网络安全

罗　敏

武汉大学计算机学院

mluo@whu.edu.cn

第11章 入侵检测技术 重点回顾

- 入侵检测技术概述
- 入侵检测分类与评估
- 入侵检测产品

第12章 VPN技术

- VPN是一种新型的网络安全传输技术。本章介绍VPN的概念、VPN的协议及VPN的应用。

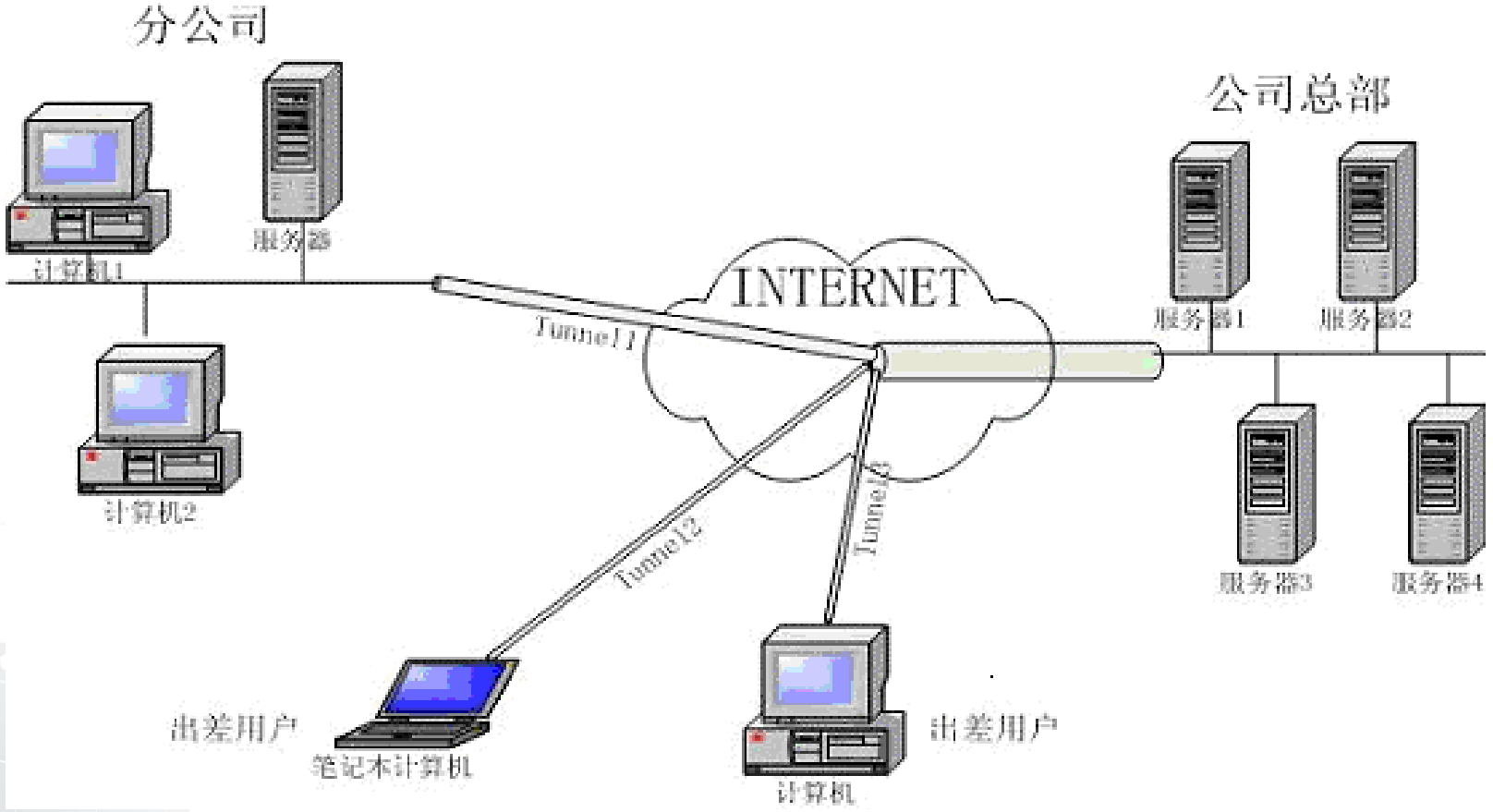
第12章 VPN技术

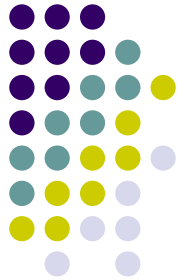
- 12.1 VPN概述
- 12.2 VPN的分类
- 12.3 VPN使用的协议与实现

