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

IDS回顾

1. 入侵检测系统按引擎类别分，可以划分为几种类型？这些引擎实现的方法如何?
2. 什么是基于模式匹配的IDS?
3. 什么是基于异常检测的IDS?
4. IDS的应用有哪些？？

VPN概述

VPN的分类

VPN的功能

VPN使用的协议

VPN的应用

VPN概述

VPN的分类

VPN的功能

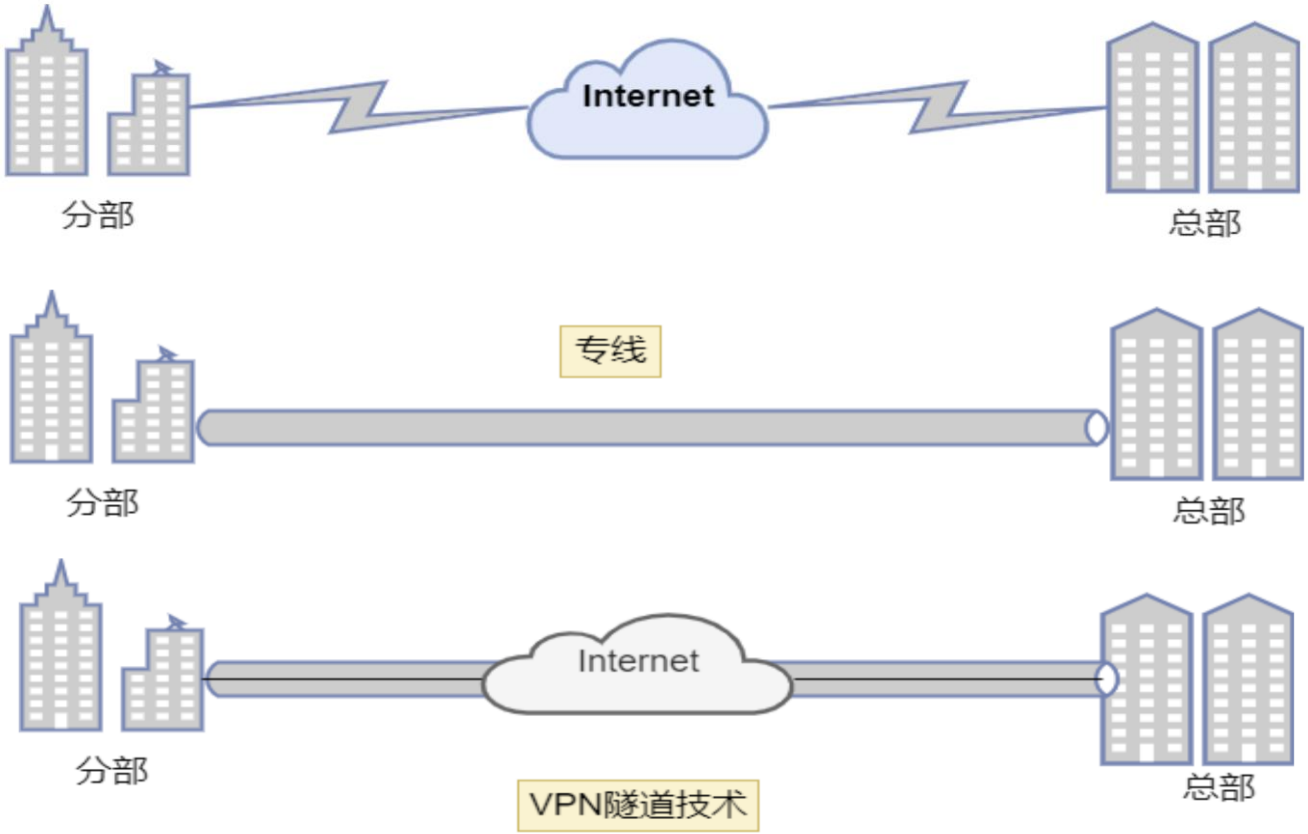
VPN使用的协议

VPN的应用

VPN概述 – 章节分解

1. VPN概念
2. VPN示例
3. 如何通过VPN安全上网
4. VPN的历史

VPN概念 1



VPN 概念 2

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概念 3

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概念 4

而使用VPN以后，用户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

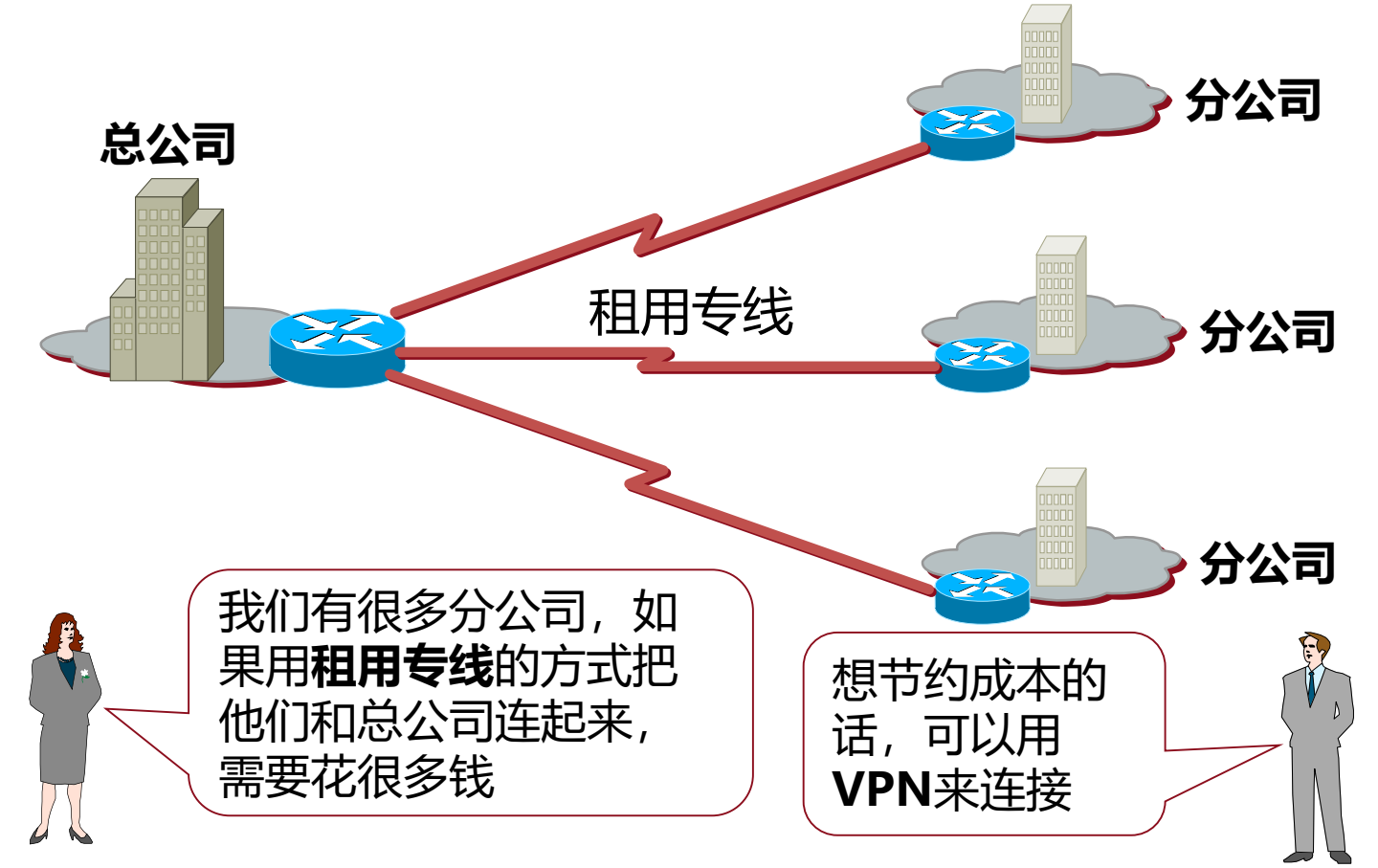
VPN概念 5

VPN是由经过相互授权的通信双方在公网上建立的安全通信隧道所组成。

通讯数据在安全隧道中进行加密传输。

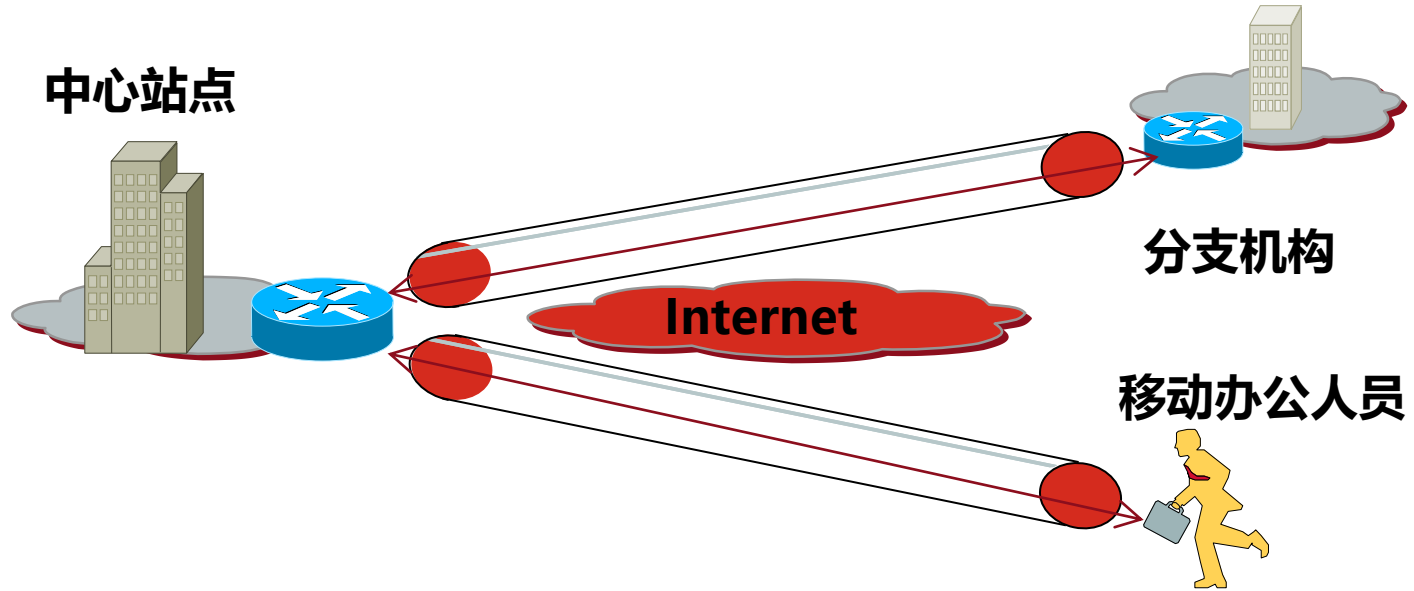
这种传输方式保证了数据的保密性，完整性及通信双方的相互授权。

VPN示例 1

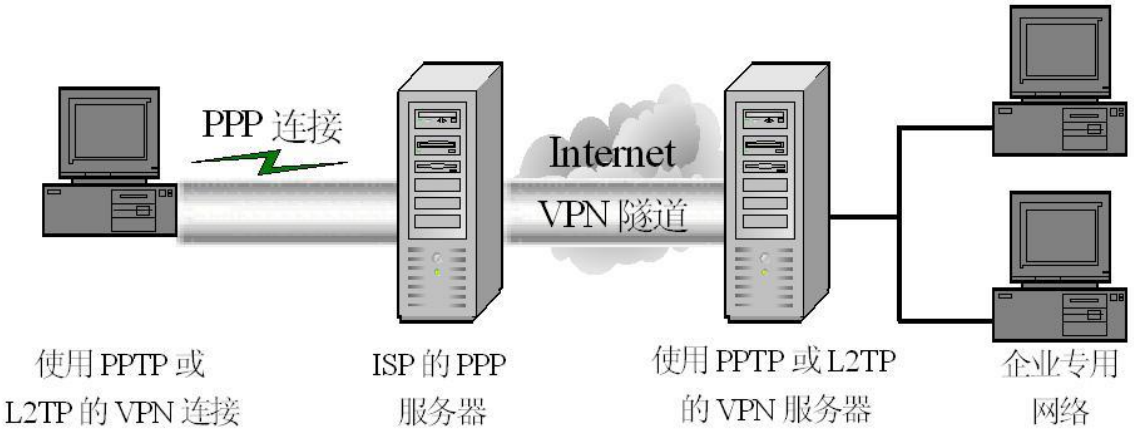

总公司
分公司
租用专线
分公司
分公司
我们有很多分公司，如果用**租用专线**的方式把他们和总公司连起来，需要花很多钱
想节约成本的话，可以用**VPN**来连接

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。



如何通过VPN安全上网 - 1



包括：客户机、传输介质、服务器

如何通过VPN安全上网 - 2

VPN可以加密上网行为，并且加密后只能借助密钥的帮助才能解码。密钥只有用户计算机和 VPN 知道，因此ISP 无法识别用户在哪里上网。

不同的 VPN 采用不同的加密流程，但通常都分三步发挥作用：

1. 只要一上线，就启用VPN。VPN充当用户与互联网之间的安全隧道。ISP 和其他第三方无法检测到该隧道
2. 现在用户设备位于 VPN 本地网络中，并且用户IP 地址可以更改为 VPN 服务器提供的 IP 地址
3. 现在用户可以随意在互联网上冲浪，因为VPN会保护用户所有个人数据

VPN的历史 - 1

自从人们开始使用互联网以来，就出现了保护和加密互联网浏览器数据的运动。早在上世纪 60 年代，美国国防部就参与了对互联网通信数据进行加密的项目。

他们的努力促成了 ARPANET（高级研究计划局网络）的建立，这个分组交换网络又进而推动了传输控制协议/互联网协议 (TCP/IP) 的发展。

