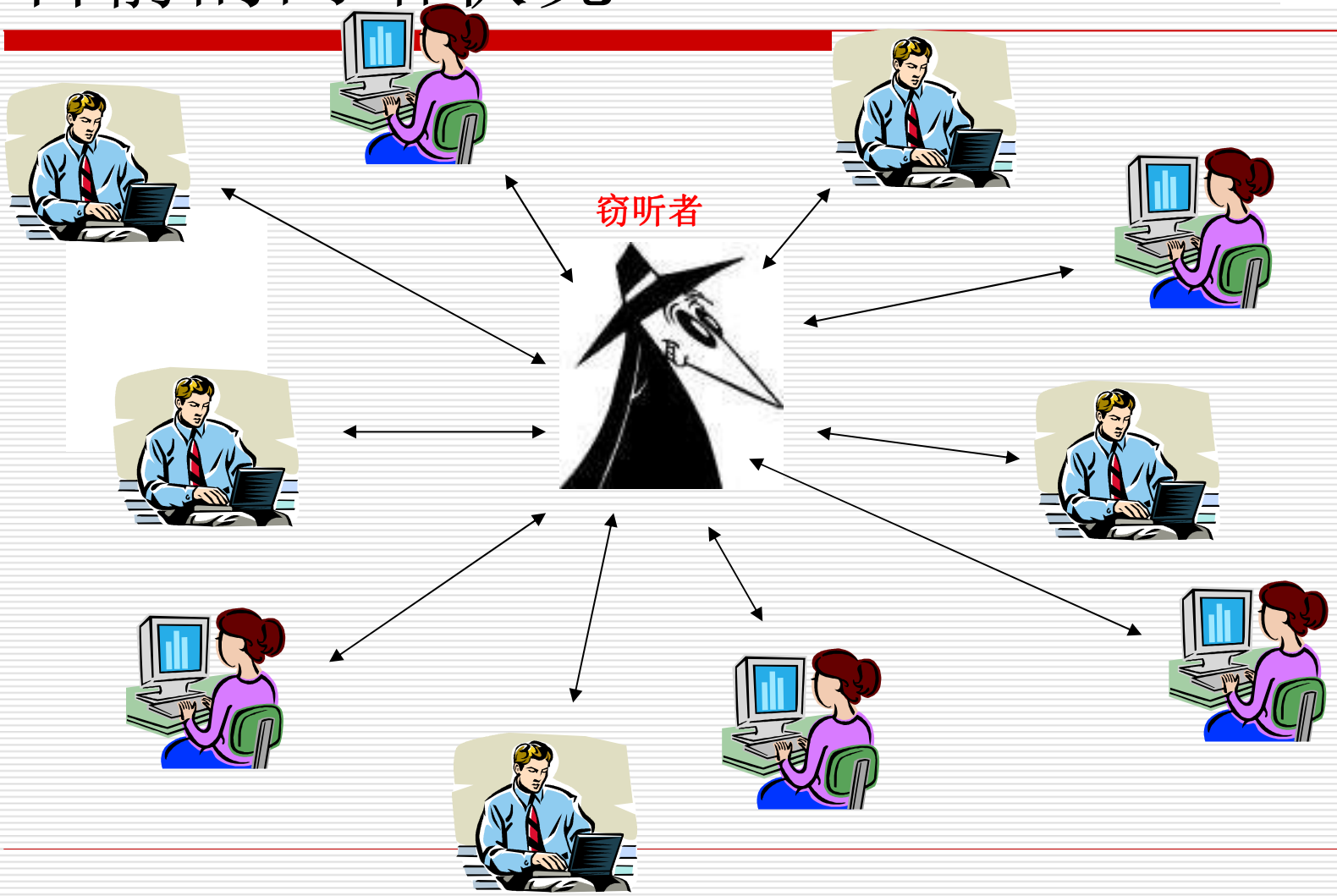
VPN的简单介绍

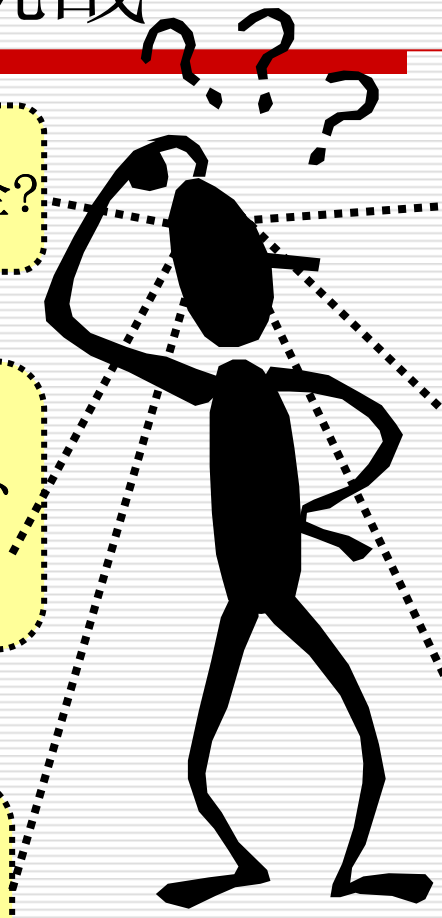
- Vpn的概念
- Vpn的优势
- Vpn的功能
- Vpn的实现方式
- Vpn的应用

http://hi.baidu.com/drkevinzhang/

目前的网络状况



用户面临的挑战



如何保证公司网络资源的安全?

如何面对**Internet**通信的增加、新的应用服务和减少成本？

如何共享和保护通过**Internet**的信息**?**

如何在合作伙伴之间布置一个灵活和模块化的解决方案？

如何有效的管理这一切？

谁能提供这一切满足未来的需要？

传统远程通信连接方式

企业总部

外地分公司

租用专用线路

帧中继

ATM

客户及供应商

外地出差员工

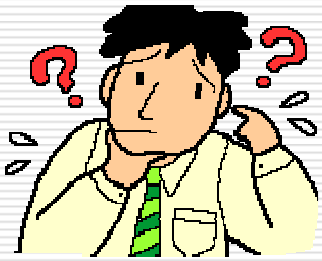
当地电信局

专用网络的优点

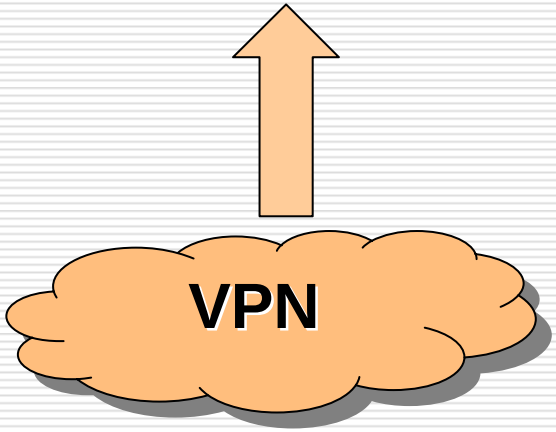
- 信息被保留“在文件夹里”
- 远程站点可以立即交换信息
- 远程用户没有隔离感

