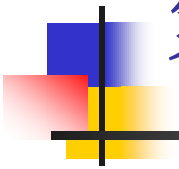
第6章　虚拟专用网（VPN）技术

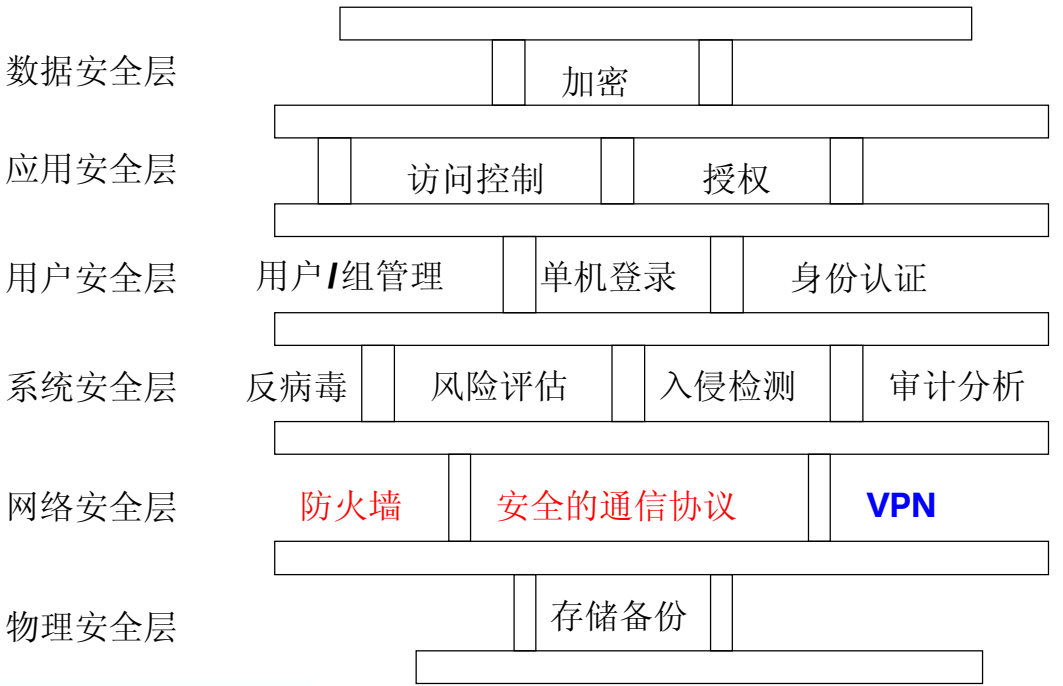


6.1　VPN的基本概念
6.2　VPN安全隧道技术
6.3　链路层VPN的实现
6.4　基于IPSec协议的VPN
6.5　应用层VPN的实现

网络与信息安全的构成

- 物理安全性
  - 设备的物理安全：防火、防盗、防破坏等
- 通信网络安全性
  - 防止入侵和信息泄露
- 系统安全性
  - 计算机系统不被入侵和破坏
- 用户访问安全性
  - 通过身份鉴别和访问控制，阻止资源被非法用户访问
- 数据安全性
  - 数据的完整、可用
- 数据保密性
  - 信息的加密存储和传输

安全的分层结构和主要技术



6.1 VPN的基本概念

- 在传统的企业网络配置中，要进行远程访问，传统的方法是租用DDN（数字数据网）专线或帧中继，这样的通讯方案必然导致高昂的网络通讯和维护费用。
- 对于移动用户（移动办公人员）与远端个人用户而言，一般会通过拨号线路（Internet）进入企业的局域网，但这样必然带来安全上的隐患。

6.1 VPN的基本概念

- **VPN（Virtual Private Network)**
  - 虚拟专用网：在公用网络上建立专用网络，进行加密通讯，可通过服务器、硬件、软件等多种方式实现。
  - 虚拟出来的企业内部专线：通过特殊的加密的通讯协议在连接到**Internet**上的、位于不同地方的、两个或多个企业内部网之间建立一个临时的、安全的连接，是一条穿过公用网络的安全、稳定的隧道
  - 综合了专用和公用网络的优点，允许有多个站点的公司拥有一个假想的完全专有的网络，而使用公用网络作为其站点之间通信的线路