- TCP/IP 具有四个层：链路层、互联网层、传输层和应用层。在互联网层，本地网络和设备可以连接到通用网络 — 暴露风险也在这里变得显而易见。

1993 年，哥伦比亚大学的一个团队在 AT&T 贝尔实验室成功创造了现代 VPN 的第一个迭代，它被称为 swIPe：软件 IP 加密协议。

第二年，Wei Xu开发IPSec网络，这是一种互联网安全协议，用于对在线共享的信息包进行身份认证和加密。1996 年，一位名叫 Gurdeep Singh-Pall 的 Microsoft 员工创造了对等隧道协议 (PPTP)。

VPN的历史 - 2

在 Singh-Pall 开发 PPTP 之后，互联网开始变得越来受欢迎，出现了对消费类复杂安全系统的需求。

那时，反病毒程序在防止恶意软件和间谍软件感染计算机系统方面已经非常有效。但是，人们和公司也开始要求能够隐藏其在互联网上的浏览历史记录的加密软件。

因此，最初的 VPN 于 2000 年代初问世，但通常仅由公司使用。然而，在大量的安全漏洞出现之后，尤其是在 2010 年代初期，消费者市场对 VPN 的需求开始有所上升。

VPN的历史 - 3

全球 VPN 用户数量在 2016 年至 2018 年之间增长了四倍以上。在泰国、印度尼西亚和中国等国家，互联网的使用受到限制和审查，多达五分之一的互联网用户会使用 VPN。在美国、英国和德国，VPN 用户的比例略低，大约为 5%，但一直在不断增加。

近年来，VPN普及的最大推动力之一是用户对受地理限制内容的访问需求不断增加。例如，Netflix、或 YouTube 等视频流服务的某些视频只能在特定国家/地区观看。借助当代 VPN，可以加密 IP 地址，使用户看起来是在其他国家/地区上网，从而可以从任何地方访问这些内容。

VPN概述

VPN的分类

VPN的功能

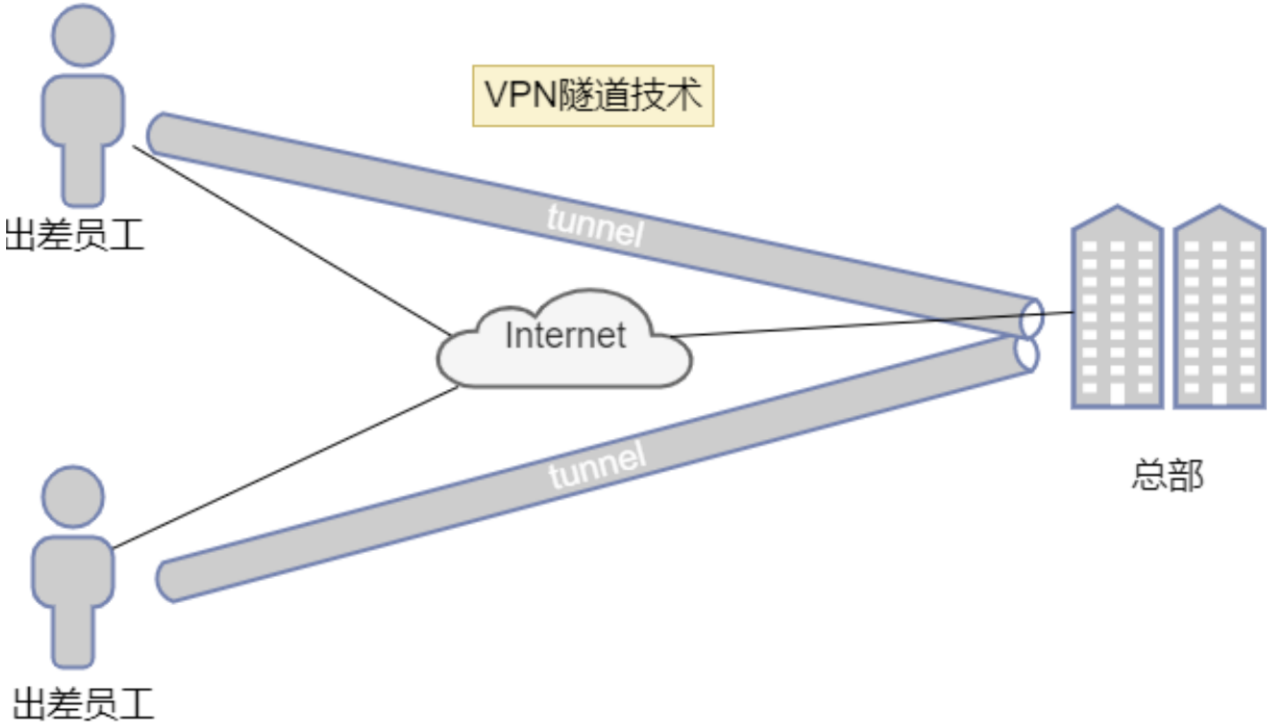
VPN使用的协议

VPN的应用

VPN的分类

1. 按组网方式分类
2. 按工作网络层分类
3. 按设备类型分类
4. 按实现方式

按组网方式分类 - 远程访问虚拟网 1



利用当地VPN服务器实现远程流动办公

按组网方式分类 - 远程访问虚拟网 2

通过VPN客户端连接，可以想象为使用延长线将家用电脑与公司连接。员工可以通过安全连接，从家里拨入公司网络，就像在办公室里一样。但是，必须要先在计算机上安装并配置 VPN 客户端。

这样用户就不是通过自己的ISP 连接互联网，而是通过VPN提供商直接连接互联网。

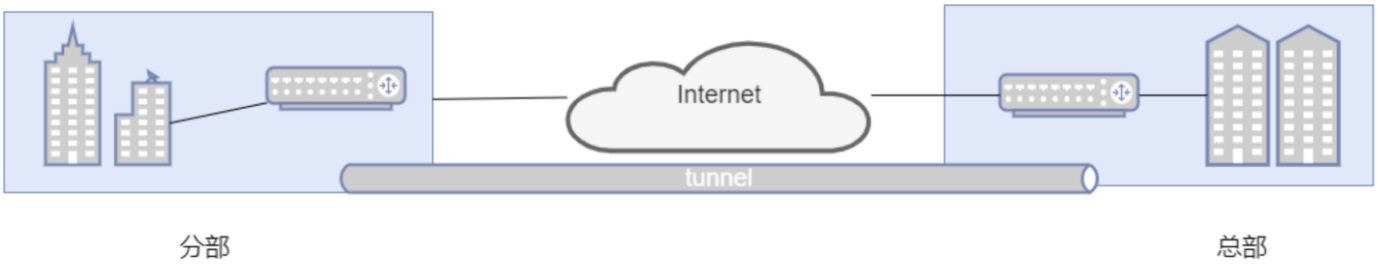
VPN可以在将数据提供给用户之前自动加密数据，而不是使用VPN创建加密隧道，来伪装已经存在的互联网连接。

按组网方式分类 - 远程访问虚拟网 3

这是一种越来越常见的VPN形式，对于不安全的公共 WLAN 的提供商来说特别有用。可以防止第三方访问和入侵网络连接，自始至终加密与提供商之间的数据。还可以防止 ISP 访问任何未经加密的数据（无论出于何种原因），并绕过对用户的互联网访问权限施加的任何限制（例如，如果该国/地区政府对互联网访问实施限制）。