专用网络的缺点

- 成本太高，不经济
- 超出预算，不现实



$ $



使用VPN解决方案的优势

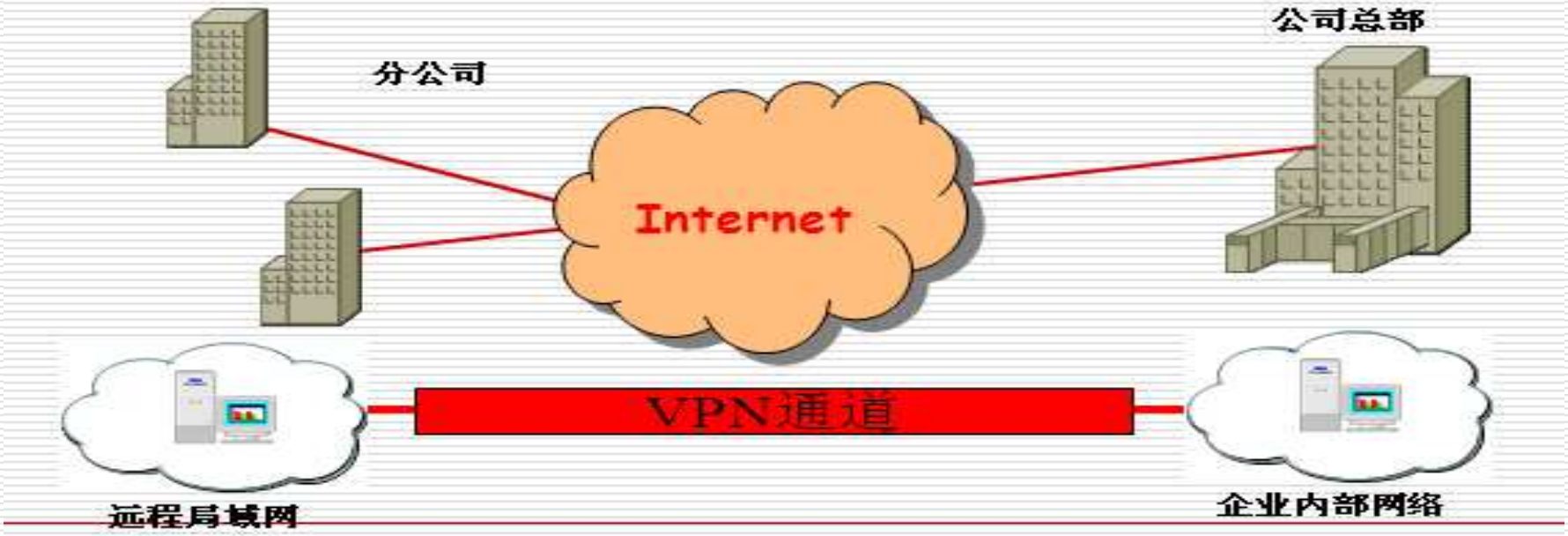
- 防止数据在公网传输中被窃听
- 防止数据在公网传输中被篡改
- 可以验证数据的真实来源
- 成本低廉（相对于专线、长途拨号）
- 应用灵活、可扩展性好

什么是vpn

- **VPN**的英文全称是“**Virtual Private Network**”，翻译过来就是“虚拟专用网络”。顾名思义，虚拟专用网络可以把它理解成是虚拟出来的企业内部专线。

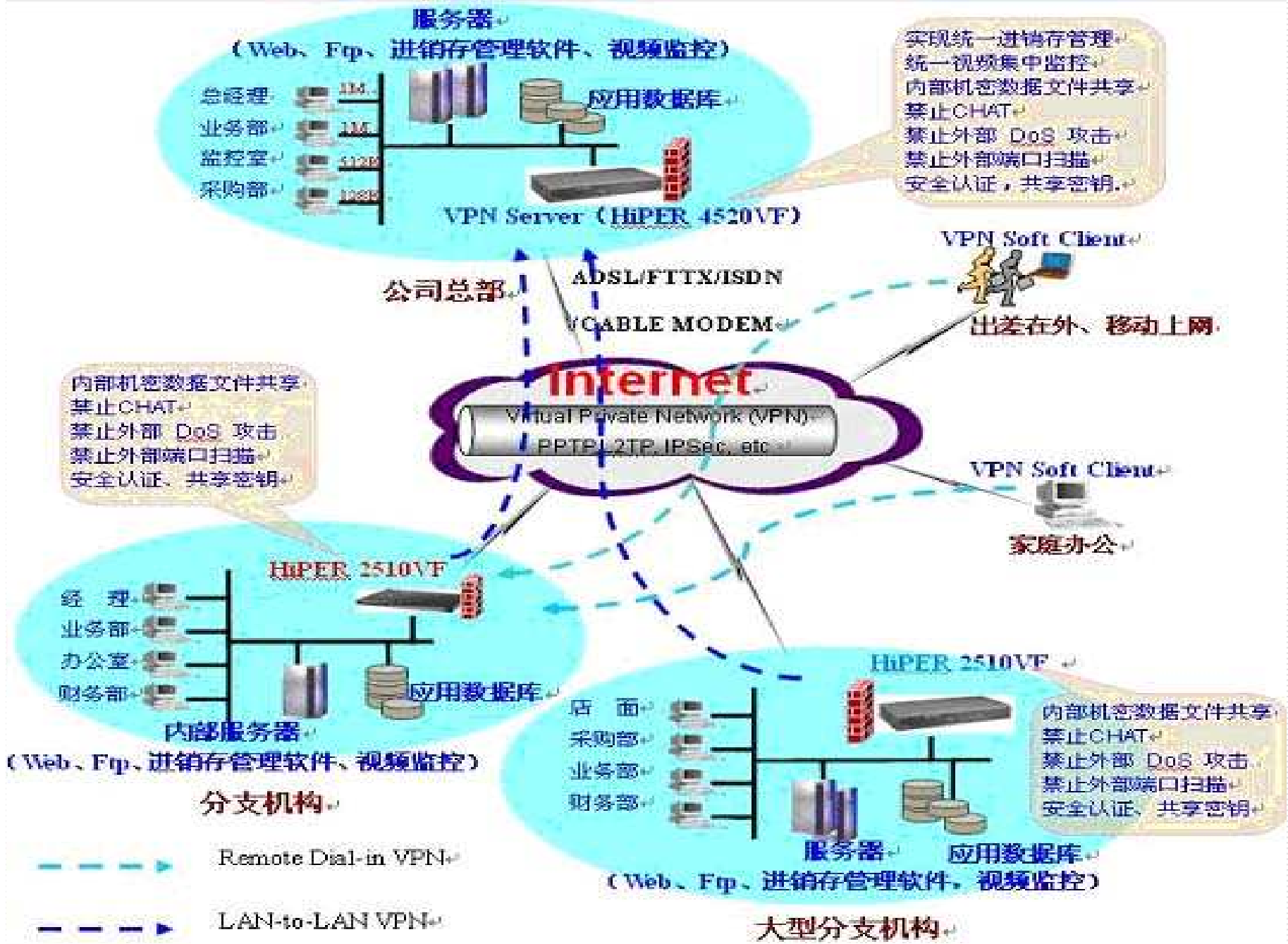
Vpn的定义

- 虚拟专用网（vpn）被定义为通过一个公用网络（通常是因特网）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。



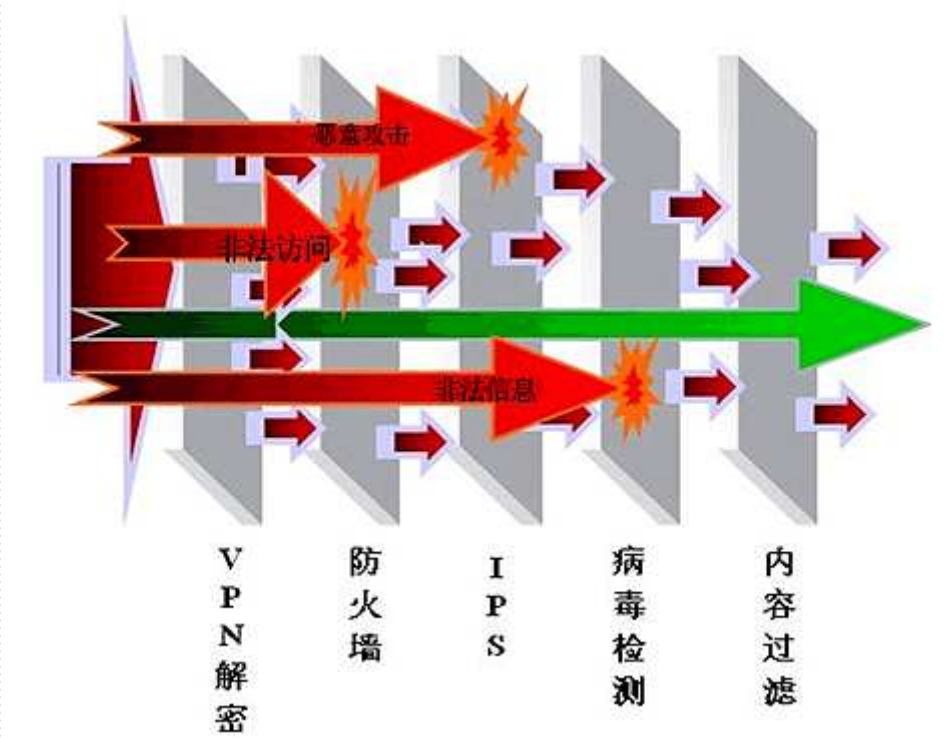
VPN的优势

- 保证安全
- 降低成本
- 便于扩充和管理
- 灵活的与合作商联网


服务器
（Web、Ftp、进销存管理软件、视频监控）
总经理
业务部
监控室
采购部
应用数据库
VPN Server（HiPER 4520VF）
实现统一进销存管理
统一视频集中监控
内部机密数据文件共享
禁止CHAT
禁止外部 DoS 攻击
禁止外部端口扫描
安全认证，共享密钥。
VPN Soft Client
出差在外、移动上网
公司总部
ADSL/FTTX/ISDN
CABLE MODEM
Internet
Virtual Private Network (VPN)
PPTP/L2TP, IPSec, etc
内部机密数据文件共享
禁止CHAT
禁止外部 DoS 攻击
禁止外部端口扫描
安全认证、共享密钥
VPN Soft Client
家庭办公
HiPER 2510VF
经 理
业务部
办公室
财务部
应用数据库
内部服务器
（Web、Ftp、进销存管理软件、视频监控）
分支机构
HiPER 2510VF
店 面
采购部
业务部
财务部
内部机密数据文件共享
禁止CHAT
禁止外部 DoS 攻击
禁止外部端口扫描
安全认证、共享密钥
服务器
应用数据库
（Web、Ftp、进销存管理软件、视频监控）
大型分支机构
Remote Dial-in VPN
LAN-to-LAN VPN