VPN的概念

- 虚拟
  - 任意两个节点之间并没有传统专网所需的物理连接；事实上，连接是使用公众网的资源动态搭建的
- 专用
  - 传输的数据的是保密的 (通过加密和安全隧道)
- 网络
  - 仿真出一个私有的广域网

为什么需要VPN

- 资源访问限制于某些IP地址
- 通过防火墙不能访问资源
- 内部人员需要在外面访问内部网
- 雇员可能在外地并需要访问网络
- 专有网太贵
- 外地的雇员也可能不是定点的
- 降低费用
- 增强的安全性，加密，透明

对VPN的需求

- 安全保障
  - VPN应保证通过公用网络平台传输数据的专用性和安全性
- 服务质量（QoS）保证
  - 对不同的用户提供不同的服务质量，如带宽、延时等保证，这取决于广域网上是否提供QoS保证
- 可扩充性和灵活性
  - 便于增加新的节点，支持多种类型的传输媒体
- 可管理性
  - 易于维护和管理

建立VPN所需的安全技术

- 隧道技术（Tunneling）
- 加解密技术（Encryption & Decryption）
  - 采用对称加密体制和公钥加密体制相结合的方法。
  - 常用的对称密码加密算法有：DES、3DES、RC4、RC5、IDEA、CAST5（Carlisle Adams and Stafford Tavares）等。
  - 常见的公钥体制有RSA、D-H和椭圆曲线等
- 密钥管理技术（Key Management）
  - SKIP基于一个D-H公钥密码体制数字证书
  - ISAKMP/OAKLEY协议（又称IKE），密钥交换协议。
- 认证技术（Authentication）
  - 用户名/口令或智能卡认证等方式
  - 一次性口令

VPN类型

- 按应用类型分类
  - **Access VPN**（远程接入**VPN**）：客户端到网关，通过**Internet**在设备之间传输**VPN**数据流量；
  - **Intranet VPN**（内联网**VPN**）：网关到网关，通过**Internet**连接来自同公司的资源，两个或多个**LAN**
  - **Extranet VPN**（外联网**VPN**）：与合作伙伴企业网构成**Extranet**，将一个公司与另一个公司的资源进行连接。
- 按实现的协议层次分类
  - 二层隧道**VPN**：**PPTP**和**L2TP OSI**模型第二层
  - 三层隧道**VPN**：**IPSec**
  - **SSL VPN**：**OpenVPN**

