

IPSEC XAUTH WINDOWS'TAN VIGOR ROUTER'A

Xauth'lu IPsec tüneli yalnızca önceden paylaşılan bir key değildir ayrıca VPN client tüneli oluştururken kimlik doğrulaması için kullanıcı adı ve parola gerektirir böylece IPsec tüneli güvenliğini artırabilir. Bu makale, Vigor Router ve Windows arasında Xauth ile IPsec tünelinin nasıl oluşturulduğunu göstermektedir.

Vigor Router Kurulumu

1. **VPN and Remote Access >> IPsec General Setup** bölümüne gidin.
 - a. Xauth kullanıcısı için **Pre-Shared Key** bölümüne şifre girin.
 - b. Kaydetmek için **OK**'a tıklayın.

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.
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** bölümüne gidin.
 - a. User account and Authentication 'u **etkinleştirin**.
 - b. IPsec Xauth dial-in türüne **izin verin**.
 - c. Kullanıcı adı ve şifre girin.
 - d. Kaydetmek için **OK**'a tıklayın.

VPN and Remote Access >> Remote Dial-in User

Index No. 1

User account and Authentication

Enable this account

Idle Timeout: 300 second(s)

Allowed Dial-In Type

PPTP

IPsec Tunnel

L2TP with IPsec Policy: None

SSL Tunnel

IPsec XAuth

Specify Remote Node

Remote Client IP: []

or Peer ID: []

Netbios Naming Packet: Pass Block

Multicast via VPN: Pass Block
(for some IGMP,IP-Camera,DHCP Relay..etc.)

Subnet

LAN 1

Assign Static IP Address

0.0.0.0

Username: user

Password: ****

Enable Mobile One-Time Passwords(mOTP)

PIN Code: []

Secret: []

IKE Authentication Method

Pre-Shared Key

IKE Pre-Shared Key: [] Max: 64 characters

Digital Signature(X.509)

None

IPsec Security Method

Medium(AH)

High(ESP): DES 3DES AES

Local ID (optional): []

Note:

Username can not contain characters " and '.

OK Clear Cancel

Windows Client Kurulumu

1. IPsec Xauth'u destekleyen Windows için VPN client yazılımını indirin. Burada örnek olarak **Shrew Soft VPN Client** kullanıyoruz.
2. VPN Access Manager'ı açın
 - a. Add'e tıklayın.



- b. General sekmesinde VPN Hostname or IP Address'i girin.

VPN Site Configuration

General Client Name Resolution Authentication

Remote Host

Host Name or IP Address: 192.168.39.236 Port: 500

Auto Configuration: ike config pull

Local Host

Adapter Mode: Use a virtual adapter and assigned address

MTU: 1380 Obtain Automatically:

Address: . . .

Netmask: . . .

Save Cancel

- Authentication sekmesinde **Mutual PSK+XAuth**'u seçin.
- Local identity ve Remote identity için sırayla **IP Address** ve **any** olarak ayarlayın.
- XAuth kullanıcısı için Pre-Shared Key girin.

