项目1 初识VPN

知识目标

- VPN的概念
- VPN的工作原理和功能
- 实现VPN的加密技术
- 实现VPN的隧道协议
- VPN产品体系

技能目标

- 基于PGP软件的文件加解密

案例引入

公司的漫游用户需要访问公司内部网络，公司的分支机构需要访问总公司的内部网络，公司的合作伙伴或供应商与公司网络的通信。在这些情况下，要保证内部网的安全性和传输数据的保密性，需要部署 VPN。

任务1-1 VPN的概念和功能

本次学习任务是能够理解什么是 VPN，VPN 的分类，VPN 的部署体系，VPN 的实现技术及 VPN 的工作原理。

1．什么是 VPN

VPN 即虚拟专用网络（Virtual Private Network），其能够利用 Internet 或其他公共互联网络基础设施，提供与专用网络一样的功能和安全保障，即在公用网络上进行加密的 VPN 通信，犹如将用户的数据在一个临时的、安全的隧道中传输，但此过程对用户是透明的，也就是说用户在使用 VPN 时感觉如同在使用专用网络进行通信，VPN（虚拟专用网络）也因此得名，如图 1-1 所示。目前 VPN 技术在企业网络中有广泛应用，VPN 是企业内部网络的扩展，使用 VPN 技术，可以帮助企业的远程用户、企业的分支机构、合作伙伴之间建立安全的网络连接，保证数据的安全传输。VPN 具有成本低、易于使用的特点。

图1-1　VPN概念示意图

2．VPN 的分类

按照 VPN 的应用领域，VPN 技术可分为如下 3 类。

（1）远程接入 VPN（Access VPN）：企业的漫游用户与其局域网之间的安全连接，即客户端到网关之间，基于公网的安全传输，能够节省企业成本。

（2）内联网 VPN（Intranet VPN）：企业分支机构之间的安全连接，即网关到网关之间的安全连接，公司的各分支机构通过公司的网络架构连接来自同公司的资源，可以节省分支机构与企业总部之间的专线费用，对于国际性的连接，这种节省更明显。

（3）外联网 VPN（Extranet VPN）：企业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安全连接。

3．VPN 体系

1）网络服务商提供的 VPN 服务

企业自身为了节约管理成本，使用网络服务商提供的 VPN 服务，帮助远程用户、公司分支机构、合作伙伴之间建立安全的连接，保证安全的数据传输。

2）企业自身进行 VPN 部署，分以下几种部署方式。

①部署 VPN 服务器：在大型局域网中，可以通过在网络中心搭建 VPN 服务器的方法实现 VPN。

②软件 VPN：可以通过专用的软件实现 VPN。

③集成 VPN：购买集成了 VPN 功能的硬件设备，如路由器、防火墙等，都含有 VPN 功能，企业可以基于这些硬件设备部署 VPN。

④硬件 VPN：可以通过专用的 VPN 硬件设备实现 VPN。

4．实现 VPN 的关键技术

1）数据加密技术

数据加密技术保证 VPN 能够实现数据的安全传输，VPN 的概念中提到的临时的、安全的隧道，其实质就是通过数据加密技术实现的安全性。

2）身份认证技术

数据通信的各方在网络中确认操作者身份而用到的解决方法即身份认证。VPN 技术在建立隧道时也需要数据通信的双方进行身份认证，身份认证技术是基于数据加密技术实现的。数据加密技术和身份认证技术将在学习任务 1-2 中进行详细讲解。

3）隧道技术

所谓隧道，实质上就是一种“封装”。隧道技术是 VPN 的底层支持技术，隧道是通过隧道协议实现的，隧道协议规定了隧道的建立、维护和删除的规则，以及如何将数据进行封装传输。隧道技术将在学习任务 1-3 中进行详细讲解。

4）密钥管理技术

密钥管理是指对密钥进行管理的行为，指从密钥的产生到密钥的销毁整个过程的管理，是实现 VPN 不可缺少的技术，主要表现于管理体制、管理协议和密钥的产生、分配、更换、保密等。