12.1 VPN概述

- VPN的概念
  - 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

12.1 VPN概述


分公司
计算机1
服务器
计算机2
INTERNET
Tunnel1
Tunnel2
Tunnel3
公司总部
服务器1
服务器2
服务器3
服务器4
出差用户
笔记本计算机
计算机
出差用户

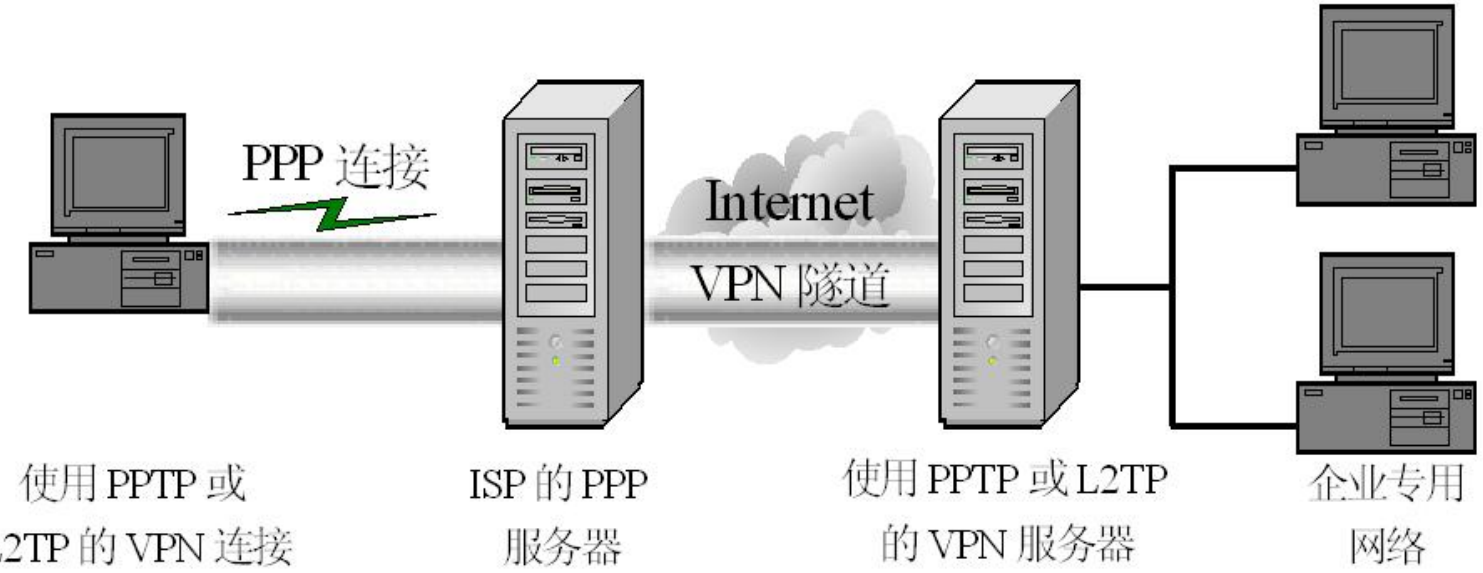


12.1 VPN概述

- VPN的概念
  - 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。公共网络仿佛是只由本网络在独占使用
  - 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

