

DSR to DSR VPN Tunnel



Here we're trying to build a VPN tunnel between two DSR units.

DSR-1000N Setup

Step 1) Go to SETUP > Network Settings.

Set the LAN IP of the product, this will need to be in a different subnet on each side.

Once done click **"Save Settings"**

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.03B12_WW

D-Link

DSR-1000N	SETUP	ADVANCED	TOOLS	STATUS	HELP
-----------	-------	----------	-------	--------	------

- Wizard
- Internet Settings
- Wireless Settings
- Network Settings
- DMZ Setup
- VPN Settings
- USB Settings
- VLAN Settings

LAN SETUP

The LAN Configuration page allows you to configure the LAN interface of the router including the DHCP Server which runs on it.

LAN TCP/IP Setup

IP Address:	<input type="text" value="192.168.10.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>

DHCP

DHCP Mode:	<input type="text" value="DHCP Server"/>
Starting IP Address:	<input type="text" value="192.168.10.100"/>
Ending IP Address:	<input type="text" value="192.168.10.254"/>
Primary DNS Server:	<input type="text"/>
Secondary DNS Server:	<input type="text"/>
WINS Server:	<input type="text"/>
Lease Time:	<input type="text" value="24"/>
Relay Gateway:	<input type="text"/>

Helpful Hints...
Changes here affect all devices connected to the router's LAN switch and also wireless LAN clients. Note that a change to the LAN IP address will require all LAN hosts to be in the same subnet and use the new address to access this GUI.
[More...](#)

Step 2) Go to SETUP > VPN Settings > SSL VPN server > Portal Layouts.

Click on **“Add”**

Under IPsec Configuration enter in the below;

Policy Name: A name that describes the tunnel

Policy Type: Auto Policy

IPSec Mode: Tunnel Mode

Local Gateway: Dedicated WAN

Remote Endpoint: This is the Public IP of the remote unit

Local IP set to **“Subnet”** and enter in the start IP of the local network

Local Subnet mask: enter in the local subnet

Remote Start IP: same as above but the remote start IP

Remote Subnet mask: The remote subnetmask

DSR-1000N	SETUP	ADVANCED	TOOLS	STATUS
Wizard	IPSEC CONFIGURATION LOGOUT			
Internet Settings	This page allows user to add/edit VPN (IPsec) policies which includes Auto and Manual policies.			
Wireless Settings	<input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/>			
Network Settings	General			
DMZ Setup	Policy Name: <input type="text" value="Office"/>			
VPN Settings	Policy Type: <input type="text" value="Auto Policy"/>			
USB Settings	IPsec Mode: <input type="text" value="Tunnel Mode"/>			
VLAN Settings	Select Local Gateway: <input type="text" value="Dedicated WAN"/>			
	Remote Endpoint: <input type="text" value="IP Address"/>			
	<input type="text" value="10.2.2.11"/>			
	Enable Mode Config: <input type="checkbox"/>			
	Enable NetBIOS: <input checked="" type="checkbox"/>			
	Enable RollOver: <input type="checkbox"/>			
	Protocol: <input type="text" value="ESP"/>			
	Enable DHCP: <input type="checkbox"/>			
	Local IP: <input type="text" value="Subnet"/>			
	Local Start IP Address: <input type="text" value="192.168.10.0"/>			
	Local End IP Address: <input type="text" value=""/>			
	Local Subnet Mask: <input type="text" value="255.255.255.0"/>			
	Remote IP: <input type="text" value="Subnet"/>			
	Remote Start IP Address: <input type="text" value="192.168.30.0"/>			
	Remote End IP Address: <input type="text" value=""/>			
	Remote Subnet Mask: <input type="text" value="255.255.255.0"/>			
	Phase1(IKE SA Parameters)			
	Exchange Mode: <input type="text" value="Main"/>			
	Direction / Type: <input type="text" value="Both"/>			

Under Phase1 enter in the below:

Exchange Mode: Main

Direction / Type: Both

Nat Transversal: If modem has NAT enabled set NAT Transversal to "ON", otherwise set to "Off"

Local Identifier Type: Local Wan IP

Remote Identifier Type: Remote Wan IP

Encryption Algorithm: AES-128

Authentication Algorithm: SHA-1

Authentication Method: Pre-shared key

Pre-shared key: Enter in a password

All other settings below Pre-shared key leave as default.

