志存高远 责任为先

VPN技术

地址：赣州市红旗大道86号 信息工程学院
网址：www.jxust.edu.cn
邮编：341000

目录/Contents

1. VPN概述
2. VPN隧道协议
3. VPN的应用和发展趋势

01
Part

VPN概述

10.1 VPN概述

- **虚拟专用网（Virtual Private Network，VPN）**
  - **利用密码技术和访问控制技术在公共网络中建立的专用通信网络**
  - **任意两个节点之间的连接并没有传统专用网所需的端到端的物理链路，而是利用某种公众网的资源动态组成**
  - **对用户端透明，用户好像使用一条专用线路进行通信**

VPN的技术要求

- **技术要求**
  - **（1）安全保障**
  - **（2）服务质量（QoS）保证**
  - **（3）可扩展性和灵活性**
  - **（4）可管理性**
- **VPN优势：**
  - **（1）可以降低成本**
  - **（2）可扩展性强**
  - **（3）提供安全保证**

VPN类型

- **远程访问虚拟网（Access VPN）**
  - **主要用来处理可移动用户、远程交换和小部门远程访问企业本部的连通性**
  - **当出差人员需要和企业或相关部门联系时，便可以利用本地相应的软件接入Internet，通过Internet和企业网络中相关的VPN网关建立一条安全通道**
  - **用户使用这条可以提供不同级别的加密和完整性保护的通道，可以传输不同级别保护的信息**

VPN类型

- **企业内部虚拟网（Intranet VPN）**
  - **企业内部虚拟网主要是利用Internet来连接企业的远程部门**
  - **只需企业的远程部门通过公用网络和企业本部互联，并且由远程部门网络的VPN网关和企业本部网络的VPN网关负责建立安全通道**
  - **在保证数据的机密性、完整性的同时又能大大的降低了整个企业网互联的运行和管理费用**

VPN类型

- **企业内部虚拟网（Intranet VPN）**
  - **企业内部虚拟网主要是利用Internet来连接企业的远程部门**
  - **只需企业的远程部门通过公用网络和企业本部互联，并且由远程部门网络的VPN网关和企业本部网络的VPN网关负责建立安全通道**
  - **在保证数据的机密性、完整性的同时又能大大的降低了整个企业网互联的运行和管理费用**

VPN的安全技术

- **隧道技术**
  - **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**
  - **隧道实质上是一种封装，它把一种协议A封装在另一种协议B中传输，实现协议A对公用网络的透明性**
  - **隧道根据相应的隧道协议来创建**
    - **隧道可以按照隧道发起点位置，划分为自愿隧道和强制隧道**
    - **自愿隧道由用户或客户端计算机通过发送VPN请求进行配置和创建，此时，用户端计算机作为隧道的一个端点。**
    - **强制隧道由支持VPN的拨号接入服务器配置和创建，此时，作为隧道端点是位于客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。**

加解密技术

- **加密技术是数据通信中一项较成熟的技术**
  - **利用加密技术保证传输数据的安会是VPN安全技术的核心**
  - **目前VPN中均采用对称加密体制和公钥加密体制相结合的方法**
    - **VPN目前常用的对称密码加密算法有：DES、3DES、RC4、RC5、IDEA、CAST等**
    - **当前常见的公钥体制有RSA、D-H和椭圆曲线等，相应的加密算法都已应用于VPN实际实现中**

密钥管理技术

- **密钥管理技术**
  - **在公用数据网上安全地传递密钥而不被窃取**
  - **现行密钥管理技术有SKIP ISAKMP/OAKLEY**
    - **SKIP基于一个D-H公钥密码体制数字证书。SKIP隐含地在通信双方实现了一个D-H交换，它简单易行，对公钥操作次数少，节省系统资源，但由于公钥长期暴露，因而存在着安全隐患**
    - **ISAKMP/OAKLEY协议（又称IKE），即通常所说的因特网密钥交换协议。它综合了OAKLEY和SKEME的优点，形成了一套具体的验证加密材料生成技术，以协商共享的安全策略**

