

隧道穿行 / 穿梭指南

这本小册子由手绘的图标制作

排版由 scribus 完成

文本字体为思源宋体

如有问题请联系
hi@psaroskalazines.gr

中文翻译：大耳朵

CC-BY-NC-SA 2020



一个关于虚拟私人网络的绘本手册



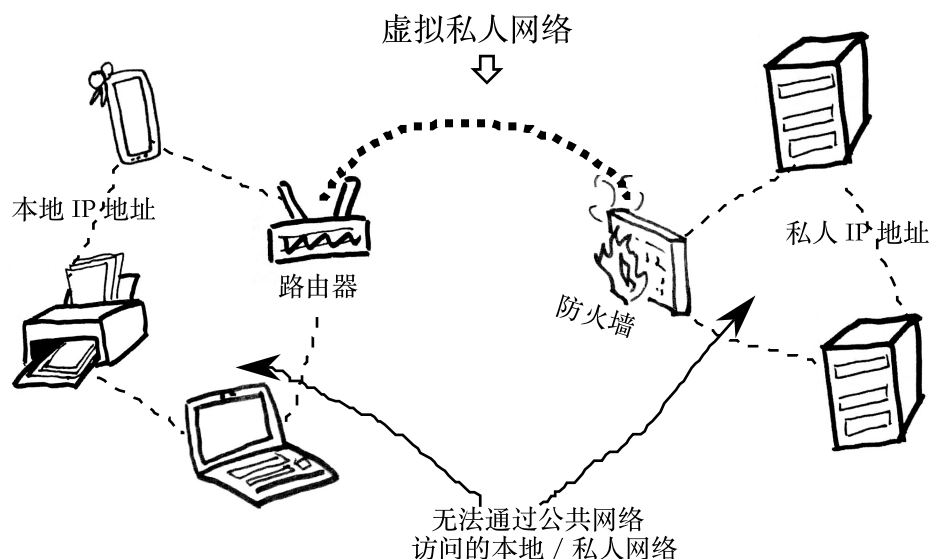


一个对隧道，隧道如何运作，隧道安全性，
和组装 IPsec 和 openVPN 工具的介绍。

什么是虚拟私人网络?

虚拟私人网络（也被称为 VPN）是基于公共网络的延伸。比如说，在家里，我们的设备能通过本地网络连接。你可以想象你的设备能连接到在另外一个家中的本地网络：）或者是连接被机构或办公室用防火墙阻隔而不能被公共网络访问的一个由一组服务器组成的私人网络。

这即是名字中的所谓的“虚拟”，因为 VPN 能够让处于不同本地网络的设备，通过一个启用直接端到端发送的通道相互通讯，避开由路由器传输的流量交通。



速查表

用 IPsec 配置站点连站点 VPN:

<https://blog.ruanbekker.com/blog/2018/02/11/setup-a-site-to-site-ipsec-vpn-with-strongswan-and-preshared-key-authentication/>

strongswan 配置 IPsec 的选择:

<https://wiki.strongswan.org/projects/strongswan/wiki/ConnSection>

一个对了解认证和封装有帮助的指南，带有插图，包含了 IPsec 的传输和隧道模式:

<http://www.unixwiz.net/techtips/iguide-ipsec.html>

用 openVPN 配置远程访问隧道:

<https://community.openvpn.net/openvpn/wiki/HOWTO>

一些关于在 TCP/IP 占领网络通讯前，原有的 OSI 模型的故事:

<https://spectrum.ieee.org/tech-history/cyberspace/osi-the-internet-that-wasnt>

维基百科冠以隧道协议的文章，附有隧道的列表:

https://en.wikipedia.org/wiki/Tunneling_protocol

关于加密如何工作的表演指南:

