

Knowledgebase > Guides and Articles (Other Language - 中国人)) > DD-WRT v40559 []OpenVPN 设置)(CS)

## DD-WRT v40559[]OpenVPN 设置)(CS)

Michael B - 2021-08-16 - Guides and Articles (Other Language - 中国人))

## 本教程逐步引导您配置使用 DD-WRT 固件版本 3.0-r40559 的路由器。

如果您想要使用基于路由器的配置,但不想自己进行设置[]FlashRouters 为这种设置提供了即插 即用的 DD-WRT Routers 预配置 Private Internet Access 路由器[]

开始之前,请确保您已下载了想要用于连接的配置文件。对于本指南来说,我们使用了标有 Default 的集合的 California 文件,请务必解压缩这个文件,以便能访问其内容。

- Default
- <u>Strong</u>
- <u>TCP</u>
- <u>Strong TCP</u>

此外,请决定适合您的需求的 DNS 服务器,共有四个选项:

- 10.0.0.241 这可提供以下所有三项的访问
- 10.0.0.242 仅 DNS
- 10.0.0.243 一 将流媒体域转发到父代理,从而能访问一些流媒体服务
- 10.0.0.244 <u>MACE</u>

这些无法在 DD-WRT 设置中指定;若要有效防止此配置的 DNS 泄露,您需要在路由器所连设备的网络设置中指定 PIA DNS[]

**第 1 步:** 设置 - 基本设置:确保使用适合您所在位置的时间设置,这样做可以预防诸多类型的连接问题。

1. 指定 PIA DNS 服务器的基本 DNS 服务器,以便在 VPN 连接之前和之外使用。您需要自行决 定来做出选择。我们使用 1.1.1.1 (Cloudflare) 作为主要 DNS[]

2. 我们使用的第二 DNS 是 8.8.8.8 (Google)[]

3. 确保 NTP Client[]NTP 客户端)为 Enabled (启用)。

4. 将 Time Zone (时区) 设为您当地的实际时间。

5. 在页面底部,点击 Apply Settings(应用设置)。



**第 2 步:** 设置 - IPv6□要防止通过 IPv6 协议泄露数据,请在 Setup (设置) > IPv6 选项卡中 将它关闭,如下图红色高亮区域所示。

1. 将 IPv6 单选按钮设为 Disable (禁用)

2. 点击 Apply Settings (应用设置)。

dd	-wrt	.com	i co	ontro	l pane	el				Tim	Firmware: D e: 21:03:59 up 33 r	D-WRT v3.0-r4055 nin, load average: WAN IP:	9 std (08/06/19) 0.00, 0.00, 0.00
Setup	Wireless	Services	Security	Access Re	estrictions	NAT / QoS	Administ	ration	Status				
Basic Se	tup IPV6	DDNS	MAC Address	s Clone	Advanced Ro	outing Se	vitch Config	Networ	king	Tunnels			
IPv6 O Enable Staable						Help IPv6	mor	e					
Apply Settings Cancel Changes													

第3步:服务 - VPN [打开 VPN 客户端,以便您打开相应的字段来输入 VPN 配置细节。

1. 在 *OpenVPN Client*[]OpenVPN 客户端)标题下,点击与 **Start OpenVPN Client**(启用 OpenVPN 客户端)对应的 **Enable** (启用)。