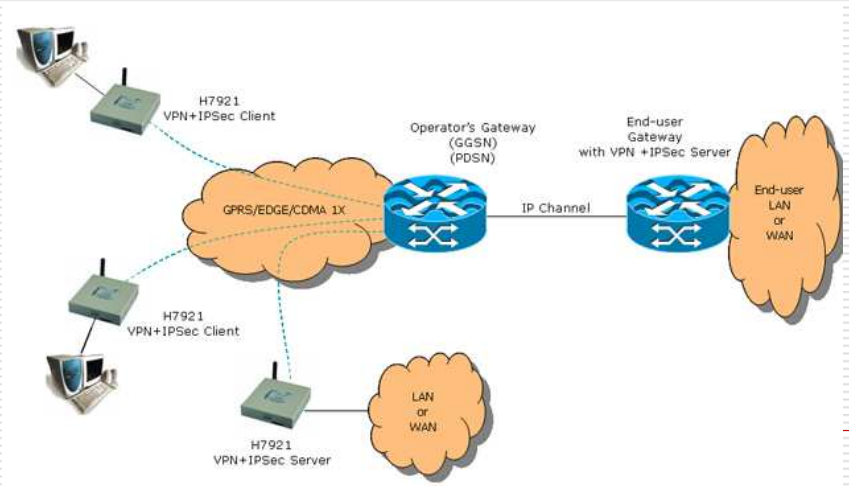
Vpn的功能

- 防火墙功能
- 认证
- 加密
- 隧道化



Vpn的实现方式

- 在路由器上实现
- 在防火墙上实现
- 在操作系统上实现
- 使用独立的加密设备实现



使用到的安全保证技术

- 隧道技术
- 加解密技术
- 密钥管理技术
- 使用者与设备身份认证技术

Vpn的应用（一）

- 远程访问vpn

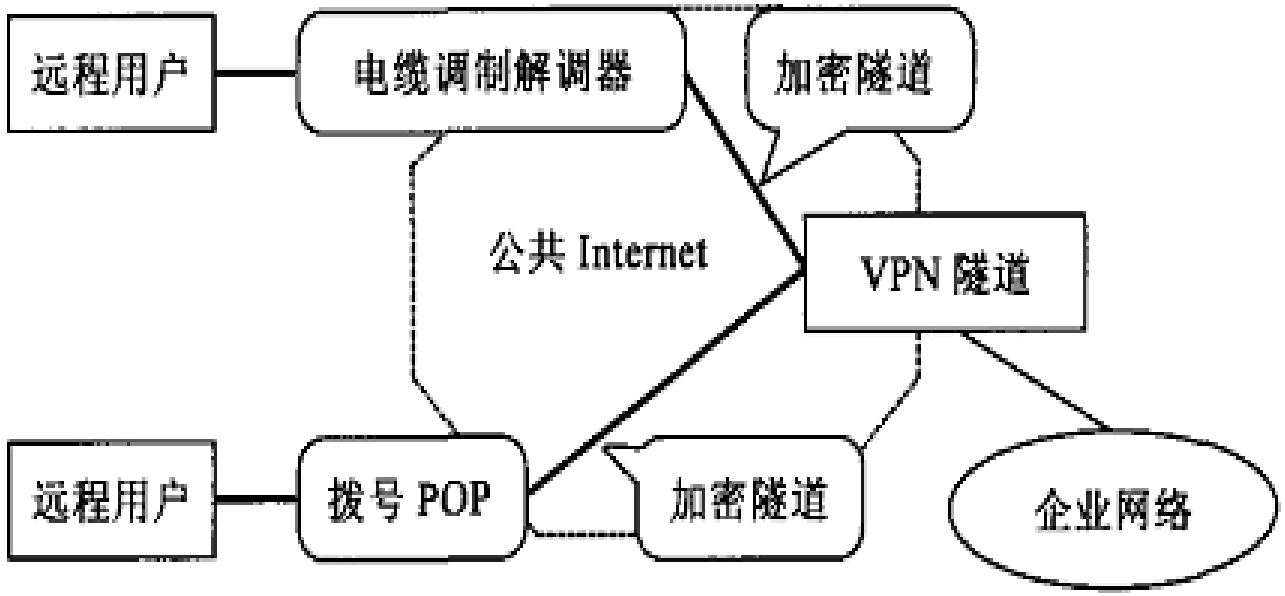


图 3　远程访问 VPN 的体系结构

Vpn的应用（二）

- 站点到站点的内联网

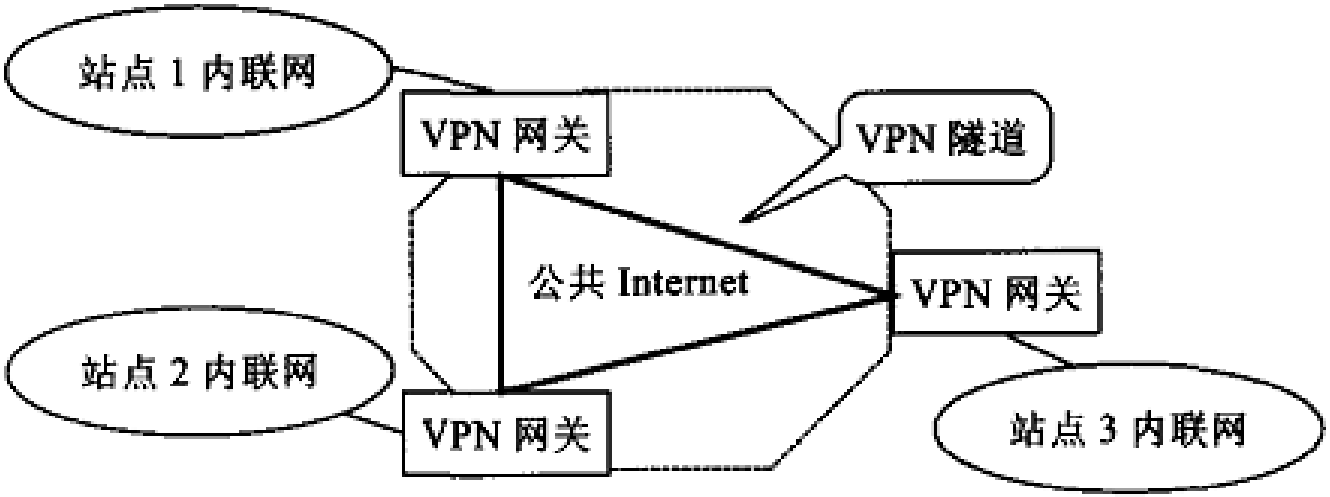


图 4　站点到站点的内联网 VPN 的体系结构

Vpn的应用（三）

- 外联网vpn

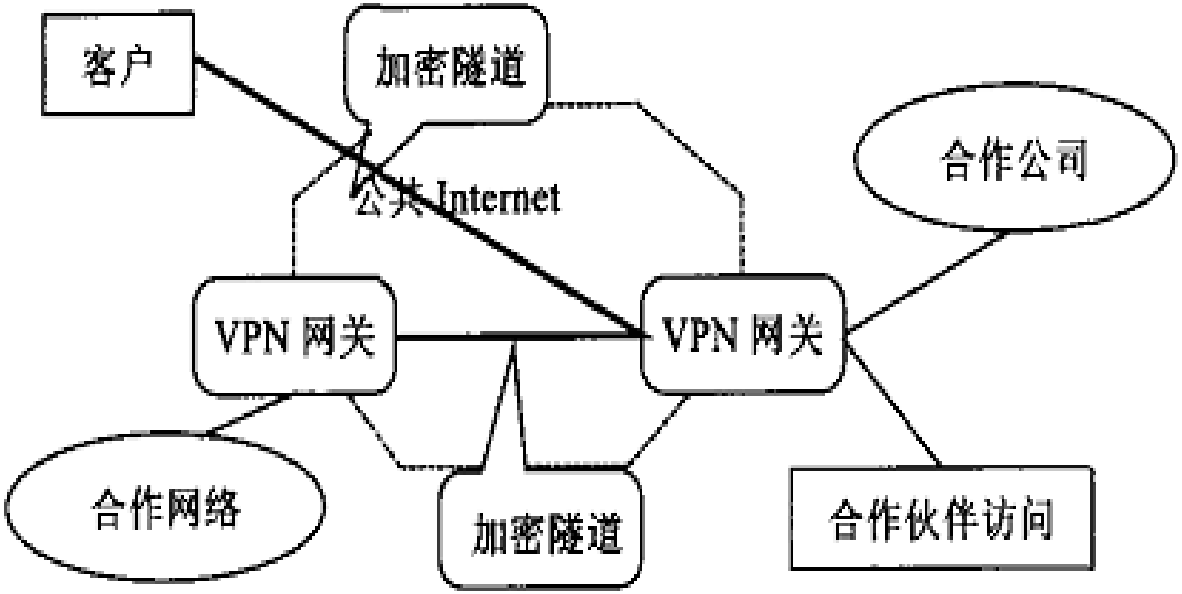
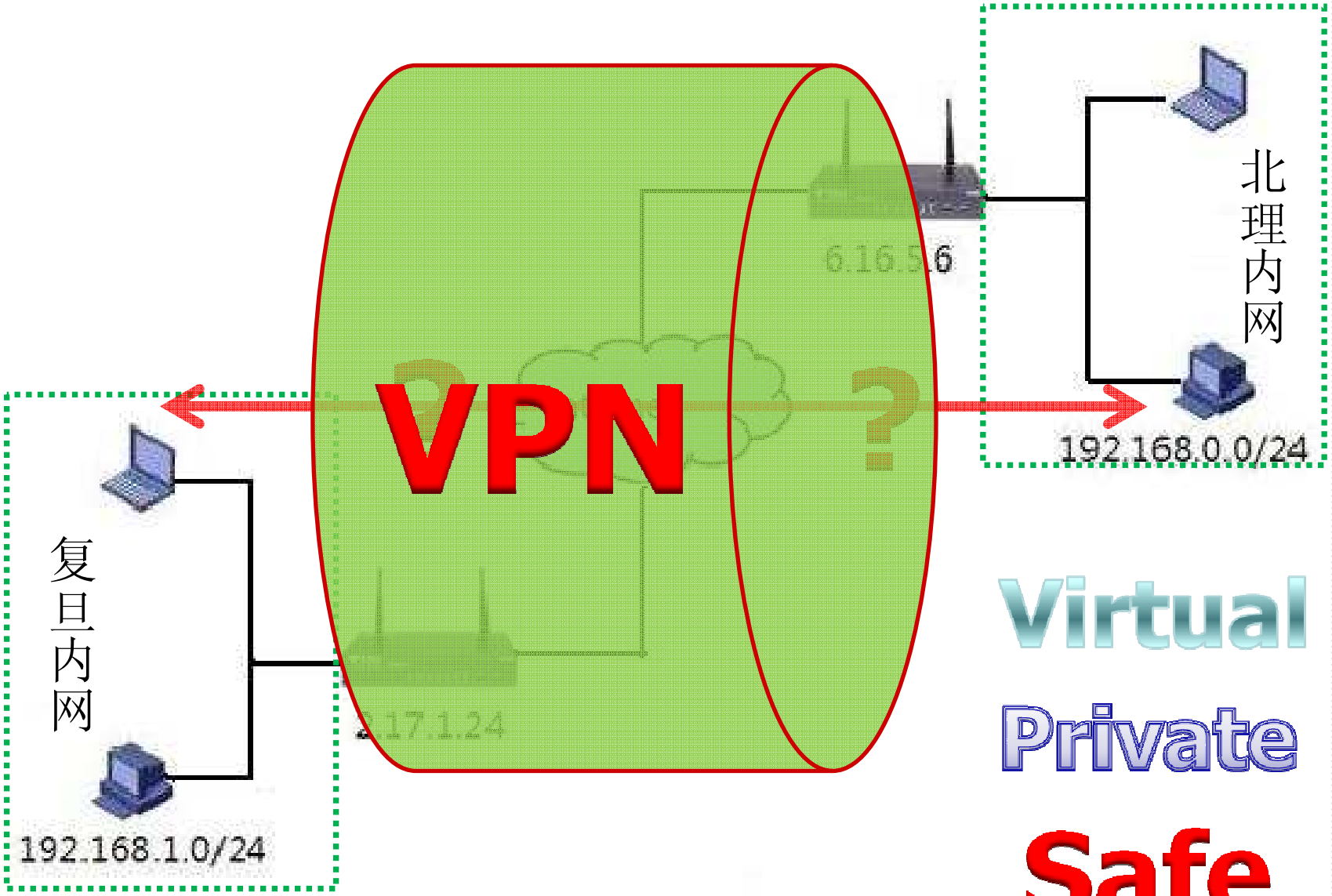


图 5　外部网络 VPN 的体系结构

虚拟专用网络（**VPN**）技术

- VPN分类简述
- VPN隧道协议
- L2TP案例
- IPSEC协议详解