5．VPN 的工作原理

首先通信双方进行协商，建立隧道；然后对传输的数据进行加密，封装成 IP 包的形式在安全的隧道中进行传输，实现双方的安全通信。

任务1-2　实现VPN的加密技术

数据加密技术是实现 VPN 的基础，理解数据加密的基本术语，VPN 技术用到的两种加密体制、消息摘要算法、数字签名和数字证书。

1．密码学基本术语

明文，即原始的、未经加密的数据。明文经过加密算法对其进行加密操作，得到密文，密文是明文经过加密后的格式。加密算法的输入是明文和密钥，输出是密文。相反，解密算法的输入是密文和密钥，输出是明文，即密文经过解密算法对其进行解密操作，还原为原始的明文。

加密时输入的密钥称为加密密钥；解密时输入的密钥称为解密密钥。

在实际应用中，加密算法和解密算法往往是公开的，但密钥是保密的，密文不能被没有密钥的用户所理解。

综上所述，一个完整的加密体制包括 4 个基本的要素：明文、密文、算法和密钥。数据加解密的流程如图 1-2 所示。

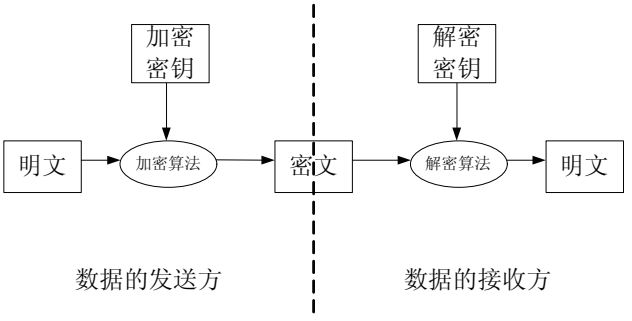


图1-2　数据加解密的流程

2．两种加密体制

1）对称加密体制

在对称加密体制中，加密密钥和解密密钥相同，或加密密钥能够从解密密钥中推算出来，同时解密密钥也可以从加密密钥中推算出来。大部分对称加密算法中，加密密钥和解密密钥是相同的，所以对称加密算法也称为秘密密钥算法或单密钥算法。它要求发送方和接收方在数据传输之前，先协商好一个密钥，它的安全性依赖于密钥的安全性，如图 1-3 所示。

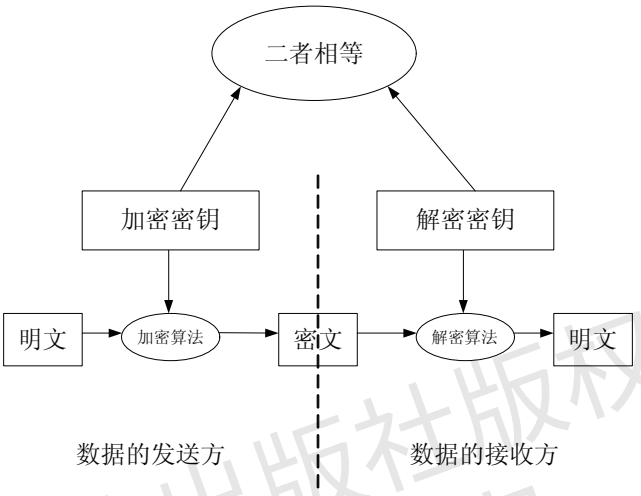


图1-3　对称加密体制

对称加密算法的特点是算法公开、计算量小、加密速度快、加密效率高。

对称加密算法的缺点是密钥管理困难。每对用户每次使用对称加密算法时，都需要使用双方协商的密钥，这会使得发、收信双方所拥有的密钥数量呈几何级数增长，密钥管理成为用户的负担。对称加密算法在分布式网络系统中使用较为困难，主要是因为密钥管理困难，使用成本较高。具有代表性的对称加密算法有 DES、3DES、AES 和 IDEA 等。美国国家标准局倡导的 AES 即将作为新标准取代 DES。

2）非对称加密体制

非对称密钥密码体制，也称公开密钥加密体制，即加密密钥和解密密钥不同，是一种由已知加密密钥推出解密密钥在计算上不可行的密码体制。其中加密密钥是公开的，也称为公开密钥（公钥），解密密钥是私有的，也称为私有密钥（私钥）。