VPN类型

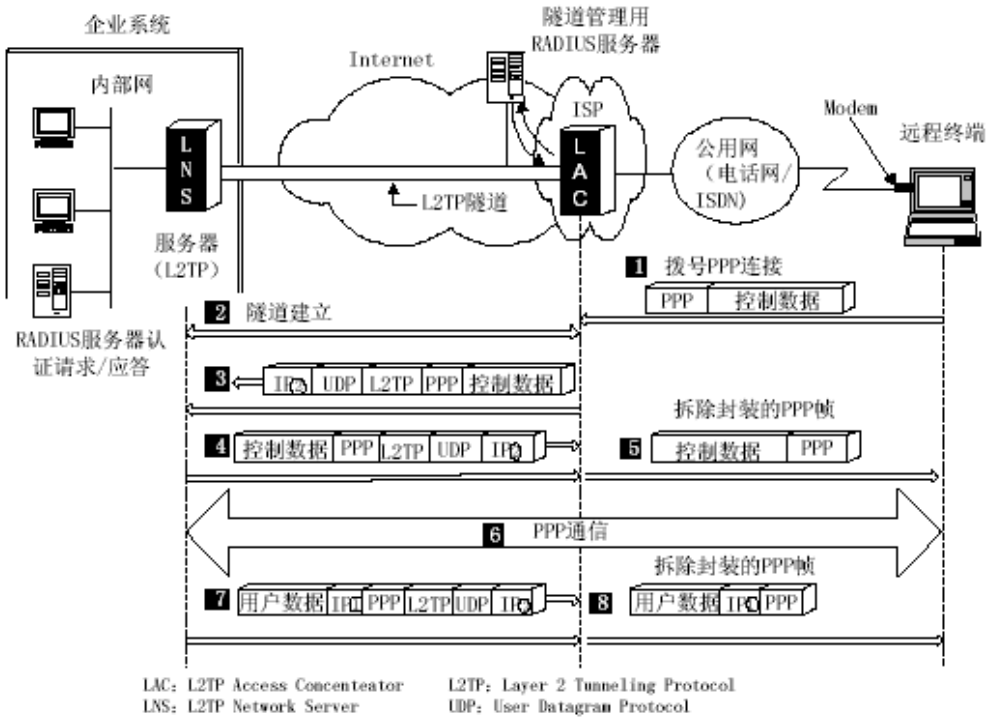
- 按所用的设备类型进行分类：

  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：

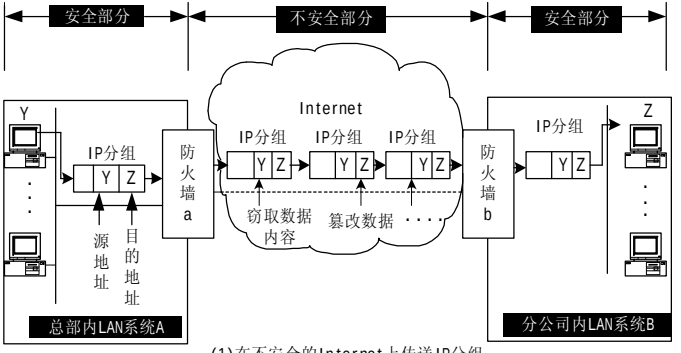
  - 路由器式VPN：路由器式VPN部署较容易，只要在路由器上添加VPN服务即可；
  - 交换机式VPN：主要应用于连接用户较少的VPN网络；
  - 防火墙式VPN：防火墙式VPN是最常见的一种VPN的实现方式，许多厂商都提供这种配置类型

  软件、硬件、软硬结合

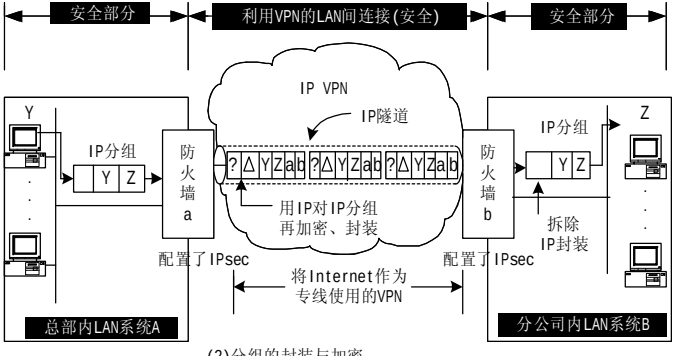
远程访问型VPN


企业系统
内部网
隧道管理用
RADIUS服务器
Internet
ISP
Modem
远程终端
公用网
（电话网/
ISDN）
L
N
S
L
A
C
L2TP隧道
服务器
（L2TP）
RADIUS服务器认
证请求/应答
1 拨号PPP连接
PPP 控制数据
2 隧道建立
3 IP UDP L2TP PPP 控制数据
拆除封装的PPP帧
4 控制数据 PPP L2TP UDP IP
5 控制数据 PPP
6 PPP通信
拆除封装的PPP帧
7 用户数据 IP PPP L2TP UDP IP
8 用户数据 IP PPP
LAC：L2TP Access Concenteator
LNS：L2TP Network Server
L2TP：Layer 2 Tunneling Protocol
UDP：User Datagram Protocol

