为什么是OpenVPN而不是其他的VPN？

1.虚拟专用网络（Virtual Private Network，VPN)

2.关于VPN中安全策略中采取的四种技术

3.OpenVPN介绍

4.OpenVPN与PPTP VPN比较

5.最危险的不是技术，而是人

6.总结

Content:

1. 虚拟专用网络（Virtual Private Network，VPN）

为什么需要VPN技术？在互联网公用的传输链路上，别有用心的人就会在互联网上截取你发送或者接受的数据包，进而进行破译，获取到他们感兴趣的内容。因此互联网因其开放性和互联性，使其存在着信息威胁和安全隐患。

所以安全的方式：自己搭建一条物理专用链路。但是这种方式的造价太高了，并且灵活性不好，除非军队等特殊的情况（笔者小时候经常在农田里见到“下游国防光缆”），但是商用的专线采用单独的物理链路不可行。这就引出了VPN链路传输。



虚拟专用网络是在公用网络链路上建立专用网络（虚拟），进行加密通讯，是一种远程访问技术。VPN网关通过对数据包的加密和数据包目标地址的转换实现远程访问，这样就利用实际已经存在的物理链路，搭建了一条虚拟的专用链路，以保障数据传输的安全。

VPN有多种分类方式，主要是按协议进行分类。VPN采取的隧道协议主要有三种：PPTP、L2TP和IPSec，其中PPTP和L2TP工作在数据链路层，被称为二层隧道协议，二IPSec工作在IP层，因此被称为三层隧道协议。

VPN可通过服务器、硬件、软件、集成VPN的硬件设备（防火墙、路由器）等多种方式实现，采用的设备有

专用的VPN路由器：在路由器上添加VPN服务即可

交换机VPN：主要用于连接比较少的VPN网络

防火墙式VPN：最常见的VPN网关，用于网络的出口，一般采取双网卡，一张网卡连接外网，一张网卡连接内网。

常用的VPN技术：

MPLS VPN:是在网络路由和交换设备上使用的技术，工作在二层交换和三层路由上。

SSL VPN：基于HTTPS的VPN技术，工作在传输层和应用层之间，充分利用SSL协议提供的基于证书的身份认证、数据加密和消息完整性验证机制，为应用层之间建立安全链接。

IPSec VPN技术是基于IPSec协议实现的VPN技术，由IPSec协议提供隧道安全保障，为互联网传输提供高质量、互操作的、基于密码学的安全保证。

1. 关于VPN中安全策略中采取的四种技术

由于VPN链路传输的是私有信息，所以VPN的安全技术是用户最关心的。目 前VPN主要采用四项技术来保证安全，这四项技术分别是隧道技术（Tunneling）、加解密技术（Encryption &Decryption）、密钥管理技术（Key Management）、使用者与设备身份认证技术（Authentication）。

隧道技术是VPN的基本技术，类似于点对点连接技术，它在公用网建立一条数据通道（隧道），让数据包通过这条隧道传输。隧道是由隧道协议形成的，分为第 二、三层隧道协议。第二层隧道协议是先把各种网络协议封装到PPP中，再把整个数据包装入隧道协议中。这种双层封装方法形成的数据包靠第二层协议进行传输。第二层隧道协议有L2F、PPTP、L2TP等。L2TP协议是目前IETF的标准，由IETF融合PPTP与L2F而形成。第三层隧道协议是把各种网络协议直接装入隧道协议中，形成的数据包依靠第三层协议进行传输。第三层隧道协议有VTP、IPSec等。IPSec（IP Security）是由一组RFC文档组成，定义了一个系统来提供安全协议选择、安全算法，确定服务所使用密钥等服务，从而在IP层提供安全保障。

加解密技术是数据通信中一项较成熟的技术，VPN可直接利用现有技术。

密钥管理技术的主要任务是如何在公用数据网上安全地传递密钥而不被窃取。现行密钥管理技术又分为SKIP与ISAKMP/OAKLEY两种。SKIP 主要是利用DiffieHellman的演算法则，在网络上传输密钥；在ISAKMP中，双方都有两把密钥，分别用于公用、私用。

身份认证技术最常用的是使用者名称与密码或卡片式认证等方式。

1. OpenVPN介绍

OpenVPN 是一个基于 OpenSSL 库的应用层 VPN 实现，**并且是开源的**。OpenVPN允许参与建立VPN的单点使用共享密钥、电子证书、或者用户名/密码来进行身份验证（因为用户名/密码方式采用简单的暴力破解方式可以破解，建议不要采用这种方式）。它大量使用了OpenSSL加密库中的SSLv3/TLSv1 协议函式库。

关于OpenVPN的通用性

因为OpenVPN是利用C/C++实现的，并且开源，可根据平台自行编译，所以OpenVPN有很好的平台兼容性，能在Solaris、Linux、OpenBSD、FreeBSD、NetBSD、Mac OS X、Windows 2000/XP/Vista及Android和iOS移动操作系统上运行，并包含了许多安全性的功能。但是它并不是一个基于Web的VPN软件，也不与IPsec及其他VPN软件包兼容（因此跟类似的浏览器插件性质的VPN性质是不同的，我们曾经使用的浏览器插件方式的VPN只能通过特定的浏览器进行数据传输）。