公钥和私钥的关系有两点非常重要，一是公钥和私钥总是成对出现，如果用公钥对数据进行加密，只有用对应的私钥才能解密；如果用私钥对数据进行加密，那么只有用对应的公钥才能解密。二是由私钥可以很容易地计算或推导出公钥，但是由公钥计算或推导私钥必须是计算上不可行的。

利用非对称加密体制进行加密和解密的流程如图 1-4 所示。

① 接收方生成一对密钥：公钥和私钥。

② 发送方获得接收方的公钥，并利用该公钥对数据进行加密。

③ 发送方将密文通过网络传输给接收方。

④ 接收方收到密文后，利用自己对应的私钥进行解密，得到原始明文。

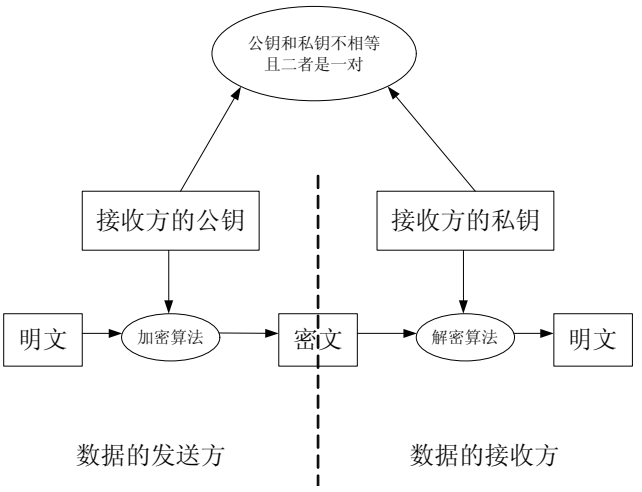


图1-4　非对称加密体制

由于私钥是接收方私有的，所以只有正确的接收方才可以解密该数据，从而起到了保护数据机密性的功能，这是非对称密码体制的一种重要功能：数据加密，用接收方公钥加密数据，用接收方私钥解密数据。

另一种情况，是用发送方私钥加密，用发送方公钥解密，这是非对称密码体制的另一种重要功能，数字签名和认证。数据的发送方用自己的私钥对数据进行加密，那么接收方用发送方与之对应的公钥才能进行解密，因为发送方的公钥是公开的，接收方可以通过各种方式获得，而发送方的私钥是私有的，因此，只要接收方用发送方的公钥能够解密其发送来的数据，那么就可以证明发送方的身份。

基于以上的阐述，要实现非对称加密，每个用户至少有一个密钥对（公钥和私钥），非对称加密体制的特点如下：

- 通信双方不需要事先共享通用的密钥，用于解密的私钥也不需要发往任何地方，公钥在传递与发布过程中即使被截获，由于没有与公钥相匹配的私钥，截获公钥也没有意义。
- 简化了密钥的管理，网络中有N 个用户之间进行通信加密，仅需要使用N对密钥即可。
- 公钥加密的缺点在于加密算法复杂，加密和解密的速度相对来说比较慢。

典型非对称加密体制算法有：RSA 公钥算法和 ECC（Elliptic Curve Cryptography）加密密钥算法等。

RSA 体制是目前应用最为广泛的公钥加密算法。RSA 是 1977 年由三位数学家 Rivest、Shamir 和 Adleman 设计的一种算法，在 VPN 技术中也有应用，下面是 RSA 算法的数学基础描述。

（1）互质：如果两个正整数，除了 1 以外，没有其他公因子，我们就称这两个数是互质的。比如，20 和 31 没有公因子，所以它们是互质关系。这说明，不是质数也可以构成互质关系。

（2）欧拉函数：通常欧拉函数以 $\phi(n)$ 表示，任意给定正整数 n，其欧拉函数 $\phi(n)$ 表示小于等于 n 的正整数之中，与 n 构成互质关系的正整数的个数。例如，对于正整数 10，其欧拉函数 $\phi(n)$ 表示，在 1 到 10 之中，与 10 构成互质关系的数的个数，即 $\phi(n)$=5，因为在 1 到 10 之中，与 10 形成互质关系的是 1、3、5、7，9，共 5 个，所以 $\phi(n)=5$。