LAN间互连型VPN

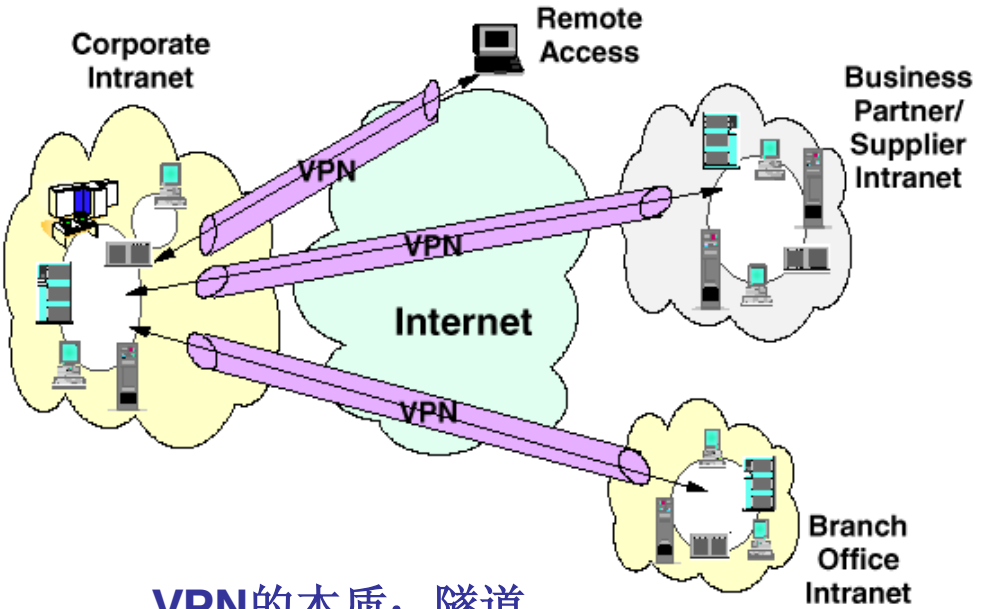


(1)在不安全的Internet上传送IP分组



(2)分组的封装与加密

6.2 VPN安全隧道技术

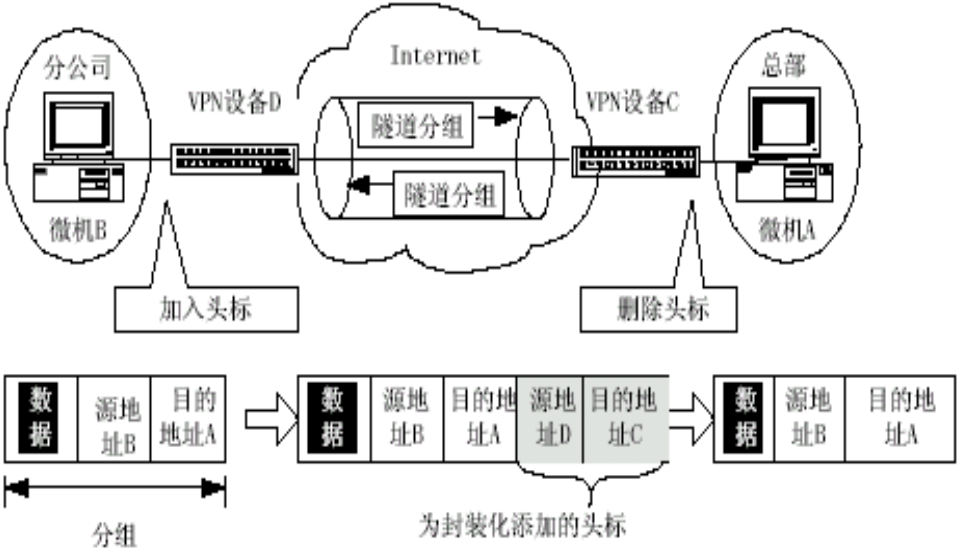


VPN的本质：隧道

隧道技术

- 隧道技术就是利用隧道协议对隧道两端的数据进行封装的技术
  - 在发送端与公网的接口处，将数据作为负载封装在一种可以在公网上传输的数据格式中，在接收端与公网的接口处将数据解封装，取出负载
  - 被封装的数据包在互联网上传递时所经过的逻辑路径被称为“隧道”。
  - 隧道协议可以是第2层或第3层隧道协议
- 第2层隧道协议
  - 先把各种网络协议封装到PPP中，再把整个数据包装入隧道协议中
  - 这种双层封装方法形成的数据包靠第二层协议进行传输
- 第3层隧道协议
  - IPSEC：本身不是隧道协议，但由于其提供的认证、加密功能适用于建立VPN环境，它既能提供LAN间VPN，也能提供远程访问型VPN

隧道的数据传输过程


分公司
VPN设备D
Internet
隧道分组
隧道分组
VPN设备C
总部
微机B
微机A
加入头标
删除头标
数据
源地址B
目的地址A
分组
数据
源地址B
目的地址A
源地址D
目的地址C
为封装化添加的头标
数据
源地址B
目的地址A

隧道使用的协议

- 第二层转发协议 (L2F)；
- 点对点隧道协议(PPTP)；
- 第二层隧道协议(L2TP)；
- IP 安全协议 (IPSec)；
- 多协议标签交换(MPLS)；
- 通用路由封装Generic Routing Encapsulation

不同隧道实现技术比较

协议名称	RFC编号	封装化	协议号码	L2/L3	加密与否	LAN间连接型VPN	远程访问型VPN
L2F	2341	L2F	UDP(17)	第2层	否	—	○
PPTP	草案	GRE	GRE(47)	第2层	否	○	○
L2TP	草案	L2TP	UDP(17)	第2层	否	○	○
ATMP	2107	GRE	GRE(47)	第3层	否	—	○
BayDVS	无	GRE	GRE(47)	第3层	否	—	○
