网络安全 – VPN技术

曹越

国家网络安全学院

武汉大学

yue.cao@whu.edu.cn

上周回顾

允许外部网络访问WWW服务器，但是禁止其他基于TCP协议的服务，如何过滤?

某IP地址不断给服务器发送TCP SYN，但是不发送ACK，可能出现了DOS

发送给某服务器的ICMP ECHO报文平均每日100次，但是某日超过10000次，可能出现了Ping攻击

网络中依次出现访问某主机端口TCP SYN报文，可能是针对该主机扫描

防火墙检测到来自于外部网络的IP数据包，但是数据包源地址属于内部网络，可能是IP地址伪造

VPN概述

VPN的分类

VPN使用的协议与实现

VPN概述

VPN的分类

VPN使用的协议与实现

VPN概述 – 概念 1

VPN即虚拟专用网

它是依靠ISP(Internet服务提供商)和其他NSP(网络服务提供商)，在公用网络中建立专用的数据通信网络的技术

VPN概述 – 概念 2

在该网中的主机将不会觉察到公共网络的存在，仿佛所有的主机都处于一个网络之中

VPN使用户节省了租用专线的费用，除了购买VPN设备外，企业所付出的仅仅是向企业所在地的ISP支付一定的上网费用，也节省了长途电话费

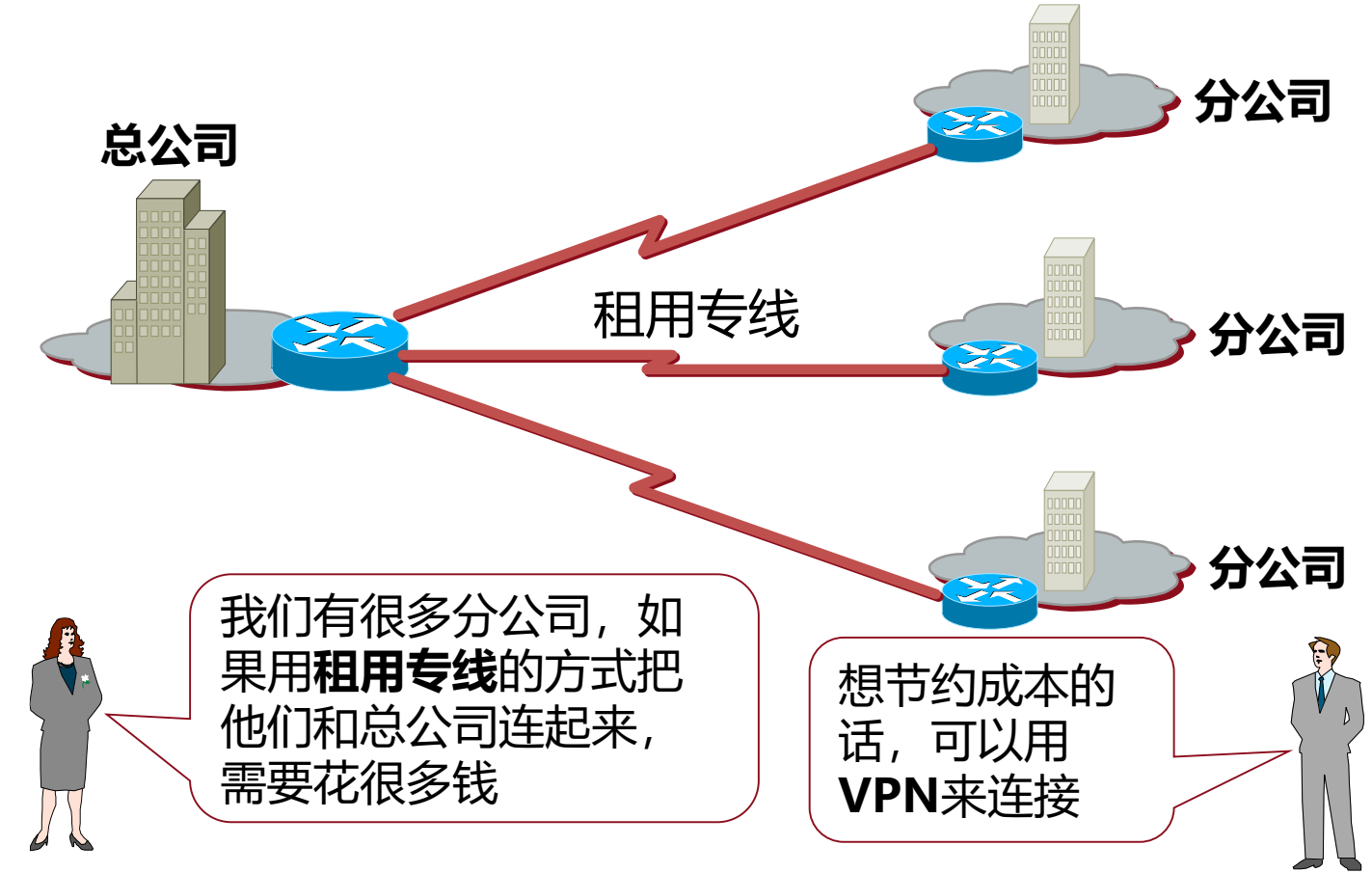
企业网在公网的延伸

VPN概述 – 概念 3

而使用VPN以后，你在网络上的访问数据被加密和隐藏，避免了个人敏感信息的泄露

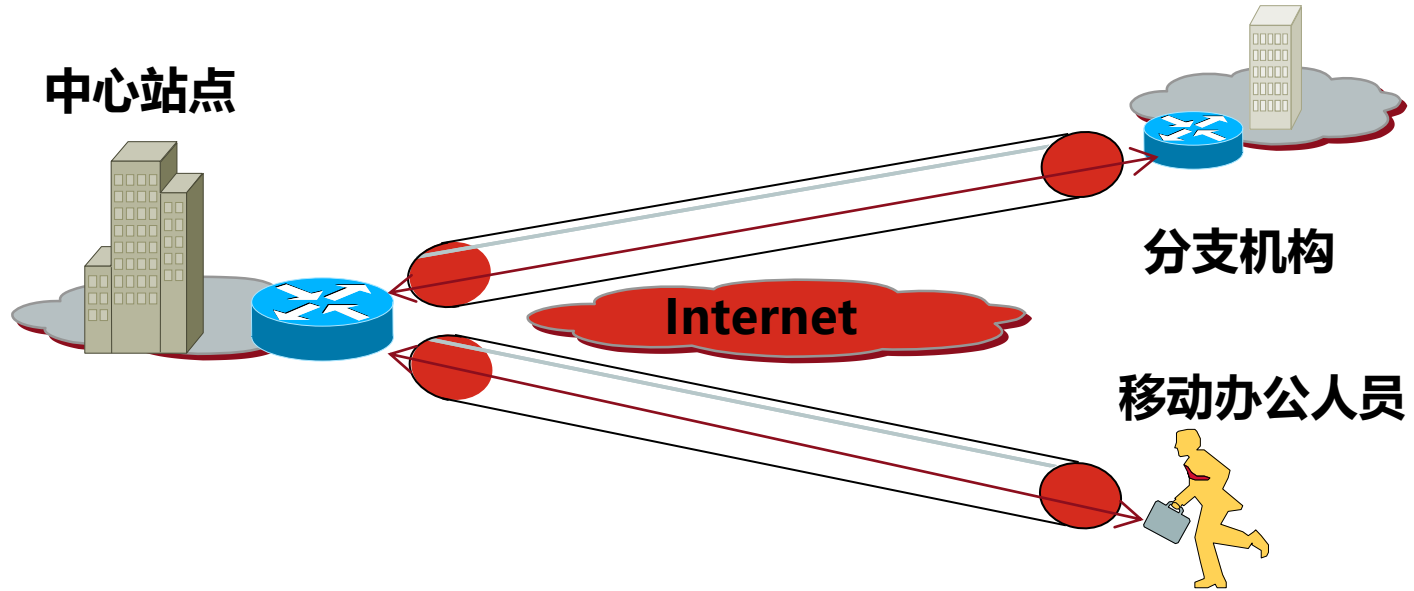
举个例子来说，网购的时候一旦泄露银行卡信息，可能会带来钱财的损失，通过VPN再进行网购，会增加安全性，当然必须是可靠的VPN服务商

VPN概述 – 示例 1

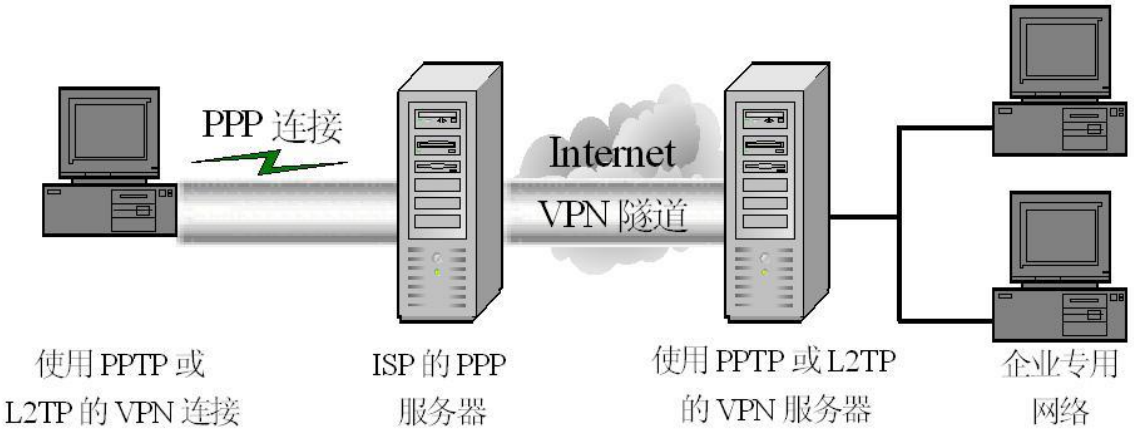

总公司
分公司
租用专线
分公司
分公司
我们有很多分公司，如果用**租用专线**的方式把他们和总公司连起来，需要花很多钱
想节约成本的话，可以用**VPN**来连接

