

How to Setup PureVPN on DrayTek Router

Configuring a PureVPN tunnel on your router is a great way to ensure the safety and security of all the devices in your home. This method is especially beneficial if you have devices that don't have VPN compatibility or you want to protect all the Wi-Fi-connected devices in your home.

Things to Consider:

1. You have a working internet connection
2. VPN Supported Router.
3. A Premium PureVPN account (If you haven't bought yet click ?[here](#) to buy)

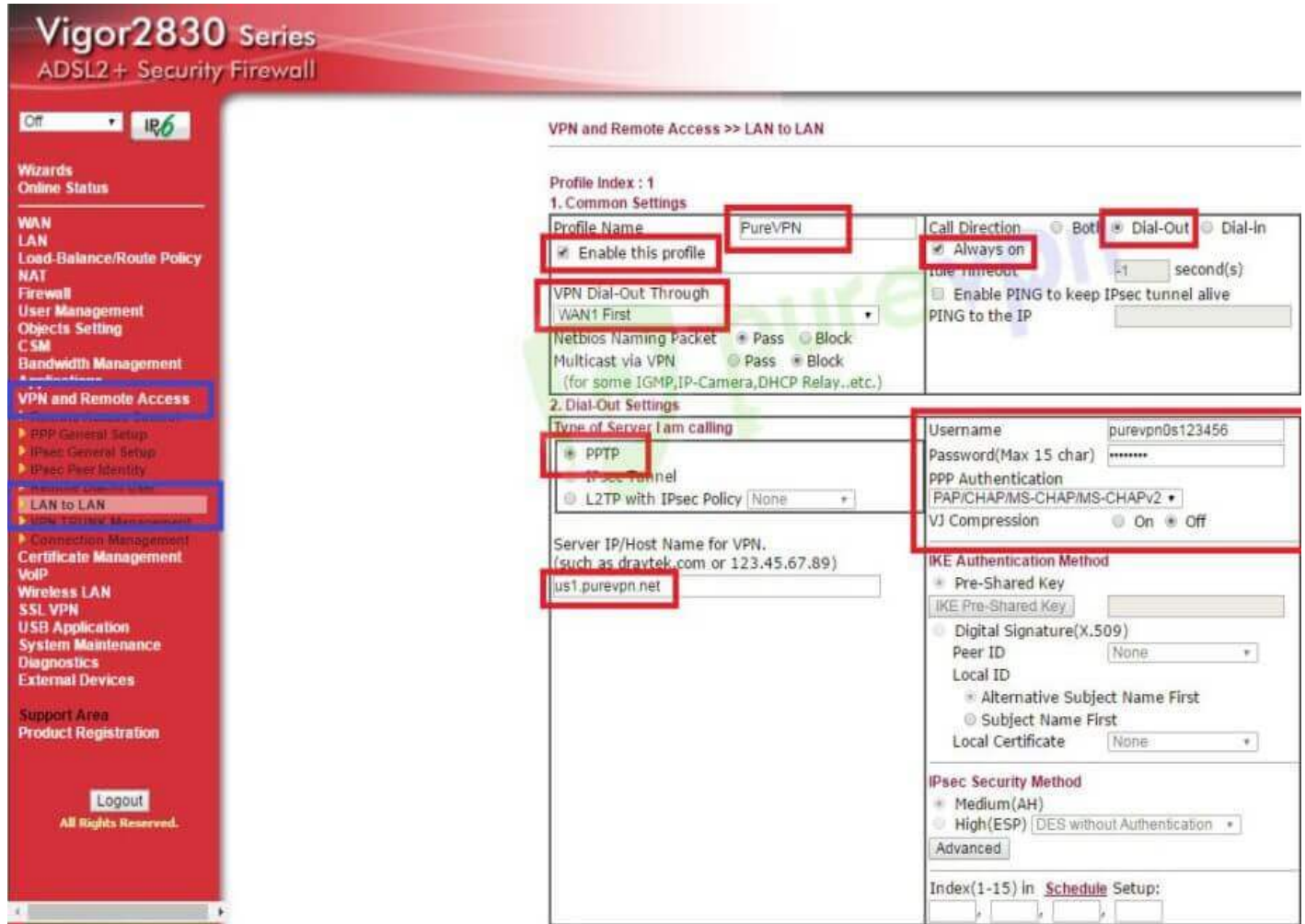
Find your VPN credentials for manual configuration.