这种VPN访问的优势是效率更高，并且能更以更通用的方式访问公司资源。例如，假设有适当的电话系统可用，员工可以使用耳机连接到系统，就像在公司的工作场所一样。例如，甚至公司的客户也分不清员工是在公司工作还是在家里。

按组网方式分类 - 企业内部虚拟网 1



企业总部与分支机构连接，采用租用专线费用高

按组网方式分类 - 企业内部虚拟网 2

本质上是一个专用网络，用于隐藏专用内部网，同时允许这些安全网络的用户访问彼此的资源。

如果公司有多个地点，并且每个地点都有自己的局域网（LAN）连接到广域网 (WAN)，那么站点到站点 VPN 就很有用。

如果有两个可以互相发送文件的独立内部网，但又不明确允许一个内部网的用户访问另一个内部网，那么设置VPN较为有用。

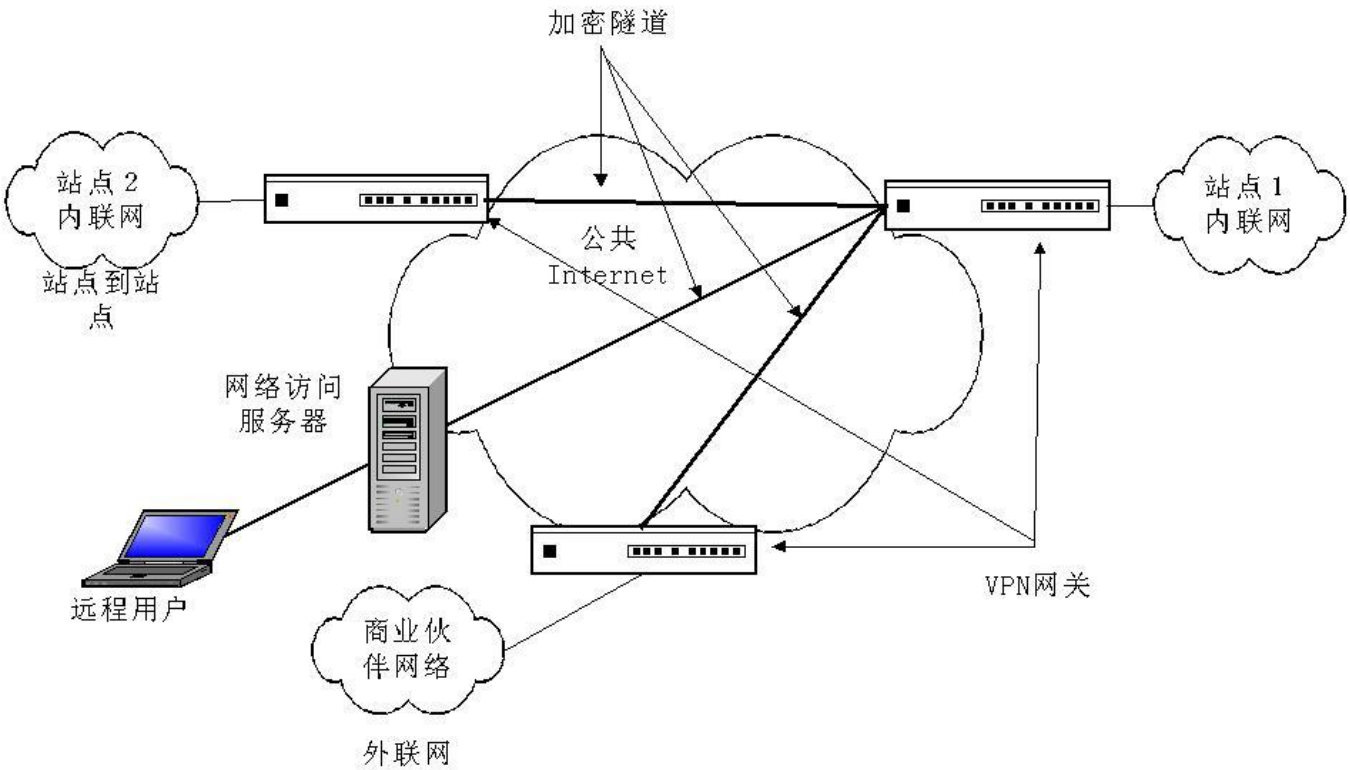
主要用于大型公司，是确保大部门内部以及相互之间进行交流最有效的方式。

按组网方式分类 - 企业扩展虚拟网 1

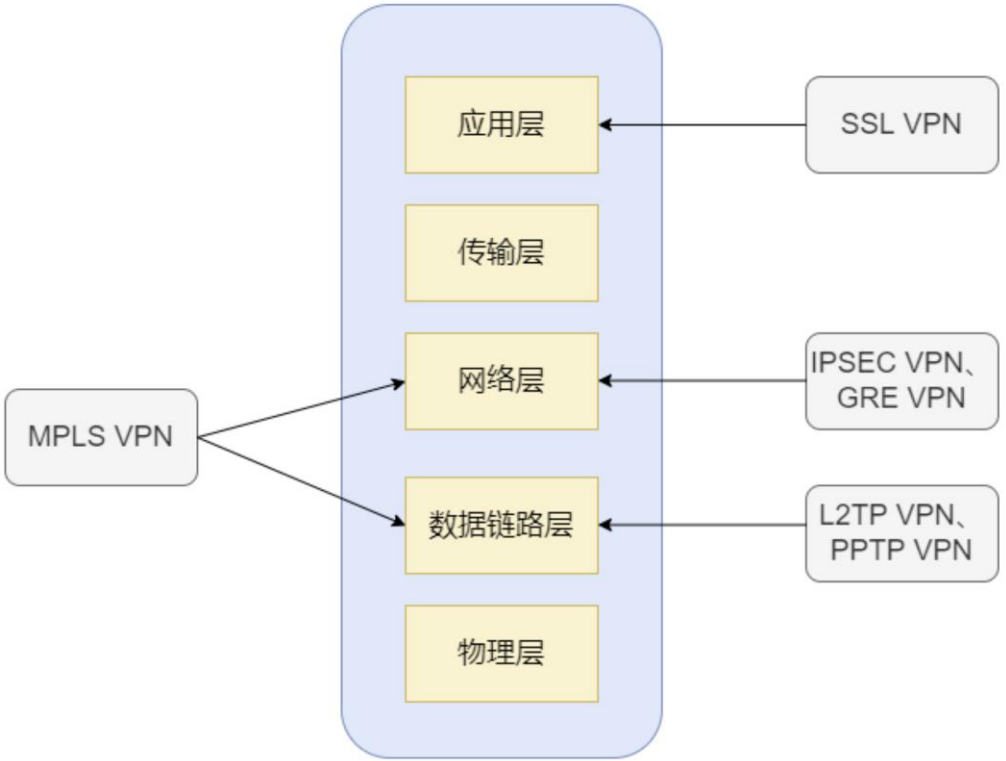
利用VPN技术可以组建安全的Extranet，既可以向客户、合作伙伴提供有效的信息服务，又可以保证自身的内部网络的安全

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

按组网方式分类 - 企业扩展虚拟网 2



按工作网络层分类


应用层
传输层
网络层
数据链路层
物理层
SSL VPN
IPSEC VPN、
GRE VPN
L2TP VPN、
PPTP VPN
MPLS VPN

按设备类型分类

网络设备提供商针对不同客户的需求，开发出不同的VPN网络设备，主要为交换机、路由器和防火墙。

路由器式VPN：路由器式VPN部署较容易，只要在路由器上添加VPN服务即可。

交换机式VPN：主要应用于连接用户较少的VPN网络。

按实现方式分类

常用的有以下四种：

- VPN服务器：大型局域网中，通过在网络中心搭建VPN服务器的方法实现VPN
- 软件VPN：通过专用的软件实现VPN
- 硬件VPN：通过专用的硬件实现VPN
- 集成VPN：某些硬件设备，如路由器、防火墙等，都含有VPN功能，但是一般拥有VPN功能的硬件设备通常都比没有这一功能的要贵。

