闪连VPN

闪连VPN 技术特性说明页面，面向关注连接效率与协议实现的用户。闪连VPN 提供 WireGuard、Shadowsocks、VLESS 等多种协议选项，数据层采用 ChaCha20-Poly1305 与 AES-256-GCM 加密。本页面以客观方式呈现闪连的技术实现特点。

https://www.shanlianqi.com.cn/

闪连VPN

面向关注连接效率与协议实现的用户。闪连VPN 提供 WireGuard、Shadowsocks、VLESS 等多种协议选项，数据层采用 ChaCha20-Poly1305 与 AES-256-GCM 加密。本页面以客观方式呈现闪连的技术实现特点，帮助有一定技术认知的用户判断产品是否匹配需求。

协议实现与数据层加密

WireGuard

基于 UDP 的高效隧道协议，内核级实现带来更低握手延迟与更高吞吐，适合对连接效率敏感的场景。

Shadowsocks

轻量级加密代理协议，采用流式加密和灵活的混淆插件，适合在网络环境复杂时维持稳定连接。

VLESS

无冗余认证的轻量传输协议，可与多种传输层组合，减少握手开销，提升长连接下的效率。

ChaCha20-Poly1305

面向移动端优化的认证加密算法，在缺乏 AES 硬件加速的设备上提供高效且安全的加密性能。

AES-256-GCM

广泛使用的对称加密标准，提供强认证与保密性，适合具备硬件加速能力的桌面与服务器环境。

连接效率

通过协议选择与加密算法组合，在安全与性能之间取得平衡，适应不同网络条件与设备能力。

技术配置步骤

选择协议

根据网络环境与设备能力，在 WireGuard、Shadowsocks、VLESS 中选择合适的传输协议。

指定加密算法

数据层可选择 ChaCha20-Poly1305 或 AES-256-GCM，移动端可优先考虑前者以获得更好性能。

建立连接

通过命令行或配置文件启动连接，观察握手延迟与吞吐表现，按需调整参数。

验证状态

检查连接状态、加密算法生效情况及实时延迟，确保配置符合预期。

协议配置示例

以下为客观的配置结构示意，不代表实际产品命令。

常见技术问题

闪连VPN 的数据层支持 ChaCha20-Poly1305 与 AES-256-GCM 两种认证加密算法。前者在无硬件加速的移动设备上表现更好，后者适合具备 AES-NI 的桌面或服务器环境。

WireGuard 是基于 UDP 的内核级隧道协议，握手快速、吞吐高；Shadowsocks 更偏向轻量加密代理，可通过插件实现混淆，适合不同网络环境。二者面向不同的连接效率与隐蔽性需求。

VLESS 是一种轻量传输协议，不携带冗余认证信息，可减少握手开销。它通常与不同的传输层（如 WebSocket、gRPC）组合，适合需要灵活部署的场景。

如果设备缺少 AES 硬件加速指令，优先选择 ChaCha20-Poly1305；如果运行在支持 AES-NI 的桌面或服务器上，AES-256-GCM 通常能提供更高的吞吐。实际选择可依据基准测试结果调整。

评估你的协议与加密组合

结合网络条件与设备能力，选择最适合的协议实现。本页面仅提供客观技术特性说明，不包含实测数据或产品推荐。