- IPSEC+VPDN案例


北理内网
192.168.0.0/24
VPN
复旦内网
192.168.1.0/24
Virtual
Private
Safe

VPN分类简述

- 按VPN的发起方式划分
- 按VPN的服务类型划分
- 按承载主体划分
- 按接入方式划分

  专线VPN、拨号VPN
- 按协议实现类型划分

  第二层隧道协议、第三层隧道协议

VPN的隧道协议

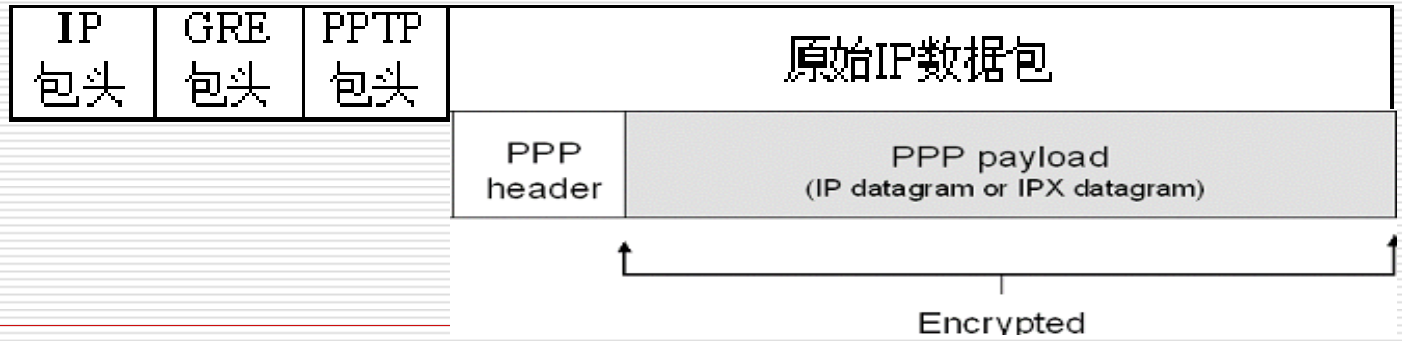
- 第二层隧道协议：点到点隧道协议（PPTP）、第二层转发协议（L2F），第二层隧道协议（L2TP）、多协议标记交换（MPLS）等。
- 第三层隧道协议：通用路由封装协议（GRE）、IP安全（IPSec）

其中GRE、IPSec和MPLS主要用于实现专线VPN业务，PPTP、L2TP主要用于实现拨号VPN业务

VPN的隧道协议(续)

1．点到点隧道协议（PPTP）

- Point to Point Tunneling Protocol
- PPTP使用TCP进行隧的创建，维护，与终止道
  - 使用GRE(通用路由封装)将PPP帧封装成隧道数据。
  - PPTP没有加密、认证等安全措施，直接使用PPP的加密、认证方案。