RSA 算法描述如下。

- 加密算法：C=Me mod n
- 解密算法：M=Cd mod n
- 私钥={d，n}
- 公钥={e，n}

其中 C 代表密文，M 代表明文，公钥和私钥通过下面的过程产生。

① 选择 p 和 q。其中 p 和 q 都是素数，且 p 和 q 不相等。

② 计算 $n=pq$ ；

③ 计算 $\phi(n)=(p-1)(q-1)$ ；

④ 选择整数 e，使之满足 gcd($\phi(n)$，e)=1，$1<e<\phi(n)$；其中 gcd（x，y）表示整数 x 和 y 的最大公约数。

⑤ 计算 d，使之满足 $(d*e) \bmod \phi(n)=1$。

⑥ 得到公钥 PU={e,n}，私钥 PR={d,n}。

数据的发送方使用接收方的公钥 PU={e,n} 加密，明文 M<n，由加密公式 C=Me mod n 得到密文，将密文通过网络传输给接收方；接收方收到密文后，用自己对应的私钥 PR={d,n}，由解密公式 M=Cd mod n 得到明文。

3．消息摘要算法

1）消息摘要算法的概念

消息摘要算法是把任意长度的输入经过一系列运算之后产生的一个长度固定的伪随机输出的算法，它的运算过程类似于不需要密钥的加密过程，但经过消息摘要算法加密的数据无法被解密，只有输入相同的明文数据经过相同的消息摘要算法才能得到相同的密文。因此消息摘要算法适用于不需要通过解密操作还原出明文的情况，也可以用它来完成消息完整性的认证，即验证消息有没有被更改过。由于其加密计算的工作量相当可观，所以以前的这种算法通常只用于数据量有限的情况下的加密，例如，计算机的口令就是用不可逆加密算法加密的。

著名的摘要算法有 RSA 公司的 MD5 算法和 SHA-1 算法及其大量的变体。在 VPN 技术中，应用较多的是 MD5 算法。 图 1-5 所示为 Windows 系统本地安全策略支持的消息摘要算法。

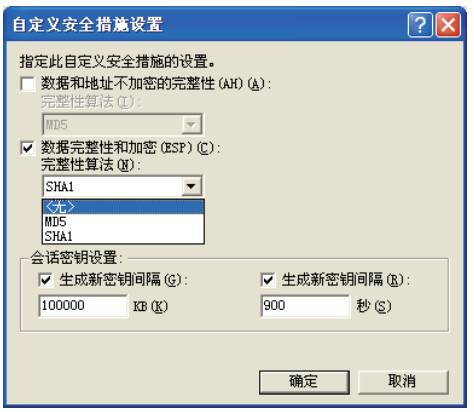


图1-5　Windows本地安全策略支持的消息摘要算法

2）消息摘要的特征

①不同长度的输入，计算出固定长度的消息摘要。例如，利用 MD5 算法得到的消息摘要是 128 位，利用 SHA-1 算法得到的摘要是 160 位，SHA-1 的变体可以产生 192 位和 256 位的消息摘要。一般认为，摘要的最终输出越长，该摘要算法就越安全。如图 1-6 所示为 SHA-1 算法得到的消息摘要示例，是用十六进制数表示的 160 位的摘要。

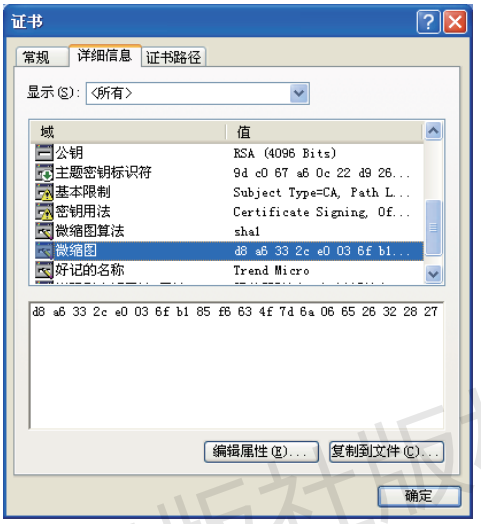


图1-6　消息摘要示例

②消息摘要是“伪随机的”。消息摘要并不是真正随机的，因为用相同的算法对相同的消息求两次摘要，其结果必然相同；而若是真正随机的，则无论如何都无法重现。因此消息摘要是“伪随机的”。