身份认证技术

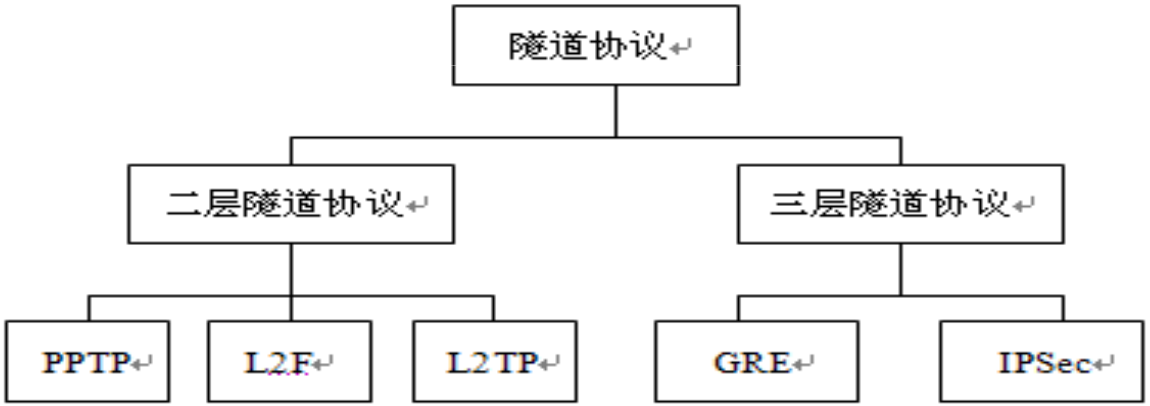
- **VPN中最常用的是用户名/口令或智能卡认证等方式**
  - **身份认证是通信双方建立VPN的第一步，保证用户名/口令，特别是用户口令的机密性至关重要**
  - **在VPN实现上，除了强制要求用户选择安全口令外，还特别采用对用户口令数据加密存放或使用一次性口令等技术**
  - **智能卡认证具有更强的安全性，它可以将用户的各种身份信息及公钥证书信息等集中在一张卡片上进行认证，做到智能卡的物理安全就可以在很大程度上保证认证机制的安全**

02
Part

VPN隧道协议

隧道协议

- **VPN具体实现是采用隧道技术**
- **隧道通过隧道协议实现**
  - **隧道协议规定了隧道的建立、维护和删除规则以及怎样将企业网的数据封装在隧道中进行传输**
    - **第二层（链路**
    - **第三层（网络**



第二层隧道协议PPTP

- **PPP（点对点协议）的基础上开发的一种新的增强型隧道协议**
  - **利用PPP协议的身份验证、加密和协议配置机制，PPTP为远程访问和VPN连接提供了一条安全路径**
  - **PPTP通过控制连接来创建、维护和终止一条隧道，并使用GRE（通用路由封装）对经过加密、压缩处理的PPP帧进行封装**
  - **通过PPTP，用户可以采用拨号方式接入到公共网络。**

PPTP控制连接

- **通过一系列PPTP消息来创建、维护与终止的逻辑连接**
  - **PPTP控制连接通信过程使用PPTP客户端上动态分配的TCP端口以及PPTP服务器上编号为1723的反向IANATCP端口**
  - **PPTP控制连接数据包包括一个IP报头，一个TCP报头和PPTP控制信息**

Data-link Header	IP	TCP	PPTP Control Message	Data-link Trailer

PPTP控制连接过程

- ① 在PPTP客户端上动态分配的TCP端口与编号为1723的TCP端口之间建立一条TCP连接。
- ② PPTP客户端发送一条用以建立PPTP控制连接的消息。
- ③ PPTP服务器通过一条PPTP消息进行响应。
- ④ PPTP客户端发送另一条消息，并且选择一个用以对从PPTP客户端向服务器发送数据的PPTP隧道进行标识的调用ID。
- ⑤ PPTP服务器通过进行应答，并且为自己选择一个用以对从服务器向客户端发送数据的PPTP隧道进行标识的调用ID。
- ⑥ PPTP客户端发送一条PPTP Set-Link-Info消息，以便指定PPP协商选项。

PPTP数据隧道

- **当通过PPTP连接发送数据时**
  - **PPP帧将使用GRE报头进行封装，GRE报头包含了用以对数据包所使用的特定PPTP隧道进行标识的信息**
  - **初始PPP有效载荷如IP数据报、IPX数据报或NetBEUI帧等经过加密后，添加PPP报头，封装形成PPP帧**
  - **PPP帧再进一步添加GRE报头，经过第二层封装形成GRE报文，在第三层封装时添加IP报头**
  - **数据链路层封装是IP数据报多层封装的最后一层，依据不同的外发物理网络再添加相应的数据链路层报头和报尾**