To find your VPN credentials log into the PureVPN members area. Click ? [here](#) to visit member area.

- Login to the **Member area** using your PureVPN registered email address and password.

How to connect PureVPN manually on DrayTek Router.

- To start setting up a VPN on a tp-link router you first have to connect to it. For that, you have to put in your browser the following address: <http://192.168.0.1> (If this doesn't work, please consult your router's manual to find what is the Default Gateway Address). Enter your router's username and password and click **Login**.
- Select LAN to LAN in the submenu
- Common Settings
- Enter your Profile Name
- Choose Enable this profile
- Call direction: Choose Dial-out and keep it on Always on
- Dial-Out Settings
- Choose PPTP
- Insert the desired server: Please refer to the server address shared below.
 1. Germany: de1.pointtoserver.com
 2. Netherlands: nl1.pointtoserver.com
 3. United Kingdom: ukl1.pointtoserver.com
 4. United States: usil1.pointtoserver.com
 5. United States: ustx1.pointtoserver.com
 6. United States: usca1.pointtoserver.com
 7. United States: usfl1.pointtoserver.com
 8. United States: usny1.pointtoserver.com
 9. United States: uswdc1.pointtoserver.com
 10. Australia: au-sd1.pointtoserver.com
- Enter your PureVPN credentials. Here is how you can ?[find your VPN credentials](#).
- PPP Authentication: PAP/CHAP/MS-CHAP/MS-CHAPv2
- VJ Compression: Off



- **TCP/IP Network Settings**

1. Choose **Change default** route to this VPN tunnel (Only single WAN support)
2. Lastly, Select **OK** to complete the process!

Vigor2830 Series
ADSL2+ Security Firewall

Off **IP6**

Wizards
Online Status

WAN
LAN
Load-Balance/Route Policy
NAT
Firewall
User Management
Objects Setting
CSM
Bandwidth Management
Applications
VPN and Remote Access
▶ Remote Access Control
▶ PPP General Setup
▶ IPsec General Setup
▶ IPsec Peer Identity
▶ Remote Dial-in User
▶ LAN to LAN
▶ VPN TRUNK Management
▶ Connection Management
Certificate Management
VoIP
Wireless LAN
SSL VPN
USB Application
System Maintenance
Diagnostics
External Devices

Support Area
Product Registration

Logout
All Rights Reserved.

Admin mode
Status: Ready

Medium(AH)
High(ESP) | DES without Authentication
Advanced

Index(1-15) In Schedule Setup:

3. Dial-In Settings

Allowed Dial-In Type

PPTP
 IPsec Tunnel
 L2TP with IPsec Policy | None

Specify Remote VPN Gateway
Peer VPN Server IP
or Peer ID

Username
Password(Max 11 char)
VJ Compression On Off

IKE Authentication Method

Pre-Shared Key
IKE Pre-Shared Key
 Digital Signature(X.509)
None

Local ID
 Alternative Subject Name First
 Subject Name First

IPsec Security Method

Medium(AH)
High(ESP) DES 3DES AES

4. GRE over IPsec Settings

Enable IPsec Dial-Out function GRE over IPsec
 Logical Traffic My GRE IP Peer GRE IP

5. TCP/IP Network Settings

My WAN IP 0.0.0.0
Remote Gateway IP 0.0.0.0
Remote Network IP 0.0.0.0
Remote Network Mask 255.255.255.0
Local Network IP 192.168.1.1
Local Network Mask 255.255.255.0
More

RIP Direction Disable
From first subnet to remote network, you have to do
Route

Change default route to this VPN tunnel (Only single WAN supports this)

OK Clear Cancel

Was this article helpful? Rate and share your comments below. Your input matters to us and everyone else in the Cyber Security Community.

