了解 WireGuard 协议

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

Private Internet Access 很高兴宣布，我们现在已在所有平台上支持 Wireguard 连接协议。

注意：WireGuard 目前无法在 **Ubuntu 16.04** 上运作，我们的开发团队正在奋力解决此问题。不过，暂时没有此问题可以解决的预计时间。另请注意，**Windows 7** 不支持 WireGuard。使用此功能需要 **Windows 8 或更新版本**。

PIA 中的 WireGuard 连接是这样工作的：向服务器发送一个 HTTPS 请求以索取 IP 地址和连接信息，然后我们会将 UDP WireGuard 流量发送到服务器。因此，WireGuard 连接需要在 VPN 服务器上同时连接 **TCP 1337 和 UDP 1337**。

目前，在桌面版应用程序中，如果您需要在 Wireguard 连接提供的速度基础上获得更快的速度，您可以使用提供的**小数据包**功能。未来也会实施通过 Wireguard 利用的其他功能，但目前它处于预览模式，我们无法提供其他选项或设置的时间表。

安装和使用 Wireguard 在所有设备上都很简单明了，但 Linux 除外，它需要 Linux 内核实施。在一些情形中，这要求您通过 Wireguard 的下载页面手动执行内核安装，具体见以下网址：

https://www.wireguard.com/install/

如果无法在上述链接上找到您的分发，但已安装了应用程序，您可以通过以下链接直接从源代码编译内核（您的系统上必须已安装了 git）：

https://www.wireguard.com/compilation/

> **注意：**由于这两种方式都需要在我们应用程序的功能之外进行安装，我们无法对安装内核时可能出现的安装错误提供支持。

如果您在任何平台上遇到与 Wireguard 相关的问题，并且问题在我们的支持范围内，请随时从这里提交支持工单来联系我们。

关于 Wireguard

WireGuard 是一种相对较新的开源 VPN 协议，由 Jason A. Donenfeld 编写和开发，有望提供比以往选择更多的优势。WireGuard 以高效、易用为宗旨，同时减少幕后所需的工作。
与 OpenVPN (600,000) 和 IPsec (400,000) 等其他 VPN 协议相比，WireGuard 由非常少的代码构成，只有不到 $4,000$ 行。这使得安全审查和识别错误变得更加快速，修正也更加简单，因为需要梳理的代码变少了。

它的一大优势在于使用现代技术。由于开销较少并且使用最新的加密技术，WireGuard 有望能减少容易断线的问题，并缩短协商连接的用时。在实现这一切的同时，还有更加安全和稳定的隧道，并通过 UDP 发送数据包来加快连接速度。所有这些功能都旨在为移动电话提供更快的连接速度、更好的电池续航，以及总体上更加可靠的连接。

下方列出了 WireGuard 使用的协议和原语，您也可在官方网站上找到更多详细信息。

- ChaCha20 用于对称加密，通过 Poly1305 进行验证，利用 RFC7539 的 AEAD 结构
- Curve25519 用于 ECDH
- BLAKE2s 用于哈希和加密哈希，如 RFC7693 中所述
- SipHash24 用于可哈希密钥
- HKDF 用户密钥衍生，如 RFC5869 中所述