

SONICWALL VE VIGOR ROUTER ARASINDA IPSEC VPN

Bu makale, SonicWALL NSA250 ve Vigor Router arasında Site-to-Site IPsec VPN'in nasıl yapılandırıldığını göstermektedir.

1. **Network >> Address Objects**'e gidin ve **Add**'e tıklayın.

- **Zone Assignment** için "VPN" seçeneğini seçin.
- **Type** için "Network" ü seçin.
- **Network and Netmask/Prefix Length**'de Vigor Router'ın LAN IP'sini ve Mask'ını girin.

The screenshot shows the SonicWALL Network Security Appliance web interface. On the left, the 'Network' menu is expanded to 'Address Objects'. The 'Add...' button is highlighted with a red box. The main window shows the configuration for a new Address Object:

- Name: VigorLAN
- Zone Assignment: VPN
- Type: Network
- Network: 192.168.1.0
- Netmask/Prefix Length: 255.255.255.0
- Status: Ready
- Buttons: OK, Cancel, Add..., Delete, Refresh

2. **VPN >> Settings**'e gidin ve **Add**'e tıklayın. General sekmesinde,

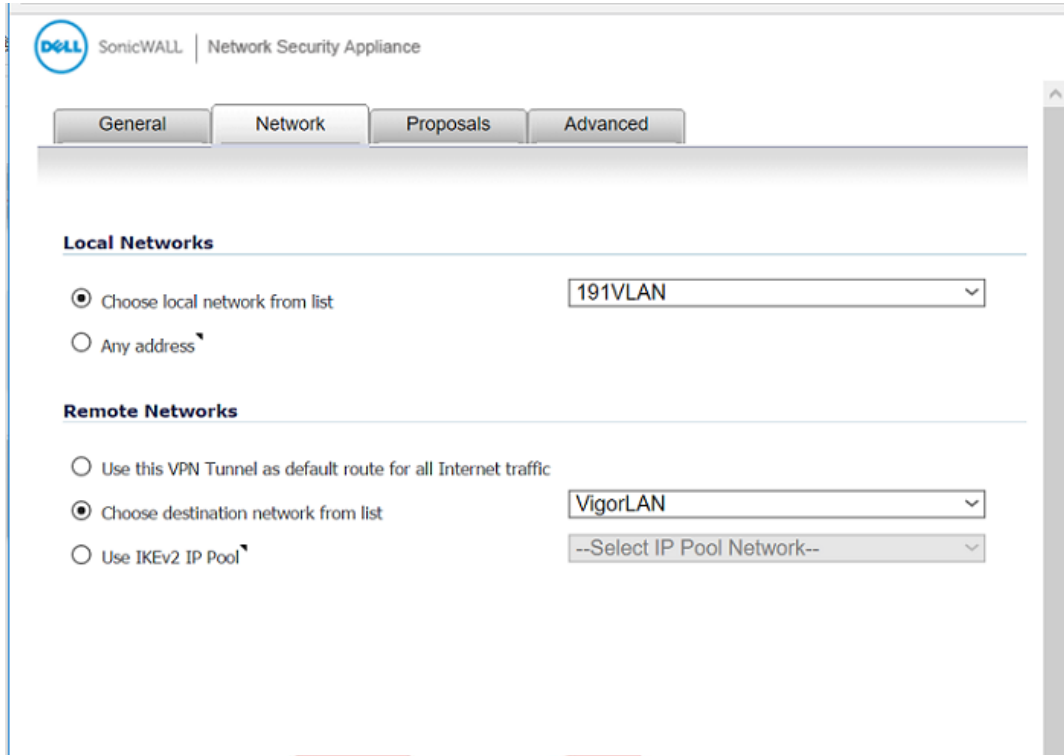
- **Policy Type** için "Site to Site" seçeneğini seçin.
- **IPsec Primary Gateway Name or Address**'de Vigor router'un WAN IP'sini ya da domain adını girin.
- Bir **Shared Secret** girin.