GRE	1701	GRE	GRE(47)	第3层	否	○	—
IPsec ESP	2406	ESP	ESP(50)	第3层	是	○	○
IPsec AH	2402	AH	AH(51)	第3层	否	○	○

6.3 链路层VPN的实现

- **L2F：Level 2 Forwarding protocol，第二层转发协议**
  - 为实现基于ISP的远程访问VPN而制订的协议
  - 建立跨越公共网络的安全隧道，将 ISP POP 连接到企业内部网关，这个隧道建立了一个用户与企业客户网络间的虚拟点对点连接
  - 允许高层协议的链路层隧道技术
- 初始连接：使用标准PPP
- 验证：使用标准CHAP或者做某些修改
- 封装：允许在L2F数据包中封装 PPP/SLIP 包

点对点隧道协议(PPTP)

- **PPTP: Point-to-Point Tunneling Protocol**，点对点隧道协议）
  - 用于在 **IP** 网络上建立 **PPP** 会话隧道
- **PPTP**协议基础：
  - 点对点协议**(PPP)**
  - 口令验证协议**(PAP)**
  - 通用路由选择封装协议**(GRE)**
  - **PPP**质询握手验证协议**(CHAP)**
- **PPTP**体系结构使用三个过程：
  - **PPP**连接和通信
  - **PPTP**控制连接，它建立到**PPTP**服务器上的连接，并建立一个虚拟隧道
  - **PPTP**数据隧道，在隧道中**PPTP**协议建立包含加密的**PPP**包的**IP**数据报，这些数据报通过**PPTP**隧道进行发送

第2层隧道协议（L2TP）

- PPTP和L2F互不兼容
- IEFT建议将PPTP和L2F的最优秀的部分组成一个工业标准，并称为第2层隧道协议(L2TP)
  - 格式基于L2F，信令（signaling）基于PPTP
- 特点：
  - 连接型的隧道封装协议，适用于通过Internet接纳远程用户的远程访问型VPN
  - 接纳移动用户（指拔号上网），每次连接都进行用户认证
  - 支持多协议（因为L2TP协议封装在PPP之外，PPP具有支持多种网络协议的功能）