VPN概述

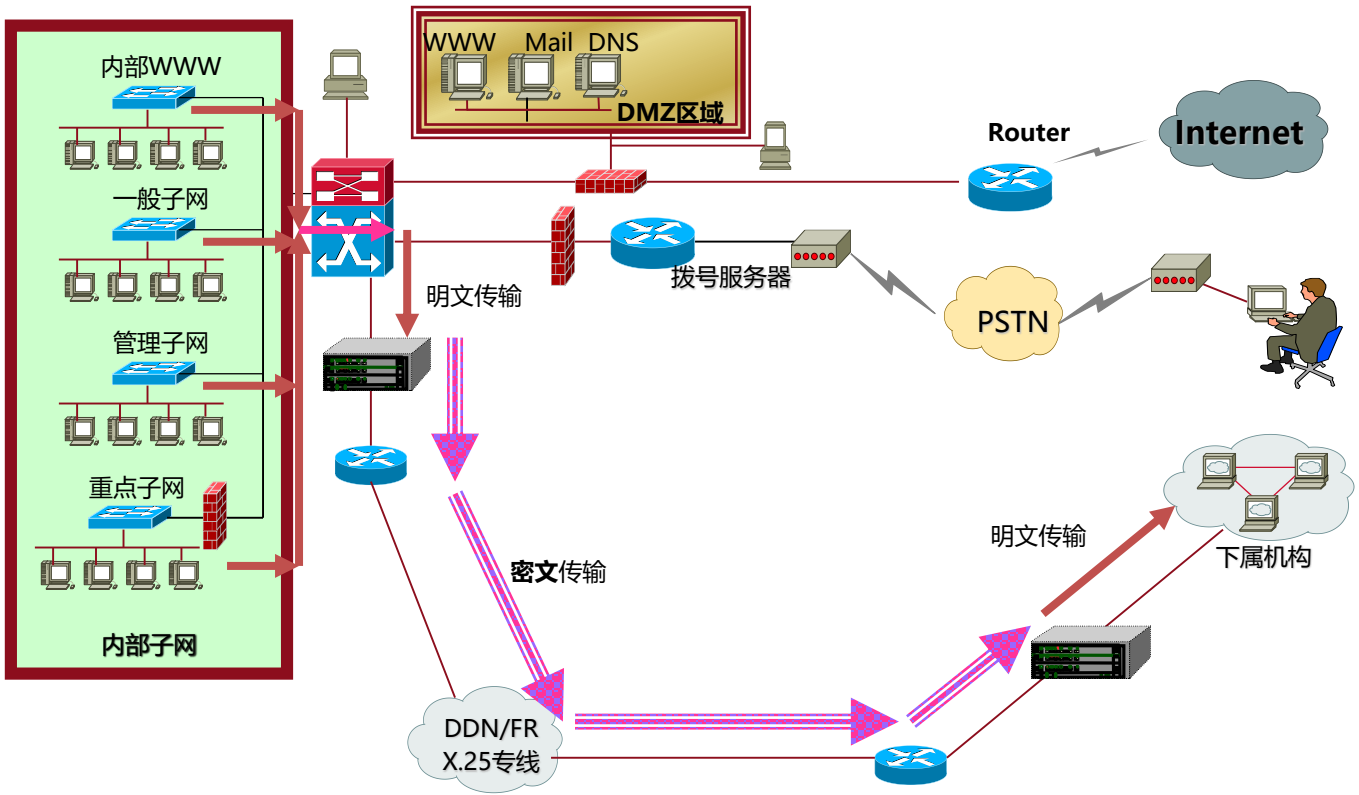
VPN的分类

VPN的功能

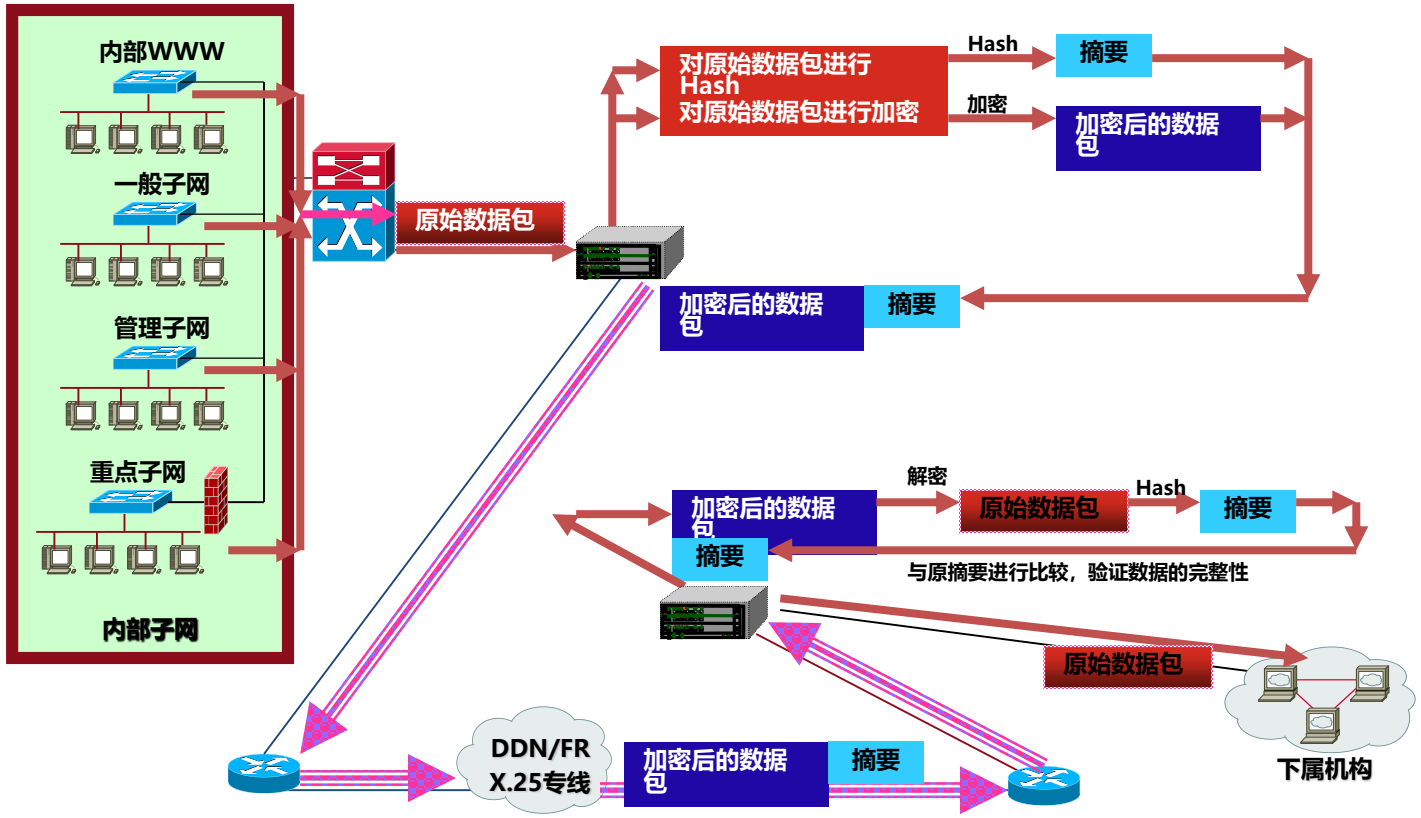
VPN使用的协议

VPN的应用

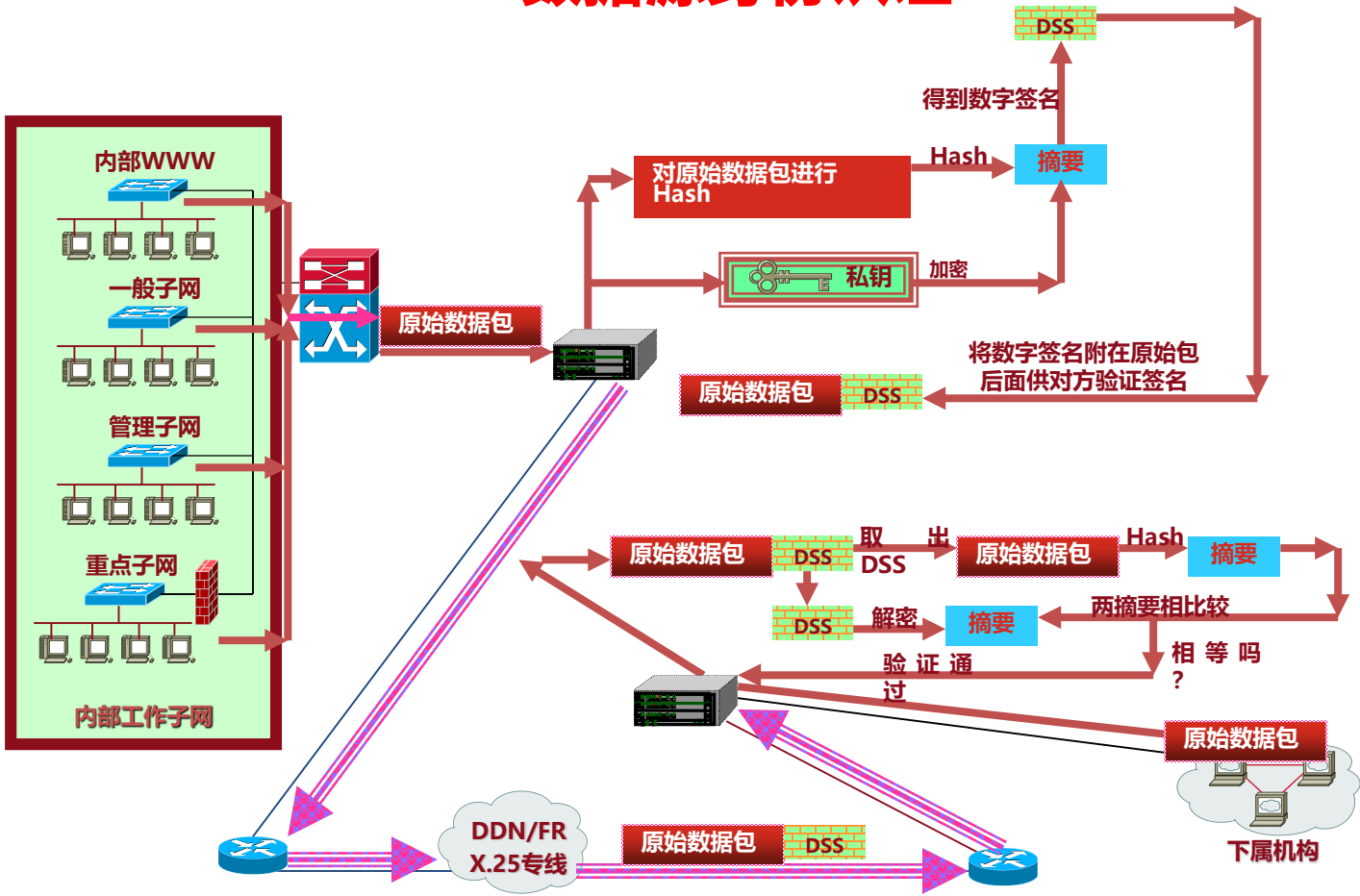
VPN数据机密性保护


内部WWW
一般子网
管理子网
重点子网
内部子网
WWW
Mail
DNS
DMZ区域
Router
Internet
拨号服务器
PSTN
明文传输
密文传输
明文传输
下属机构
DDN/FR
X.25专线

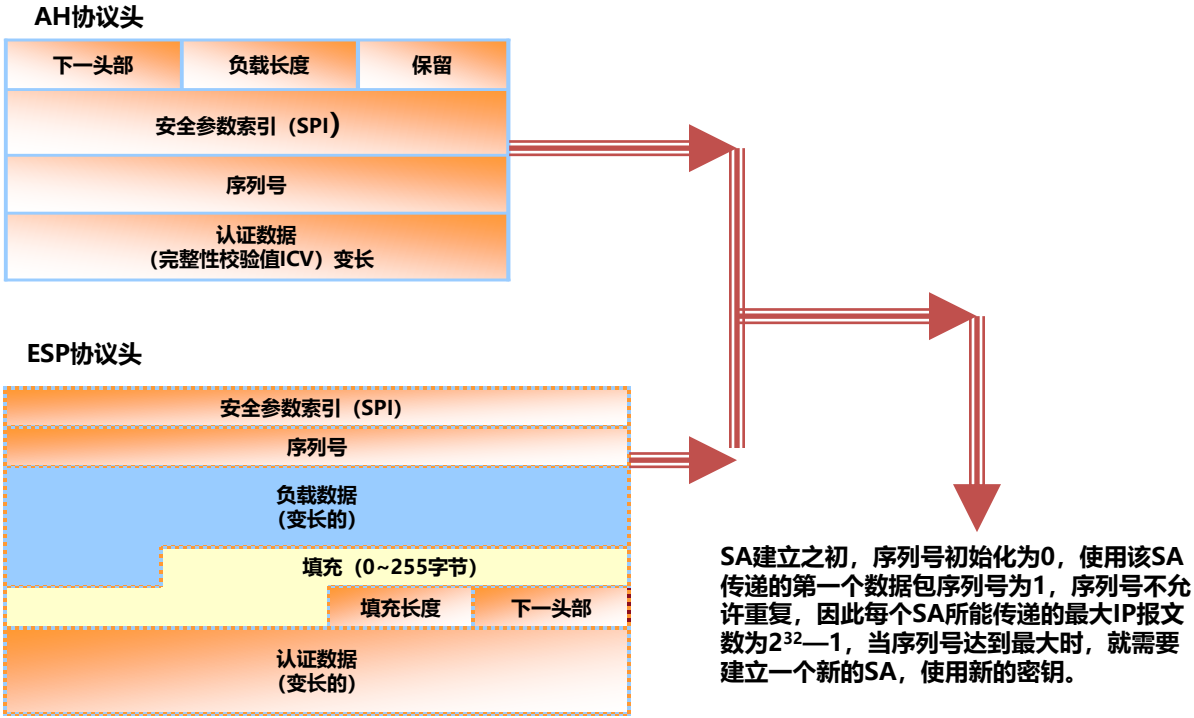
VPN数据完整性保护


内部WWW
一般子网
管理子网
重点子网
内部子网
原始数据包
对原始数据包进行Hash
对原始数据包进行加密
Hash
摘要
加密
加密后的数据包
加密后的数据包
摘要
解密
加密后的数据包
原始数据包
Hash
摘要
摘要
与原摘要进行比较，验证数据的完整性
原始数据包
下属机构
DDN/FR
X.25专线
加密后的数据包
摘要