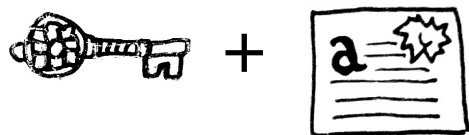
<http://ooooo.be/cryptodance/>



OpenVPN

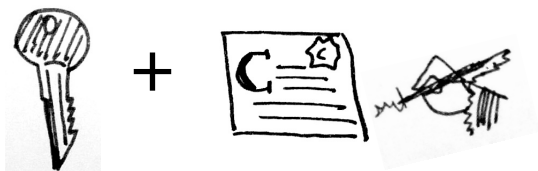
OpenVPN 使用 openssl 来生成下列生成密钥和证书:

- 签署其他证书的证书授权中心

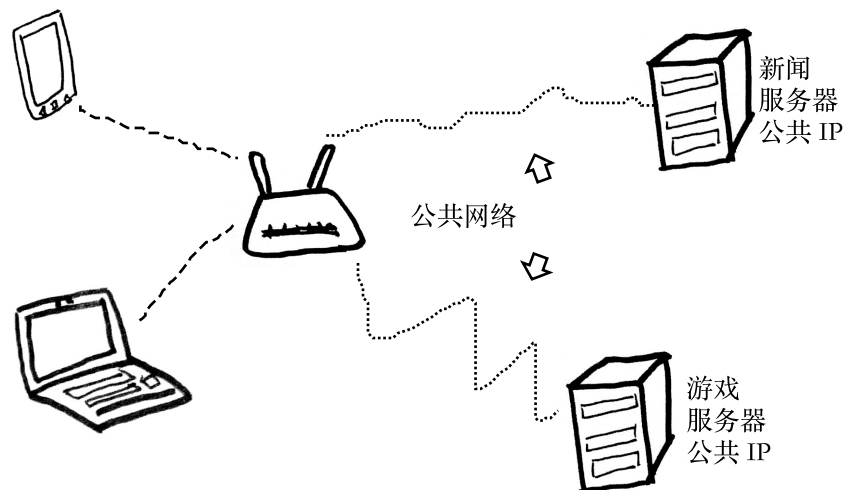


- 服务器

- 用户, 用户可有自己个人的证书, 或者共享相同的证书 (更容易, 但是用户数量多的话会有安全隐患)



同时连接的用户数量可以在 server.conf 配置文件中设置。这个文件包含了所有我们需要为隧道设置的参数, 是被 openVPN 软件安装的。* 重要: Diffie-Helman 参数需要填一个高的数值 * 另一个安装了 openVPN 的库是 easy-rsa, 用来生成密钥和证书。当这些都被生成之后, 客户端的配置文件会有跟 server.conf 相同的配置, 并和证书和密钥一同被发送到服务器。

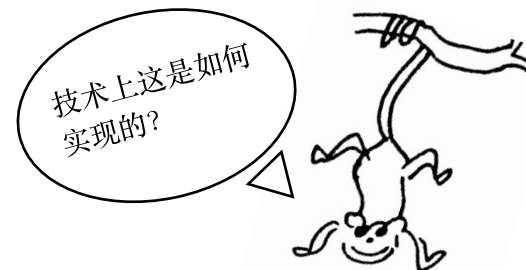


使用公共网络将你家里 / 办公室里的设备连接到配有公共 IP 地址的服务器。

VPN 的种类:

- 主机连主机 (远程访问, 比如说设备连服务器)
- 站点连站点 / 网关连网关 / 网络连网络

这两种 VPN 都能帮助访问被防火墙屏蔽的服务, 比如说虚拟机, 媒体存储空间; 而第一种则能帮助访问被审查的站点。



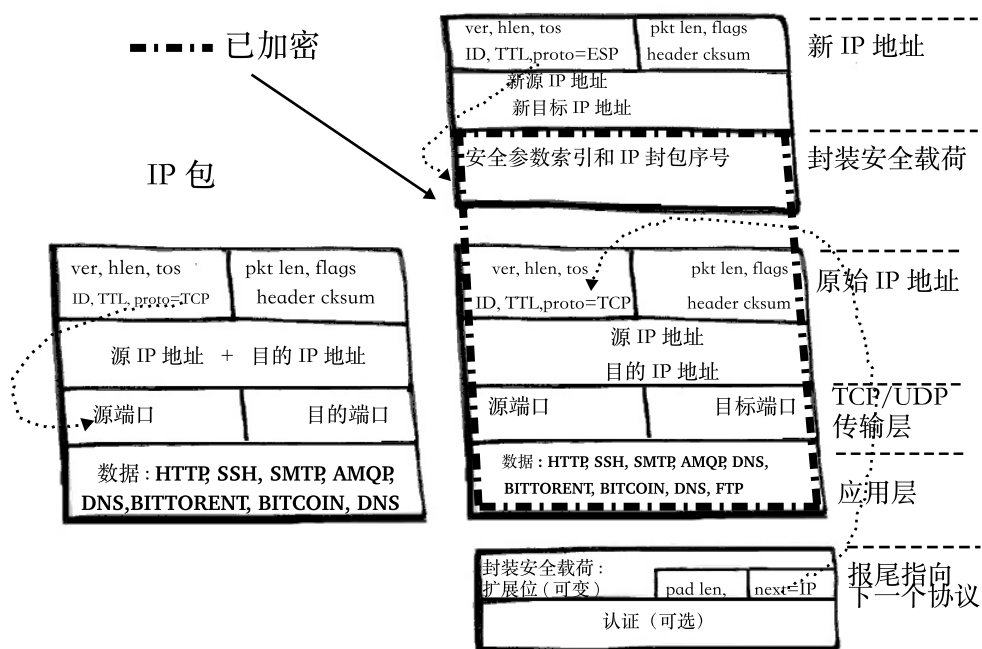
VPN 是怎么运作的?

VPN 使用隧道协议（一种通讯协议），将互联网视作一个私人网络从中传输数据。

为了实现这个目的，隧道将 IP 包封装（简而言之就是包裹）在一个新的 IP 报头中。

被封装后原有的 IP 报头里包含了目标（私人）地址，而新的 IP 层包含了 VPN 服务器的公共 IP 地址作为目标地址。

经过封装的 IP 包



IPsec



一个用来建造 IPsec 的自由软件选择是带有各种验证的加密方法的 strongswan。



IPsec 有两种模式：

运输模式。在运输模式中，IP 包中只有载荷部分被加密或被验证。路由部分是完整的，因为 IP 报头没有被修改或加密。注意：在使用认证报头时，IP 地址不能通过网络地址转换，因为这个过程会改变前后 IP 地址，从而作废哈希值。

隧道模式。在隧道模式中，整个 IP 包会被加密和被验证。接着，IP 包会被封装到一个带有新 IP 报头的新 IP 包中。隧道模式是用来建造虚拟私人网络货真价实的隧道，通常用于网络连网络的通讯（例如用于连接站点的路由器），但也可以用于用户连网络的通讯（比如远程用户访问）和服务器连服务器的通讯（比如私人会话）。

有什么工具能用来搭建隧道呢？

IPsec 和 OpenVPN 是涵盖通用设置的自由软件选择。首先，我们需要决定我们想建立什么样的连接。如果我们想连接被防火墙屏蔽的设备（门户到门户），而且我们不担心审查机制（因为如果我们担心的话，IPSec 的标准接口 50,51,500 和 4500 会很容易被权力机关屏蔽）。但是如果过滤不是一个问题，而且我们想保持隧道的通畅，那么 IPSec 是可行的。

对于使用客户端连服务器远程访问（主机连主机）来访问在公共网络中受限制的网站，或者我们想使用隧道来重新对我们的流量进行 forward，那么 OpenVPN* 是比较方便了，因为它可以设置任意开放的接口（也就是没有被别的协议占用的接口，比如说 SMTP, VoIP, TLS), 并保持隧道不被权力机关或服务供应商发现的私密性。它可将很多用户连接到 VPN 上，也便于在移动端上安装使用。