12.1 VPN概述

- VPN的组成

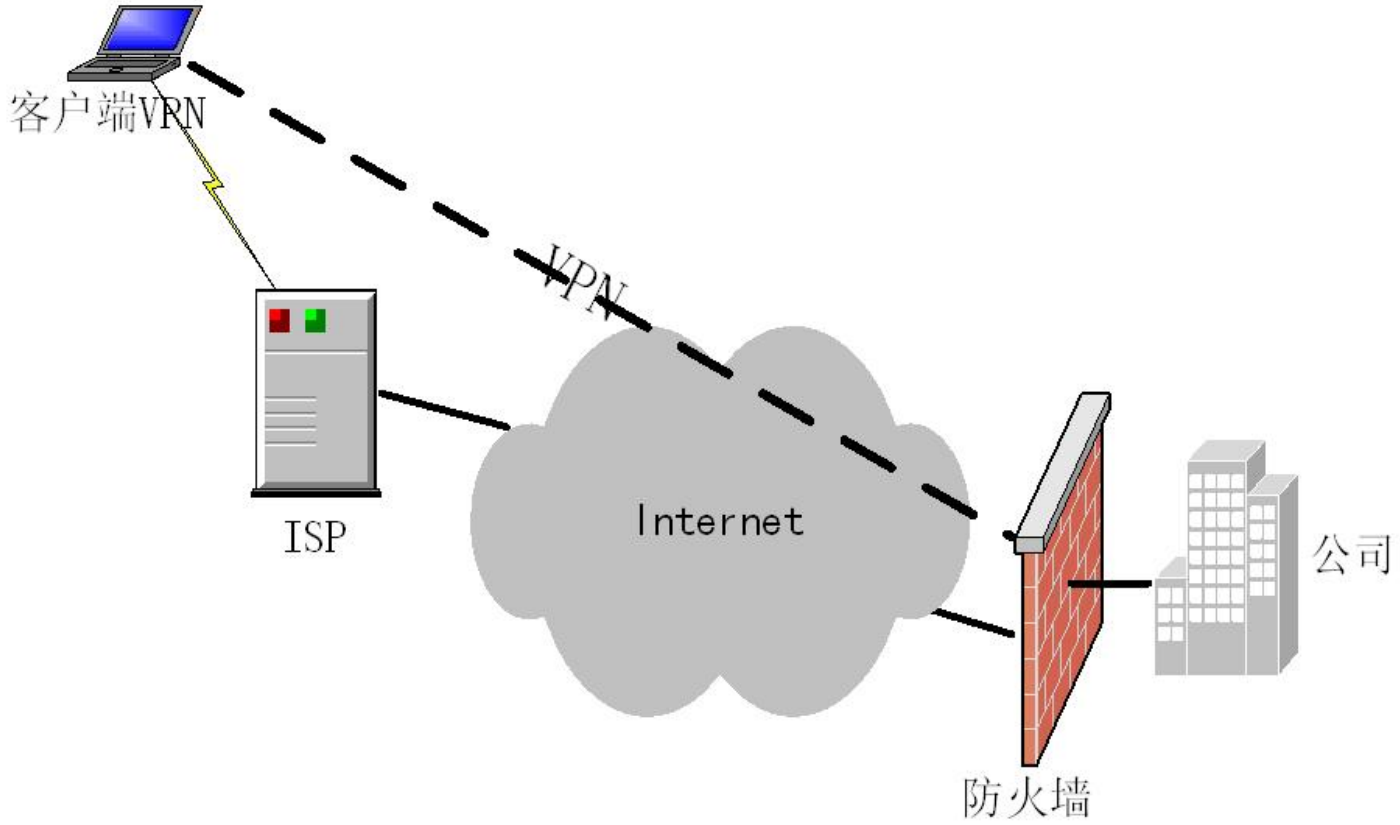


12.2 VPN的分类

- 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）

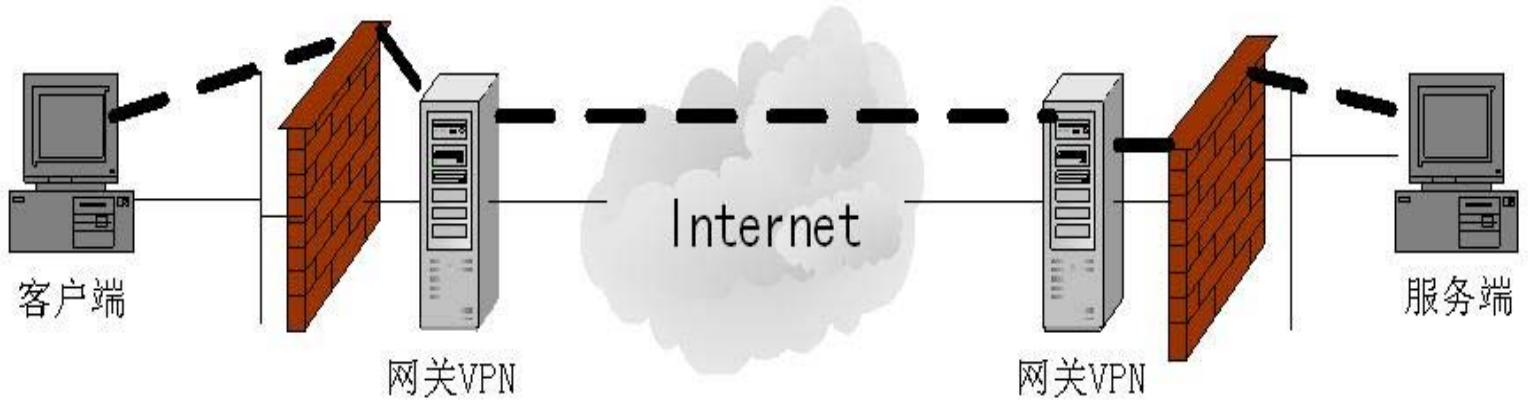
12.2 VPN的分类

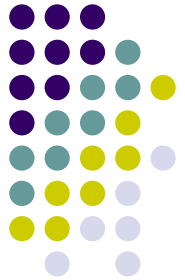