接收端的处理过程

① 处理并去除数据链路层报头和报尾

② 处理并去除IP报头

③ 处理并去除GRE和PPP报头

④ 如需要，对PPP有效载荷即传输数据进行解密或解压缩

⑤ 对传输数据直接接收或者转发处理

第三层隧道协议GRE

- **通用路由封装（GRE）是网络中通过隧道将通信从一个专用网络传输到另一个专用网络的协议，它属于网络层协议**
- **运行过程**
  - **当路由器接收了一个需要封装的上层协议数据报文，首先这个报文按照GRE协议的规则被封装在GRE协议报文中，而后再交给IP层**
  - **由IP层再封装成IP协议报文便于网络的传输，等到达对端的GRE协议处理网关时，按照相反的过程处理，就可以得到所需的上层协议的数据报文了**

GRE优点

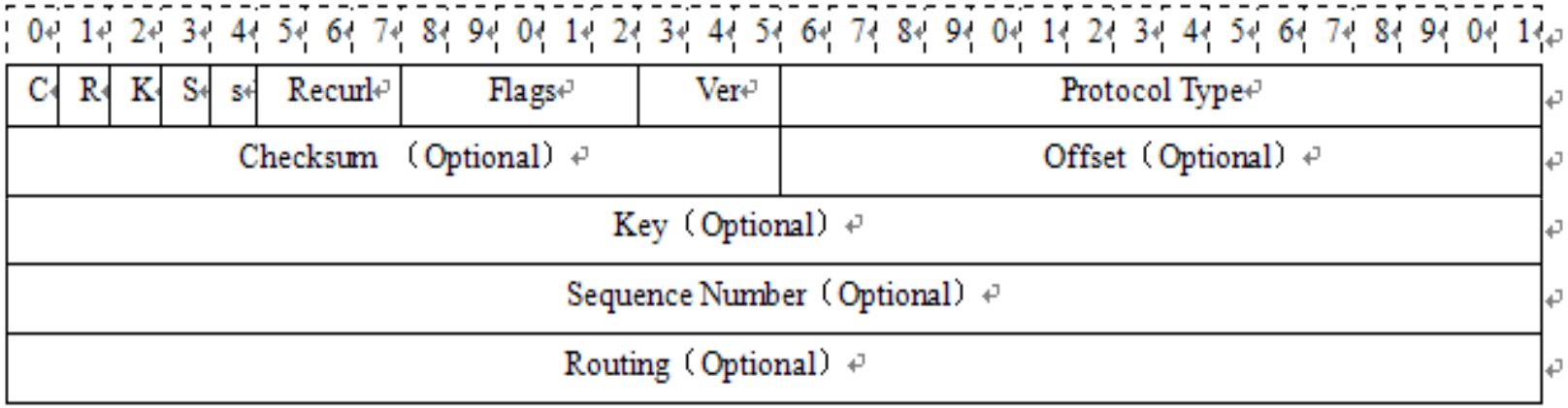
- ① 多协议的本地网可以通过单一协议的骨干网实现传输
- ② 可以将一些不能连续的子网连接起来，用于组建VPN
- ③ 扩大了网络的工作范围。包括那些路由网关有限的协议
  - 例如IPX包最多可转发16次，而在一个隧道连接中看上去只经过一个路由器