*OpenVPN 有一个社群版本，还有一个更商业的版本。商业的版本有一个更容易设置的网页端的交互页面，但需要购买连接用户的数额。而社群版本则不限用户数量。

** 网络运营商 / 权力机关会出于过滤目的阻隔一些端口。

常见隧道协议

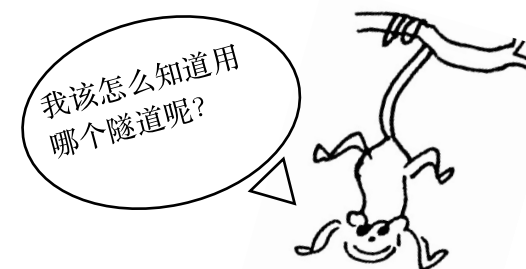
- IP in IP (例子：能连接两个不能通讯的 IPv4 网络，比如在负载均衡器中转发数据包的虚拟 IP，和有真实 IP 地址的服务器)
- IPsec (互联网安全协议) - OpenVPN
- OpenVPN
- GRE (Cisco 的通用路由封装，可以将 IPv6 地址封装在 IPv4 里面)

在这里，我们关注 IPsec 和 OpenVPN

对于门户连门户的隧道来说更理想，而 OpenVPN 对远程访问（客户端连服务器）隧道来说更理想。

IPsec 和 GRE

GRE（通用路由封装协议）隧道能在 Cisco 的路由器上安装，来实现将一层网络层协议封装在另一层内的目的。比如说，我们能安装一个 GRE 隧道来在一个只用 IPv6 的网络中传输 IPv4 的数据包。GRE 不提供加密功能，所以 GRE 隧道能跟 IPsec 合用，以达到安全和隐私的目的。



什么时候我们需要使用隧道？



决定使用哪一种隧道，取决于我们网络的设置和我们想达到的目标：

1. 绕开由政府，大学，工作单位设置的网络传输过滤机制，也就是通常所说的“审查”。通过使用隧道，我们的数据在到达 VPN 服务器之前都在隧道中藏着；从 VPN 服务器开始，这些数据会被转发到最终的目的地服务器（例如说社交媒体，视频和新闻站点）。
2. 连接物理上和我们设备分离的内网（也就是私人或本地网络）。比如说 SSH 可以让远程的服务器访问一个由公共 IP 地址的服务器。通过使用隧道可以用 SSH 访问私人服务器。或者访问别人在家里设置的设备；)

用什么 IPsec 和 OpenVPN？



IKE（互联网安全协议）是一个用于为 IPsec 配置安全联盟的协议。我们可以使用这种安全联盟来发起私密的共享会话，来生成传输数据的密钥。IKE（互联网安全协议）也被用来验证两个持有预先沟通过密钥，或者持有公开 / 私密密钥的 IPsec 用户。

ESP（封装）模块在 IPsec 中使用能够以块状作为单位处理数据的加密算法。这就是为什么 ESP 报尾有一个填充部分，来将加密数据调整成算法要求的加密块大小。（参考第三页的 IP 加密数据包）。

IPsec 加密密钥能通过 DES/3DES/AES 算法生成。

Diffie-Hellman 加密算法被用来加密钥匙和传送钥匙（简短的说明）

在 openVPN 里，Diffie-Hellman 加密算法被用来交换密钥。DH 的参数被发到客户端来生成一个共享的秘密。之后，这个新秘密就被用来作为加密通讯数据的会话密钥。