Windows VPN

- 采用点对点隧道协议 (PPTP) 或第二层隧道协议 (L2TP)
- VPN连接是通过 PPP 用户级身份验证方法进行验证的。这些方法包括密码身份验证协议 (PAP)、质询握手身份验证协议 (CHAP)、Shiva 密码身份验证协议 (SPAP)、Microsoft 质询握手身份验证协议 (MS-CHAP) 和可选的可扩展身份验证协议 (EAP)。
- 通过使用新的可扩展身份验证协议 (EAP) 和 Internet 协议安全 (IPSec) 安全选项， Windows VPN为远程用户提供了增强的安全性。
  - 远程访问服务器配置为使用 EAP 进行授权，则对于远程访问服务器的拨号连接或虚拟网络连接，实施最高级别的身份验证。
  - 利用点对点协议 (PPP) 身份验证和加密选项，定义远程访问服务器上的 PPTP 筛选，并限制 Internet 上的远程访问服务器仅接受那些已验证的加密数据的 PPTP 客户端
- Android VPN客户端 PPTP

MPLS

- **MPLS (Multi Protocol Label Switching)**：多协议标记（标签）交换
  - 一种支持多种网络层协议的快速转发技术，它就象一个垫片（**shim**），处于**OSI**的第**2**、**3**层之间。
  - **MPLS**吸收了**ATM**网络的**VPI/VCI**交换思想，集成了**IP**路由技术的灵活性和**2**层交换的简捷性，为**IP**网络提供了面向连接的交换。
- **MPLS VPN**
  - 利用标记通道为用户提供有安全的、有服务质量保证的虚拟专网服务。
  - 利用**MPLS**构建**VPN**时，只需对不同的企业集团分配不同的标记通道
  - 利用标记堆叠来实现**VPN**，在一个**IP**分组上叠加两个**MPLS**标记头标进行转发，外侧标记用于转发，内侧标记用于**VPN**

6.4 基于IPSec协议的VPN

- IPSec VPN是基于IPSec协议的VPN技术，由IPSec协议提供隧道安全保障。IPSec是一种由IETF设计的端到端的确保基于IP通讯的数据安全性的机制。它为Internet上传输的数据提供了高质量的、可互操作的、基于密码学的安全保证。
- 通过IKE支持动态密钥交换，采用预共享密钥或公钥机制认证身份，协商加密、认证密钥，具有数据传输的完整性认证、加密功能
- 实现方式
  - VPN专用设备
  - 将IPSec嵌入到防火墙软件
  - 将IPSec嵌入到路由器软件
  - 动态IP地址的IPSec VPN（利用动态域名服务器）

6.4 基于IPSec协议的VPN

- IPSec在4个层次上起作用：加密和封装、验证和重放容错、密钥管理以及数字签名和数字证书。
- IPSec 基于端对端的安全模式， 就是说它在从一台机器到另一台计算机途中信息仍然是加密的，并且只能由另一端的计算机解密。IPSec同样使用公钥加密技术，不同的是两端都生成共享密钥，而且共享密钥不能在网络上传输。
- 该模式允许为下列企业方案成功部署 IPSec：
  - 局域网 (LAN)：客户端/服务器和对等网络
  - 广域网 (WAN)：路由器到路由器和网关到网关
  - 远程访问：拨号客户机和从专用网络访问 Internet
- 通常，两端都需要 IPSec 配置（称为 IPSec 策略）来设置选项与安全设置，以允许两个系统对如何保护它们之间的通讯达成协议。

6.4 基于IPSec协议的VPN

IPSec的工作方式：

- 计算机A通过一个不可靠IP网络发送数据给计算机B。在开始传输之前，计算机A上的算法查看是否应该依照建立在A上的安全策略保护数据。安全策略包含一些规则，可以确定通信的敏感程度。
- 如果过滤器发现有匹配的结果，A首先与B通过称为Internet密钥交换（Internet Key Exchange，IKE）的协议开始进行安全协商。然后两台计算机依照在安全规则中指定的验证方法交换凭据。验证方法可以是Kerberos、公钥凭据或者是预先确定的密钥值。