GRE报文格式

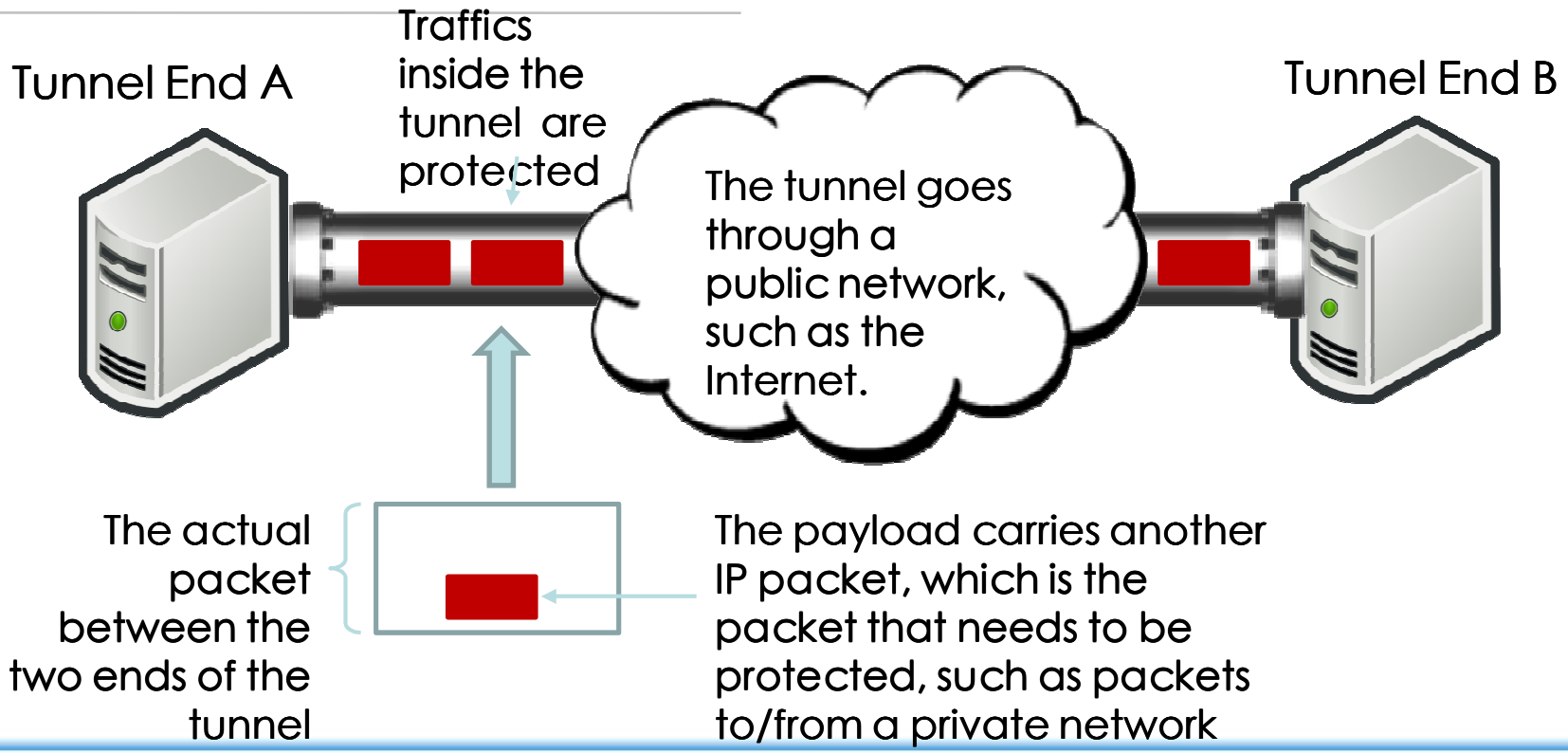
- **传输的头是IPv4的头**
- **有效载荷分组可以是IPv4的头，或者其它协议。GRE允许非IP协议在有效载荷中传输**
- **使用IPv4头的GRE分组被归入IP协议，类型号为47。当为GRE生成过滤时这是一条很重要的信息**
- **当GRE中封装的分组是IPv4时，GRE头协议类型域被设定为0x800。**