VPN概述 – 示例 2

VPN 利用开放的公众Internet网络建立专用数据传输通道，将远程的分支机构、移动办公人员等连接起来。



VPN的组成



包括：客户机、传输介质、服务器

VPN概述

VPN的分类

VPN使用的协议与实现

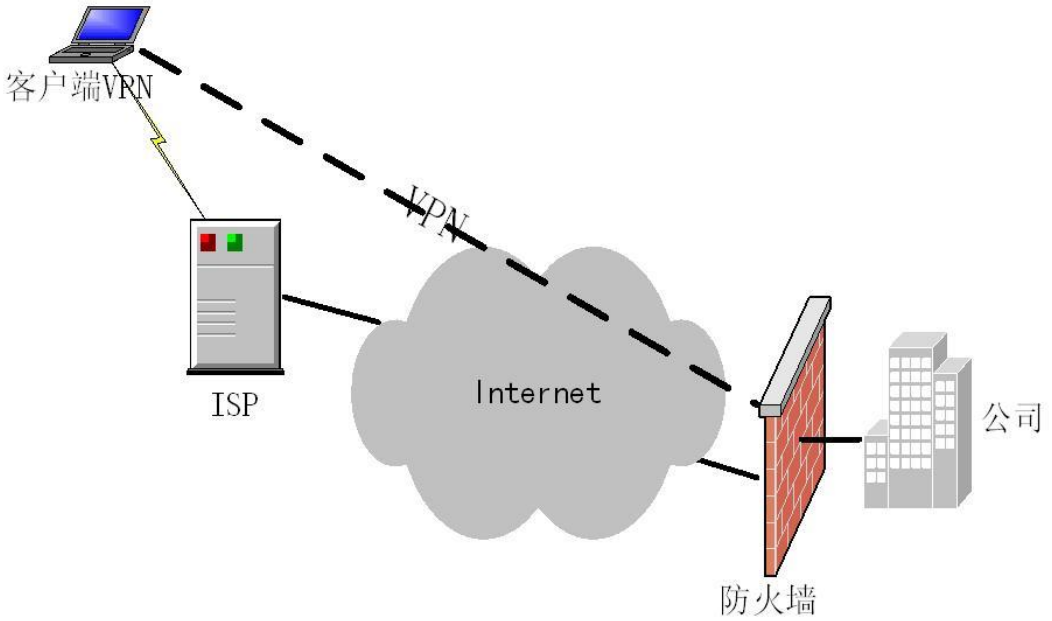
VPN的分类

远程访问虚拟网（Access VPN）

企业内部虚拟网（Intranet VPN）

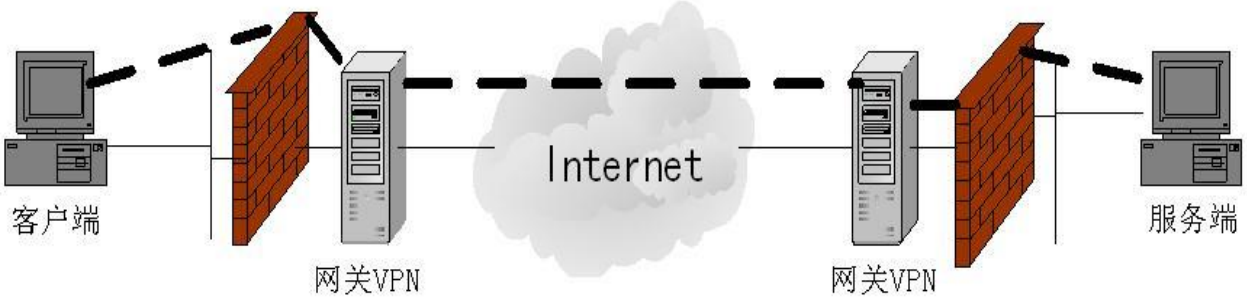
企业扩展虚拟网（Extranet VPN）

VPN的分类 - 远程访问虚拟网



利用当地VPN服务器实现远程流动办公

VPN的分类 - 企业内部虚拟网



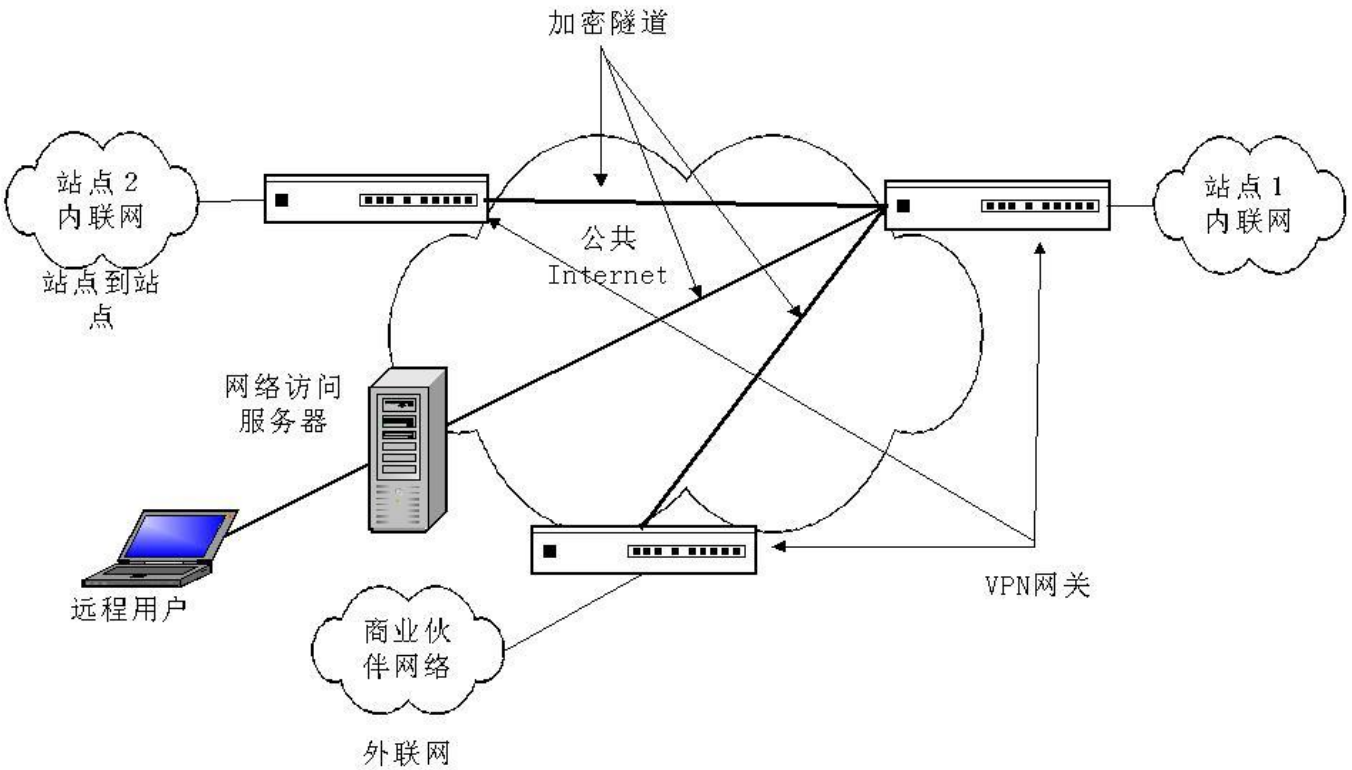
企业总部与分支机构连接，采用租用专线费用高

VPN的分类 - 企业扩展虚拟网

利用VPN技术可以组建安全的Extranet，既可以向客户、合作伙伴提供有效的信息服务，又可以保证自身的内部网络的安全

此种类型与Intranet VPN没有本质的区别，但它涉及的是不同公司的网络间的通信，所以它要更多的考虑设备的互联、地址的协调、安全策略的协商等问题

VPN的分类 - 企业扩展虚拟网 - 示例



VPN概述

VPN的分类

VPN使用的协议与实现

VPN使用的协议与实现

VPN使用三个方面的技术保证了通信的安全性

- **身份验证**
- **隧道协议**
- **数据加密**

VPN使用的协议与实现 - 验证流程

1. 客户机向VPN服务器发出请求，VPN服务器响应请求并向客户机发出身份质询
2. 客户机将加密的响应信息发送到VPN服务器
3. 如果账户有效，VPN服务器将检查该用户是否具有远程访问权限
4. 如果该用户拥有远程访问的权限，VPN服务器接受此连接
5. 在身份验证过程中产生的客户机和服务器公有密钥将用来对数据进行加密

