

WINDOWS'TAN VIGOR ROUTER'A IPsec AGGRESSIVE MODU VPN

Agresif modda IPsec VPN, Windows ve Vigor Router arasında eş kimlikleriyle ve pre-shared key ile Shrew VPN Client kullanarak bağlantı kurabilir. Bu makalede, Vigor Router ve Windows arasında nasıl bir IPsec tüneli oluşturulacağı gösterilmektedir.

Router Kurulumu

1. VPN and Remote Access >> Remote Dial-in User sayfasına gidin.

- Enable this account'u işaretleyin.
- Allowed Dial-In Type'de "IPsec Tunnel" ine izin verin.
- "Specify Remote Node" u etkinleştirin.
- Peer ID girin.

VPN and Remote Access >> Remote Dial-in User

Index No. 2

<p>User account and Authentication</p> <p><input checked="" type="checkbox"/> Enable this account</p> <p>Idle Timeout <input type="text" value="300"/> second(s)</p> <p>Allowed Dial-In Type</p> <p><input type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> IPsec Tunnel</p> <p><input type="checkbox"/> IPsec XAuth</p> <p><input type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/></p> <p><input type="checkbox"/> SSL Tunnel</p> <p><input type="checkbox"/> OpenVPN Tunnel</p> <p><input type="checkbox"/> IKEv2 EAP</p> <p><input checked="" type="checkbox"/> Specify Remote Node</p> <p>Remote Client IP <input type="text"/></p> <p>or Peer ID <input type="text" value="test"/></p> <p>Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block</p> <p>Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block</p> <p>(for some IGMP,IP-Camera,DHCP Relay..etc.)</p> <p>Subnet</p> <p><input type="text" value="LAN 1"/></p> <p><input type="checkbox"/> Assign Static IP Address</p> <p><input type="text" value="0.0.0.0"/></p>	<p>Username <input type="text" value="???"/> Max: 19 characters</p> <p>Password <input type="text" value="Max: 19 characters"/></p> <p><input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP)</p> <p>PIN Code <input type="text"/></p> <p>Secret <input type="text"/></p> <p>IKE Authentication Method</p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p><input checked="" type="checkbox"/> IKE Pre-Shared Key <input type="text" value="Max: 64 characters"/></p> <p><input type="checkbox"/> Digital Signature(X.509)</p> <p><input type="text" value="None"/></p> <p>IPsec Security Method</p> <p><input checked="" type="checkbox"/> Medium(AH)</p> <p>High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p> <p>Local ID (optional) <input type="text"/></p>
--	--

- IKE Pre-Shared Key'e tıklayın.
 - Pre-Shared Key girin.
 - OK'a tıklayın.
- Kaydetmek için OK'a tıklayın.

IKE Authentication Method

Pre-Shared Key	<input type="text" value="...."/>
Confirm Pre-Shared Key	<input type="text" value="...."/>