GRE报文头

- **RFC1701**



IP Tunneling

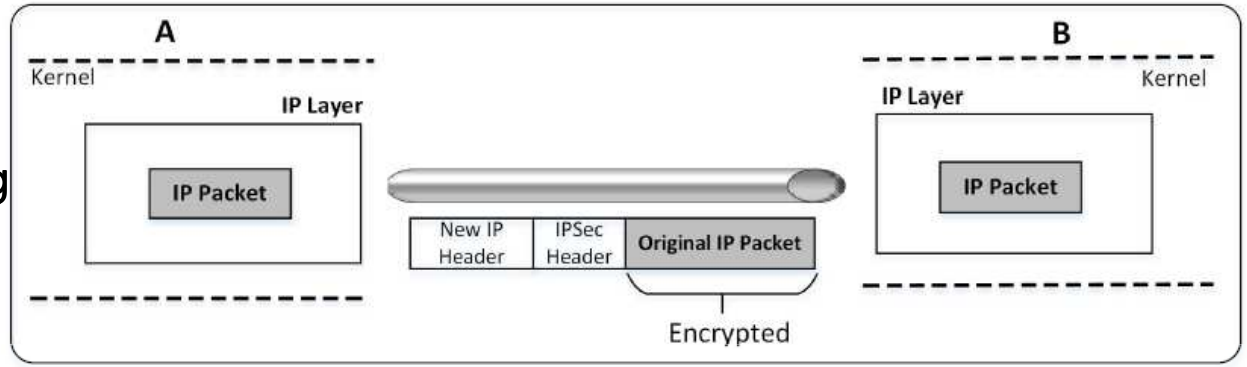


Two Types of IP Tunneling

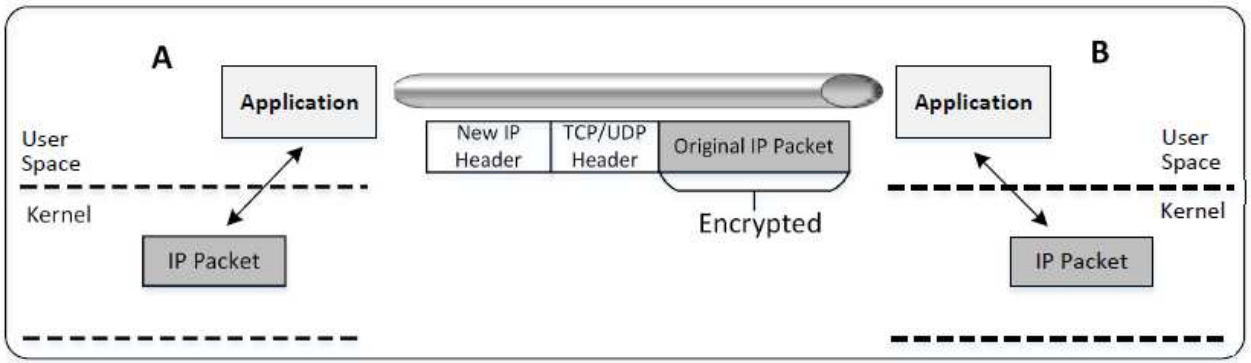
- **IPSec Tunneling:**
  - **Utilizes the Internet Protocol Security protocol**
  - **IPSec has a mode called Tunneling mode, where the original IP packet is encapsulated and placed into a new IP packet**
- **TLS/SSL Tunneling:**
  - **Tunneling done outside the kernel, at the application level**
  - **Idea is to put each VPN-bound IP packet inside a TCP or UDP packet**
  - **The other end of the tunnel will extract the IP packet from the TCP/UDP payload**
  - **To secure the packets, both ends will use TLS/SSL protocol on top of TCP/UDP**

Two Types of IP Tunneling

IPSec Tunneling



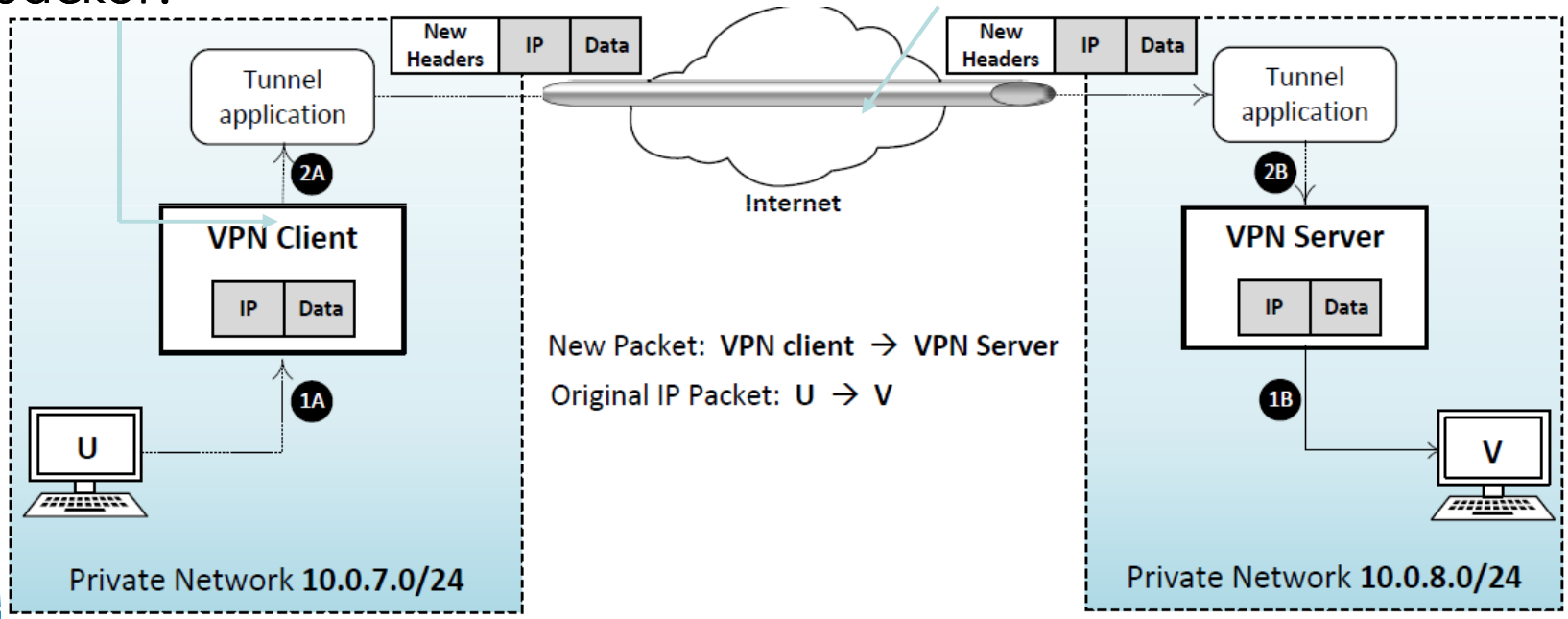
TLS/SSL Tunneling (we will focus on this type)