VPN使用的协议与实现 - 隧道技术

VPN的核心是被称为“隧道”的技术

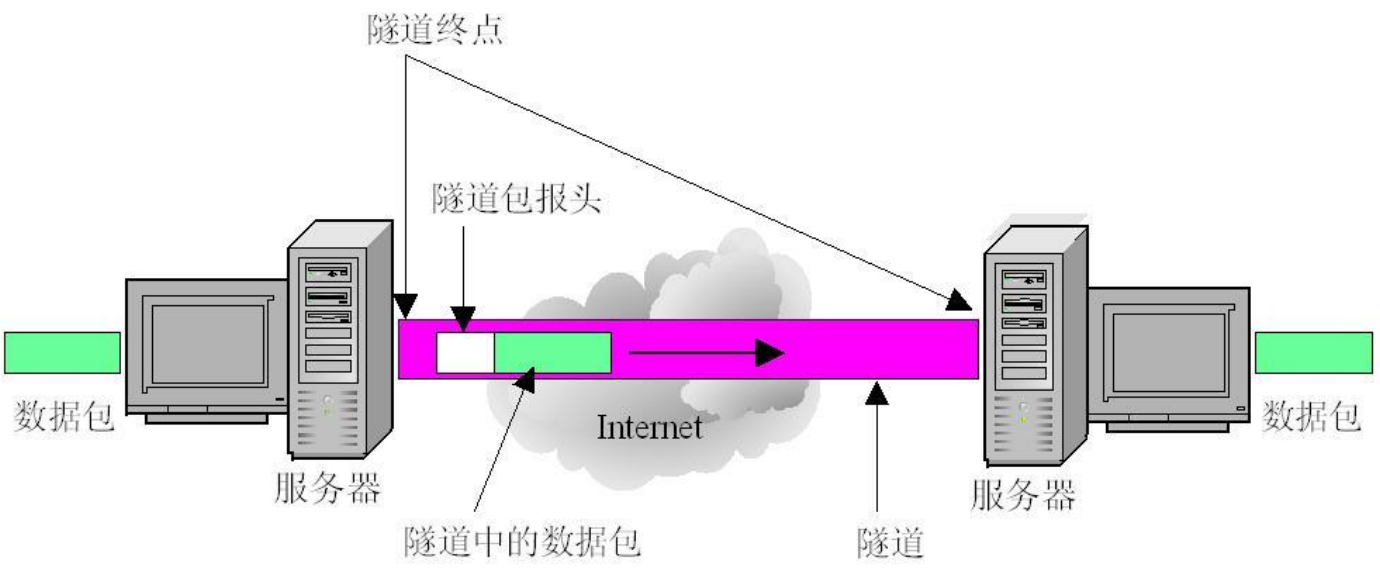
隧道技术是一种通过使用互联网络的基础设施在网络之间传递数据的方式

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

隧道协议将这些其它协议的数据帧或包重新封装在新的包头中发送

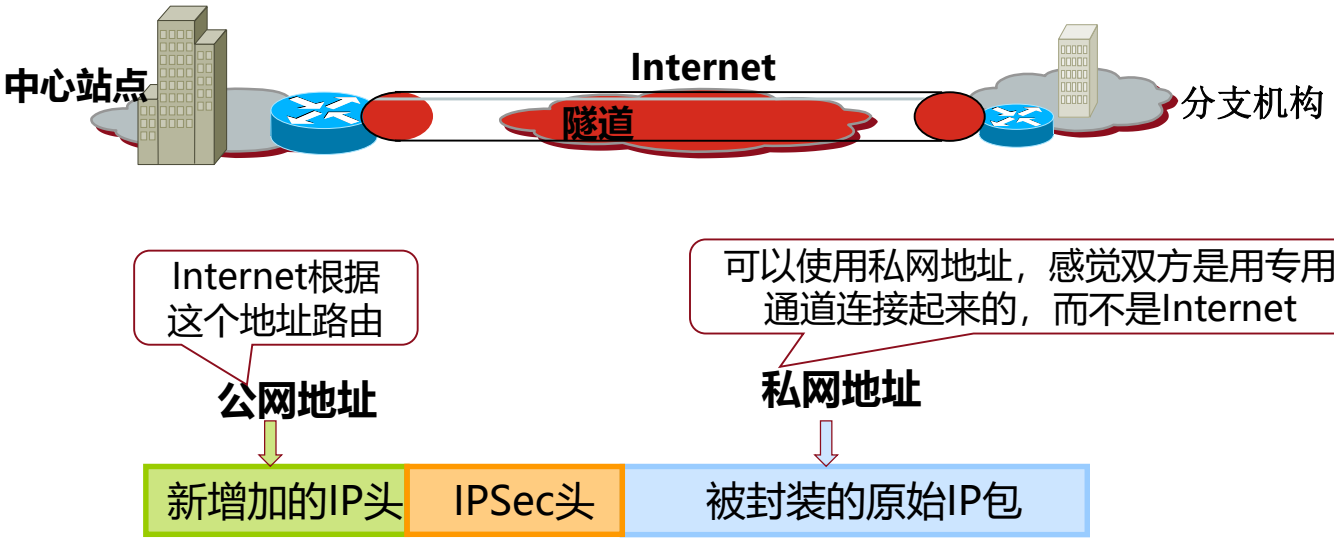
被封装的数据包在公共互联网络上传递时所经过的逻辑路径称为隧道

VPN使用的协议与实现 - 隧道技术 - 1



VPN使用的协议与实现 - 隧道技术 - 2

隧道保证了VPN中分组的封装方式，承载网络的封装方式及使用地址无关



VPN使用的协议与实现 - 隧道协议

点对点隧道协议

- **PPTP，Point-to Point Tunneling Protocol**

第2层隧道协议

- **L2TP, Layer 2 Tunneling Protocol**

IP安全协议

- **IPSec**

VPN使用的协议与实现 - PPTP 1

由3Com公司和Microsoft公司合作开发

支持Windows、Linux、Solaris

PPP

- Point to Point Protocol
- 点对点通信协议
- 链路层协议
- IPX、TCP/IP、NetBEUI和AppleTalk等其他协议组合

VPN使用的协议与实现 - PPTP 2

PPP工作流程

- **在远程计算机和服务器之间建立帧传输规则，通过该规则的建立，才允许进行连续的通信(通常称为“帧传输”)**
- **远程访问服务器通过使用PPP协议中的身份验证协议，来验证远程用户的身份**