6.4 基于IPSec协议的VPN

- 一旦协商开始，在两台计算机之间会建立两种协商协议，称为安全关联（**security association**）。第一种叫做**Phase I IKE SA**，它指定了两台计算机将如何彼此信任。第二种是关于两台计算机如何保护应用程序通信的协议，叫做**Phase II IPSec Sec Sas**，它指定了安全方法和各方向通信的密钥。**IKE**为每个**SA**自动创建并刷新共享秘密密钥。秘密密钥分别在网络两端创建，不会在网络中传输。
- 为了保证信息的完整性，计算机**A**对发出的数据包签名，并且依照双方协商好的方法加密或不加密数据包。然后将数据包传送到**B**。
- 计算机**B**查看数据包的完整性，如有需要则将其解密。然后数据沿着**IP**堆栈向上传送到通常的应用程序中。

6.4 基于IPSec协议的VPN

IPSec有以下三个特点：

1. 原来的局域网机构彻底透明。透明表现为三方面：系统不占用原网络系统中任何IP地址：装入VPN系统后，原来的网络系统不需要改变任何配置；原有的网络不知道自己与外界的信息传递已受到了加密保护，该特点不仅能够为安装调试提供方便，也能够保护系统自身不受外来网络的攻击。
2. IPSec内部实现与IP实现融为一体，优化设计，具有很高的运行效率。
3. 安装VPN的平台通常采用安全操作系统内核并以嵌入的方式固化，具有无漏洞、抗病毒、抗攻击等安全防范性能。

预防攻击

IPSec 对数据的保护使攻击者感到破解相当困难或根本不可能。提供的保护级别是由在 IPSec 策略结构中指定的安全级别的强度决定的。

IPSec 的许多功能可大大减少或防止下列攻击：

- 嗅探器、探测器（缺少保密性）

  IPSec 中的“封装安全有效负载 (ESP)”协议通过对 IP 数据包的有效负载加密可提供数据保密。

- 数据修改

  IPSec 使用基于加密的、仅由发送计算机与接收计算机共享的密钥，为每个 IP 数据包创建一个加密校验和。对数据包所做的任何修改都会改变校验和，该检验和会告诉接收计算机数据包在传输过程中已被修改。

- 标识欺骗攻击、基于密码的攻击、应用程序层攻击以及拒绝服务攻击

  IPSec 允许在不将标识信息暴露给攻击者进行破解的情况下对标识进行交换与验证。相互验证（身份验证）用来在通讯系统间建立信任，只有受信任的系统才能彼此通讯。建立标识之后，IPSec 使用基于加密的、仅由发送计算机与接收计算机共享的密钥，为每个 IP 数据包创建一个加密校验和。加密校验和可确保只有知道密钥的计算机才会发送每个数据包。

- 中间人攻击

  IPSec 将相互验证与基于加密的共享密钥结合使用。

- 拒绝服务攻击

  IPSec 以 IP 数据包筛选方法为基础并根据 IP 地址范围、IP 协议甚至特定的 TCP 与 UDP 端口来确定是允许、保护还是阻止通讯。

Windows IPSec

- Windows IPSec 遵循“Internet工程任务组(IETF)”IPSec工作组开发的业界标准，其相关服务部分由 Microsoft 与 Cisco Systems, Inc. 共同开发。
- 为降低开销，采用了基于策略的管理。
- IPSec 策略（而不是应用程序接口 (API)）用来配置 IPSec 安全服务。
- 通过配置 IPSec 策略可满足计算机、应用程序、组织单位、域、站点或全局企业的安全需要。可使用 Windows 中提供的“IP 安全策略”管理单元来为 Active Directory 中的计算机（对于域成员）或本地计算机（对于不属于域的计算机）定义 IPSec 策略。
- 不同版本的Windows系统对IPSec支持有差异