The screenshot shows the SonicWALL Network Security Appliance web interface. On the left, the 'VPN' menu is expanded to 'Settings'. The 'Add...' button is highlighted with a red box. The main window shows the configuration for a new VPN policy:

- Policy Type: Site to Site
- Authentication Method: IKE using Preshared Secret
- Name: IPsec
- IPsec Primary Gateway Name or Address: vigor.vpnclient.com
- IPsec Secondary Gateway Name or Address: (empty)
- Shared Secret: (masked)
- Confirm Shared Secret: (masked)
- Local IKE ID: IPv4 Address
- Peer IKE ID: IPv4 Address
- Mask Shared Secret:

3. Network sekmesine gidin,

- **Local Networks**'de Sonicwall'un LAN'ının adres objesini seçin.
- **Remote Networks**'de Vigor Router'ın LAN'ının adres objesini seçin.



SonicWALL | Network Security Appliance

General Network Proposals Advanced

Local Networks

Choose local network from list 191VLAN

Any address

Remote Networks

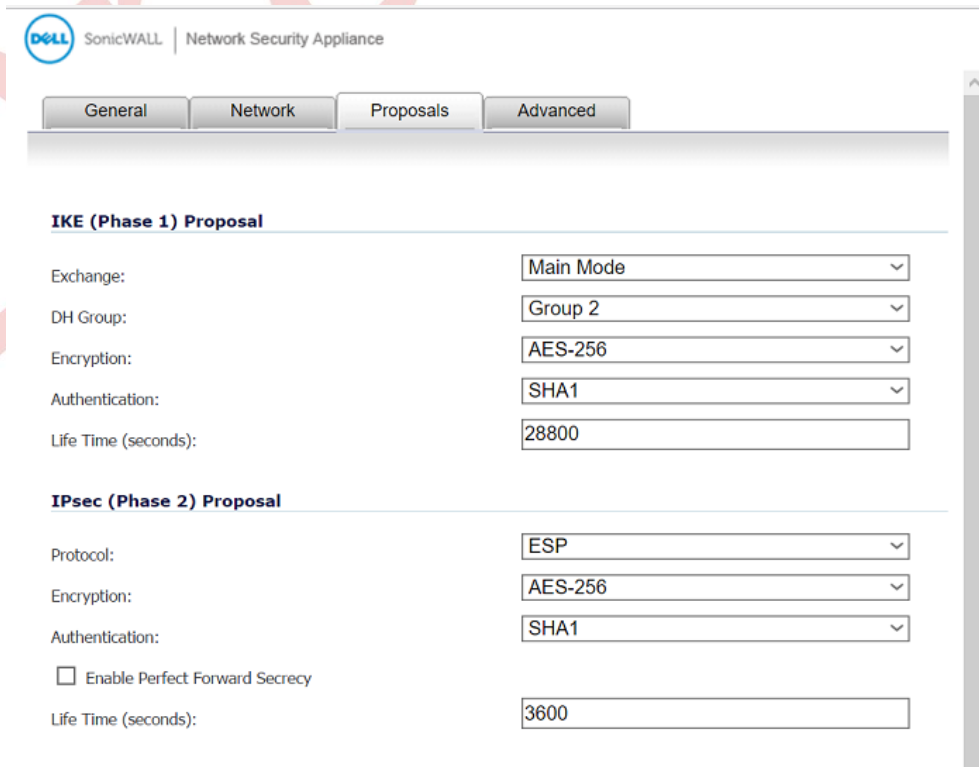
Use this VPN Tunnel as default route for all Internet traffic

Choose destination network from list VigorLAN

Use IKEv2 IP Pool --Select IP Pool Network--

4. Proposal sekmesine gidin,

- **Exchange** için "Main Mode" seçeneğini seçin.
- IKE Phase 1 ve Phase 2 proposallarını seçin. Vigor Router yapılandırmasıyla aynı olacağını unutmayın.