- 远程访问虚拟网（Access VPN）



12.2 VPN的分类

- 企业内部虚拟网（Intranet VPN）

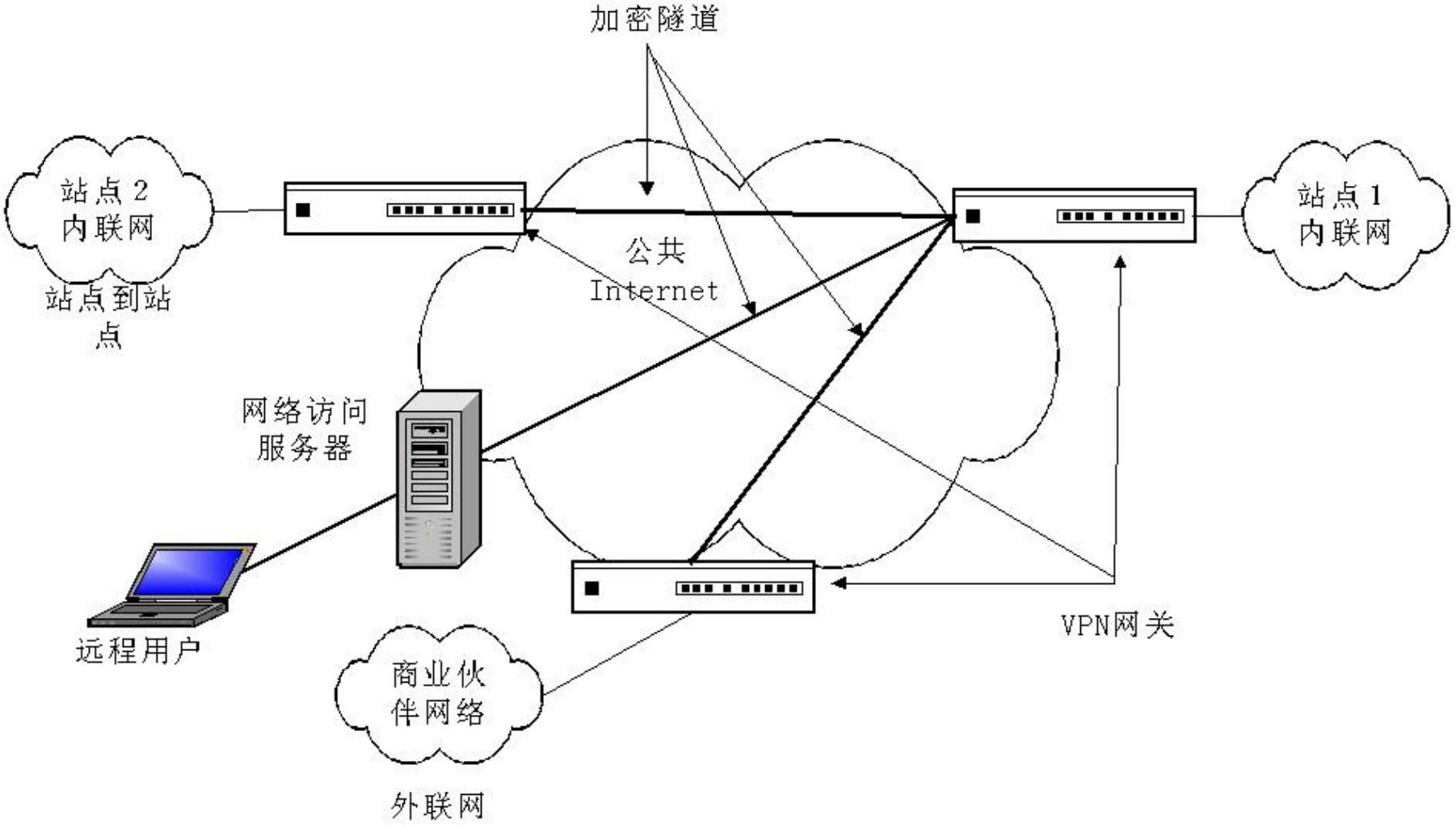




12.2 VPN的分类

- 企业扩展虚拟网（Extranet VPN）
  - 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