- **身份验证完毕后，如果用户启用了回拨，则远程访问服务器将挂断并呼叫远程访问客户机，实现服务器回拨**
- **“网络控制协议”(NCP)启用，并配置远程客户机，使得所用的LAN协议与服务器端进行PPP通信连接**

VPN使用的协议与实现 - PPTP 3

PPTP协议是PPP协议的扩展

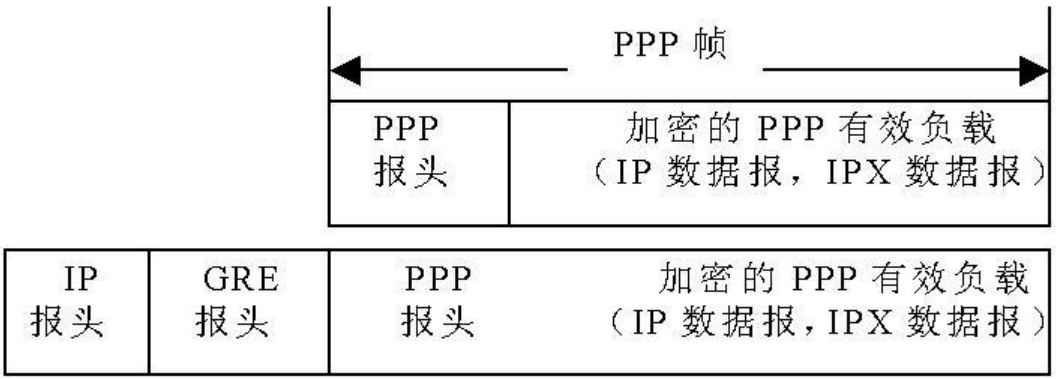
增强了PPP协议的认证、压缩和加密功能

增加了一个新的安全等级，并且可以通过因特网进行多协议通信

VPN使用的协议与实现 - PPTP 4

基于PPTP的VPN

- 封装服务
- 使用一般路由封装(GRE)头文件和IP报头数据包装PPP帧(包含一个IP数据包或一个IPX数据包)



VPN使用的协议与实现 - PPTP 5

基于PPTP的VPN

- **加密服务**
  - **通过使用从PPP协议的身份验证过程中生成的密钥**
  - **PPP帧加密**
  - **PPTP只是对先前加密的PPP帧进行封装**

VPN使用的协议与实现 - PPTP 6

PPTP协议数据传输过程

- **首先远程VPN客户端通过诸如Windows系统的拨号网络中的远程访问服务与本地ISP进行PPP连接**
- **当PPP连接激活后，通过PPTP协议在客户端使用VPN第二次拨号**
- **连接VPN服务器端的WAN适配器的IP地址或者域名，开通**

VPN使用的协议与实现 - L2TP 1

1999年8月，RFC2661

L2TP也是PPP协议的扩展

由IETF (Internet Engineering Task Force，因特网工程任务组)管理，由Cisco、Microsoft、Ascend、3Com和其他网络设备供应商在修改了十几个版本后联合开发并认可