VPN数据源身份认证


DSS
得到数字签名
Hash
摘要
对原始数据包进行Hash
私钥
加密
内部WWW
一般子网
管理子网
重点子网
内部工作子网
原始数据包
将数字签名附在原始包后面供对方验证签名
原始数据包
DSS
原始数据包
DSS
取出
DSS
原始数据包
Hash
摘要
DSS
解密
摘要
两摘要相比较
验证通过
相等吗？
原始数据包
DDN/FR
X.25专线
原始数据包
DSS
下属机构

重放攻击保护


AH协议头
下一头部
负载长度
保留
安全参数索引（SPI）
序列号
认证数据
（完整性校验值ICV）变长
ESP协议头
安全参数索引（SPI）
序列号
负载数据
（变长的）
填充（0~255字节）
填充长度
下一头部
认证数据
（变长的）
SA建立之初，序列号初始化为0，使用该SA传递的第一个数据包序列号为1，序列号不允许重复，因此每个SA所能传递的最大IP报文数为2^{32}—1，当序列号达到最大时，就需要建立一个新的SA，使用新的密钥。

VPN概述

VPN的分类

VPN的功能

VPN使用的协议

VPN的应用

VPN工作原理

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**

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

隧道技术 - 1

VP

隧道

数据

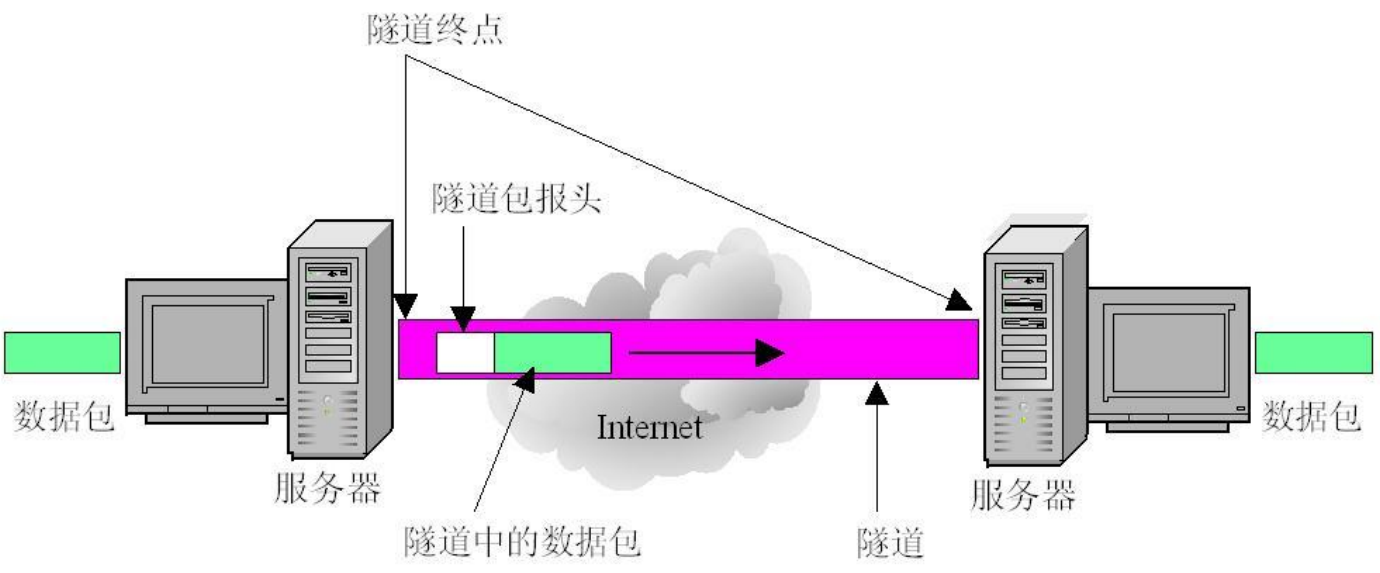
使用

隧道

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

隧道技术 - 2



隧道技术 - 3

隧道可在网络的任一层实现

最常用的是两层：数据链路层和网络层

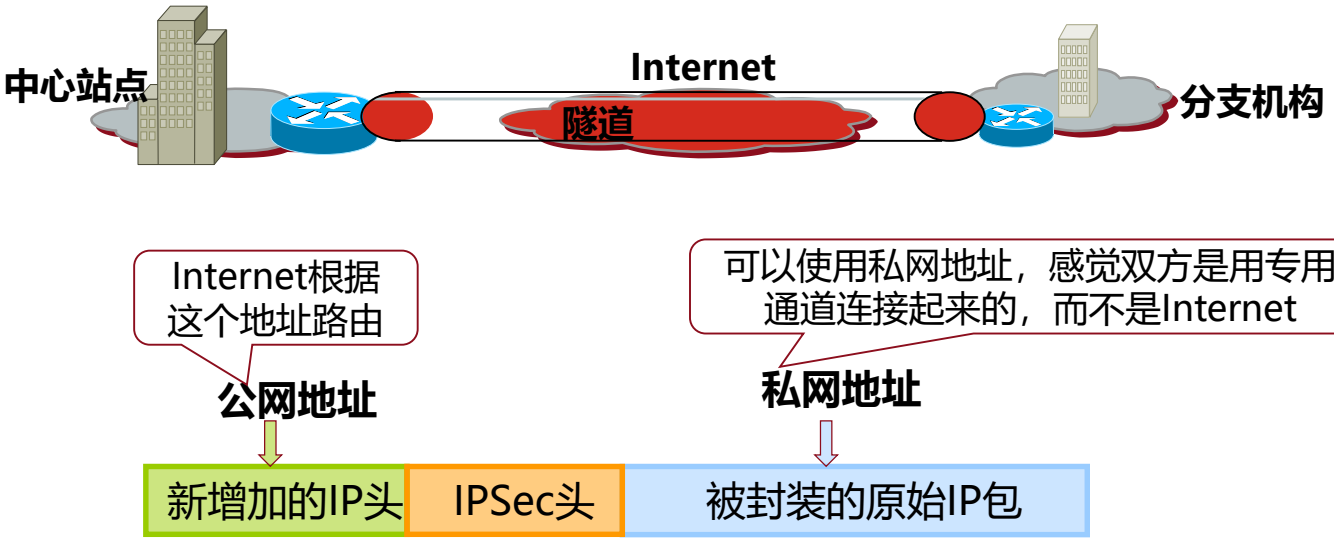
数据链路层隧道：一个链路帧被放到了其它链路层的协议数据单元（PDU）中,该链路层还包括另外的链路帧，如：PPTP, L2F, L2TP 构成的VPN

网络层隧道：第三层的包被放到其它层或另外的第三层包中，如IPsec 的AH和ESP隧道模式；

封装：当某层的PDU被放到另外一个PDU中的有效载荷时，把这种处理方式叫做封装

隧道技术 - 4

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



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**

隧道协议 - 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

隧道协议 - 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**

隧道协议 - PPTP 3

PPTP协议是PPP协议的扩展

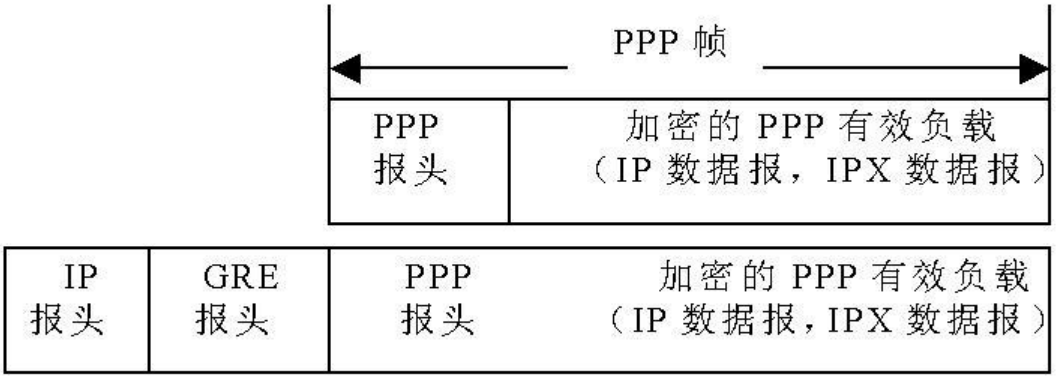
增强了PPP协议的认证、压缩和加密功能

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

隧道协议 - 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)



隧道协议 - PPTP 5

封装过程：

1. 应用层数据封装成IP数据包
2. 将IP数据包发送到VPN的虚拟接口
3. VPN的虚拟接口将IP数据包压缩和加密，并增加PPP头
4. VPN的虚拟接口将PPP帧发送给PPTP协议驱动程序
5. PPTP协议驱动程序在PPP帧外添加GRE报头
6. PPTP协议驱动程序将GRE报头提交给TCP/IP协议驱动程序
7. TCP/IP协议驱动程序为GRE驱动添加IP头部
8. 为IP数据包进行数据链路层封装后通过物理网卡发送出去