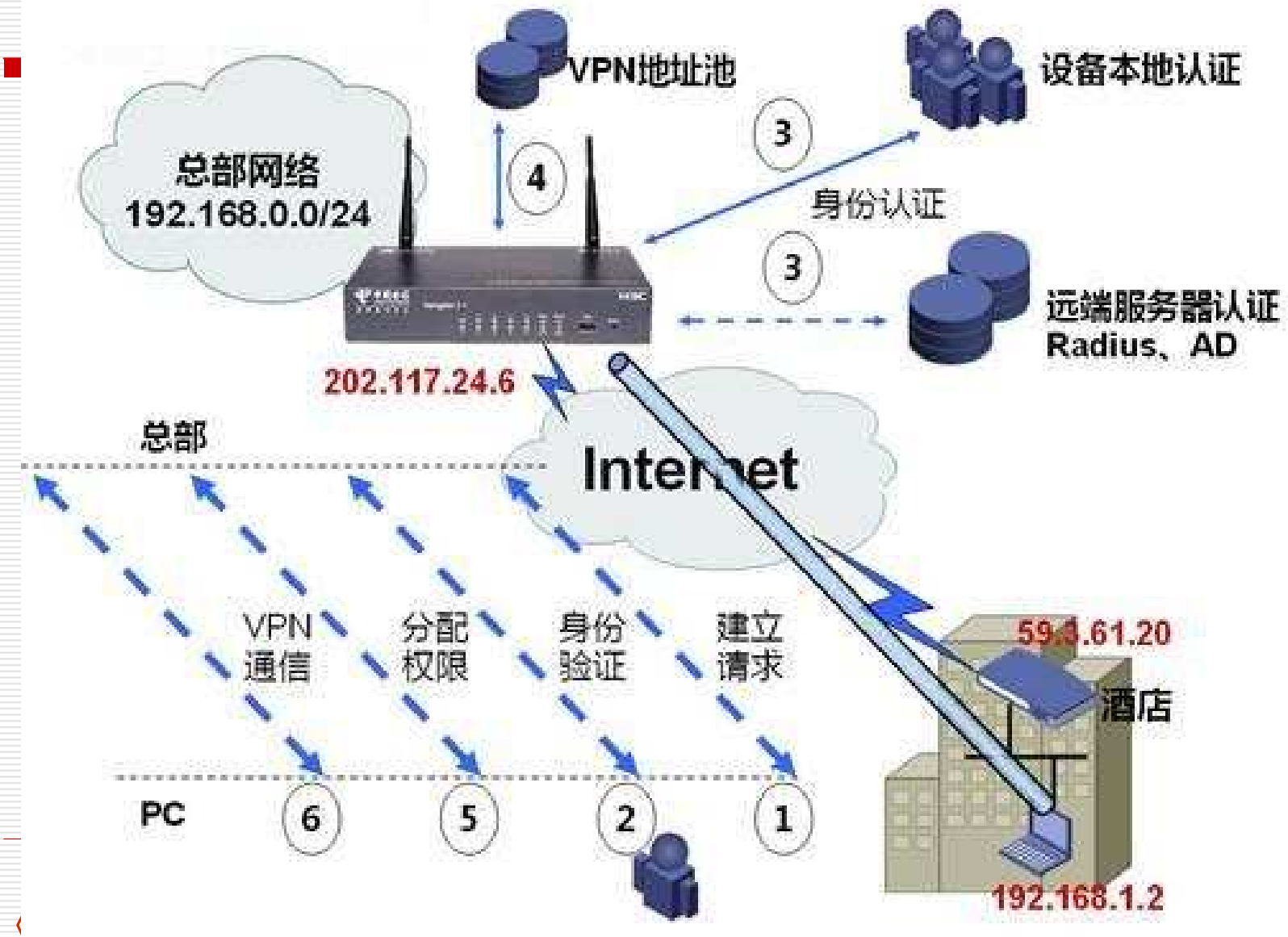


VPN的隧道协议(续)

2．第二层隧道协议（L2TP）

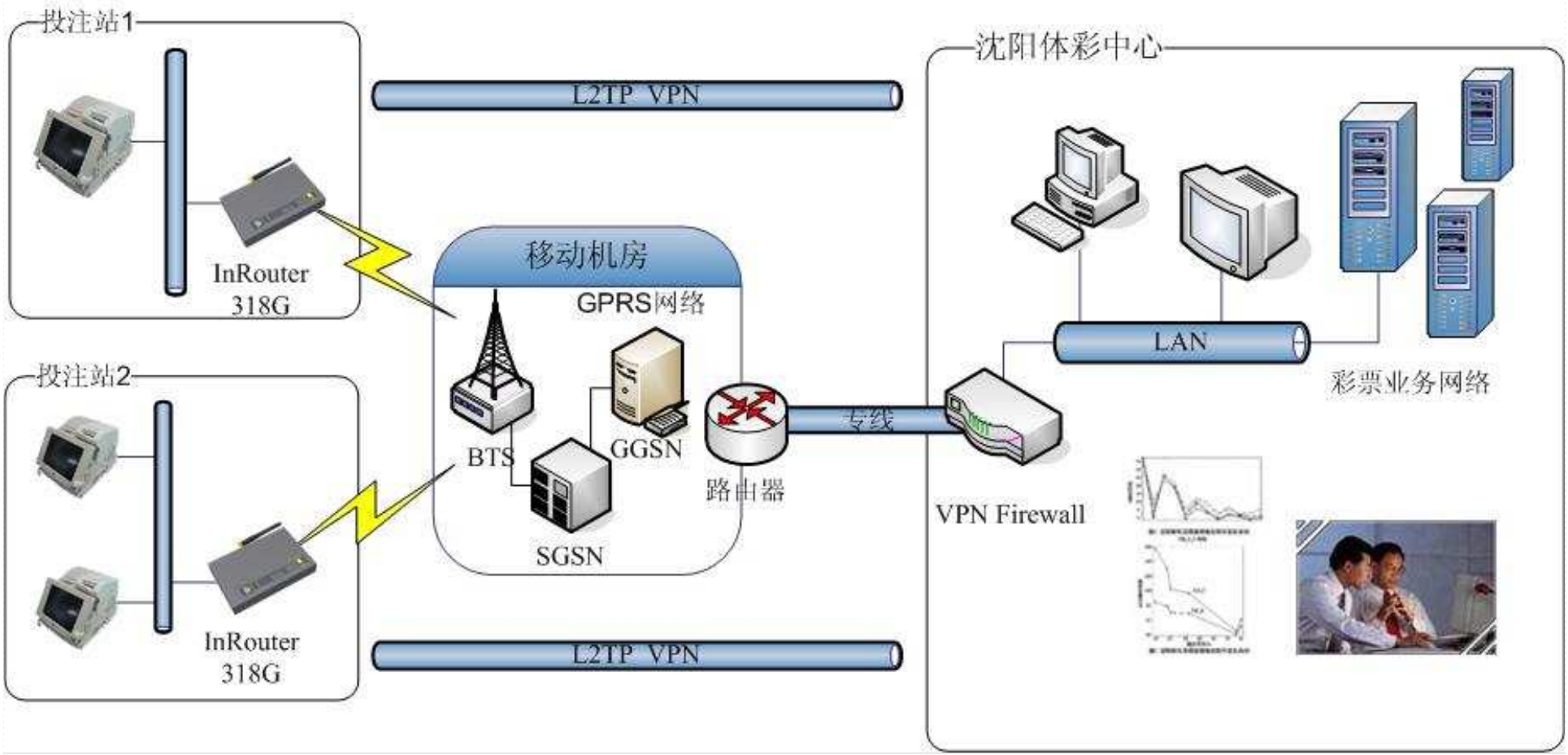
- Layer 2 Tunneling Protocol
- 在L2F和PPTP的基础上开发
- L2F (Layer Two Forwarding)，可以在多种介质如ATM、帧中继、IP网上建立VPN。
- 提供隧道验证，加密方案采用与IPSec结合