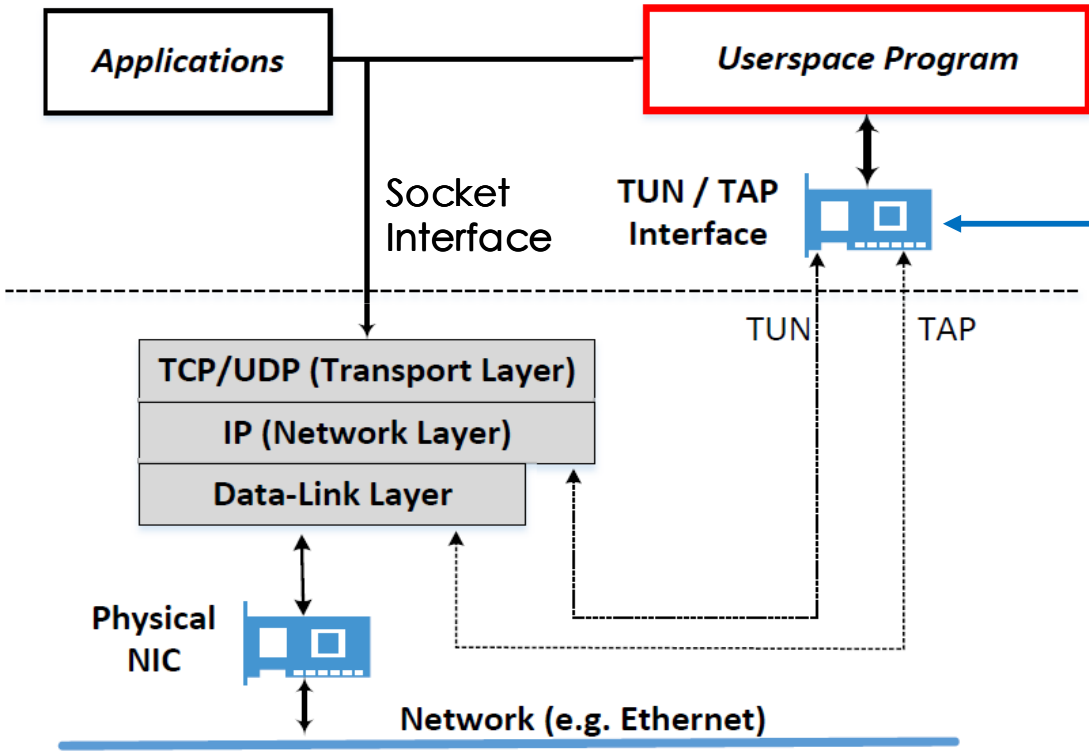
An Overview of How TLS/SSL VPN Works

Question: How can the Tunnel application get an IP packet?