SonicWALL | Network Security Appliance

General Network Proposals Advanced

IKE (Phase 1) Proposal

Exchange: Main Mode

DH Group: Group 2

Encryption: AES-256

Authentication: SHA1

Life Time (seconds): 28800

IPsec (Phase 2) Proposal

Protocol: ESP

Encryption: AES-256

Authentication: SHA1

Enable Perfect Forward Secrecy

Life Time (seconds): 3600

DrayOS

1. **VPN and Remote Access >> LAN to LAN** sayfasına gidin ve profili ayarlamak için boş bir index numarasına tıklayın. Common Settings’de,
 - **Profil adı** girin.
 - **Enable this profile**’ı etkinleştirin.
 - **Call Direction** için “Dial-Out” seçeneğini seçin.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name <input type="text" value="IPsec"/>	Call Direction <input type="radio"/> Both <input checked="" type="radio"/> Dial-Out <input type="radio"/> Dial-in
<input checked="" type="checkbox"/> Enable this profile	<input type="checkbox"/> Always on
VPN Dial-Out Through <input type="text" value="WAN1 First"/>	Idle Timeout <input type="text" value="0"/> second(s)
Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block	<input type="checkbox"/> Enable PING to keep IPsec tunnel alive
Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)	PING to the IP <input type="text"/>

2. Dial-out settings’de,

- **Type of Server I am Calling** için “IPsec Tunnel” seçeneğini seçin.
- **Server IP**’de SonicWALL’un WAN IP’sini girin.
- SonicWALL’da girilen Shared Secret değerini **Pre-shared Key**’e girin.
- **IPsec Security Method**’da "High(ESP) AES with Authentication" ı seçin.

2. Dial-Out Settings

Type of Server I am calling <input type="radio"/> PPTP <input checked="" type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy <input type="text" value="None"/> <input type="radio"/> SSL Tunnel	Username <input type="text" value="???"/> Password(Max 15 char) <input type="text"/> PPP Authentication <input type="text" value="PAP/CHAP/MS-CHAP/MS-CHAPv2"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) <input type="text" value="sonicwall.vpnserver.net"/> Server Port (for SSL Tunnel): <input type="text" value="443"/>	IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key <input type="text" value="...."/> <input type="radio"/> Digital Signature(X.509) Peer ID <input type="text" value="None"/> Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First Local Certificate <input type="text" value="None"/>
	IPsec Security Method <input type="radio"/> Medium(AH) <input checked="" type="radio"/> High(ESP) <input type="text" value="AES with Authentication"/> <input type="button" value="Advanced"/>
	Index(1-15) in Schedule Setup: <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>

3. **Advanced at IPsec Security Method**'u tıklayın. IKE advanced settings'de SonicWALL yapılandırmasında girilen **IKE phase 1** ve **phase 2 proposal** değerlerini seçin. Ardından kaydetmek için **OK**'a tıklayın.

192.168.1.1/doc/I2llkeDt.htm

IKE advanced settings

IKE phase 1 mode Main mode Aggressive mode

IKE phase 1 proposal AES256_SHA1_G2

IKE phase 2 proposal AES256_SHA1

IKE phase 1 key lifetime 28800 (900 ~ 86400)

IKE phase 2 key lifetime 3600 (600 ~ 86400)

Perfect Forward Secret Disable Enable

Local ID

Note: If you select "Auto" in IKE phase 1 proposal, the router will send the following proposals to negotiate with the remote site. The proposals include: DES_(MD5/SHA)_G1, 3DES_MD5_G1, 3DES_MD5_G2, 3DES_(MD5/SHA)_G5, AES128_MD5_(G2/G5), AES256_SHA_(G2/G5), AES256_SHA_G14

OK Close

4. TCP/IP Network Settings'de **Remote Network IP**'de Sonicwall Router'ın LAN IP'sini girin. Ardından kaydetmek için **OK**'a tıklayın.

