



**How To configure a Site to Site
VPN tunnel between a
SonicWall and Linksys VPN
Router**

**KNOWLEDGE
DATABASE**

How To configure a Site to Site VPN tunnel between a SonicWall and Linksys VPN Router

Procedure:

SonicWall Configuration

First, on the SonicWall, you must create an address object for the remote network.

- 1) Log into the SonicWall.
- 2) Browse to **Manage > Policies > Objects > Address Objects**
- 3) Create a new **Address Object** for the network on the LinkSys VPN router end you wish to reach (LinkSys LAN).

The screenshot shows the SonicWall management console. On the left is a navigation menu with categories like Updates, Licenses, Firmware & Backups, WXA Firmware, Restart, Connectivity, VPN, SSL VPN, SonicPoints, Wireless, 3G/4G/Modem, Policies, Rules, and Objects. The 'Objects' category is expanded to show 'Address Objects'. In the center, there is a table of existing address objects with columns for ID, Name, and a checkbox. A modal dialog box titled 'Add Address Object - Microsoft Edge' is open, showing a 'Certificate error' message. The dialog contains the following fields: Name (LinkSys LAN), Zone Assignment (VPN), Type (Network), Network (192.168.5.0), and Netmask/Prefix Length (255.255.255.0). At the bottom of the dialog, there is a 'Ready' status bar and 'ADD' and 'CLOSE' buttons.

Next, on the SonicWall you must create an SA.

- 1) Browse to **VPN**, then Settings (default view for VPN).
- 2) Ensure that **"Enable VPN"** is selected.
- 3) Click Add.
- 4) Change the Authentication Method to "IKE using pre-shared secret".
- 5) Name the SA, in this example "Tunnel to LinkSys VPN Router".
- 6) Enter the WAN IP of the LinkSys VPN router for "IPSec Primary Gateway Name or Address:".
- 7) Enter your shared secret, in this example "P@ss20140603"

8) Define Local IKE ID & Peer IKE ID. In this example the Local IKE ID is "Yahoo.com" and the Peer IKE ID is "Google.com"

The screenshot shows the SonicWall Network Security Appliance configuration interface. The main window is titled "VPN Policy - Microsoft Edge" and displays the "VPN Policy" configuration page. The "Network" tab is selected, showing the "IKE Authentication" section. The configuration includes:

- Policy Type:** Site to Site
- Authentication Method:** IKE using Preshared Secret
- Name:** Tunnel to LinkSys VPN Router
- IPsec Primary Gateway Name or Address:** 123.456.789.111
- IPsec Secondary Gateway Name or Address:** (empty)
- Shared Secret:** P@ss20140603
- Confirm Shared Secret:** (empty)
- Mask Shared Secret:** (unchecked)
- Local IKE ID:** Domain Name dropdown set to yahoo.com
- Peer IKE ID:** Domain Name dropdown set to google.com

The interface also shows "VPN Global Settings" with "Enable VPN" checked and a list of "VPN Policies" (WAN GroupVPN, WLAN GroupVPN, sdf) with "ADD" and "DELETE" buttons. The "Currently Active VPN" section shows "No Active IPv4 VPN Tunnels".

- 1) Select the "Network" tab.
- 2) Select "Lan Subnets" for Local Networks from the drop down box
- 3) Select the address object previously created for the destination network.

The screenshot displays the SonicWall Network Security Appliance management interface. The 'MANAGE' tab is active, and the 'VPN Policy' configuration page is open in a Microsoft Edge browser window. The browser shows a certificate error for the URL 'myit.hopto.org:8443/vpnConfig_0_0.html#'. The VPN Policy configuration is set to 'Proposals'.

VPN Global Settings:

- Enable VPN
- Unique Firewall Identifier: [Empty]

VPN Policies:

#	Name
<input type="checkbox"/>	1 WAN GroupVPN
<input type="checkbox"/>	2 WLAN GroupVPN
<input type="checkbox"/>	3 sdfsf

Site To Site Policies: 1 Policy
GroupVPN Policies: 2 Policies

Local Networks:

- Choose local network from list (LAN Subnets)
- Any address

Remote Networks:

- Use this VPN Tunnel as default route for all Internet traffic
- Choose destination network from list (LinkSys LAN)
- Use IKEV2 IP Pool (---Select IP Pool Network---

Currently Active VPN Tunnels:

#	Created
No Entries	

No Active IPv4 VPN Tunnels

Ready

Buttons: OK, CANCEL, HELP

- 1) Select the "Proposals" tab.
- 2) Configure DH group under IKE Phase 1 to "Group 1".
- 3) Configure Phase 1 Encryption "3DES" & authentication "SHA1".
- 4) Configure Phase 2 Encryption "3DES" & authentication "SHA1".
- 5) Enable Perfect Forward Secrecy. And Select the DH Group as "Group1"
- 6) Configure Phase 1 & Phase 2 Life Time "28800"

The screenshot displays the SonicWall Network Security Appliance management interface. The top navigation bar includes 'MONITOR', 'INVESTIGATE', 'MANAGE', and 'QUICK CONFIGURATION'. The left sidebar shows various configuration categories, with 'VPN' selected. The main content area is titled 'VPN Policy - Microsoft Edge' and shows a 'Certificate error' message. The 'Proposals' tab is active, displaying the 'IKE (Phase 1) Proposal' and 'Ipsec (Phase 2) Proposal' settings. The 'IKE (Phase 1) Proposal' settings include: Exchange: Aggressive Mode, DH Group: Group 1, Encryption: 3DES, Authentication: SHA1, and Life Time (seconds): 28800. The 'Ipsec (Phase 2) Proposal' settings include: Protocol: ESP, Encryption: 3DES, Authentication: SHA1, and Life Time (seconds): 28800. The 'Advanced' tab is selected, and the 'Ready' status is shown at the bottom.

1) Select **"Advanced"** tab.

2) Ensure that keep alive is enabled on only one end of the tunnel, it would be mostly on the device which is running on the DHCP WAN IP. In this example it is the LinkSys VPN Router.

3) Select "Enable Windows Networking (NetBIOS) Broadcast" if you would like to pass NetBIOS across the VPN.

The screenshot shows the SonicWall Network Security Appliance configuration interface. The main window is titled "VPN Policy - Microsoft Edge" and displays the "Advanced Settings" tab for a VPN policy. The interface includes a left-hand navigation menu with categories like Updates, Licenses, Connectivity, VPN, Policies, System Setup, and Security Configuration. The "VPN" section is expanded, showing "Base Settings" and "Advanced Settings". The "Advanced Settings" tab is active, displaying various options such as "Enable Keep Alive", "Suppress automatic Access Rules creation for VPN Policy", "Disable IPsec Anti-Replay", "Enable Windows Networking (NetBIOS) Broadcast", "Enable Multicast", "Permit Acceleration", "Display Suite B Compliant Algorithms Only", "Apply NAT Policies", and "Allow SonicPointN Layer 3 Management". The "Management via this SA" section includes checkboxes for "HTTPS", "SSH", and "SNMP". The "User login via this SA" section includes checkboxes for "HTTP" and "HTTPS". The "Default LAN Gateway (optional)" field is empty, and the "VPN Policy bound to:" dropdown menu is set to "Zone WAN". The status bar at the bottom indicates "Ready".

LinkSys VPN Router Configuration

Go to VPN Gateway to Gateway >> Edit the tunnel

1. Define the Tunnel/Gateway.
2. Select interface WAN1
3. Check the "Enable" option.

The screenshot shows the LinkSys VPN Router configuration interface. The main window is titled "LINKSYS" and displays the "VPN" configuration page. The "Edit the Tunnel" section is active, showing the "Tunnel to" field set to "WAN1". The "Enable" checkbox is checked, and a red arrow points to it with the text "this option should be enabled/checked." The "Local Security Gateway Type" is set to "IP - Domain Name (P2P) Authentication". The "Domain Name" is "google.com". The "Local Security Group Type" is set to "Subnet". The "Remote Security Gateway Type" is set to "IP - Domain Name (P2P) Authentication". The "Domain Name" is "yahoo.com". The "Remote Security Group Type" is set to "Subnet".

>> Local Group Setup

1. Select the "Local Security Gateway Type" as "IP + Domain name (FQDN) Authentication"
2. Choose a domain name. In this example it is "Google.com".
3. Choose "Local Security Group Type" as "Subnet"
4. Mention the IP address and subnet mask of the local network which are behind the Linksys VPN Router

>>Remote Group Setup

1. Select the "Remote Security Gateway Type" as "IP + Domain name (FQDN) Authentication"
2. Mention the IP address of the remote firewall. In this case it is the IP of the SonicWall Firewall.
3. Choose a domain name. In this example it is "Yahoo.com"
4. Choose "Remote Security Group Type" as "Subnet"
5. Mention the IP address of the network which are behind the SonicWall or the network which you want to access behind the SonicWall

The screenshot shows the Linksys VPN configuration page for a 10/100 4-port VPN Router (RV042). The interface is divided into several sections:

- Edit the Tunnel:** Tunnel No. 1, Tunnel Name: Schenectady-to-CliftonPa, Interface: WAN1, Enable:
- Local Group Setup:**
 - Local Security Gateway Type: IP + Domain Name(FQDN) Authentication
 - Domain Name: google.com
 - IP address: 192 . 168 . 213 . 153
 - Local Security Group Type: Subnet
 - IP address: 192 . 168 . 5 . 0
 - Subnet Mask: 255 . 255 . 255 . 0
- Remote Group Setup:**
 - Remote Security Gateway Type: IP + Domain Name(FQDN) Authentication
 - IP address: 66 . 152 . 110 . 210
 - Domain Name: yahoo.com
 - Remote Security Group Type: Subnet
 - IP address: 192 . 168 . 0 . 0
 - Subnet Mask: 255 . 255 . 255 . 0

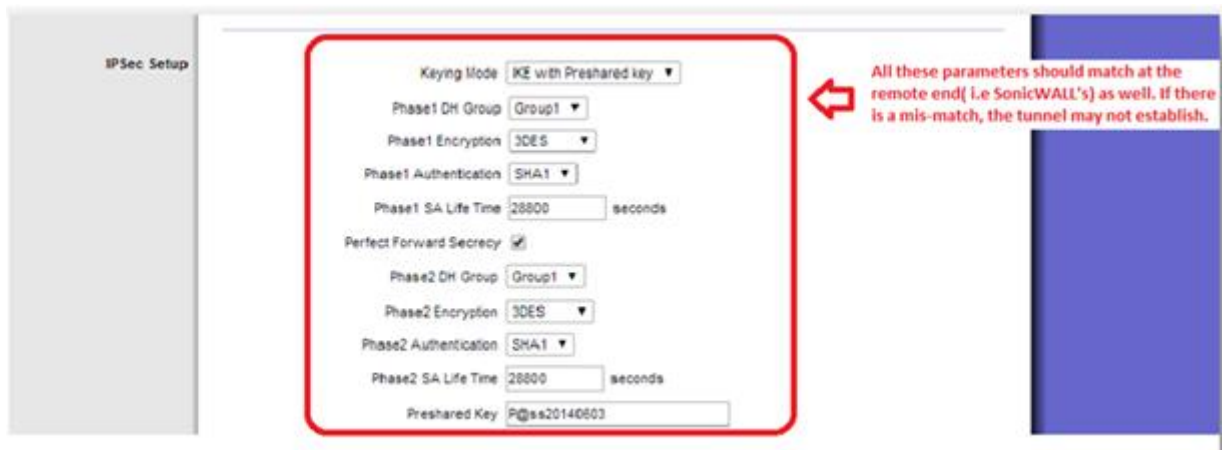
Red annotations with arrows point to specific fields:

- A red box highlights the Local Security Gateway Type, Domain Name, and IP address fields.
- A red box highlights the Local Security Group Type, IP address, and Subnet Mask fields, with an arrow pointing to it from the text: "Local Network/LAN network behind the LinkSys VPN Router".
- A red box highlights the Remote Security Gateway Type, IP address, and Domain Name fields, with an arrow pointing to it from the text: "X1 IP / WAN IP of the SonicWALL device".
- A red box highlights the Remote Security Group Type, IP address, and Subnet Mask fields, with an arrow pointing to it from the text: "LAN network at SonicWALL end which you wish to reach".

On the right side, there is a "SITEMAP" section with instructions: "By setting this page, users can add the new tunnel between two VPN devices. Tunnel No. - The tunnel number will be generated automatically from 1-50. Tunnel Name: Enter the Tunnel Name, such as LA Office, Branch Site, Corporate Site, etc. More..."

>>IPSec Setup

1. Select Keying mode as "IKE with Preshared key"
2. Select Phase 1 DH Group as "Group1"
3. Select Phase 1 encryption as "3DES"
4. Select Phase 1 Authentication as "SHA1"
5. Mention the Phase 1 SA lifetime as "28800"
6. Enabled Perfect Forward Secrecy
7. Select Phase 2 DH Group as "Group1"
8. Select Phase 2 encryption as "3DES"
9. Select Phase 2 Authentication as "SHA1"
10. Mention the Phase 2 SA lifetime as "28800"
11. Mentioned the Pre-shared key. This key should be same on both the devices, Sonicwall as well as LinkSys VPN router.



>>Click on "Advanced"

1. Enable the Aggressive Mode
2. Enable Keep Alives
3. Enable NetBios (If needed)
4. Enable Dead Peer Detection (If needed)