加密

加密有两种方法：

不规则加密算法 - 用到两个密钥，一个公开密钥，一个私有密钥。这个也被称为公开密钥加密。邮件客户端会使用 pgp 加密来操作这个方法。

对称加密算法用一个密钥来加密和解密数据。

RSA 公开密钥交换属于不规则加密算法。这种方法可以和数字签名，密钥交换一起使用，还有实现加密。

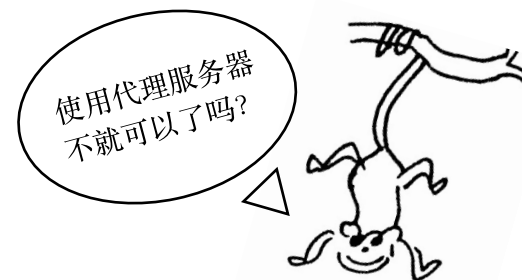
Diffie-Hellman 加密算法

是为每次活动生成新钥匙，并在活动结束后弃用来保障前向保密的常用选择。

这个过程包含了两个对象对通常的参数取得同意，并使用 ta 们的私有密钥生成一个密钥。接着他们使用接线网络来交换这个对称密钥。这个过程中，两个对象收到的密钥都会和 ta 们各自的私人密钥再次结合。结果是 ta 们都收到了和对方相一致的最终密钥。Ta 们可以使用这个一致密钥（不需使用接线网络）来加密 ta 们接下来的通讯。

* 长度短的 Diffie-Hellman 被后斯诺登时代被验证能被解密。

** https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange#Secrecy_chart



虽然代理可以隐藏你的 IP，其安装过程也更简单或者供应商提供的价钱更便宜，但代理不能加密你的流量。VPN 隧道能够帮助访问被防火墙阻隔的资源，而代理只能将流量导向另一个服务器。所以代理包含了第一点，对抗 IP 过滤的匿名性，虽然不提供加密；不包含第二点，建立私人网络和访问被防火墙阻隔的资源。

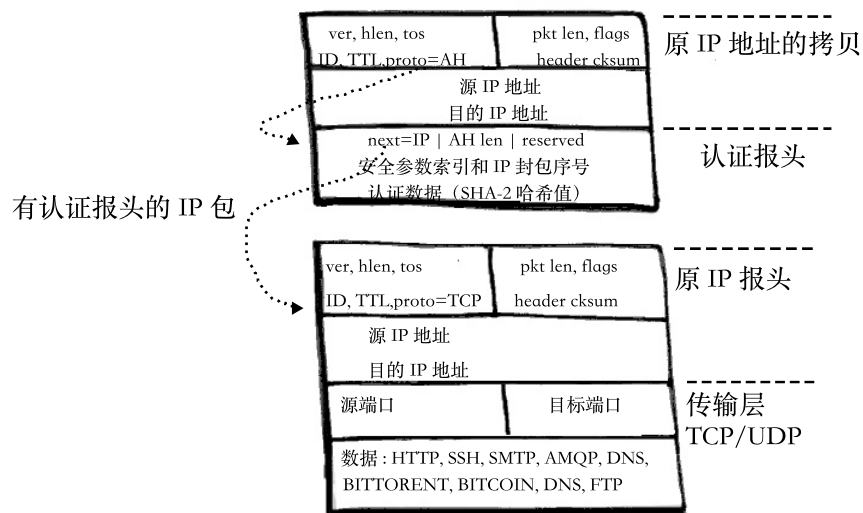
所以 VPN 比代理更安全，因为

它提供了加密或不加密的隧道。但它总会要求验证，并可以确定数据的一致性，确认数据在传输过程中没有被他人干扰。也可以被加密。OpenVPN 使用私钥和证书。

认证报头

认证报头为一个用户或网络通过用户名和 / 或密码认证访问权限。

IPsec 认证通常是根据预先分享的密钥，或者是具有私钥和证书的复杂设置。



一致性

确保数据没有在传输过程中被更改或截获。哈希算法被用于实现这个目的。VPN 服务器用来确保数据一致性的有两种算法，分别为 SHA 类和 MD 类。例如 hmac-md5, hmac-sha2* 和 hmac-sha3**，都是使用加密哈希算法和密钥的消息认证码。金钥杂凑讯息鉴别码不会加密 IP 包。作为替代，消息验证码的哈希值必须随着 IP 包发送。当 IP 包到达隧道接受端后，持有密钥的用户可以计算 IP 包的哈希值，如果这个值是可信的，接收到和计算过的哈希值应该一致。如果不一致，IP 包将被废弃。

* 由美国国家安全局设计

** 由美国国家标准技术研究所设计，为美国商务部下属的一个研究所。

又及：难怪对美国机密部门来说，去探究这些算法的弱点是非常可行的。