隧道协议 - PPTP 6

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**

隧道协议 - PPTP 7

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**

隧道协议 - 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

隧道协议 - 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

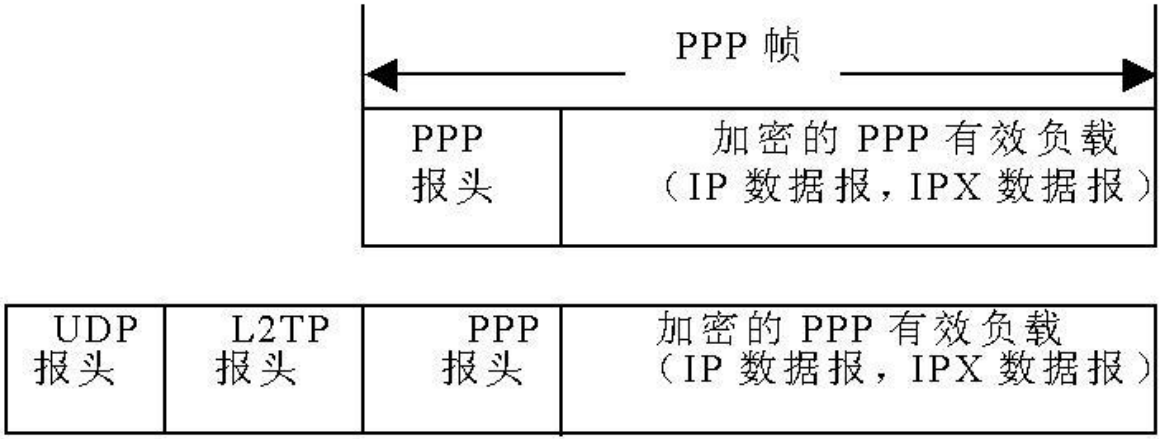
允许在物理上连接到不同NAS的PPP链路，在逻辑上的终点为同一个物理设备

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)

隧道协议 - L2TP 3

L2TP封装



隧道协议 - L2TP 4

L2TP 头文件和 UDP 头数据包封装

隧道协议 - 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**

隧道协议 - GRE 1

用于将使用一个路由协议的数据包封装在另一协议的数据包中。“

封装”是指将一个数据包包装在另一个数据包中，就像将一个盒子放在另一个盒子中一样。

GRE 是在网络上建立直接点对点连接的一种方法，目的是简化单独网络之间的连接。它适用于各种网络层协议。

隧道协议 - GRE 2

要了解其工作原理，请想像一下汽车和渡轮之间的区别。汽车在陆地上行驶，而渡轮在水上行驶。汽车通常不能在水上行驶，但是可以将汽车装载到渡轮上。

在这个类比当中，地形类型好比是支持某些路由协议的网络，而车辆则好比是数据包。

GRE 是一种将一种类型的数据包装载到另一种类型的数据包中的方式，以便第一个数据包可以穿越它通常无法穿越的网络，就像一种类型的运输工具（汽车）被装载到到另一种类型的运输工具（渡轮）上，以便穿越原本无法行驶的地形。

隧道协议 - GRE 3

例如，假设一家公司需要在位于两个不同办公室的局域网（LAN）之间建立连接。

两个 LAN 都使用最新版本的互联网协议 IPv6。但是，为了从一个办公网络到达另一个办公网络，流量必须通过一个由第三方管理的网络（仅支持较旧的 IPv4 协议）。

借助GRE，该公司可以将IPv6数据包封装在IPv4数据包中，然后便可通过此网络传输流量。回到那个类比，IPv6数据包是汽车，IPv4数据包是渡轮，而第三方网络则是水。

隧道协议 - GRE 4

例如，RIP路由协议是一种距离矢量路由协议，最大跳数为15。如果网络直径超过15，设备将无法通信。这种情况下，可以使用GRE技术在两个网络节点之间搭建隧道，隐藏它们之间的跳数，扩大网络的工作范围。

而GRE本身并不支持加密，因而通过GRE隧道传输的流量是不加密的。

将IPSec技术与GRE相结合，先建立GRE隧道对报文进行GRE封装，然后再建立IPSec隧道对报文进行加密，这样就只可以保证报文传输的完整性和私密性。

隧道协议 - 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

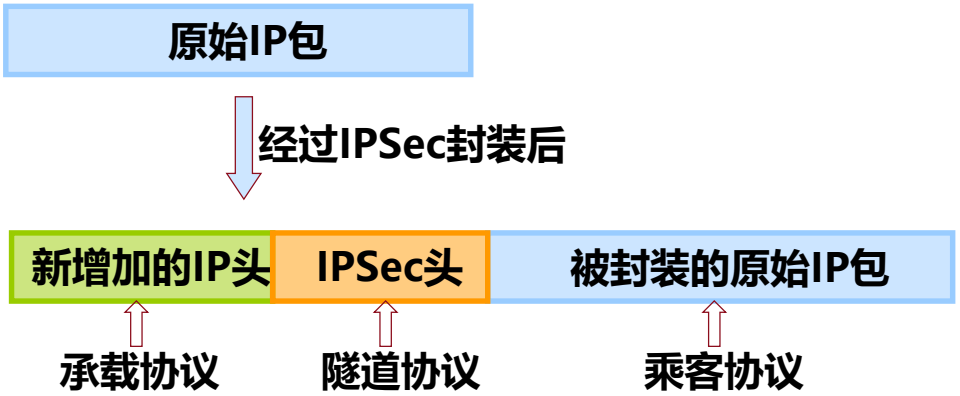
隧道协议 - IPSec协议 2

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**

隧道协议 - 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。



隧道协议 - 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、抗重放攻击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

隧道协议 - 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

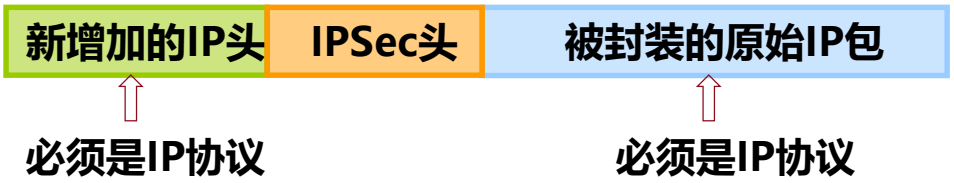
Tunnel Mode

- 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

隧道协议 - 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

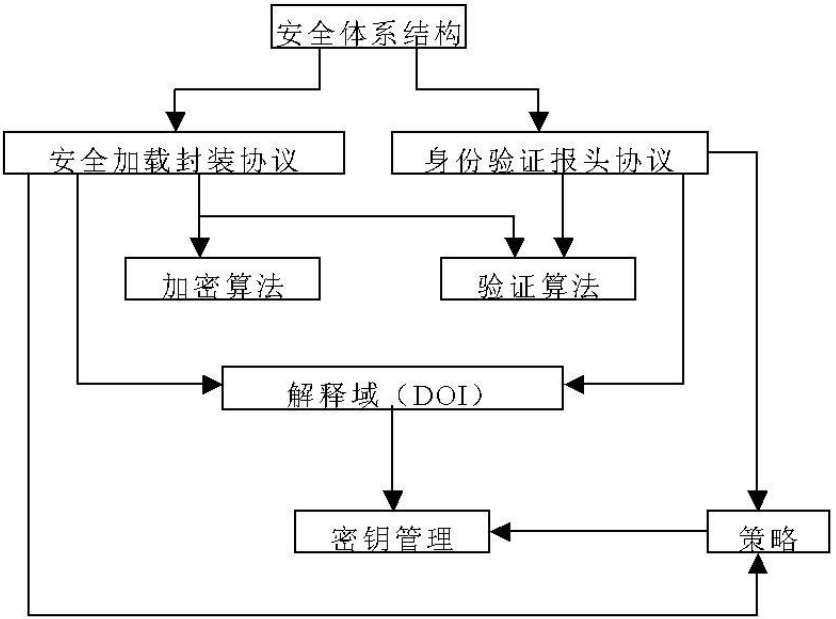
IPSec是一种开放标准的框架结构，特定的通信方之间在IP层通过加密和数据哈希(hash)等手段，来保证数据包在Internet 网上传输时的私密性(confidentiality) 、完整性(data integrity)和真实性(origin authentication)



隧道协议 - 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

IPSec的安全体系



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**

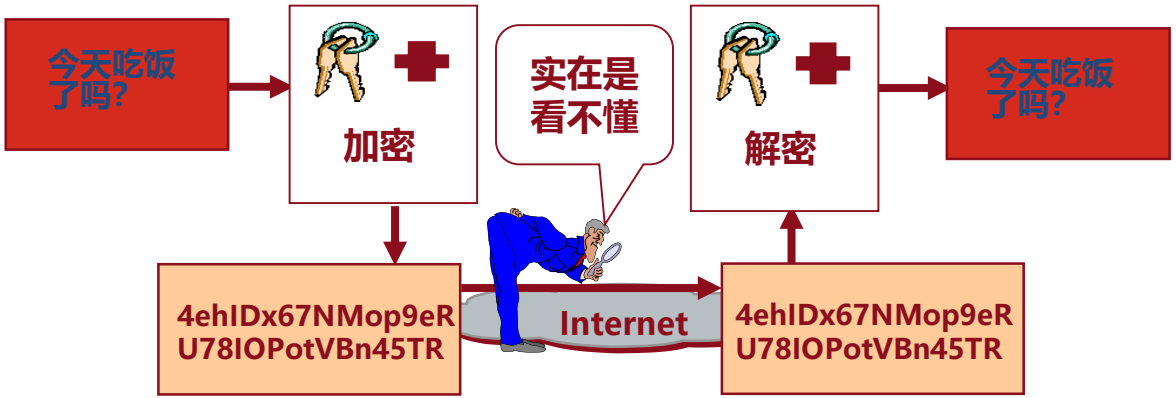
秘密性(Confidentiality)