③一般的，不同的输入，对其进行摘要算法以后产生的消息摘要也必不相同；但相同的输入必会产生相同的输出。这正是消息摘要算法被用来验证消息完整性的特征。

④消息摘要函数是无陷门的单向函数。所谓无陷门的单向函数，被认为是该函数正向计算上是容易的，但其求逆计算在计算上是不可行的，即从其输出计算输入是非常困难的。例如，已知 x，很容易计算 $f(x)$。但已知 $f(x)$，却难于计算出 x。就好比燃烧一张纸要比使它从灰烬中再生容易得多；把盘子打碎成数千片碎片很容易，把所有这些碎片再拼成一个完整的盘子则很难。消息摘要就是利用这种无陷门的单向函数计算生成的，即只能进行正向的计算摘要，无法从摘要中恢复出任何原有的信息。除非采用强力攻击的方法，即尝试每一个可能的信息，计算其摘要，与已有摘要进行比较，比较相同则找到该摘要的原始信息，但实际上这是无效的。

⑤好的摘要算法，是无“碰撞”的，即无法找到两条消息，使它们的摘要相同。

3）消息摘要的用途

消息摘要最重要的用途，就是用于构造数字签名。数字签名正是基于公钥加密算法和消息摘要算法完成的，是保证信息的完整性和不可否认性的方法。

数字签名的基本原理如下：

发送方将消息按双方约定的单向散列算法计算得到一个固定位数的消息摘要，然后使用公钥加密对该消息摘要进行加密，这个被加密了的摘要作为发送者的数字签名。

接收方收到数字签名后，用同样的单向散列函数算法对消息计算摘要，然后与发送者的公开密钥进行解密的消息摘要相比较，如果相等，则说明消息确是来自发送者（验证），因为只有用发送者的签名，私钥加密的信息才能用发送者的公钥揭开，从而保证了数据的真实性。

发送方 A 和接收方 B 的通信过程如下：

① A 利用消息摘要算法产生文件的消息摘要。

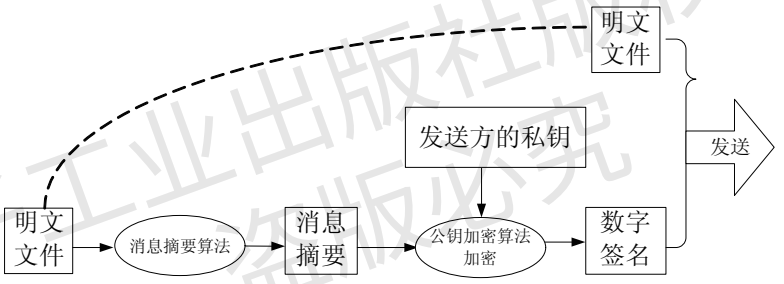
② A 用其私钥对该摘要进行非对称算法的加密操作，这个加密后的摘要就是 A 对该文件的数字签名。

③ A 将文件和数字签名发送给 B。

④ B 收到后，对 A 发送的文件进行相同的消息摘要计算，得到一个新的摘要，同时用 A 的公钥对数字签名进行非对称算法的解密操作，得到 A 计算的消息摘要，与 B 自己计算的新摘要进行比较，如果二者匹配，签名是有效的。既验证了发送方 A 的身份，又验证了消息的完整性。