6.5 应用层VPN的实现

- 随着SSL（安全套接层协议层） VPN技术的发展，SSL VPN产品所能提供的终端网络功能已经与传统的IPSec VPN产品几乎一样强大，SSL VPN接入方式是点对网VPN接入的最佳选择的观点也越来越深入人心。
- SSL VPN是以HTTPS（Secure HTTP，安全的HTTP，即支持SSL的HTTP协议）为基础的VPN技术，工作在传输层和应用层之间。SSL VPN充分利用了SSL协议提供的基于证书的身份认证、数据加密和消息完整性验证机制，可以为应用层之间的通信建立安全连接。SSL VPN广泛应用于基于Web的远程安全接入，为用户远程访问公司内部网络提供了安全保证。

OpenVPN

- OpenVPN 是一个应用层 VPN 实现，大量使用了OpenSSL加密库中的SSLv3/TLSv1 协议库函数，开源软件by James Yonan and is published under the GNU General Public License (GPL).。
- OpenVPN允许参与建立VPN的站点使用共享密钥，电子证书，或者用户名/密码来进行身份验证。OpenVPN2.0后引入了用户名/口令组合的身份验证方式（需PAM pluggable authentication module），可以省略客户端证书，但是仍需一份服务器证书用作加密（公钥）。
- IANA（Internet Assigned Numbers Authority）指定给OpenVPN的官方端口为1194。OpenVPN 2.0以后版本每个进程可以同时管理数个并发的隧道。 默认且推荐使用UDP协议，也支持TCP 。OpenVPN支持大多数的代理服务器包括HTTP代理，并且能够在NAT的环境中很好地工作。
- 运行平台 - Solaris、Linux、OpenBSD、FreeBSD、NetBSD、Mac OS X、Android与Windows 等，包含了许多安全性的功能。
- 不是一个基于Web的VPN软件，也不与IPsec及其他VPN软件包兼容。

OpenVPN

- 服务端具有向客户端“推送”某些网络配置信息的功能，这些信息包括：IP地址、路由设置等。OpenVPN提供了两种虚拟网络接口：通用Tun/Tap驱动，可以建立三层IP隧道，或者虚拟二层以太网，后者可以传送任何类型的二层以太网络数据。传送的数据可通过LZO算法压缩。
  - 虚拟网卡是使用网络底层编程技术实现的一个驱动软件，安装后在主机上多出现一个网卡，可以像其它网卡一样进行配置。服务程序可以在应用层打开虚拟网卡，如果应用软件（如IE）向虚拟网卡发送数据，则服务程序可以读取到该数据，如果服务程序写合适的数据到虚拟网卡，应用软件也可以接收得到。虚拟网卡在很多的操作系统下都有相应的实现，这也是OpenVpn能够跨平台一个很重要的理由。
- 在OpenVpn中，如果用户访问一个远程的虚拟地址（属于虚拟网卡配用的地址系列，区别于真实地址），则操作系统会通过路由机制将数据包（TUN模式）或数据帧（TAP模式）发送到虚拟网卡上，服务程序接收该数据并进行相应的处理后，通过SOCKET从外网上发送出去，远程服务程序通过SOCKET从外网上接收数据，并进行相应的处理后，发送给虚拟网卡，则应用软件可以接收到，完成了一个单向传输的过程，反之亦然。

OpenVPN

- OpenVPN与生俱来便具备了许多安全特性：它在用户空间运行，无须对内核及网络协议栈作修改；初始完毕后以chroot方式运行，放弃root权限；使用mlockall以防止敏感数据交换到磁盘。
- OpenVPN通过PKCS＃11支持硬件加密标识，如智能卡。 Public-Key Cryptography Standards
- OpenVPN使用通用网络协议（TCP与UDP）的特点使它成为IPsec等协议的理想替代，尤其是在ISP（Internet service provider）过滤某些特定VPN协议的情况下。
- OpenVPN衍生产品 – BartVPN等