2. 点击 Apply Settings (应用设置)。

dd-wrtcor		Firmware: DD-WRT v3.0+40559 std (08) Time: 21:05:42 up 35 min, load average: 0.00, 0.0 WAN IP:		
Setup Wireless Service	Security Access Restrictions NAT / QoS Administration Status			
Services FreeRadius PP	Pot Server VPN USB NAS Hotspot Adblocking SpeedChecker			
PPTP Server		Help more		
PPTP Server		OpenVPN		
PPTP Server	○ Enable	General: 3 auth methods are supported: pics12 (+dh on server), static, standard certs. Enable MSS only on one side of the link, fragment on both.		
PPTP Citenc		OpenVPN Server/Daemon		
PPTP Client		Additional Config:		
PPTP Client Options	O Enable ® Disable	To push routes to clients and push "route IP mask gateway", to push DNS/WINS add push "thcp-option DNS (or WINS) IP" to the config.		
OpenVPN Server/Daemo	n	client connect directory: When USB or JFF5 is mounted to //ffs,		
OpenVPN Server/Daemon		scripts will be called from /jffs/etc /openvpn/cod/		
Open/VPN	○ Enable   Disable	OpenVPN Client		
OpenVPN Client		Add JPs/NETs in the form 0.0.0.0/0 to force clients to use the turnel as		
OpenVPN Client		IP Address/Netmask:		
Start Open//PN Client	Strable      Disable	Must be set when using DRCP+Poxy mode and local TAP is NOT bridged		
SoftEther VPN				
Server	O Enable      O Disable			
Bridge	O Enable      Disable			
Client	O Enable      Disable			
Config				
		-41)		
	Apply Settings Cancel Changes			

第4步:服务-VPN□输入具体的 VPN 配置详情。

1. 输入 **Server IP/Name**(服务器 IP/名称) — 您可以在我们提供的 <u>OpenVPN 配置文件</u>的 **remote** 一行中找到此信息。(本指南使用了 us-west.privateinternetaccess.com[]]

2. 输入 Port (端口) 编号,具体根据以下依赖项表格中所示。

AUTH	CIPHER	CERTIFICATE	UDP PORT	TCP PORT
SHA1	AES-128-CBC/GCM	ca.rsa.2048.crt	1198	502
SHA256	AES-256-CBC/GCM	<u>ca.rsa.4096.crt</u>	1197	501

3. 对于 Tunnel Device (隧道设备□□PIA VPN 连接使用的是 TUN 接口。

4. 在本指南中,**Tunnel Protocol**(隧道协议)将设为 **UDP**。在大多数情形中[]UDP 能提供优于 **TCP** 的速度。如果使用 **TCP**[请务必使用 *依赖项表格*中所示的端口]

5. Encryption Cipher (加密密码) 也视您在 依赖项表格中的选择而定[]

6.Hash Algorithm(哈希算法)也是一项特定于依赖项表格中的选择的设置。

7.User Pass Authentication (用户凭证验证)必须设为 Enable(启用)。

8. 在 **Username**(用户名)字段中,请输入您的 PIA 用户名,其格式始终为 *p1234567*[*而且 无法替换为其他信息。* 

9.**Password**(密码)字段中需要输入您的 PIA 帐户密码,系统为您分配了密码,但您可以在客户端控制面板中进行自定义。

10. 将 Advanced Options(高级选项)设为 Enable(启用),这可以显示要求输入信息的 其他字段。

11. 在下拉菜单中,将 TLS Cipher[]TLS 密码)设为 None. (无)。

12. 在下拉菜单中,将 LZO Compression [] LZO 压缩)设为 Yes (是)。

13.Additional Config(其他配置)部分中需要输入多行个特定的行;请将以下几行复制并粘贴到这个字段中:

persist-key

persist-tun

tls-client

remote-cert-tls server

pull-filter ignore "auth-token"

сору

14.CA Cert[]CA 证书)需要从*依赖项表格*下载,具体视您使用的加密类型而定。本指南开头的 *依赖项表格*中可以找到三种证书各自的链接。在文本编辑器中打开证书,再将其内容复制到 CA Cert[]CA 证书)字段中。(注意:此字段的内容也必须包含 *begin* 和 *end* 证书行,请务 必复制完整的内容。)

