网络安全vpn学习报告

## 任务1：了解VPN技术有哪些类型，这些技术各自有些什么特点，分别适用于什么场景？

**VPN技术有哪些类型?特点?适用场景?**

VPN的隧道协议主要有四种，PPTP、L2TP、IPSec和SSL，其中PPTP和L2TP协议工作在OSI模型的第二层，又称为二层隧道协议；IPSec是第三层隧道协议；而SSL是工作在OSI会话层之上的协议，如果按照TCP/IP协议模型划分，即工作在应用层。

1、PPTP,即PPTP协议。该协议是在PPP协议的基础上开发的一种新的增强型安全协议，支持多协议虚拟专用网（VPN），可以通过密码身份验证协议（PAP）、可扩展身份验证协议（EAP）等方法增强安全性。可以使远程用户通过拨入ISP、通过直接连接Internet或其他网络安全地访问企业网。

2、L2TP是一种工业标准的Internet隧道协议，功能大致和PPTP协议类似，比如同样可以对网络数据流进行加密。不过也有不同之处，比如PPTP要求网络为IP网络，L2TP要求面向数据包的点对点连接；PPTP使用单一隧道，L2TP使用多隧道；L2TP提供包头压缩、隧道验证，而PPTP不支持。

3、IPSec 是安全联网的长期方向。它通过端对端的安全性来提供主动的保护以防止专用网络与 Internet 的攻击。在通信中，只有发送方和接收方才是唯一必须了解 IPSec 保护的计算机。在 Windows XP 和 Windows Server 2003 家族中，IPSec 提供了一种能力，以保护工作组、局域网计算机、域客户端和服务器、分支机构（物理上为远程机构）、Extranet 以及漫游客户端之间的通信。

4、SSL VPN是解决远程用户访问公司敏感数据最简单最安全的解决技术。与复杂的IPSec VPN相比，SSL通过简单易用的方法实现信息远程连通。任何安装浏览器的机器都可以使用SSL VPN， 这是因为SSL 内嵌在浏览器中，它不需要象传统IPSec VPN一样必须为每一台客户机安装客户端软件。

**PPTP，L2TP和IPsec的区别及优缺点**

1、PPTP协议是点对点隧道协议：

其将控制包与数据包分开，控制包采用TCP控制，用于严格的状态查询及信令信息；数据包部分先封装在PPP协议中，然后封装到GRE V2协议中。

2、L2TP是国际标准隧道协议：

它结合了PPTP协议以及第二层转发L2F协议的优点，能以隧道方式使PPP包通过各种网络协议，包括ATM、SONET和帧中继。但是L2TP没有任何加密措施，更多是和IPSec协议结合使用，提供隧道验证。

3、两者的联系与区别：

PPTP和L2TP联系：

都使用PPP协议对数据进行封装，然后添加附加包头用于数据在互联网络上的传输。尽管两个协议非常相似，但是仍存在以下几方面的不同

PPTP和L2TP区别：

1）PPTP要求互联网络为IP网络。L2TP只要求隧道媒介提供面向数据包的点对点的连接。L2TP可以在IP（使用UDP），桢中继永久虚拟电路（PVCs），X.25虚拟电路（VCs）或ATM VCs网络上使用。

2）PPTP只能在两端点间建立单一隧道。L2TP支持在两端点间使用多隧道。使用L2TP，用户可以针对不同的服务质量创建不同的隧道。

3）L2TP可以提供包头压缩。当压缩包头时，系统开销（overhead）占用4个字节，而PPTP协议下要占用6个字节。

4）L2TP可以提供隧道验证，而PPTP不支持隧道验证。但当L2TP或PPTP与IPSEC共同使用时，可由IPSEC提供隧道验证，不需在第2层协议上验证隧道。

简单来说:

PPTP使用TCP协议，适合没有防火墙限制的网络。

L2TP使用UDP协议，一般可以穿透防火墙，适合有防火墙限制、局域网用户，如公司、网吧、学校等场合。

## 任务2：分析基于SSL/TLS的VPN，是如何实现对两端流量的正确路由的？TUN/TAP接口在当中起什么作用？

**找不到资料**

SSL/TLS 协议基本流程：

1.客户端向服务器索要并验证服务器的公钥。

2.双方协商生产「会话秘钥」。

3.双方采用「会话秘钥」进行加密通信。

前两步也就是 SSL/TLS 的建立过程，也就是 TLS 握手阶段。

TLS 的「握手阶段」涉及四次通信，使用不同的密钥交换算法，TLS 握手流程也会不一样的，现在常用的密钥交换算法有两种：RSA 算法 (opens new window)和 ECDHE 算法

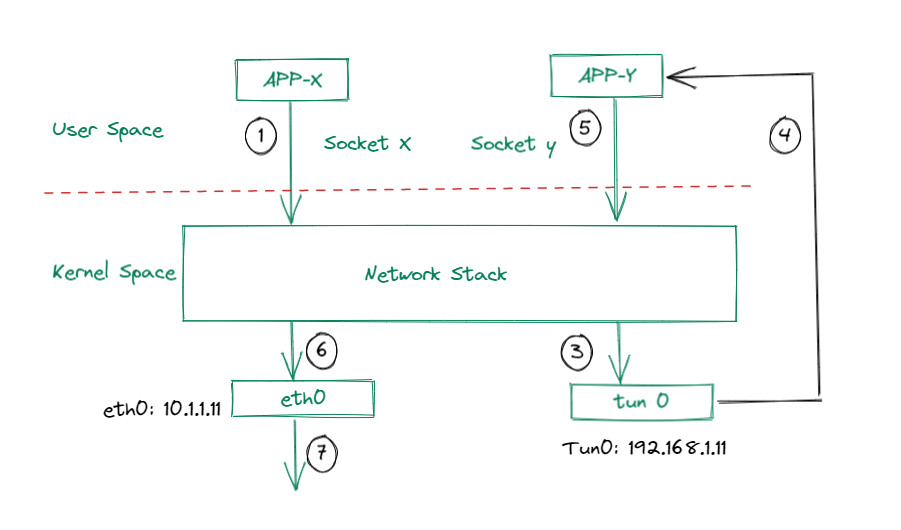
如果想控制VPN的访问策略，必须为TUN/TAP接口创建防火墙规则.**来源**：<https://blog.51cto.com/u_14892047/5201768>

openvpn的TUN/TAP：<https://blog.shell909090.org/blog/archives/2724/>

以下内容来自：<https://www.linuxea.com/2747.html>

tun、tap作为虚拟网卡，除了不具备物理网卡的硬件功能外，它们和物理网卡的功能是一样的，此外tun、tap负责在内核网络协议栈和用户空间之间传输数据。

程序 A 希望构造数据包发往 192.168.1.0/24 网段的主机 192.168.1.1。



数据包要转发，是比要从用户空间转发到内核空间，到了内核空间后，如果是普通报文就直接送往网络设备上了(1，6，7)。

但是有了tun设备的介入，数据在传递的时候查看了路由表，数据不应该被送往到物理网卡，而是要传送到tun进程打开的设备上。tun设备本身就可以把内核的报文送回给用户空间，用户空间收到后仍然想正常的报文一样处理，但是不同的是，会将报文做一些修改,因为用户空间本身不能做封装，这些修改的内容最终发送到内核空间，内核空间就照单全收，根据数据包信息进行发送。（1-3-4-5-6-7）

1.应用程序 X 构造数据包，目的 IP 是 192.168.1.1，通过 socket X 将这个数据包发给协议栈。

2.协议栈根据数据包的目的 IP 地址，匹配路由规则，发现要从 tun0 出去。

3.tun0 发现自己的另一端被应用程序 Y 打开了，于是将数据发给程序 Y.