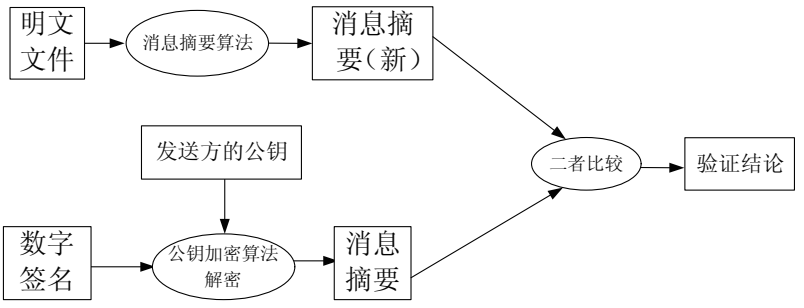
其中签名算法一般由公开密钥密码算法（RSA、ELGamal、DSA、ECDSA 等）和单向散列函数（MD5 或 SHA 等）构成。

数字签名的过程如图 1-7 所示。数字签名的验证过程如图 1-8 所示。



数据的发送方

图1-7　数字签名的过程



数据的接收方

图1-8　数字签名的验证过程

在 VPN 技术中，应用较多的是 MD5 算法。

4．数字证书

数字证书是各类终端实体和最终用户在网络上的“身份证”，是各类实体在网上进行信息交流及商务活动的身份证明，是一段包含用户身份信息、用户公钥信息及身份验证机构数字签名的数据。

数字证书是由证书认证中心 CA 颁发的。证书认证中心 CA 是一家能向用户签发数字证书以确认用户身份的管理机构。

一个标准的 X.509 数字证书包含下列信息：

① 证书的版本信息。

② 证书的序列号，每个证书都有一个唯一的证书序列号。

③ 证书所使用的签名算法。

④ 证书的发行机构名称，命名规则一般采用 X.500 格式。

⑤ 证书的有效期，现在通用的证书一般采用 UTC 时间格式，它的计时范围为 1950 ～ 2049。

⑥ 证书所有人的名称，命名规则一般采用 X.500 格式。

⑦ 证书所有人的公开密钥。

⑧ 证书发行者对证书的签名。

在 Windows 系统中，要查看数字证书，可在浏览器的“Internet 选项”对话框的“内容”标签页单击“证书”按钮，如图 1-9 所示；证书按其目的分类有安全电子邮件、客户端验证等，如图 1-10 所示。

图1-9　查看证书

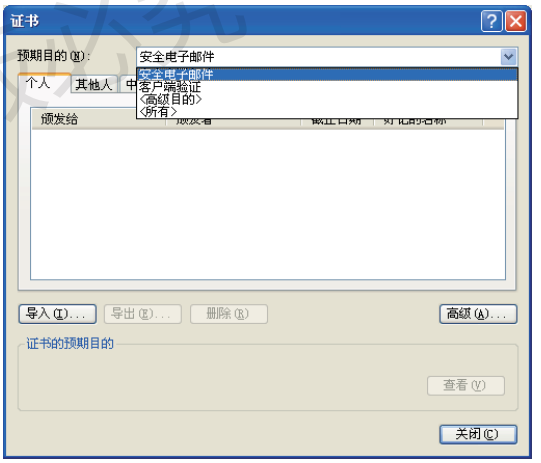


图1-10　证书分类

数字证书最重要的功能是身份认证，身份认证即确认实体就是自己所声明的实体，鉴别身份的真伪。如 A 与 B 双方的认证，首先 A 要验证 B 的证书的真伪，当 B 在网上将证书传送给 A 时，A 首先要用证书颁发机构 CA 的公钥验证证书上 CA 的数字签名，如签名有效，证明 B 持有的证书是真的；其次 A 还要验证 B 身份的真伪，B 可以将自己的口令用自己的私钥进行数字签名传送给 A，A 已经从 B 的证书中或从证书库中查得了 B 的公钥，A 就可以用 B 的公钥来验证 B 用自己独有的私钥进行的数字签名。如果该签名通过验证，B 的身份就能够得到确认。

任务1-3　实现VPN的隧道技术

隧道是利用一种协议传输另一种协议的技术，即用隧道协议来实现 VPN 功能。为创建隧道，隧道的客户机和服务器必须使用同样的隧道协议。理解第二层隧道协议：PPTP，L2F/L2TP；第三层隧道协议：IPSec，GRE；SSL 协议。