VPN使用的协议与实现 - L2TP 2

支持多种协议，用户可以保留原有的IPX或公司原有的IP地址

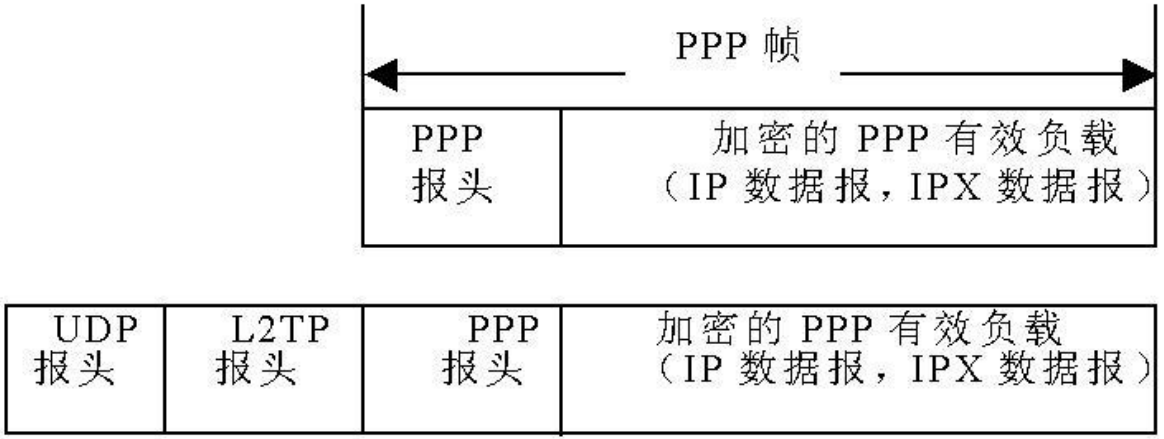
允许在物理上连接到不同NAS的PPP链路，在逻辑上的终点为同一个物理设备

允许第2层连接的终点和PPP会话的终点分别设在不同的设备上

L2TP能把PPP协议的终点从传统的LAC（L2TP Access Concentrator，第2层隧道协议接入集线器）延伸到LNS (L2TP Network Server，第2层隧道协议网络服务器)

VPN使用的协议与实现 - L2TP 3

L2TP封装



VPN使用的协议与实现 - L2TP 4

L2TP 头文件和 UDP 头数据包封装

VPN使用的协议与实现 - PPTP与L2TP比较

网络基础

- PPTP：IP网络
- L2TP：面向数据包的点对点的连接
  - 例如：IP（UDP），虚拟电路、ATM交换电路

隧道

- PPTP：单一隧道，不支持隧道验证
- L2TP：支持多隧道和隧道验证，不同服务质量创建不同隧道

压缩头的开销

- PPTP/L2TP：6/4 byte

四种VPN的比较

	PPTP	L2TP	IPSec
隧道协议类型	第二层	第二层	第三层
是否支持数据加密	支持	不支持	支持
对设备的要求	只要求边缘设备支持	只要求边缘设备支持L2TP	只要求边缘设备支持IPSec