5. TCP/IP Network Settings

My WAN IP	0.0.0.0	RIP Direction	Disable
Remote Gateway IP	0.0.0.0	From first subnet to remote network, you have to do	
Remote Network IP	10.225.191.0		Route
Remote Network Mask	255.255.255.0	<input type="checkbox"/> IPsec VPN with the Same Subnets	
Local Network IP	192.168.1.1	<input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)	
Local Network Mask	255.255.255.0		

More

OK Clear Cancel

5. VPN'i başarılı olup olmadığını görmek için **VPN and Remote Access >> Connection Management** sayfasına gidin yeni oluşturulan VPN profilini seçin ve **Dial**'e tıklayın.

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Seconds : 10 Refresh

General Mode:	(IPsec) 10.225.191.0	Dial
Backup Mode:		Dial
Load Balance Mode:		Dial

6. VPN başarıyla bağlandığında VPN durumunu göreceğiz.

VPN Connection Status

Current Page: 1 Page No. Go >>

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime
1	IPsec Tunnel (IPsec) AES-SHA1 Auth	10.225.191.0 via WAN1	10.225.191.0/24	4	7	4	7	0:0:31 Drop

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

Linux

1. **VPN and Remote Access >> VPN profiles >> IPsec** sayfasına gidin ve profil ekleyin. Basic sekmesinde,
 - Profil adı girin.
 - **Enable**'yi işaretleyin.
 - **Local IP and Subnet Mask** için Vigor39002ün LAN Subnet'ini girin.
 - **Remote Host**'da SonicWALL'un WAN IP'sini veya domain adını girin.
 - **Local IP ve Subnet Mask** SonicWALL'un LAN Subnet'ini girin.
 - **Preshared Key** girin.

IPsec

Profile : vigor

Enable

Basic Advanced GRE Proposal

Auto Dial-Out : Enable Disable

For Remote Dial-In User : Enable Disable

Dial-Out Through : wan2 Default WAN IP WAN Alias IP

Failover to :

Local IP / Subnet Mask : 192.168.32.1 255.255.255.0/24

Local Next Hop : 0.0.0.0 (0.0.0.0 : default gateway)

Remote Host : sonicwall.vonsarver.net

Remote IP / Subnet Mask : 10.225.191.0 255.255.255.0/24

Add Save

IP	Subnet Mask
No items to show.	

More Remote Subnet :

IKE Phase 1 : Main Mode Aggressive Mode

Auth Type : PSK

Preshared Key : **** (If Aggressive mode is disabled and Remote Host IP is (

Security Protocol : ESP

2. Proposal sekmesine gidin,
 - SonicWALL'da yapılandırılan **IKE Phase 1** ve **Phase 2** proposallarını seçin.
 - Ayarları kaydetmek için **Apply**'a tıklayın.

IPsec

Profile : vigor

Enable

Basic Advanced GRE Proposal

IKE Phase1 Proposal [Dial-Out] : AES256 G2

IKE Phase1 Authentication [Dial-Out] : ALL

IKE Phase2 Proposal [Dial-Out] : AES256 with auth

IKE Phase2 Authentication [Dial-Out] : ALL

Accepted Proposal [Dial-In] : acceptall

1. VPN'i başarılı olup olmadığını görmek için **VPN and Remote Access >> Connection Management** sayfasına gidin yeni oluşturulan VPN profili için **Connect**'e tıklayın.

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

Connection Management History

Dial-Out tool

IPsec PPTP SSL Profiles : vigor Auto Refresh : 1 Minute Green :Data is encrypted
White :Data isn't encrypted

2. VPN başarıyla bağlandığında VPN durumunu göreceğiz.

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	R	Virtual Network	Up Time	RX Rate	TX Rate	RX Byte	TX Byte	Operation	
1	vigor	IPsec/AES_HMAC_SHA1	wan2	41...	10.225.191.0/24	00:03:34	336(bps)	760(bps)	336(Byte)	1000(Byte)	<input type="button" value="Refresh"/> <input type="button" value="Stop"/>