L2TP VPN通信过程



L2TP案例

沈阳体育彩票项目网络结构图



采用无线方式的优点

1、更加灵活的配置彩票机，扩大彩票服务的应用范围

2、传送速率较高，传输容量满足要求

3、具有竞争力的性能价格比

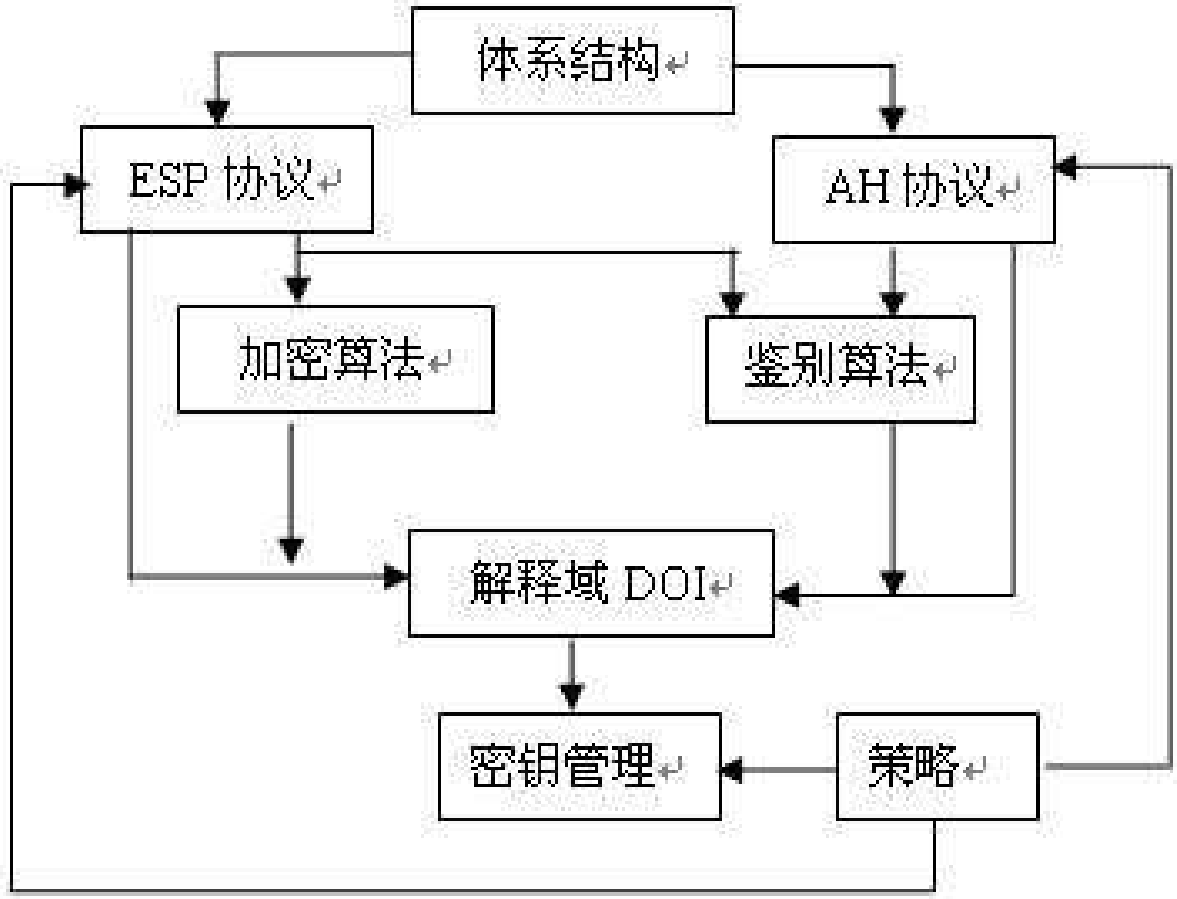
4、部署灵活快速，突出移动性能

5、减少网络建设和维护成本

IPSec协议详解

- IP security
- 第三层安全协议，仅仅传输IP协议数据包
- 提供VPN功能
- 提供强大的安全、认证、加密和密钥管理功能
- 适合大规模VPN使用

IPSec安全体系结构



IPSec的三个主要协议

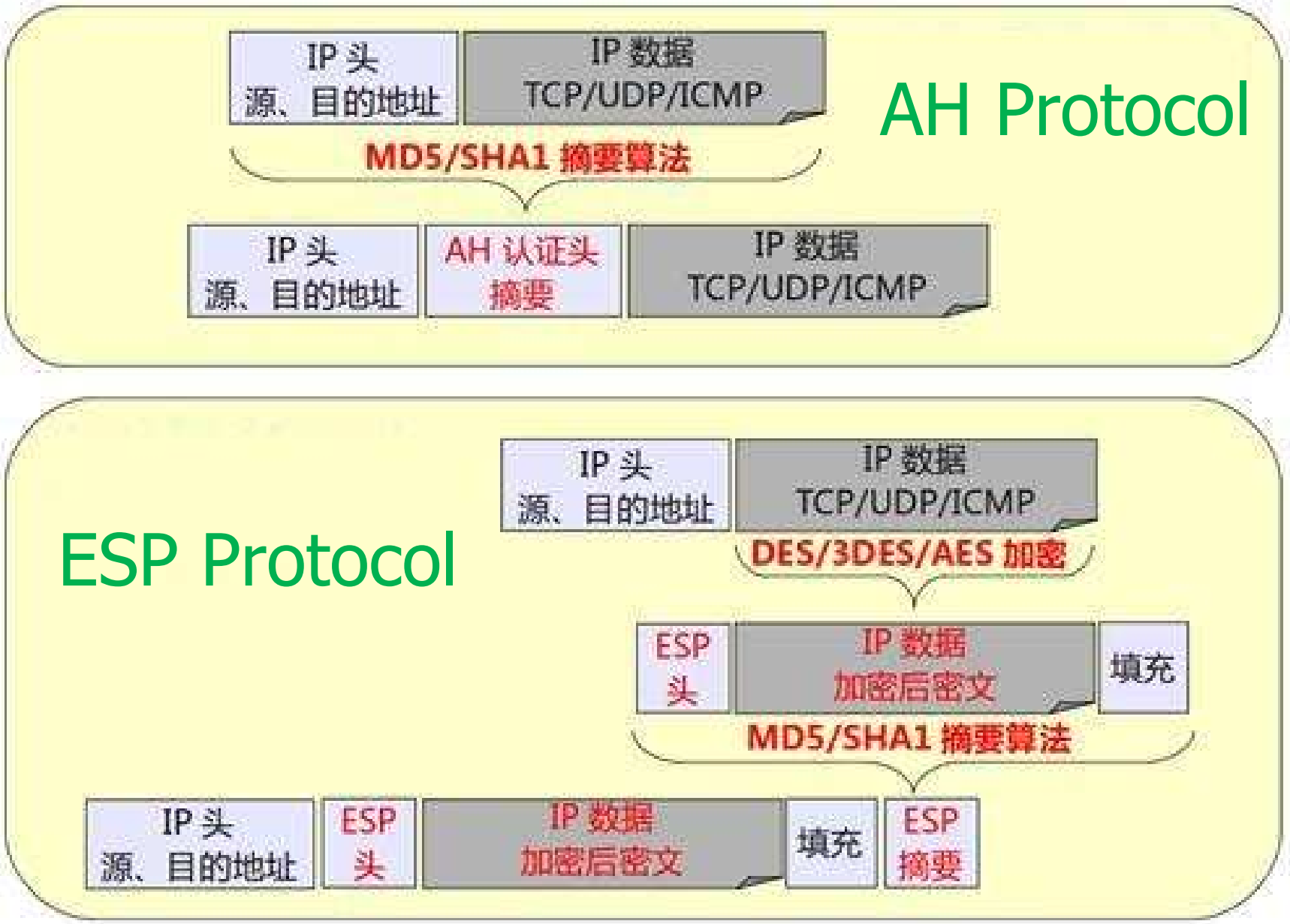
AH(Authentication Header)

ESP（Encapsulating Security Payload)

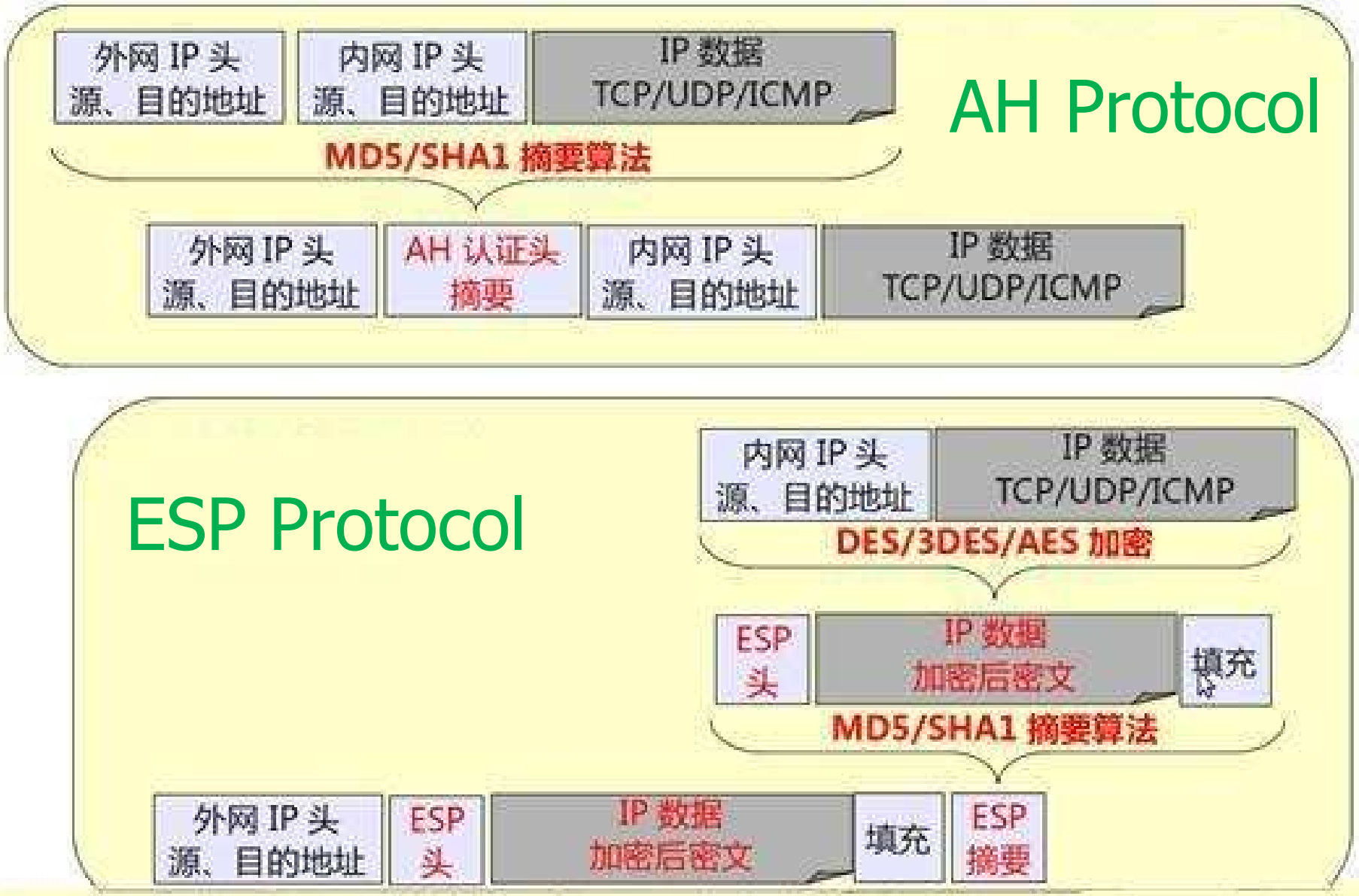
IKE(Internet Key Exchange)