VPN使用的协议与实现 - IPSec协议 1

IPSec是IETF于1998年11月公布的第三层安全协议

保护IP数据包或上层数据

- 不需要再应用层加密，减少密钥协商开销

可以定义哪些数据流需要保护，怎样保护及应该将这些受保护的数据流转发给谁

提供具有较强的互操作能力、高质量和基于密码的安全

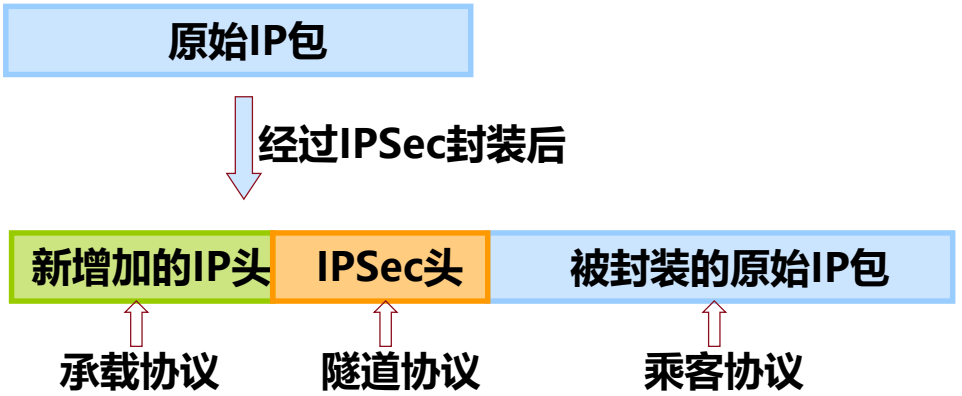
VPN使用的协议与实现 - IPSec协议 2

IPv4与IPv6

- **IPSec有两种版本，一种是基于IPv4协议的，另一种是基于IPv6协议的**
- **IPSec对于IPv4是可选的，对于IPv6是强制性的**

VPN使用的协议与实现 - IPSec协议 3

共涉及三种协议，包括：乘客协议、隧道协议和承载协议。



VPN使用的协议与实现 - IPSec协议 4

IPSec在IP层上对数据包进行高强度的安全处理，提供数据源地验证、无连接数据完整性、数据机密性、抗重播和有限业务流机密性等安全服务

各种应用程序可以享用IP层提供的安全服务和密钥管理，而不必设计和实现自己的安全机制

VPN使用的协议与实现 - IPSec协议 5

Transmission Mode

- 传输方式是用来保护上层协议，仅对数据进行加密，原IP包的地址部分不处理
- IPSec包头加在IP包头和上层协议包头之间

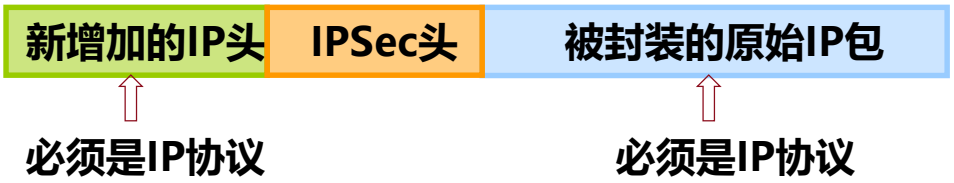
Tunnel Mode

- 保护整个IP数据包
- 整个IP包都封装在一个新的IP包中，并在新的IP包头和原来的IP包头之间插入IPSec头

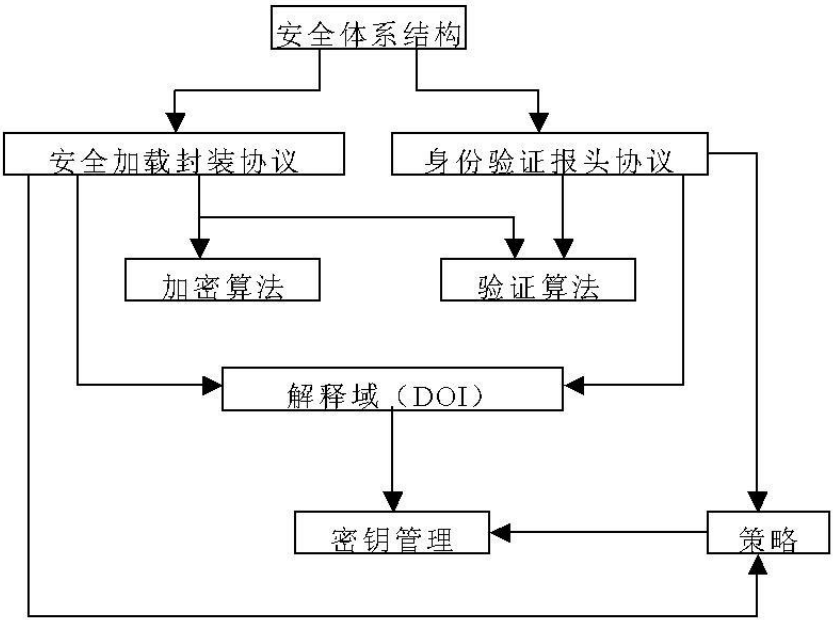
VPN使用的协议与实现 - IPSec协议 6

IPSec只能工作在IP层，要求乘客协议和承载协议都是IP协议

IPSec是一种开放标准的框架结构，特定的通信方之间在IP层通过加密和数据哈希(hash)等手段，来保证数据包在Internet 网上传输时的私密性(confidentiality) 、完整性(data integrity)和真实性(origin authentication)



VPN使用的协议与实现 - IPSec的安全体系



策略包含SA,SAD,SPD

VPN使用的协议与实现 - IPSec保护技术 1

验证(Authentication)

- 确保发送数据者的真实性

完整性(Integrity)

- 确保数据在传输过程中没有被篡改

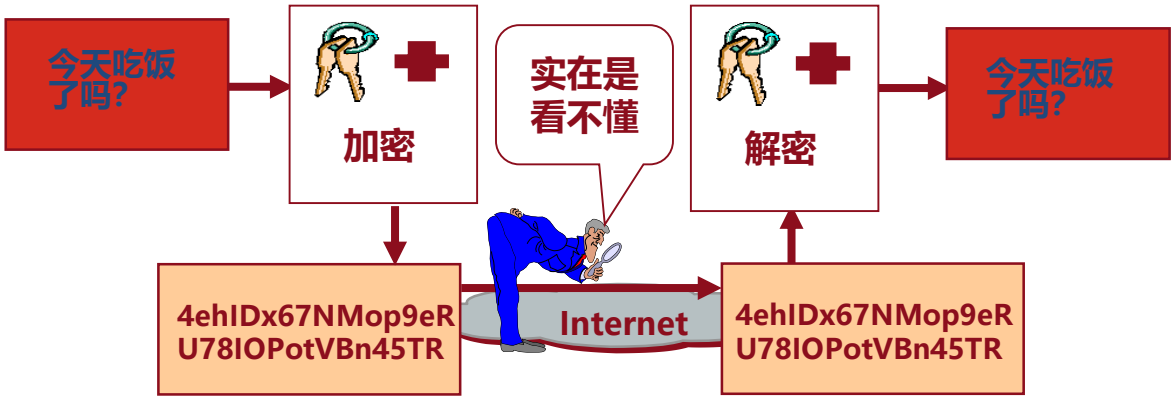
秘密性(Confidentiality)

- 确保数据不被非法读取

VPN使用的协议与实现 - IPSec保护技术 2

私密性：防止信息泄漏给未经授权的个人

通过加密把数据从明文变成无法读懂的密文，从而确保数据的私密性



VPN使用的协议与实现 - IPSec保护技术 3

Authentication Header (AH)

- AH协议包头可以保证信息源的可靠性和数据的完整性
- 工作原理
  - 发送方将IP包头、高层数据、密钥这三部分通过某种散列算法进行计算，得出AH包头中的验证数据，并将AH包头加入数据包中
  - 接收方将收到的IP包头、数据和密钥以相同的散列算法进行运算，并把得出的结果和收到的数据包中的AH包头进行比较，如果相同，则表明数据在传输过程中没有被修改，并且是从真正的信息源处发出的

VPN使用的协议与实现 - IPSec保护技术 4

Encapsulating Security Payload (ESP)

- **ESP可以提供数据的完整性和可靠性**
- **使用非对称密钥技术**
- **密钥交换采用IKE(Internet Key Exchange)**
  - **IKE不是在网络上直接传送密钥，而是通过一系列数据的交换，最终计算出双方共享的密钥，并且即使第三者截获了双方用于计算密钥的所有交换数据，也不足以计算出真正的密钥**