12.2 VPN的分类


加密隧道
站点2
内联网
站点到站点
公共
Internet
站点1
内联网
网络访问
服务器
远程用户
商业伙伴网络
外联网
VPN网关

12.3 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

12.3 VPN使用的协议与实现

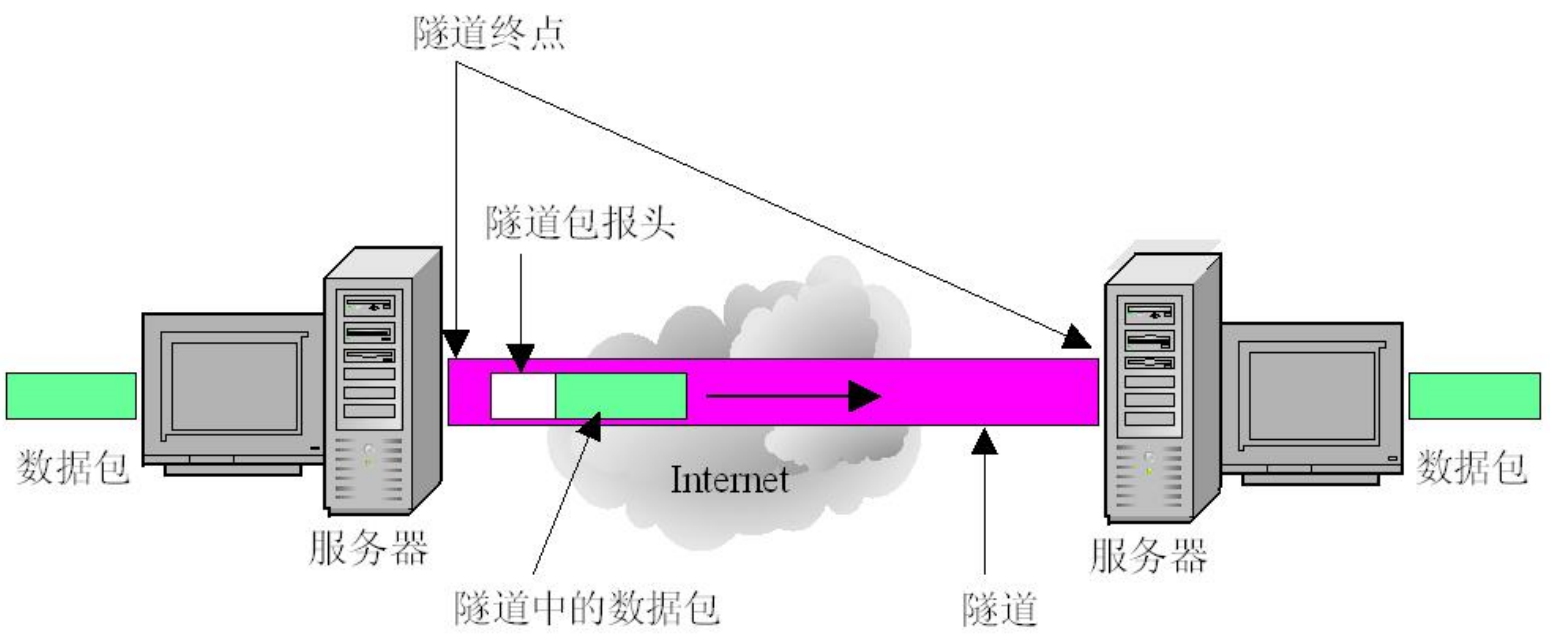
- VPN的一般验证流程
  - 客户机向VPN服务器发出请求，VPN服务器响应请求并向客户机发出身份质询
  - 客户机将加密的响应信息发送到VPN服务器
  - 如果账户有效，VPN服务器将检查该用户是否具有远程访问权限
  - 如果该用户拥有远程访问的权限，VPN服务器接受此连接
  - 在身份验证过程中产生的客户机和服务器公有密钥将用来对数据进行加密

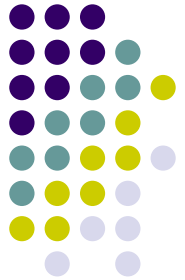
12.3 VPN使用的协议与实现

- 隧道
  - 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

12.3 VPN使用的协议与实现

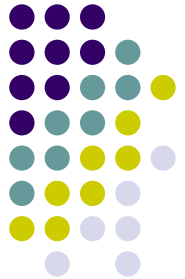
- 隧道





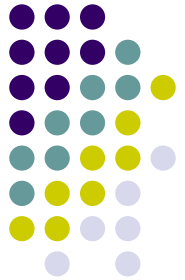
12.3 VPN使用的协议与实现

- 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



12.3 VPN使用的协议与实现

- PPTP
  - 由3Com公司和Microsoft公司合作开发
  - Windows、Linux、Solaris

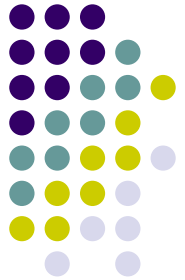


12.3 VPN使用的协议与实现

- PPTP
  - PPP
    - Point to Point Protocol
    - 点对点通信协议
    - IPX、TCP/IP、NetBEUI和AppleTalk