SA(Security Association)

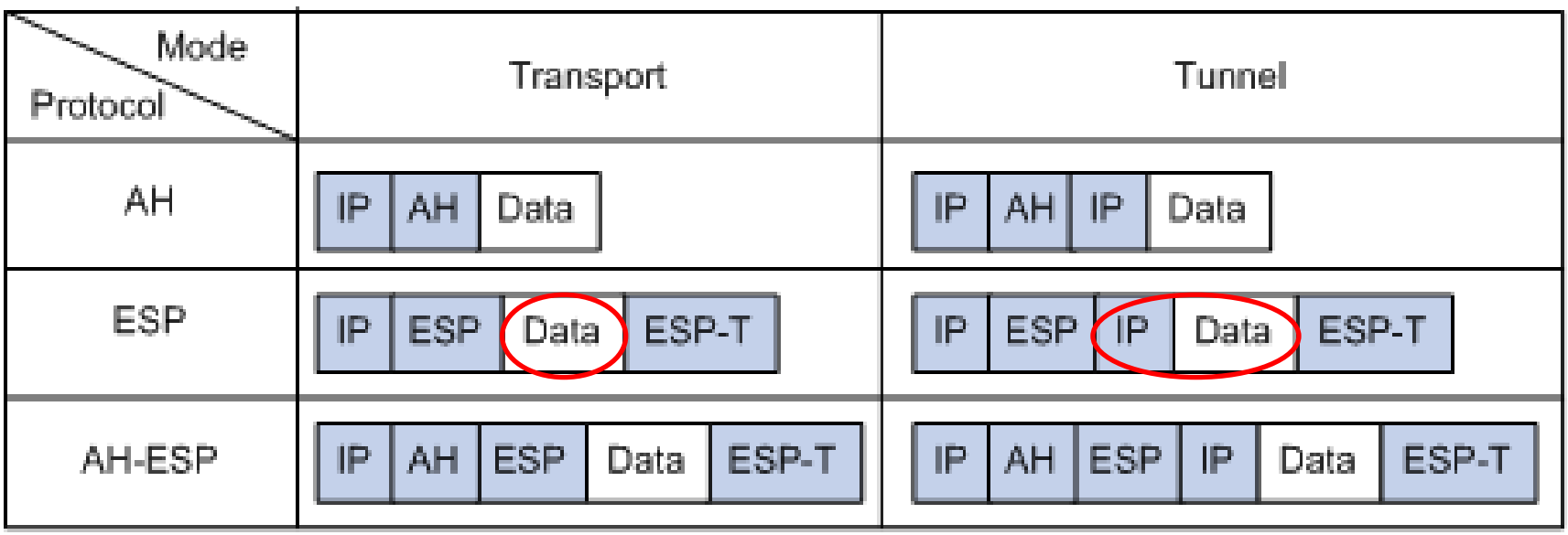
IPSec 的两种应用方式——传输模式



IPSec 的两种应用方式——隧道模式

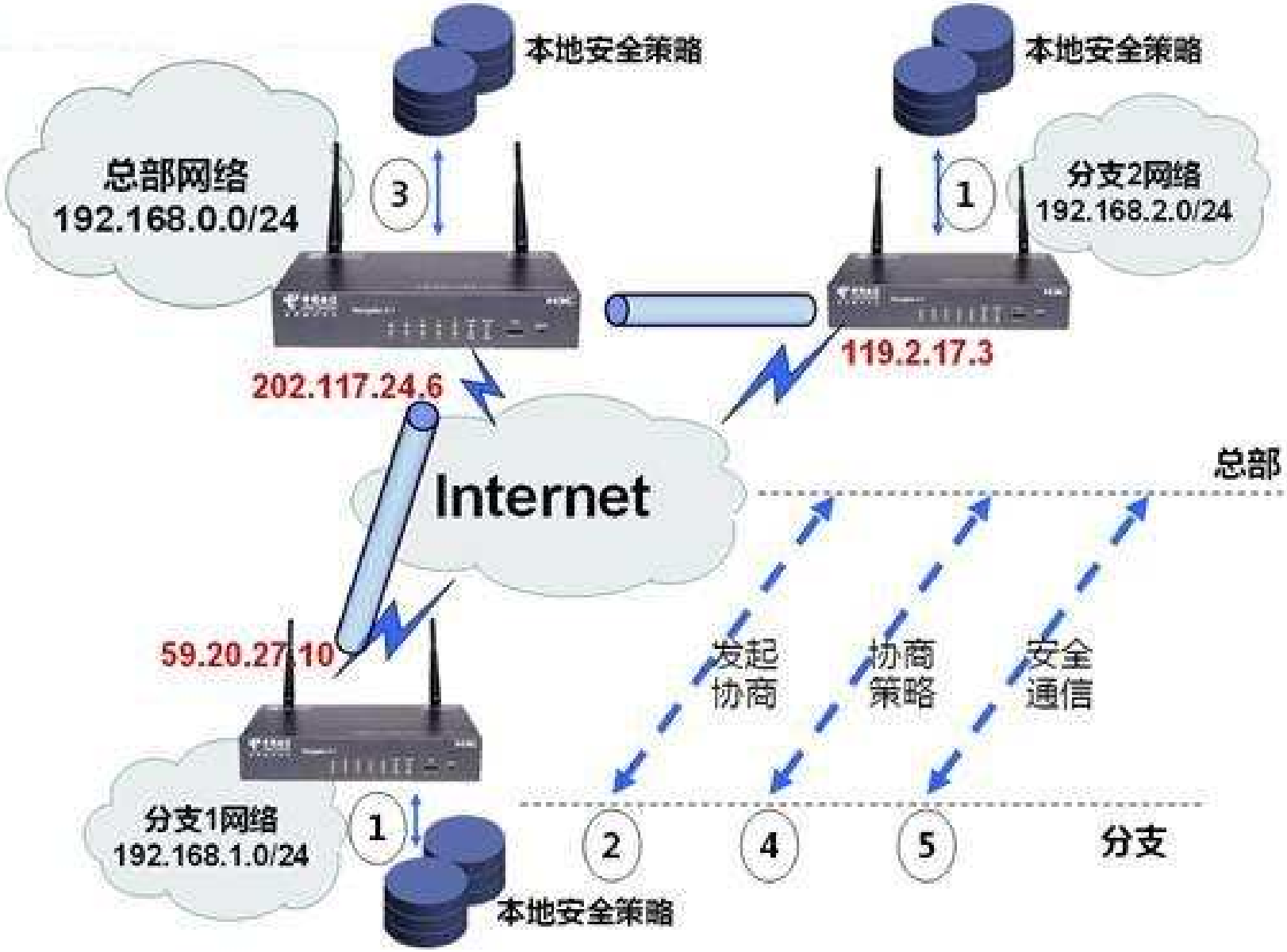


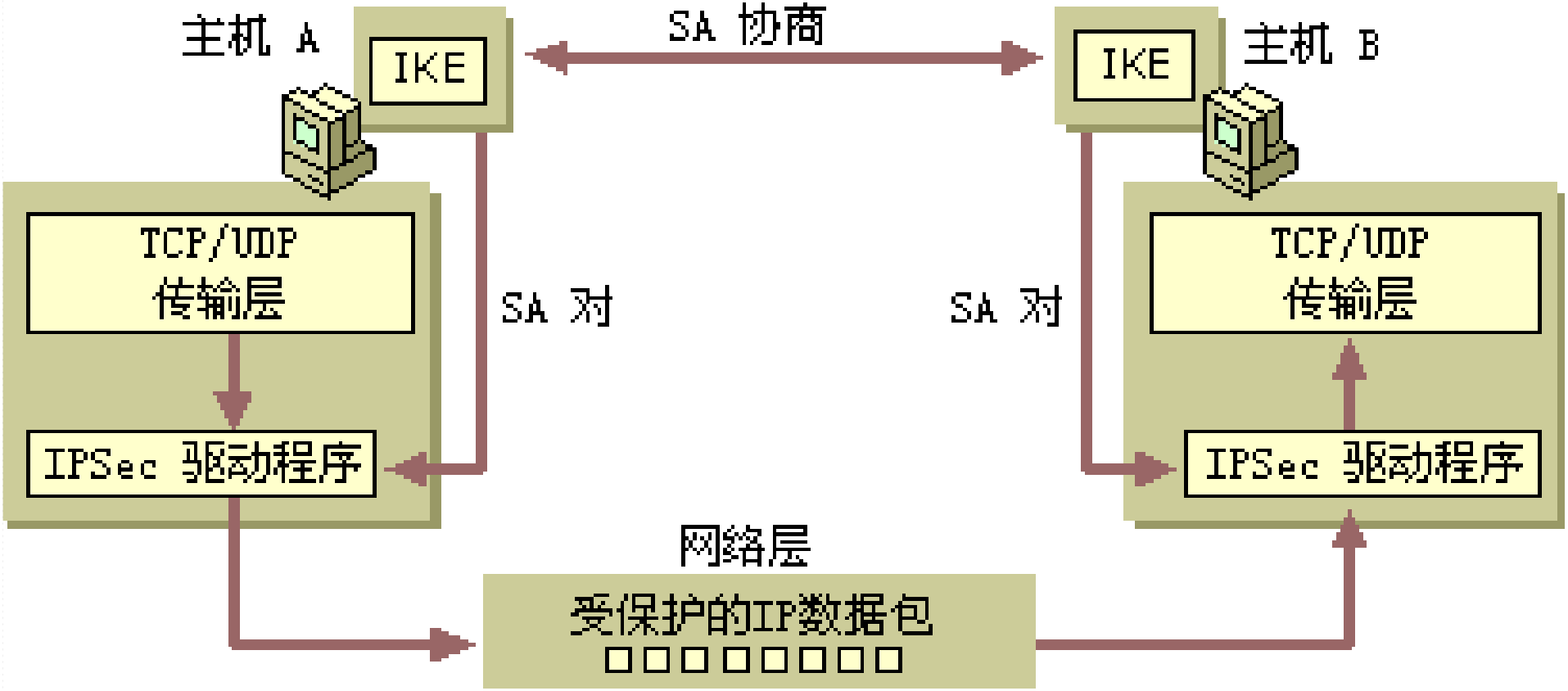
IPSec协议格式



- AH协议只有AH抱头
- ESP协议用一个ESP报头和一个ESP报尾来围绕原始的IP数据包,报文的末端增加了一个ESP认证报尾

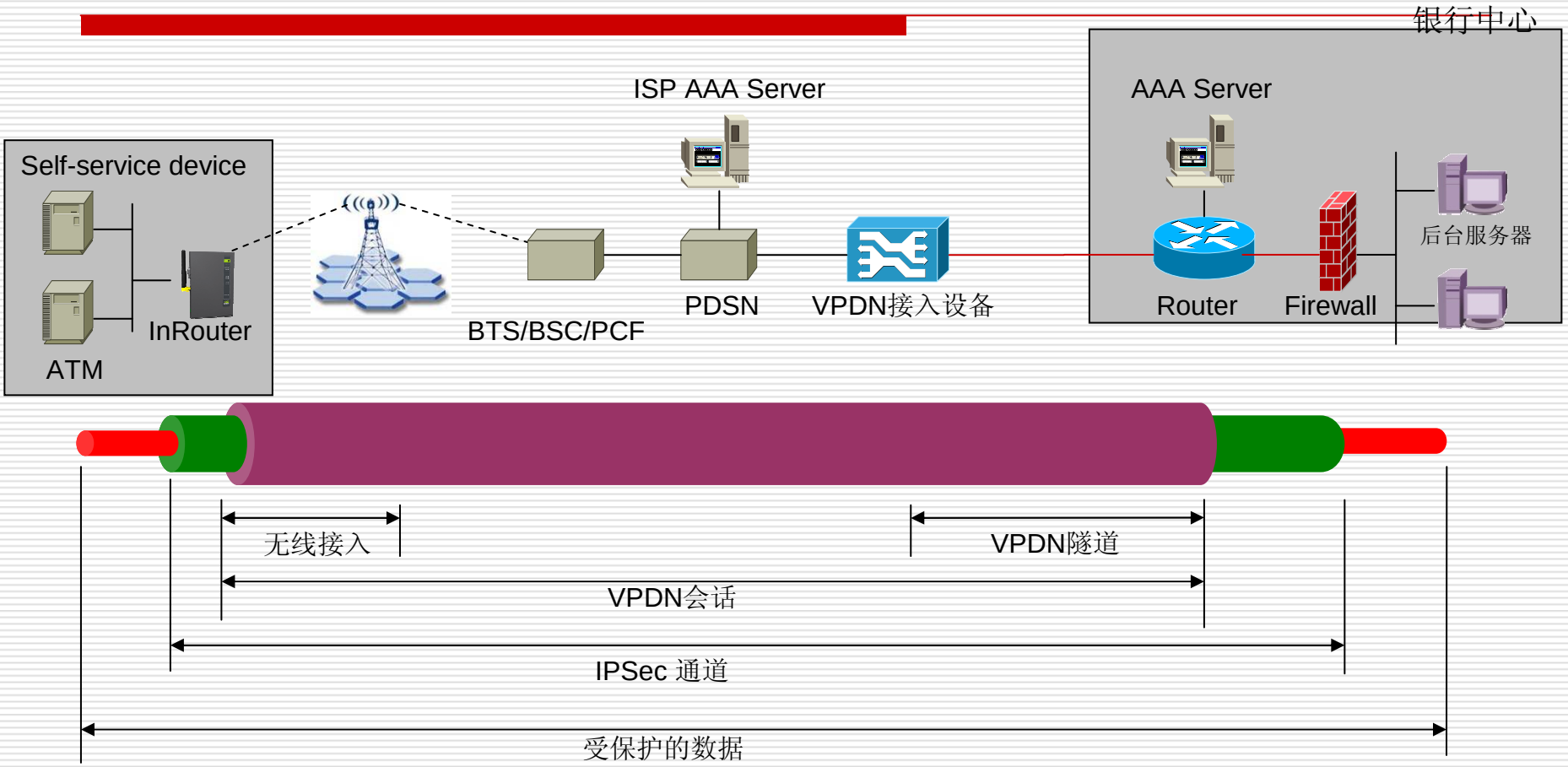
IPSec VPN通信过程




主机 A
IKE
SA 协商
IKE
主机 B
TCP/UDP
传输层
SA 对
SA 对
TCP/UDP
传输层
IPSec 驱动程序
IPSec 驱动程序
网络层
受保护的IP数据包

IPSec应用案例

银行项目 （VPDN + IPSec）



银行ATM采用 VPDN + IPSec 无线方式优点

1、更加灵活地配置ATM设备，扩大刷卡服务范围

2、配置简单快捷，方式灵活

3、传输容量和速率高，能够满足ATM数据量的要求

4、高安全性，强伸缩性；

5、性能价格比高，较有线通信价格低廉

6、减少网络建设成本，缩短建设周期

7、使银行业务在激烈的市场经济中更具竞争力


MashiMaro
www.mashimaro.co.kr
恳请老师同学点评！
Contact
Email: kevinzhang@bit.edu.cn
Welcome to visit my blog
http://hi.baidu.com/drkevinzhang/
Copyright © 2001 CLKO Entertainment Co.,Ltd. All rights reserved. Produced by Entermedia