4.程序 Y 收到数据后，做一些跟业务相关的操作，然后构造一个新的数据包，源 IP 是 eth0 的 IP，目的 IP 是 10.1.1.0/24 的网关 10.1.1.1，封装原来的数据的数据包，重新发给协议栈。

5.协议栈再根据本地路由，将这个数据包从 eth0 发出。

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

虚拟专用网（virtual personal network，VPN）是利用internet等公共网络的基础设施，

通过隧道技术，为用户提供的专用网络具有相同通信功能的安全数据通道。

在没有VPN之前，企业的总部和分部之间的互通都是采用运营商的internet进行通信，那么Internet中往往是不安全的，通信的内容可能被窃取、修改等，从而造成安全事件。当然可以通过拉专线的方式，不过这种方式成本高，且维护困难。VPN通过在现有的Internet网中构建专用的虚拟网络，实现企业总部和分部的通信，解决了互通、安全、成本的问题。

**VPN技术的优势**

安全：在远端用户、驻外机构、合作伙伴、供应商与公司总部之间建立可靠的连接，保证数据传输的安全性。这对于实现电子商务或金融网络与通讯网络的融合特别重要。

成本低：利用公共网络进行信息通讯，企业可以用更低的成本连接远程办事机构、出差人员和业务伙伴。

支持移动业务：支持出差VPN用户在任何时间、任何地点的移动接入，能够满足不断增长的移动业务需求。

可扩展性：由于VPN为逻辑上的网络，物理网络中增加或修改节点，不影响VPN的部署。

灵活性强：可支持通过各种网络的任何类型的数据流，支持多种类型的传输媒介，可同时满足传输语音、图像和数据等的需求

服务质量佳：为企业提供不同等级的服务质量保证。不同用户和业务对服务质量保证的要求差别较大，对于拥有众多分支机构的专线VPN，交互式内部企业网应用则要求网络提供良好的稳定性。

**VPN技术实现**

VPN是再Internet等公共网络基础上，综合利用隧道技术、加解密技术、密钥管理技术和身份认证技术实现的。

**隧道技术**

隧道技术是一种通过使用互联网络的基础设施在网络之间传递数据的方式。使用隧道传递的数据(或负载)可以是不同协议的数据帧或包。隧道协议将这些其他协议的数据帧或包重新封装在新的包头中发送。新的包头提供了路由信息，从而使封装的负载数据能够通过互联网络传递。

隧道可分为自愿隧道和强制隧道两种。

1.自愿隧道

自愿隧道是使用最普遍的隧道类型。客户端可以通过发送VPN请求配置和创建一条自愿隧道。为建立自愿隧道，客户端计算机必须安装适当的隧道协议，并需要一条IP连接(可通过局域网或拨号线路)。如果使用拨号方式，客户端必须在建立隧道之前创建与公共互联网的一个拨号连接。

2.强制隧道

强制隧道由支持VPN的拨号接入服务器配置和创建。在这种情况下，用户计算机不作为隧道端点，而是由位于用户计算机和隧道服务器之间的远程接入服务器作为隧道客户端，成为隧道的一个端点。

**身份认证、数据加密、数据验证**

身份认证：VPN网关对接入VPN的用户进行身份认证，保证接入的用户都是合法用户。

数据加密：将明文通过加密技术成密文，哪怕信息被获取了，也无法识别。

数据验证：通过数据验证技术验证报文的完整性和真伪进行检查，防止数据被篡改。

**VPN的3种工作模式**

1. Web浏览器模式

远程计算机使用Web浏览器通过SSL-VPN服务来访问企业内部的资源。SSL-VPN 服务器相当于一个数据中转服务器(代理服务器)，所有Web浏览器对服务器的访问都经过SSL-VPN服务器的认证后发给服务器，服务器发往Web浏览器的数据经过SSL-VPN服务器加密后送到Web浏览器。

1. VPN客户端模式

此模式与前一种模式差别是需要在远程计算机上安装--一个VPN客户端程序，远程计算机访问企业内部的应用服务器时，需要经过VPN客户端和SSL-VPN服务器之间的保密传输才能到达。

1. LAN到LAN模式

此模式下客户端不需要做任何安装和配置，仅在SSL- VPN 服务器上安装和配置。当一个网内的计算机要访问远程网络内的应用服务器时，需要经过两个网的SSL- VPN服务器之间的保密传输后才能到达。