IKE阶段 - 1

协商建立IKE安全通道所使用的参数 ⇄ 协商建立IKE安全通道所使用的参数

交换对称密钥 ⇄ 交换对称密钥

双方身份认证 ⇄ 双方身份认证

建立IKE安全通道 ⇄ 建立IKE安全通道

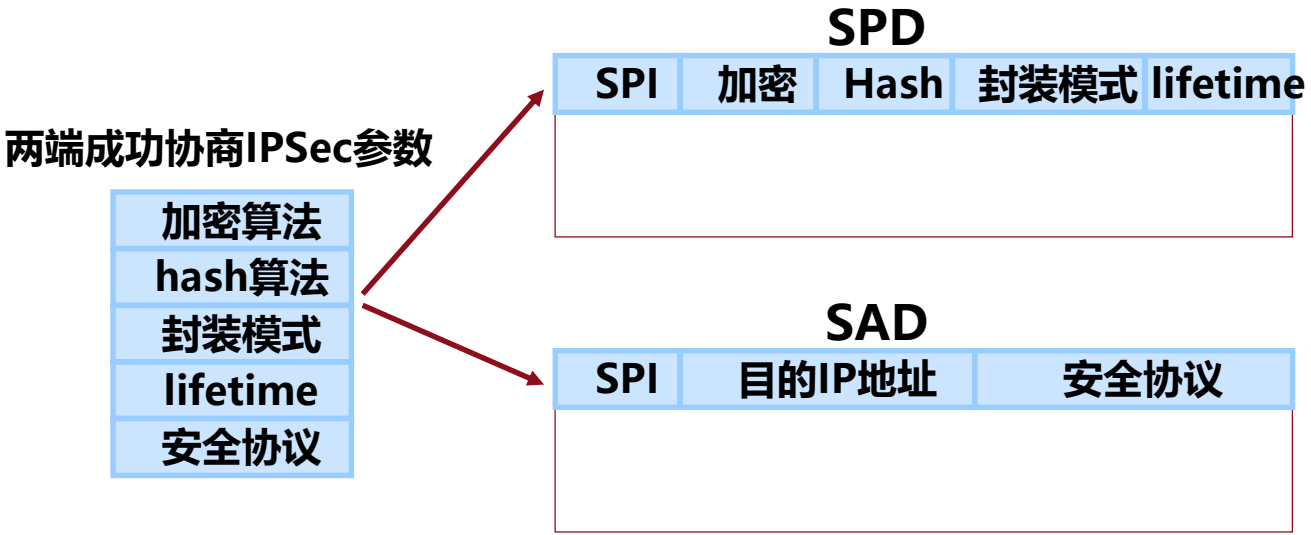
IKE阶段 - 2


Host A
Router A
Router B
Host B
IKE 阶段2
10.0.1.3
10.0.2.3
协商IPSec安全参数
协商IPSec安全参数
建立IPSec SA
建立IPSec SA

IPSec SA - 1

IPSec SA (安全关联，Security Association)：

- 由 SPD (Security Policy Database) 和 SAD (SA database)组成



IPSec SA - 2

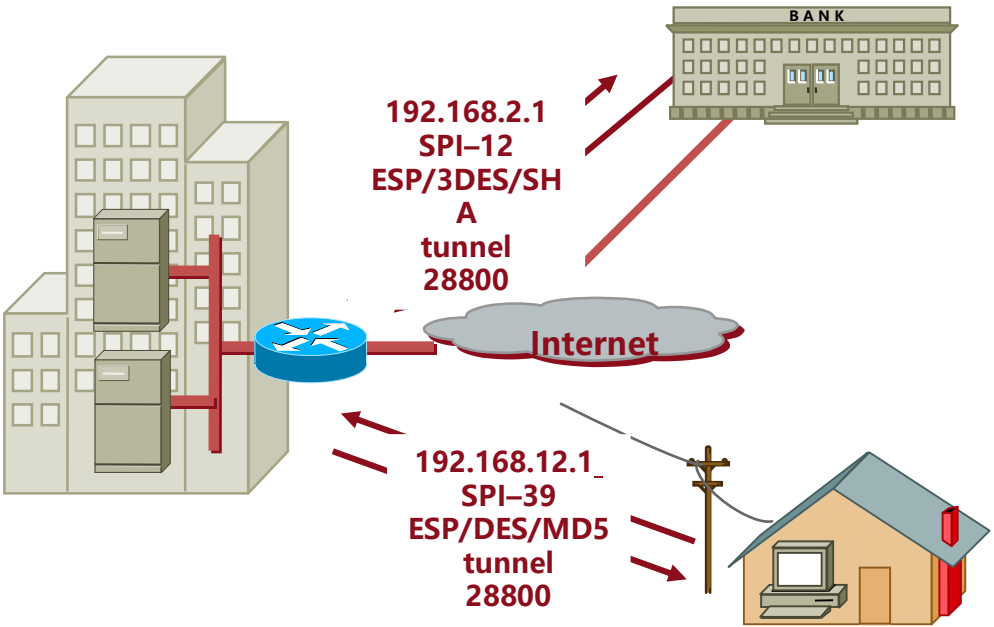
IPSec SA (安全关联，Security Association)：

- SPI (Security Parameter Index)，由IKE自动分配
- 发送数据包时，会把SPI插入到IPSec头中
- 接收到数据包后，根据SPI值查找SAD和SPD，从而获知解密数据包所需的加解密算法、hash算法等。
- 一个SA只记录单向的参数，所以一个IPSec连接会有两个IPSec SA。

IPSec SA - 3

IPSec SA (安全关联，Security Association)：

- **使用SPI可以标识路由器与不同对象之间的连接**



IPSec SA - 4

IPSec SA (安全关联，Security Association)：

- 达到lifetime以后，原有的IPSec SA就会被删除
- 如果正在传输数据，系统会在原SA超时之前自动协商建立新的SA，从而保证数据的传输不会因此而中断

思考题

1. VPN的组成
2. 比较PPTP与L2TP
3. 简述IPSec中AH协议的功能
4. 简述IPSec中ESP协议的功能