This is just a normal TCP or UDP based SSL connection



TUN/TAP Interface

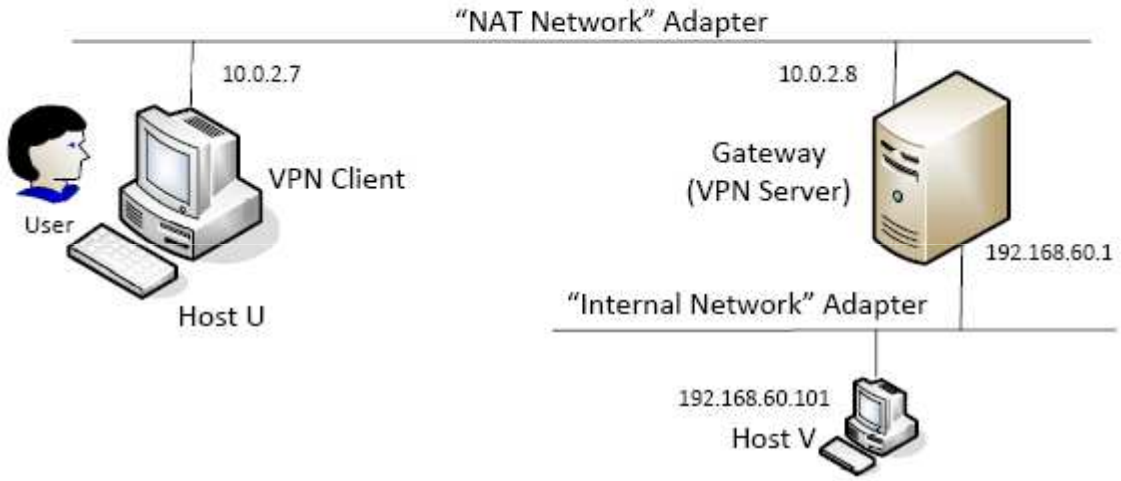


- **Question: How can the Tunnel application get an IP packet?**
  - **Typically, applications interact with kernel using socket**
  - **Using socket, kernel only gives the data part of a packet to applications**
  - **Applications need to use a different way to interact with kernel**

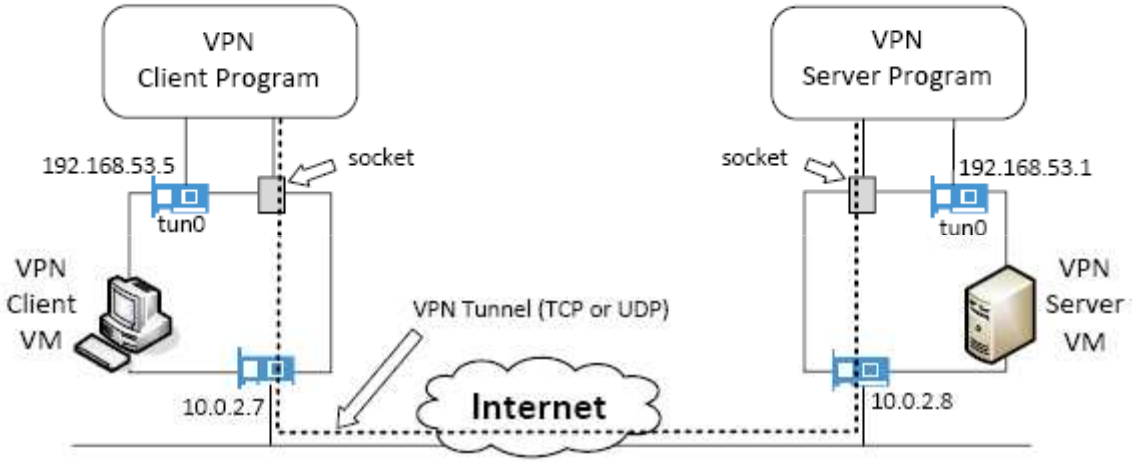
TUN/TAP Interface

- **Most operating systems have two types of network interfaces:**
  - **Physical: Corresponds to the physical Network Interface Card (NIC)**
  - **Virtual: It is a virtualized representation of computer network interfaces that may or may not correspond directly to the NIC card. Example: *loopback* device**
- **TUN Virtual Interface**
  - **Work at OSI layer 3 or IP level**
  - **Sending any packet to TUN will result in the packet being delivered to user space program**
- **TAP Virtual Interfaces**
  - **Work at OSI layer 2 or Ethernet level**
  - **Used for providing virtual network adapters for multiple guest machines connecting to a physical device of the host machine**

实验拓扑


"NAT Network" Adapter
10.0.2.7
10.0.2.8
VPN Client
User
Host U
Gateway
(VPN Server)
192.168.60.1
"Internal Network" Adapter
192.168.60.101
Host V

原理


VPN
Client Program
VPN
Server Program
192.168.53.5
socket
socket
192.168.53.1
tun0
tun0
VPN
Client
VM
VPN Tunnel (TCP or UDP)
VPN
Server
VM
Internet
10.0.2.7
10.0.2.8