12.3 VPN使用的协议与实现

- 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(如：MS-CHAP、EAP、CHAP、SPAP、PAP等)，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

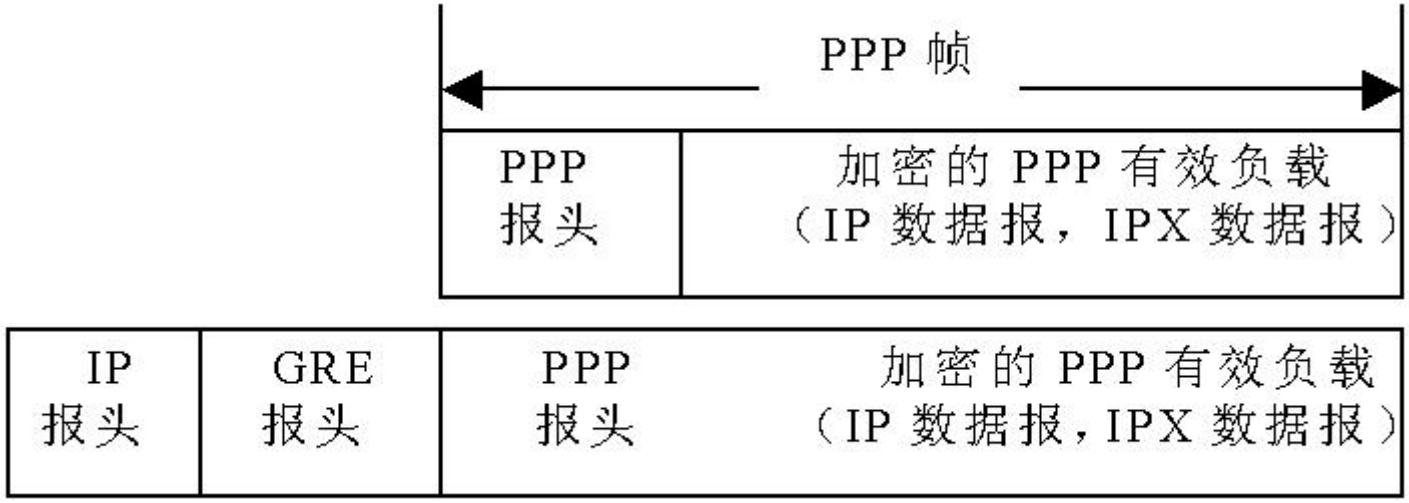


12.3 VPN使用的协议与实现

- PPTP协议概述
  - 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

12.3 VPN使用的协议与实现

- 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)



12.3 VPN使用的协议与实现

- 基于PPTP的VPN
  - 加密服务
    - 通过使用从PPP协议的MS-CHAP或EAP-TLS身份验证过程中生成的密钥
    - PPP帧以MPPE方式进行加密
    - PPTP只是对先前加密了的PPP帧进行封装

12.3 VPN使用的协议与实现

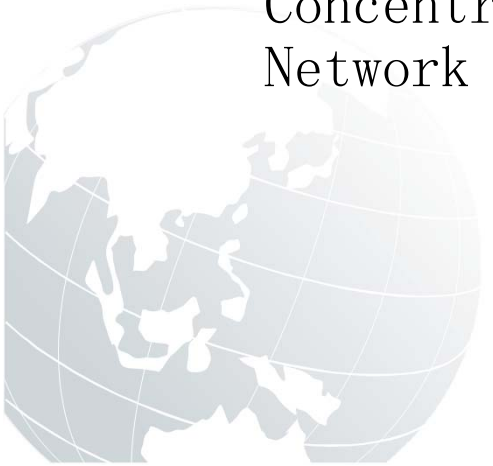
- PPTP协议数据传输过程
  - 首先远程VPN客户端通过诸如Windows系统的拨号网络中的远程访问服务(RAS)与本地ISP进行PPP因特网连接
  - 当PPP连接激活后，通过PPTP协议在客户端，连接VPN服务器端的WAN适配器的IP地址或者域名