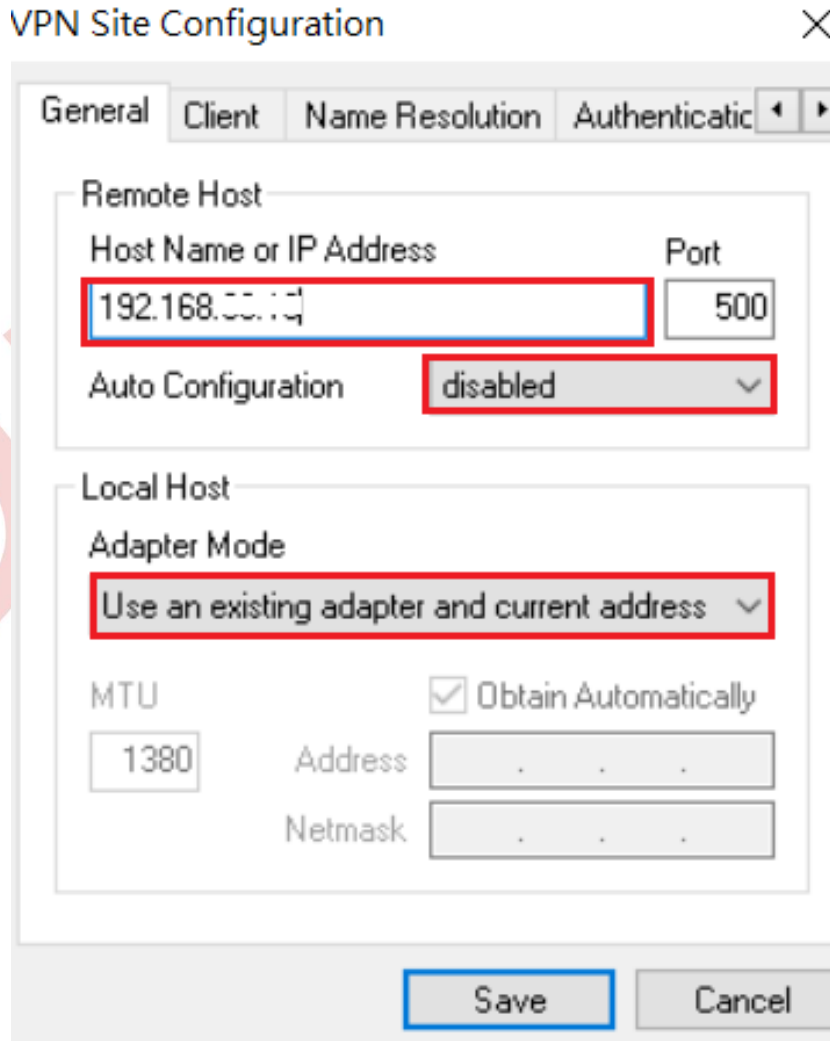
Ok

Windows Client Kurulumu

1. Shrew Soft VPN Client indirin.
2. VPN Access Manager'i açın.
 - Add'e tıklayın.



- General Setup'da,
 - i. VPN Hostname veya Server IP'si olarak router domaini veya WAN IP adresini girin.
 - ii. Auto Configuration'u devre dışı bırakın.
 - iii. Use an existing adapter and current address seçeneğini seçin.



- Name Resolution ayarlarında tüm onay kutularını devre dışı bırakın.

VPN Site Configuration

General Client **Name Resolution** Authentication

DNS Split DNS WINS

Enable DNS Obtain Automatically

Server Address #1 . . .

Server Address #2 . . .

Server Address #3 . . .

Server Address #4 . . .

Obtain Automatically

DNS Suffix

Save Cancel

- Authentication kurulumunda,
 - i. “Mutual PSK” seçeneğini seçin.
 - ii. Local Identity için “Fully Qualified Domain Name” olarak ayarlayın.
 - iii. Peer Kimliği için FQDN String girin.

VPN Site Configuration

Client Name Resolution **Authentication** Phase

Authentication Method **Mutual PSK**

Local Identity Remote Identity Credentials

Identification Type **Fully Qualified Domain Name**

FQDN String **test**

Save Cancel

- Phase 1 kurulumunda “aggressive” modu seçin
- Save’e tıklayın.

VPN Site Configuration

Name Resolution Authentication **Phase 1** Pha: < >

Proposal Parameters

Exchange Type	aggressive ▾
DH Exchange	group 2 ▾
Cipher Algorithm	auto ▾
Cipher Key Length	▾ Bits
Hash Algorithm	auto ▾
Key Life Time limit	86400 Secs
Key Life Data limit	0 Kbytes

Enable Check Point Compatible Vendor ID

Save Cancel

- IPsec tüneli oluşturmak için kaydedilen VPN istemcisine tıklayın ve bağlanın.

VPN Access Manager

File Edit View Help

Connect Add Modify Delete

92.168.3...

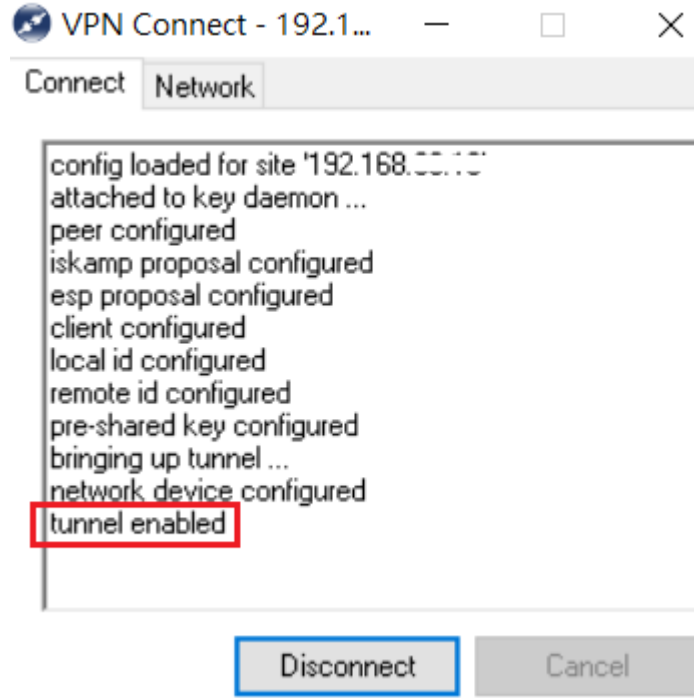
VPN Connect - 192.1...

Connect Network

config loaded for site '192.168.30.10'

Connect Exit

Sonunda VPN Connect mesajı görünecektir.



Ardından VPN tüneline tetiklemek için uzak ağa ping atın.

```

C:\Users\Will>ping 192.168.100.1

Pinging 192.168.100.1 with 32 bytes of data:
Reply from 192.168.100.1: bytes=32 time=4ms TTL=255
Reply from 192.168.100.1: bytes=32 time=2ms TTL=255
Reply from 192.168.100.1: bytes=32 time=2ms TTL=255
Reply from 192.168.100.1: bytes=32 time=2ms TTL=255

Ping statistics for 192.168.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 4ms, Average = 2ms

```

Vigor Router'da 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. via WAN2	192.168.3.10/32	195	4.46 K	238	1.30 K	0:1:21 Drop