配置

- **Server**
  - **sudo ./vpnserver**

```
int createTunDevice() {
   int tunfd;
   struct ifreq ifr;
   memset(&ifr, 0, sizeof(ifr));

   ifr.ifr_flags = IFF_TUN | IFF_NO_PI;

   tunfd = open("/dev/net/tun", O_RDWR);
   ioctl(tunfd, TUNSETIFF, &ifr);
   system("sudo ifconfig tun0 192.168.53.1 up");
   system("sudo route add -net 192.168.53.0/24 tun0");
   return tunfd;
}
```

配置

- **Client**
  - **sudo ./vpnclient**

```
int createTunDevice() {
    int tunfd;
    struct ifreq ifr;
    memset(&ifr, 0, sizeof(ifr));

    ifr.ifr_flags = IFF_TUN | IFF_NO_PI;

    tunfd = open("/dev/net/tun", O_RDWR);
    ioctl(tunfd, TUNSETIFF, &ifr);
    system("sudo ifconfig tun0 192.168.53.5 up");
    system("sudo route add -net 0.0.0.0 tun0");
    return tunfd;
}
```

测试

```
[12/26/18]seed@VM:
Trying 192.168.60.
Connected to 192.1
Escape character i
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Wed De
Welcome to Ubuntu

 * Documentation:
 * Management:
 * Support:

3 packages can be
0 updates are secu
```

```
[12/26/18]seed@VM:~$ ifconfig
ens33     Link encap:Ethernet  HWaddr 00:0c:29:9f:27:9b
          inet addr:10.0.2.8  Bcast:10.255.255.255  Mask:255.0.0
          inet6 addr: fe80::8bf3:e2b8:31ee:1636/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2945 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1512 errors:0 dropped:0 overruns:0 carrier:
          collisions:0 txqueuelen:1000
          RX bytes:352883 (352.8 KB)  TX bytes:190016 (190.0 KB)
          Interrupt:19 Base address:0x2000

ens38     Link encap:Ethernet  HWaddr 00:0c:29:9f:27:a5
          inet addr:192.168.60.1  Bcast:192.168.60.255  Mask:255
55.255.0
          inet6 addr: fe80::d3a5:7c7:c6d0:a9ec/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:377 errors:0 dropped:0 overruns:0 frame:0
          TX packets:82 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:35118 (35.1 KB)  TX bytes:13923 (13.9 KB)
```

服务器端抓包

10.0.2.8	10.0.2.7	UDP	157	55555 → 40484 Len=115
10.0.2.7	10.0.2.8	UDP	94	40484 → 55555 Len=52
10.0.2.8	10.0.2.7	UDP	96	55555 → 40484 Len=54
10.0.2.7	10.0.2.8	UDP	94	40484 → 55555 Len=52
10.0.2.8	192.168.60.1	192.168.53.5	TCP	52 23 → 36700 [ACK] Seq=2
10.0.2.7	192.168.60.1	192.168.53.5	TELNET	64 Telnet Data ...
10.0.2.8	192.168.53.5	192.168.60.1	TCP	52 36700 → 23 [ACK] Seq=3
10.0.2.7	192.168.60.1	192.168.53.5	TELNET	91 Telnet Data ...
10.0.2.8	192.168.53.5	192.168.60.1	TCP	52 36700 → 23 [ACK] Seq=3
10.0.2.7	192.168.53.5	192.168.60.1	TELNET	118 Telnet Data ...
10.0.2.8	192.168.60.1	192.168.53.5	TCP	52 23 → 36700 [ACK] Seq=2
10.0.2.7	192.168.60.1	192.168.53.5	TELNET	55 Telnet Data ...
	192.168.53.5	192.168.60.1	TELNET	55 Telnet Data ...
	192.168.60.1	192.168.53.5	TELNET	55 Telnet Data ...
	192.168.53.5	192.168.60.1	TELNET	55 Telnet Data ...
	192.168.60.1	192.168.53.5	TELNET	72 Telnet Data ...

VPN技术发展趋势

- （1）基于IPSec的VPN产品将成为市场的主流
- （2）VPN所用密码算法的抗攻击性不断增强
- （3）VPN向集成化的方向发展
- （4）新的VPN实现技术将会不断推出

志存高远 责任为先

感谢聆听

网址：www.jxust. edu.cn
邮编：341000