12.3 VPN使用的协议与实现

- L2TP
  - 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

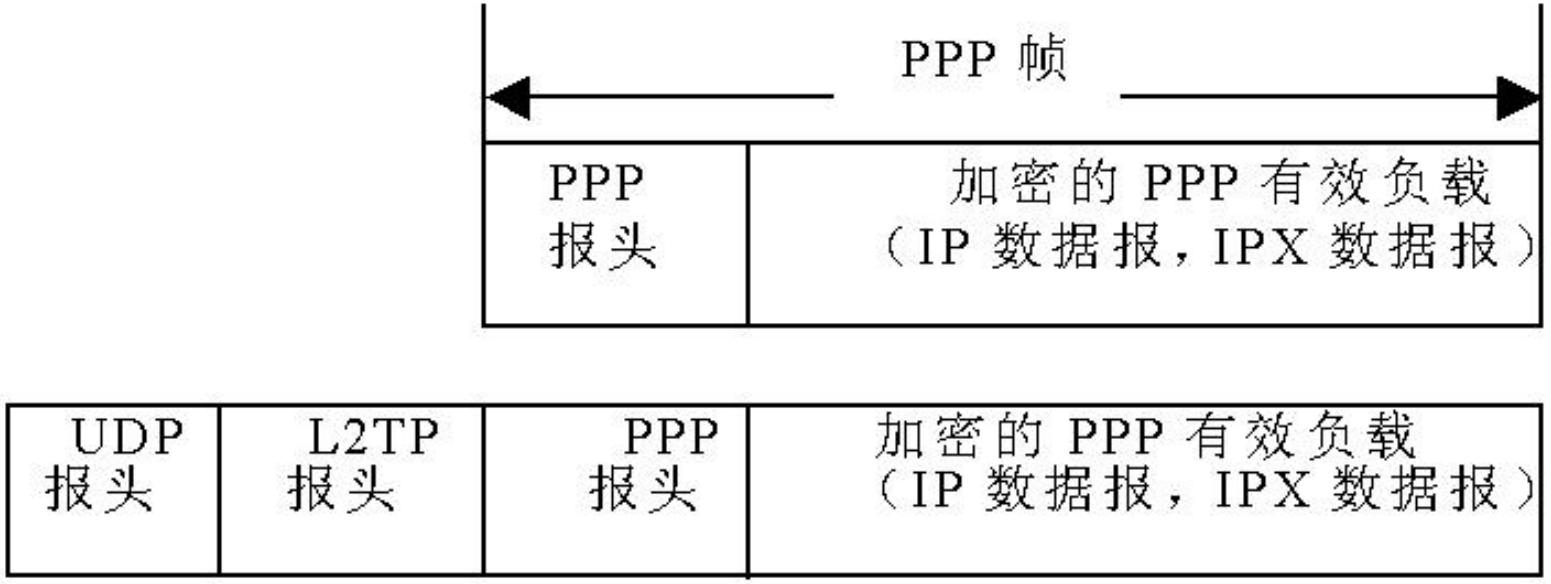
12.3 VPN使用的协议与实现

- L2TP
  - 支持多种协议，用户可以保留原有的IPX、Appletalk等协议或公司原有的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)



12.3 VPN使用的协议与实现

- L2TP封装



12.3 VPN使用的协议与实现

- IPSec封装

UDP 报头	L2TP 报头	PPP 报头	加密的 PPP 有效负载（IP 数据报，IPX 数据报）

IP 报头	IPSec ESP 报头	UDP 报头	L2TP 报头	PPP 报头	加密的 PPP 有效负载（IP 数据报，IPX 数据报）	IPSec ESP 报尾	IPSec Auth 报尾

12.3 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，帧中继永久虚拟电路（PVCs）,X.25虚拟电路（VC）或ATMVC
  - 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
  - 压缩头的开销
    - PPTP/L2TP：6/4 byte

12.3 VPN使用的协议与实现

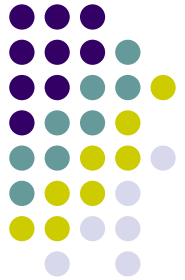
- IPSec协议
  - IPSec是IETF于1998年11月公布的第三层安全协议
  - 保护IP数据包或上层数据
  - 可以定义哪些数据流需要保护，怎样保护及应该将这些受保护的数据流转发给谁
  - 提供具有较强的互操作能力、高质量和基于密码的安全

12.3 VPN使用的协议与实现

- IPSec协议
  - 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

12.3 VPN使用的协议与实现

- IPSec协议
  - 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

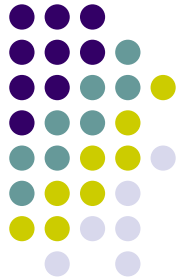


12.3 VPN使用的协议与实现

- IPSec协议
  - 验证(Authentication)
  - 完整性(Integrity)
  - 秘密性(Confidentiality)

12.3 VPN使用的协议与实现

- IPSec协议
  - 验证(Authentication)
    - 确保发送数据者的真实性
  - 完整性(Integrity)
  - 秘密性(Confidentiality)