VPN Site Configuration

Client Name Resolution Authentication Phase

Authentication Method: Mutual PSK + XAuth

Local Identity Remote Identity Credentials

Identification Type: IP Address

Address String

Use a discovered local host address

Save Cancel

VPN Site Configuration

Client Name Resolution Authentication Phase

Authentication Method: Mutual PSK + XAuth

Local Identity Remote Identity Credentials

Identification Type: Any

Save Cancel

VPN Site Configuration

Authentication Phase 1 Phase 2 Policy

Authentication Method: Mutual PSK + XAuth

Local Identity Remote Identity Credentials

Server Certificate Authority File

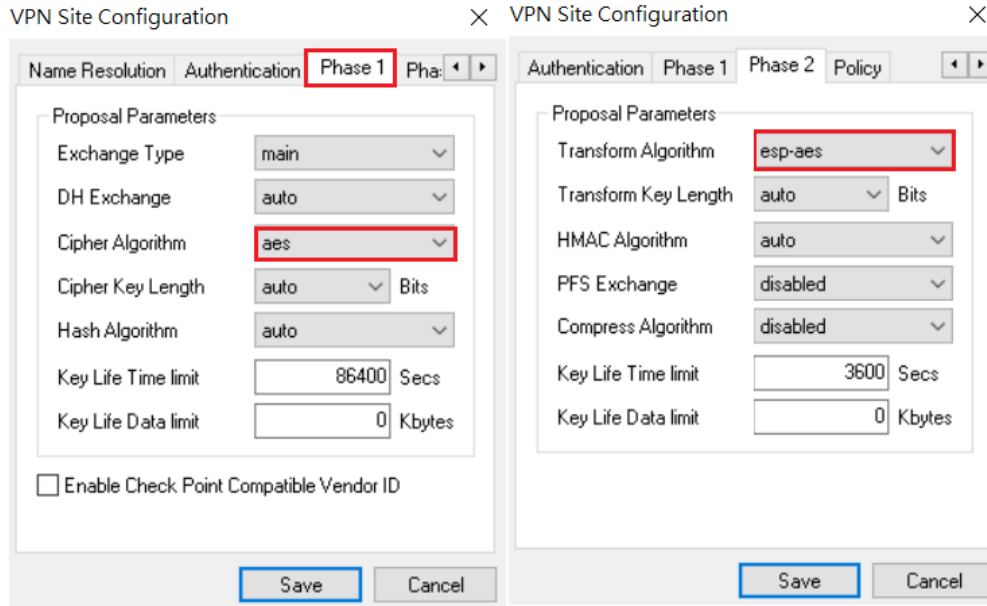
Client Certificate File

Client Private Key File

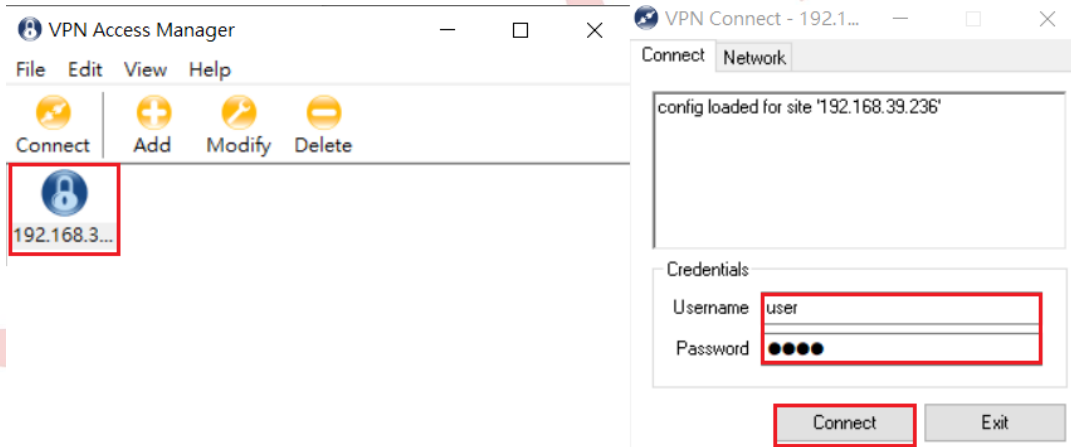
Pre Shared Key: ●●●●

Save Cancel

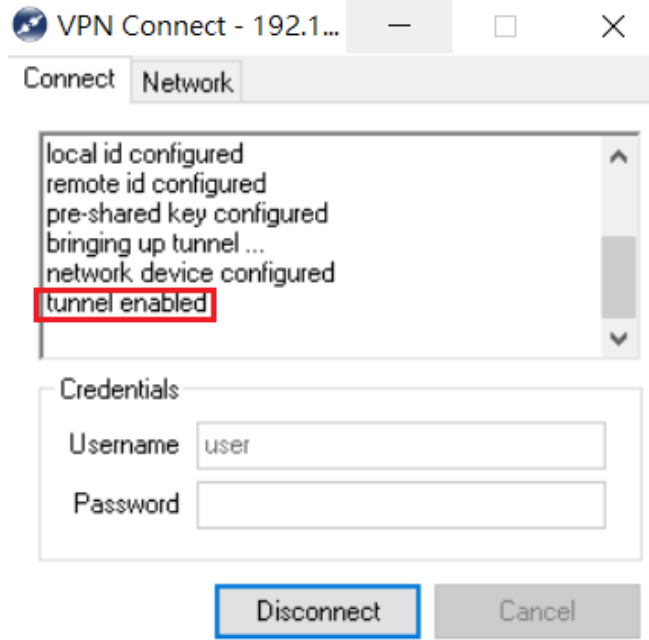
- Phase 1 kurulumunda Cipher Algorithm bölümünü **aes** olarak ayarlayın.
- Phase 2 kurulumunda Transform Algorithm bölümünü **esp-aes** olarak ayarlayın.



- h. Save butonuna tıklayın.
- i. Kaydedilen VPN Client'a tıklayın ve IPsec VPN tüneline oluşturmak için içerdeki kullanıcının kullanıcı adını ve şifresini girin.



Son olarak, VPN Connect mesajı aşağıdaki gibi görünecektir.



Ve Vigor Router'ın VPN durumunu **VPN and Remote Access >> Connection Management** sayfasından görebilirsiniz.

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(bps)	Rx Pkts	Rx Rate(bps)	UpTime
1 (user)	IPsec Tunnel AES-MD5 Auth	192.168.39.232 via WAN2	192.168.1.26/32	3096	32	1423	48	0:9:54 <input type="button" value="Drop"/>