- **确保数据不被非法读取**

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



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**

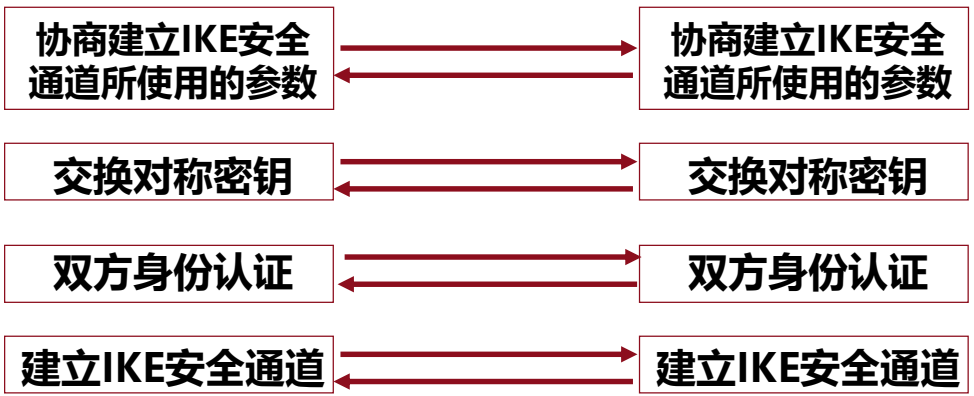
IPSec保护技术 4

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


Host A
Router A
Router B
Host B
10.0.1.3
IKE 阶段 1
10.0.2.3


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

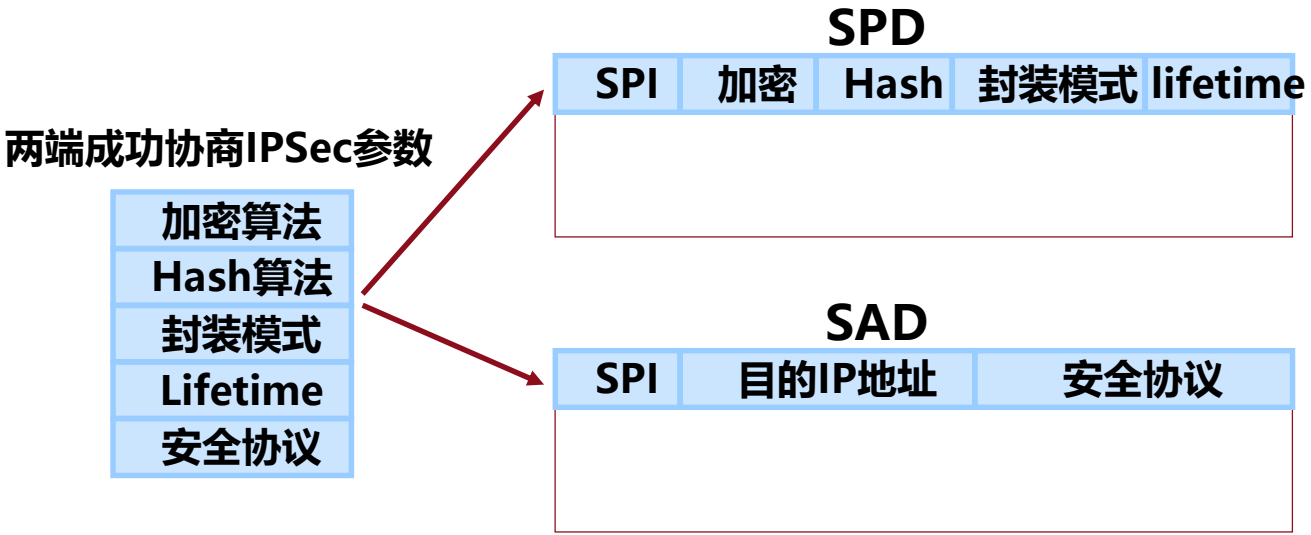
协商IPSec安全参数 ⇄ 协商IPSec安全参数

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

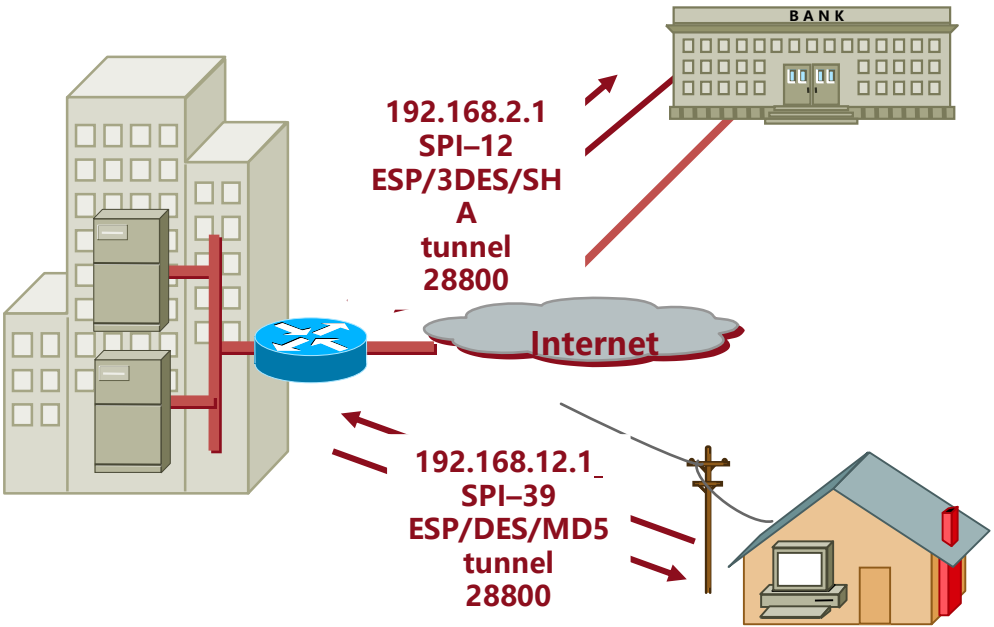
IPSec SA (安全关联，Security Association)：

- 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

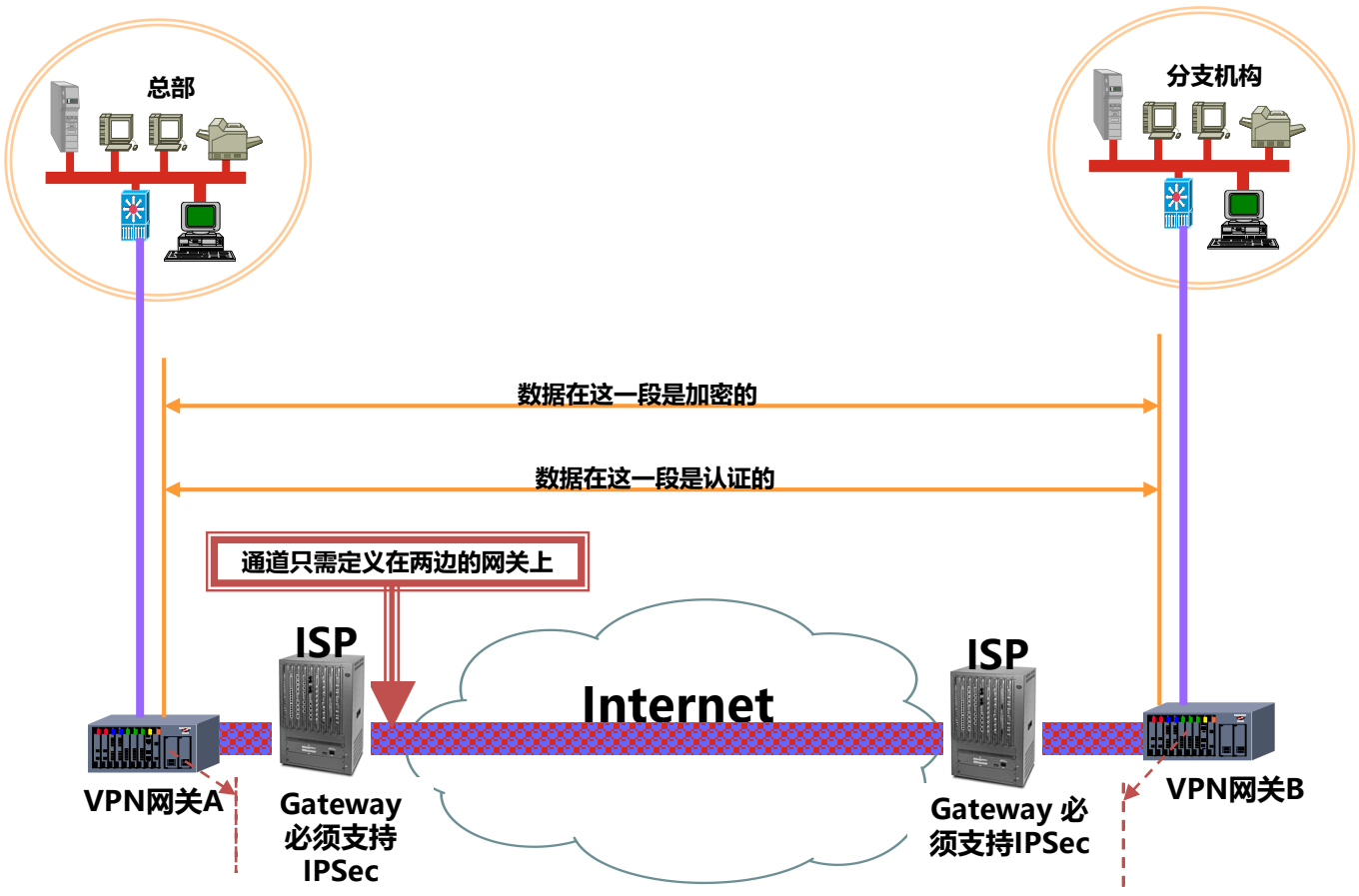
VPN概述

VPN的分类

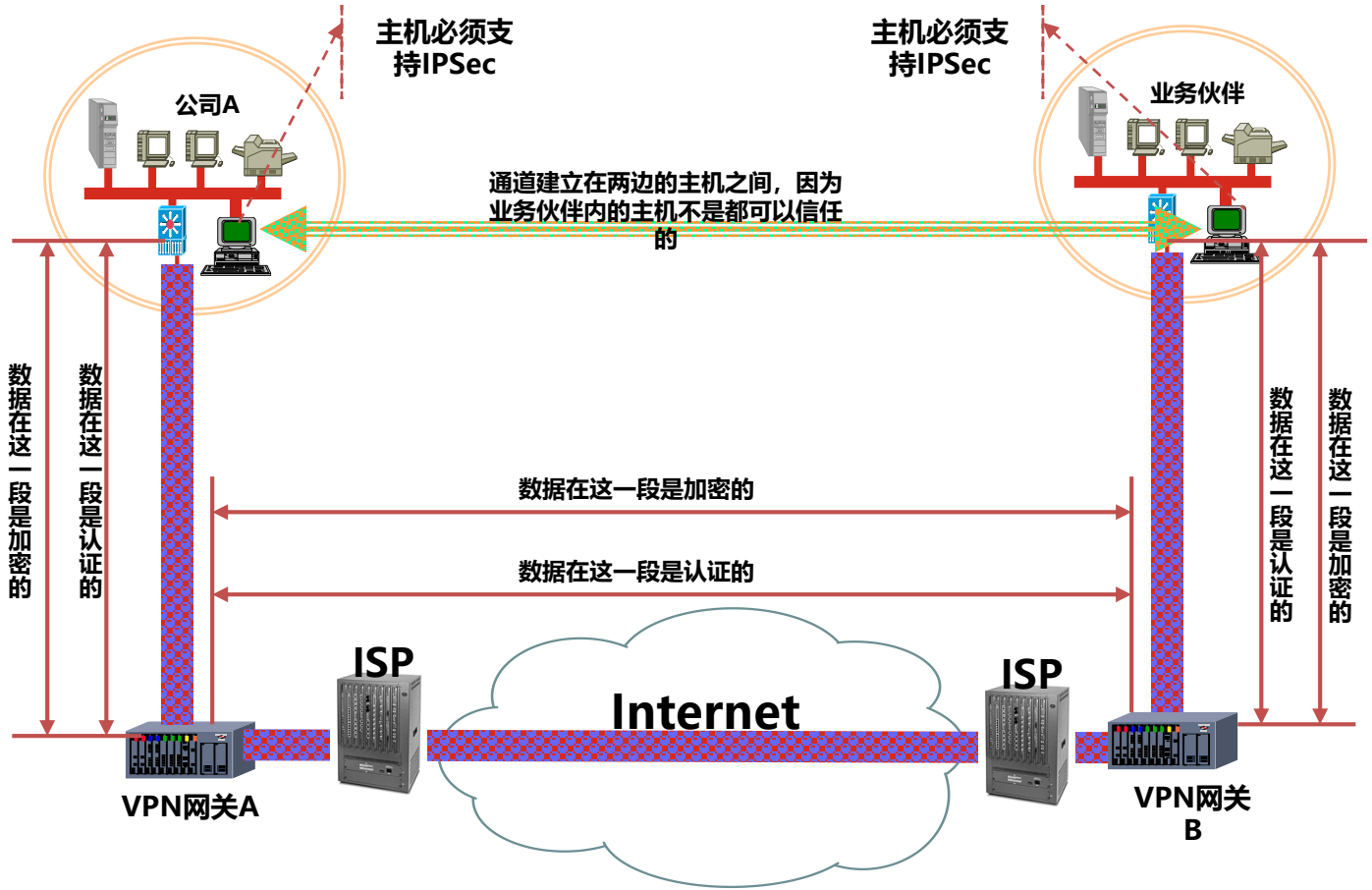
VPN使用的协议

VPN的应用

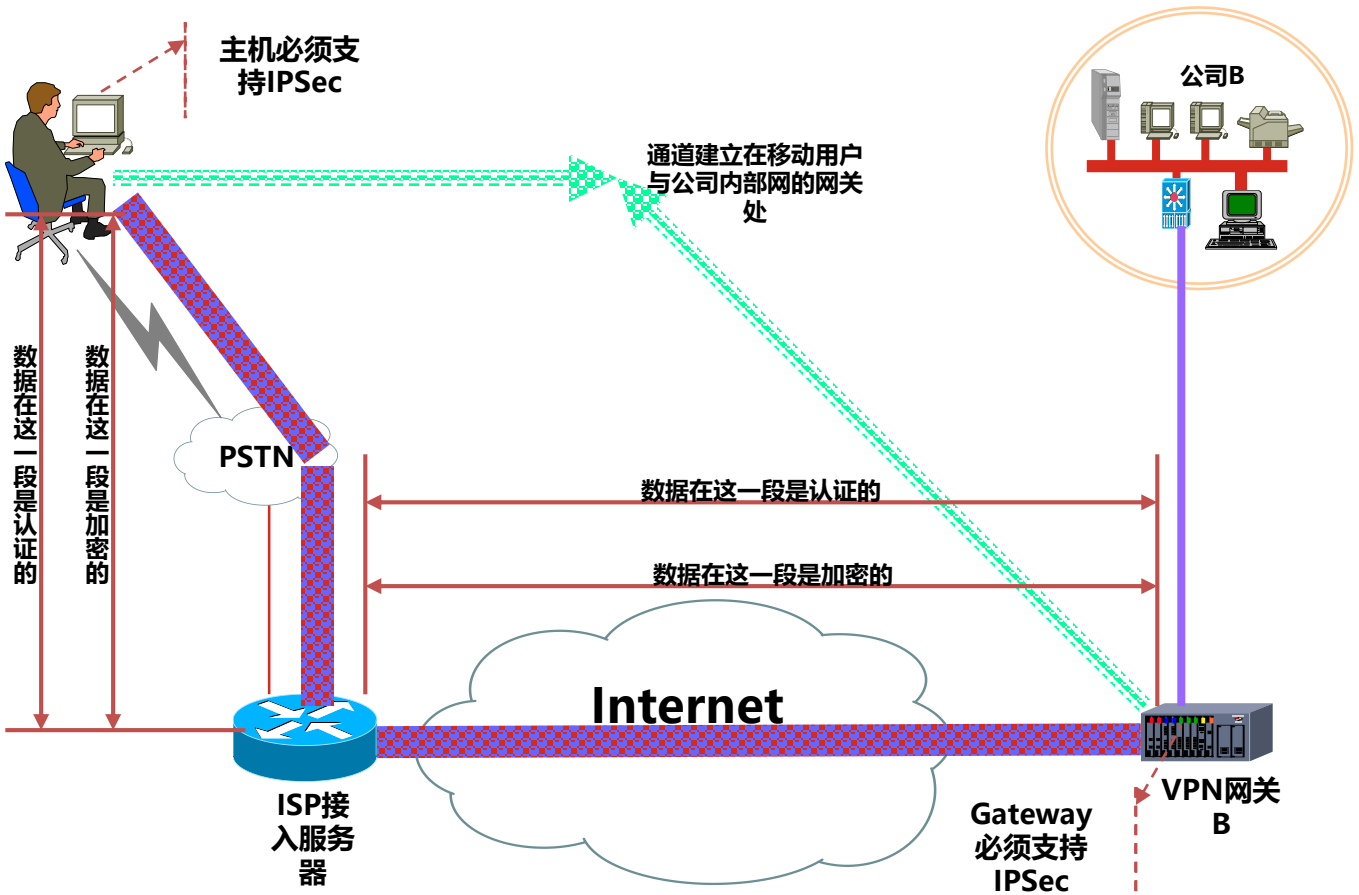
用VPN连接分支机构


总部
分支机构
数据在这一段是加密的
数据在这一段是认证的
通道只需定义在两边的网关上
ISP
Internet
ISP
VPN网关A
Gateway
必须支持
IPSec
Gateway 必
须支持IPSec
VPN网关B

用VPN连接合作伙伴


主机必须支持IPSec
主机必须支持IPSec
公司A
业务伙伴
通道建立在两边的主机之间，因为业务伙伴内的主机不是都可以信任的
数据在这一段是加密的
数据在这一段是认证的
数据在这一段是加密的
数据在这一段是认证的
数据在这一段是加密的
数据在这一段是认证的
ISP
Internet
ISP
VPN网关A
VPN网关B

用VPN连接远程用户


主机必须支持IPSec
公司B
通道建立在移动用户与公司内部网的网关处
数据在这一段是认证的
数据在这一段是加密的
PSTN
数据在这一段是认证的
数据在这一段是加密的
Internet
ISP接入服务器
Gateway必须支持IPSec
VPN网关B

VPN的优点

1. 利用VPN，可节省专用和拨号连接的成本
2. 基于VPN技术，能够迅速建立和重构网络
3. 简化了企业联网和广域网操作
4. 提高了网络可靠性
5. VPN网络有很好的兼容性和可扩展性
6. 企业可以利用 VPN 迅速开展新的服务和连接全球的设施

VPN的缺点

企业不能直接控制基于互联网的VPN的可靠性和性能。机构必须依靠提供VPN的互联网服务提供商保证服务的运行。