Phase1(IKE SA Parameters)	
Exchange Mode:	Main
Direction / Type:	Both
Nat Traversal:	
On:	<input checked="" type="radio"/>
Off:	<input type="radio"/>
NAT Keep Alive Frequency (in seconds):	20
Local Identifier Type:	Local Wan IP
Local Identifier:	10.2.2.10
Remote Identifier Type:	Remote Wan IP
Remote Identifier:	10.2.2.11
Encryption Algorithm:	AES-128
Key Length:	
Authentication Algorithm:	SHA-1
Authentication Method:	Pre-shared key
Pre-shared key:	testing123
Diffie-Hellman (DH) Group:	Group 2 (1024 bit)
SA-Lifetime (sec):	28800
Enable Dead Peer Detection:	<input type="checkbox"/>
Detection Period:	10
Reconnect after failure count:	3
Extended Authentication:	None
Authentication Type:	User Database
Username:	
Password:	

Phase2-(Manual Policy Parameters)

SPI-Incoming:	<input type="text" value="0x"/>
SPI-Outgoing:	<input type="text" value="0x"/>
Encryption Algorithm:	<input type="text" value="AES-128"/> ▾
Key Length:	<input type="text"/>
Key-In:	<input type="text"/>
Key-Out:	<input type="text"/>
Integrity Algorithm:	<input type="text" value="SHA-1"/> ▾
Key-In:	<input type="text"/>
Key-Out:	<input type="text"/>

Phase2-(Auto Policy Parameters)

SA Lifetime:	<input type="text" value="3600"/>	<input type="text" value="Seconds"/> ▾
Encryption Algorithm:	<input type="text" value="AES-128"/> ▾	
Key Length:	<input type="text"/>	
Integrity Algorithm:	<input type="text" value="SHA-1"/> ▾	
PFS Key Group:	<input checked="" type="checkbox"/>	<input type="text" value="DH Group 2 (1024 bit)"/> ▾

Step 3) Remote unit setup.

The remote unit will be setup with mirror settings to the first.

E.G. The local subnet on the first unit will become the remote subnet on the second unit.

See below for screen shots with the mirror settings.

DSR-1000N	SETUP	ADVANCED	TOOLS	STATUS
Wizard	IPSEC CONFIGURATION LOGOUT			
Internet Settings	This page allows user to add/edit VPN (IPsec) policies which includes Auto and Manual policies.			
Wireless Settings	<input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/>			
Network Settings				
DMZ Setup				
VPN Settings	General			
USB Settings	Policy Name: <input type="text" value="Office"/>			
VLAN Settings	Policy Type: <input type="text" value="Auto Policy"/>			
	IPsec Mode: <input type="text" value="Tunnel Mode"/>			
	Select Local Gateway: <input type="text" value="Dedicated WAN"/>			
	Remote Endpoint: <input type="text" value="IP Address"/>			
	<input type="text" value="10.2.2.10"/>			
	Enable Mode Config: <input type="checkbox"/>			
	Enable NetBIOS: <input checked="" type="checkbox"/>			
	Enable RollOver: <input type="checkbox"/>			
	Protocol: <input type="text" value="ESP"/>			
	Enable DHCP: <input type="checkbox"/>			
	Local IP: <input type="text" value="Subnet"/>			
	Local Start IP Address: <input type="text" value="192.168.30.0"/>			
	Local End IP Address: <input type="text" value=""/>			
	Local Subnet Mask: <input type="text" value="255.255.255.0"/>			
	Remote IP: <input type="text" value="Subnet"/>			
	Remote Start IP Address: <input type="text" value="192.168.10.0"/>			
	Remote End IP Address: <input type="text" value=""/>			
	Remote Subnet Mask: <input type="text" value="255.255.255.0"/>			

Phase1(IKE SA Parameters)

Exchange Mode:	Main
Direction / Type:	Both
Nat Traversal:	
On:	<input checked="" type="radio"/>
Off:	<input type="radio"/>
NAT Keep Alive Frequency (in seconds):	20
Local Identifier Type:	Local Wan IP
Local Identifier:	10.2.2.11
Remote Identifier Type:	Remote Wan IP
Remote Identifier:	10.2.2.10
Encryption Algorithm:	AES-128
Key Length:	
Authentication Algorithm:	SHA-1
Authentication Method:	Pre-shared key
Pre-shared key:	testing123
Diffie-Hellman (DH) Group:	Group 2 (1024 bit)
SA-Lifetime (sec):	28800
Enable Dead Peer Detection:	<input type="checkbox"/>
Detection Period:	10
Reconnect after failure count:	3
Extended Authentication:	None
Authentication Type:	User Database
Username:	
Password:	

Phase2-(Manual Policy Parameters)	
SPI-Incoming:	<input type="text" value="0x"/>
SPI-Outgoing:	<input type="text" value="0x"/>
Encryption Algorithm:	<input type="text" value="AES-128"/>
Key Length:	<input type="text"/>
Key-In:	<input type="text"/>
Key-Out:	<input type="text"/>
Integrity Algorithm:	<input type="text" value="SHA-1"/>
Key-In:	<input type="text"/>
Key-Out:	<input type="text"/>

Phase2-(Auto Policy Parameters)	
SA Lifetime:	<input type="text" value="3600"/> <input type="text" value="Seconds"/>
Encryption Algorithm:	<input type="text" value="AES-128"/>
Key Length:	<input type="text"/>
Integrity Algorithm:	<input type="text" value="SHA-1"/>
PFS Key Group:	<input checked="" type="checkbox"/> <input type="text" value="DH Group 2 (1024 bit)"/>

Once finished try to ping a device on the remote side. If the device has a firewall installed (E.G. windows 7 firewall) please disable this as it will block the ping.

Also some AV software can also block ping, if you have a print server or non PC device try to ping this as its less likely to block ping.