关于OpenVPN的一些性质

OpenVPN提供了两种虚拟网络接口：通用Tun/Tap驱动，通过它们， 可以建立三层IP隧道，或者虚拟二层以太网，后者可以传送任何类型的二层以太网络数据。

传送的数据可通过LZO算法压缩。

在选择协议时候，需要注意2个加密隧道之间的网络状况，如有高延迟或者丢包较多的情况下，请选择TCP协议作为底层协议，UDP协议由于存在无连接和重传机制，导致要隧道上层的协议进行重传，效率非常低下。使用TCP方式，在传输层进行数据的完整性检查，但是对于一些数据比如音视频的传输，对于数据的完整性要求不是很高，可以采用UDP方式进行传输。

同时也正是OpenVPN使用通用网络传输层协议（TCP与UDP）的特点使它成为IPsec等协议的理想替代，尤其是在ISP（Internet service provider）过滤某些特定VPN协议的情况下，比如某些校园网、某些运营商网络会过滤VPN数据包，但是OpenVPN通过TCP、UDP协议传输，可以很好的绕开这个限制，同时OpenVPN还可以很好的穿透NAT机制，对于使用NAT的网络环境十分有效。

上面的三点特性在OpenVPN的配置文件中有体现，再配置文件的时候要注意根据实际情况进行选择。

1. OpenVPN与PPTP VPN比较

在PPTP和OpenVPN二者之间做出选择的一个重要考虑因素，也是我们无法控制的因素，就是有时互联网服务供应商会阻止 PPTP连接。当网络上存在地址转换设备时，PPTP VPN可能不能正常连接。大部分用户反映使用长宽、有线、铁通的网络时无法连接。此情况下我们无计可施，只能选择使用OpenVPN。PPTP具有一些独特优势，但此刻用OpenVPN会是不错的选择。如果将OpenVPN的端口改成443，并且采用TCP协议方式，那么运营商是区别不出数据包是HTTPS还是OpenVPN，这样是无论如何不会被禁的。

PPTP加密技术使用密码作为密钥，它的数据流载有可获取的混编密码。如果中间有人拦截到了数据流并且破译了密码（尽管可能但很难），那么他就可以破译你的信息。然而OpenVPN使用非常强大的加密（Blowfish）技术。即使有人拦截你的数据流，他们也无计可施。这使得OpenVPN比PPTP安全得多。如果你希望得到高安全性以及更加关注数据安全传输问题，那么你应该使用OpenVPN。

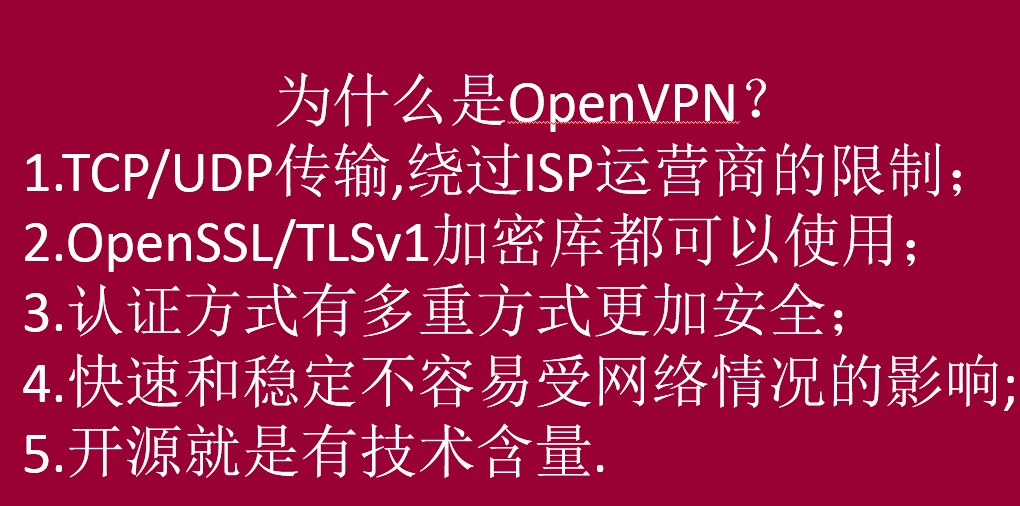
1. 最危险的不是技术，而是人

虽然VPN技术提供了安全的数据链路，但前提是连接VPN的客户端是安全的。如果客户端被黑客控制，链路是安全的、连接也是安全的，只有人是最危险的，因此在使用VPN访问内部网络的时候，需要确保客户端的计算机不被黑客控制，同事在客户端装好防火墙。如果使用linux作为VPN，建议将VPN的配置文件设置为root用户，只有root用户有读取执行的权限，并且禁止linux的远程登录机制。

1. 总结

为什么是OpenVPN？我总结了下面几点

1. 开源代码的软件，可以自行修改编译
2. 是利用TCP/UDP进行传输，有效的规避了某些ISP运行商的限制
3. OpenVPN加密机制采用了OpenSSL/TLSv1加密库，这个库提供了丰富的高难度的复杂加密算法，安全
4. OpenVPN的认证方式有多重方式，并且采用证书认证、公钥密钥加密解密算法等等，比传统的VPN 在网络中传输用户名密码更加安全。
5. OpenVPN 不容易受网络情况的影响，当网络不稳定的情况下，OpenVPN的也非常的快速和稳定。
6. 因为OpenVPN的难度（技术含量）比其他VPN更加有挑战性，逼格高。



备注：

文章以OpenVPN官网文档为基础，参考了很多博客的资源，再次表示感谢。个人整理这些知识仅仅以学习和总结为目的，所以难免出现内容相似的地方，敬请谅解！

文卿

2016年8月13日