企业创建和部署VPN线路并不容易。这种技术需要高水平地理解网络和安全问题，需要认真的规划和配置。

不同厂商的VPN产品和解决方案总是不兼容的，因为许多厂商不愿意或者不能遵守VPN技术标准。因此，混合使用不同厂商的产品可能会出现技术问题。

当使用无线设备时，VPN有安全风险。在接入点之间漫游特别容易出问题。当用户在接入点之间漫游的时候，任何使用高级加密技术的解决方案都可能被攻破。

VPN的安全威胁 1

拨入段数据泄漏风险

- 攻击者可以很容易的在拨入链路上实施监听
- ISP很容易检查用户的数据
- 可以通过链路加密来防止被动的监听，但无法防范恶意窃取数据的ISP。

因特网上数据泄漏的风险

- 数据在到达终点之前要经过许多路由器，明文传输的报文很容易在路由器上被查看和修改
- 监听者可以在其中任一段链路上监听数据
- 逐段加密不能防范在路由器上查看报文，因为路由器需要解密报文选择路由信息，然后再重新加密发送
- 恶意的ISP可以修改通道的终点到一台假冒的网关

安全网关中数据泄漏的风险

- 数据在安全网关中是明文的，因而网关管理员可以直接查看机密数据
- 网关本身可能会受到攻击，一旦被攻破，流经安全网关的数据将面临风险

内部网中数据泄漏的风险

- 内部网中可能存在不信任的主机、路由器等
- 内部员工可以监听、篡改、重定向企业内部网的数据报文
- 来自企业网内部员工的其他攻击方式

VPN的安全威胁 2

VPN 连接虽然会保护用户IP并加密互联网历史记录，但它无法保护您的计算机免于外部入侵。要做到这一点，一定要使用反病毒软件。因为单独使用 VPN 无法保护您免受木马、病毒、僵尸病毒及其他恶意软件的侵害。

一旦恶意软件找到入侵设备的方法，无论是否运行 VPN，它都会窃取或损坏数据。因此，结合使用 VPN 和全面的反病毒程序从而确保最高的安全性非常重要。

选择可以信任的 VPN 提供商也非常重要。虽然现在 ISP 无法看到您的互联网流量，但VPN提供商可以。如果您的VPN提供商被入侵，您也会被入侵。

好的 VPN 应该做什么?

可以依靠 VPN 来进行一个或多个任务。VPN 本身也应该可以抵御威胁。以下是一个全面的 VPN 解决方案应该具备的功能:

- **加密 IP 地址**:VPN 的主要工作就是对 ISP 和其他第三方隐藏用户 IP 地址。这样当在线发送和接收信息时,就不用担心会有被除了用户和 VPN 提供商以外的任何人看到的风险。
- **加密协议**:VPN 还应该防止留下痕迹,例如,互联网历史记录、搜索历史记录和 cookie。加密 cookie 尤其重要,因为能阻止第三方访问保密信息,如个人数据、财务信息和网站上的其他内容。
- **自杀开关**:如果VPN 连接突然中断,安全连接也会中断。好的 VPN 能检测到这种突然停机,并终止预先选择的程序,从而降低数据被泄露的可能性。
- **双因素身份验证**:通过使用各种身份验证方法,强大的VPN能够检查试图登录每个人。例如:用户可能会被提醒输入密码,然后会将代码发送到用户手机。这使得未经邀请的第三方难以访问用户的安全连接。

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