15. 在页面底部,点击 Apply Settings(应用设置)以保存您进行的设置并设定连接。

dd-wrt.		Firmware: DD-WRT v3.0-r40559 std (08)06/19 e: 13:55:55 up 1 min, load average: 0.15, 0.10, 0.0 WAN IP: 192.168.86.11
Setup Wireless	Security Access Restrictions NAT / QoS Admi	inistration Status
DDTD Server	USB NAS Hotspot Addiocku	Nelo more
PPTP Server		OpenVPN
PPTP Server	○ Enable	General: 3 auth methods are supported: pics12 (+dh on server), static, standard certs. Enable MSS only on one side of the link device to every
PPTP Client		Open/VPN Server/Daemon
PPTP Client PPTP Client Options	○ Enable    ● Disable	Additional Config: To push routes to clents add 'push 'route IP mask pateway'', to push DNS/WINS add 'push' "dhcp-option DNS (or WINS) IP to the confid
OpenVPN Server/E	Daemon	dent connect directory: When USB or JFFS is mounted to /jffs,
OpenVPN Server/Daem	00	/apenvpn/ccd/
OpenVPN Client	⊖ Enable	OpenVPN Client Policy based Routing: Add IPs/NETS in the form 0.0.0.0/D to force clients to use the tunnel as
OpenVPN Client		default gateway. One line per IP/NET. IP Address/Netmask: Must be set when using DHCP-Proxy
Start OpenVPN Client	OEnable O Disable	mode and local TAP is NOT bridged
Server IP/Name	1 us-california.privacy.network	
Port	2 1198 (Default: 1194)	
Tunnel Device		
Tunnel Protocol	4 UDP Y	
Encryption Opher	AES-128 CBC	
Hash Algorithm	6 sha1	
User Page Authentication	7 Originalia O Disable	
Username		
Password	9	
Advanced Options	10 Ocnable O Disable	
TLS Cipher	11 None	
LZO Compression	12 Yes 🗸	
NAT	O Enable    Disable	
IP Address		
Subnet Mask		
Tunnel MTU setting	1500 (Default: 1500)	
Tunnel UDP Fragment	(Default: Disable)	
Tunnel UDP MSS-Fix	O Enable      Disable	
nsCertType verification		
TLS Auth Key		
Additional Config		
persist-key		^
persist-tun tis-client	13	¥
Policy based Routing		
		ж
PKCS12 Key		
		A
Static Key		
CA Cert	E	^
MIIHqzCCBZOgAwIBAg	(JAJOu+vODZJntMA0GCSqGSIb3DQEBDQUAMIHoMQswCQYD 14	~
Date Clean Cast		
Public Client Cert		
Private Clent Var		- 11
Finance Codit Ney		
SoftEther VPN		
Server	O Enable   Disable	
Bridge	C Enable  Disable	
Config	Usable Usable	
		4
15	Apply Settings Cancel Changes	

您的路由器现在已完成设置,可以建立 PIA VPN 连接了。您可以在 Status[]状态[]> OpenVPN 选项卡中确认连接状态,如红色高亮部分中所示。

	Firmware: DD-WRT V3.0-440559 std (08/06/19) Time: 14:27:47 up 4 min, load average: 0.03, 0.14, 0.07 WAN IP:
Setup Wireless Services Security Access Restrictions NAT / QoS Administration State	15
Router WAN LAN Wireless OpenVPN Bandwidth Syslog Sys-Info	
State Clinit: CONNECTED SUCCESS	Help
Local Address: 10.57.10.6 Remote Address: 10.57.10.5	
Status	
VPN Clent Stats	
TUN/TAP read bytes 27195	
TUN/TAP write bytes 9050	
TCP/UDP read bytes 18786	
TCP/UDP write bytes 61958	
Auth read bytes 9210	
pre-compress bytes 0	
post-compress bytes 0	
pre-decompress bytes 0	
post-decompress bytes u	

如果在指定并应用了设置后没有启动连接,请关闭路由器,等待 10 秒钟,再重新开机。路由器重启后,应当会启动 VPN 连接了。