12.3 VPN使用的协议与实现

- IPSec协议
  - 验证(Authentication)
  - 完整性(Integrity)
    - 确保数据在传输过程中没有被篡改
  - 秘密性(Confidentiality)

12.3 VPN使用的协议与实现

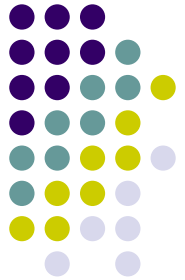
- IPSec协议
  - 验证(Authentication)
  - 完整性(Integrity)
  - 秘密性(Confidentiality)
    - 确保数据不被非法读取

12.3 VPN使用的协议与实现

- IPSec的保护技术
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)

12.3 VPN使用的协议与实现

- IPSec的保护技术
  - 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、高层的数据、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
  - Encapsulating Security Payload (ESP)



12.3 VPN使用的协议与实现

- IPSec的保护技术
  - Authentication Header (AH)
  - 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)

12.3 VPN使用的协议与实现

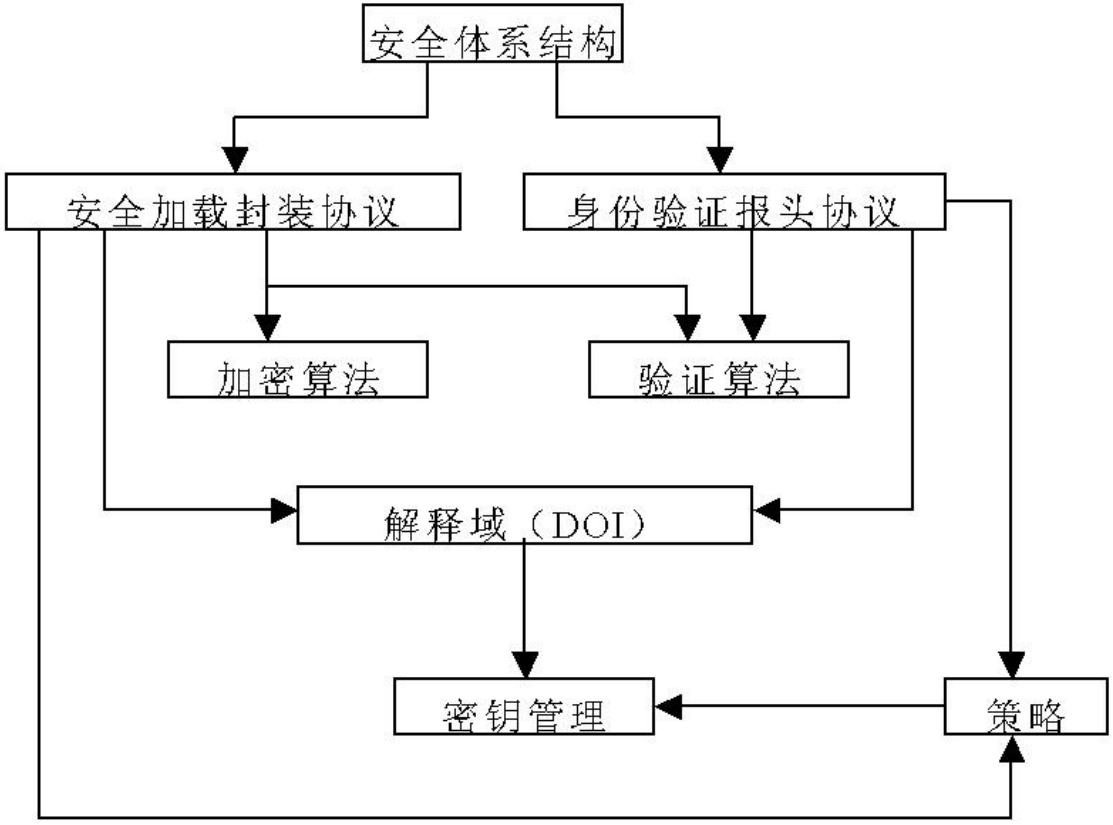
- IPSec的工作方式
  - Transmission mode
  - Tunnel mode

12.3 VPN使用的协议与实现

- IPSec的工作方式
  - Transmission mode
    - 传输方式是用来保护上层协议，仅对数据净荷进行加密，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

12.3 VPN使用的协议与实现

- IPSec的安全体系



第12章 VPN技术

- VPN概述
- VPN的分类
- VPN使用的协议与实现

第12章 VPN技术

- 课后习题
  - VPN的组成
  - 比较PPTP与L2TP
  - 简述IPSec中AH协议的功能
  - 简述IPSec中ESP协议的功能