfasına gidin ve **Pre-Shared Key** girin.

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	
Pre-Shared Key
Confirm Pre-Shared Key
IPsec Security Method	
<input checked="" type="checkbox"/> Medium (AH)	Data will be authenticated, but will not be encrypted.
<input type="checkbox"/> High (ESP)	<input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
Data will be encrypted and authenticated.	

OK Cancel

2. **VPN and Remote Access >> Remote Dial-in User** sayfasına gidin ve uygun bir indexe tıklayın.

- **Enable this account**'u etkinleştirin.
- **Username** ve **Password** girin.
- Allow Dial-In Type bölümünde **IPsec Xauth**'u etkinleştirdiğinizden emin olun.

VPN and Remote Access >> Remote Dial-in User

Index No. 1

User account and Authentication	
<input checked="" type="checkbox"/> Enable this account	
Idle Timeout	0 second(s)
Allowed Dial-In Type	
<input checked="" type="checkbox"/> PPTP	
<input checked="" type="checkbox"/> IPsec Tunnel	
<input checked="" type="checkbox"/> L2TP with IPsec Policy	None
<input checked="" type="checkbox"/> SSL Tunnel	
<input checked="" type="checkbox"/> IPsec XAuth	
<input type="checkbox"/> Specify Remote Node	
Remote Client IP	
or Peer ID	
Username	VPNuser
Password
<input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP)	
PIN Code	
Secret	
IKE Authentication Method	
<input checked="" type="checkbox"/> Pre-Shared Key	
IKE Pre-Shared Key	Max: 64 characters
<input type="checkbox"/> Digital Signature(X.509)	
None	
IPsec Security Method	
<input checked="" type="checkbox"/> Medium(AH)	
<input type="checkbox"/> High(ESP)	<input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES

- İstemcinin çevrim içi olup olmadığını **VPN and Remote Access >> Connection Management** sayfasından kontrol edebilirsiniz.

VPN and Remote Access >> Connection Management

Dial-out Tool | Refresh |

General Mode:	<input type="text"/>	Dial
Backup Mode:	<input type="text"/>	Dial
Load Balance Mode:	<input type="text"/>	Dial

VPN Connection 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 Drop

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

2. Linux

- User Management >> User Profile sayfasına gidin ve **Add**'e tıklayın.

- Username** ve **Password** girin.
- Enable** tıklayın.
- IPsec User Settings sekmesinde **Xauth** için "Enable" seçin.

User Management >> User Profile >> User Profile

User Profile Apply All

Add Edit Delete Refresh Search

User Profile

Username : VPNuser

Enable

Password : Strength : Excellent

System User : false

PPTP/L2TP/SSL/PPPoE Server General Setup

Idle Timeout(sec) : 300

DHCP from : lan1

Static IP Address : (Optional)

User Management
 PPTP/L2TP/SSL Server
 PPPoE Server
 FTP/SAMBA User Setting
 Radius User Setting
 IPsec User Setting

XAuth : Enable Disable (IPsec User Preshared Key must be configured)

2. **VPN and Remote Access >> IPsec General Setup** sayfasına gidin. **IPsec User Preshared Key** girin. Sonra **Apply**'a tıklayın.

VPN and Remote Access >> IPsec General Setup

IPsec General Setup

Preshared Key : (Max 46 characters)

IPsec User Preshared Key : (Only for XAuth, Max 46 characters)

WAN Profile : wan1, wan2

DHCP LAN Profile : lan1

IKE Port : 500

NAT-T Port : 4500

IPsec MSS : 1360

3. **VPN and Remote Access >> VPN Profile** sayfasına gidin ve aşağıdaki adımları izleyerek bir profil ekleyin.
- Bir Profil adı girin.
 - **Enable** 'ı işaretleyin.
 - **For Remote Dial-In User** için "Enable" seçin.
 - **Local IP / Subnet Mask** için routerın LAN IP'sini girin.

IPsec

Profile : Xauth

Enable

Basic Advanced GRE Proposal Multiple SAs

Auto Dial-Out : Enable Disable

For Remote Dial-In User : Enable Disable

Dial-Out Through : wan1 Default WAN IP WAN Alias IP

Fallback to :

Local IP / Subnet Mask : 192.168.239.0 255.255.255.0/24

Local Next Hop : 0.0.0.0 (0.0.0.0 : default gateway)

Remote Host : 0.0.0.0

Remote IP / Subnet Mask : 0.0.0.0 255.255.255.0/32

More Remote Subnet : No items to show.

IKE Protocol : IKEv1

4. İstemcinin çevrim içi olup olmadığını **VPN and Remote Access >> Connection Management** sayfasından kontrol edebilirsiniz.

VPN and Remote Access >> Connection Management >> Connection Management

Connection Management History

Dial-Out tool

IPsec PPTP SSL Profiles :

Auto Refresh : 1 Minute

Green : Data is encrypted. White : Data isn't encrypted.

VPN Connection Status

VPN	Type	Interface	Remote	Virtual Network	Up Time	RX Rate	TX Rate	RX Byte	TX Byte	Operation
1	VPNuser	IPsec/AES_HMAC...	wan2	220.132...	192.168.239.15/32	00:00:41	4.43 (Kbps)	3.31 (Kbps)	116.39 (KB)	510.44 (KB)

iOS Kurulumu

- VPN konfigürasyonunu aşağıdaki gibi eklemek için **Settings >> General >> VPN** gidin.
 - Type** için "IPsec" seçin.
 - Server**'da routerin WAN IP adresini ya da domainini girin.
 - Account** ve **Password** girin.
 - Secret**'da IPsec Xauth pre-shared key girin.



- VPN bağlantısını başlatmak için profili aktifleştirin.