1．PPP 协议

PPP 协议即 Point to Point Protocol（点对点协议），PPP（点到点协议）是 OSI 模式中的第二层（链路层）协议，其设计目的主要是用来通过拨号或专线方式建立点对点连接发送数据，使其成为各种主机、网桥和路由器之间简单连接的一种共通的解决方案。PPP 除了 IP 以外还可以携带其他协议，包括 DECnet 和 Novell 的 Internet 网包交换（IPX）。第二层隧道协议 PPTP、L2F/L2TP 很大程度上依靠 PPP 协议的特性，因此首先要理解 PPP 协议。PPP 拨号会话过程可以分成 4 个不同的阶段。

第一阶段：创建 PPP 链路

链路控制协议（LCP）负责创建、维护或终止 PPP 链路。在 LCP 阶段的初期，将对基本的通信方式进行选择，即 PPP 通信双方通过 LCP 交换配置信息，包括验证协议的选择、是否进行数据压缩和数据加密等。配置信息交换成功后，链路即创建成功。在链路建立的过程中，任何非链路控制协议的包都会被没有任何通告地丢弃。

第二阶段：链路认证

在链路建立后进行通信双方身份验证，其目的是为了防止攻击者未经授权的情况下成功连接，从而导致泄密。验证过程在 PPP 协议中为可选项。PPP 方案只提供了有限的验证方式，包括口令验证协议（PAP），挑战握手验证协议（CHAP）和微软挑战握手验证协议（MSCHAP）。

1）口令验证协议（PAP）

PAP 协议的用户名 / 口令以明文形式传输。因此这种验证方式的安全性较差，第三方可以很容易地获取被传送的用户名和口令。

2 ）挑战 - 握手验证协议（CHAP）

CHAP 是一种加密的验证方式，能够避免建立连接时传送用户的真实密码。NAS 向远程用户发送一个挑战口令（challenge），其中包括会话 ID 和一个任意生成的挑战字串（arbitrary challengestring）。远程客户必须使用 MD5 单向哈希算法（one-wayhashingalgorithm）返回用户名、加密的挑战口令、会话 ID 及用户口令，其中用户名以非哈希方式发送。

CHAP 对 PAP 进行了改进，不再直接通过链路发送明文口令，而是使用挑战口令以哈希算法对口令进行加密。因为服务器端存有客户的明文口令，所以服务器可以重复客户端进行的操作，并将结果与用户返回的口令进行对照。CHAP 为每一次验证任意生成一个挑战字串来防止受到再现攻击（replay attack）。在整个连接过程中，CHAP 将不定时地向客户端重复发送挑战口令，从而避免第 3 方冒充远程客户（remoteclient impersonation）进行攻击。

第三阶段：调用网络层协议

PPP 会话双方完成上述两个阶段的操作后，开始使用相应的网络层控制协议配置网络层的协议，如 IP、IPX 等。

第四阶段：链路终止

链路控制协议用交换链路终止包的方法终止链路。引起链路终止的原因很多：载波丢失、认证失败、链路质量失败、空闲周期定时器期满或管理员关闭链路等。

2．隧道协议 PPTP

PPTP 是一种支持多协议 VPN 的隧道协议，是第二层协议 PPP 的扩展。PPTP 通过控制链接来创建、维护和终止一条隧道，并使用通用路由封装 GRE（Generic Routing Encapsulation）对 PPP 帧进行封装。

1）PPTP 协议的封装过程

（1）PPP 帧的封装

初始 PPP 有效载荷经过加密、压缩或两者的混合处理后，添加 PPP 报头，封装形成 PPP 帧。PPP 帧进一步添加 GRE 报头，经过第二层封装形成 GRE 报文。

（2）GRE 报文的封装

PPP 有效载荷的第三层封装是在 GRE 报文外，再添加 IP 报头。IP 报头包含数据包源端及目的端 IP 地址。

（3）数据链路层封装

数据链路层封装是 IP 数据包多层封装的最后一层，依据不同的外发物理网络再添加相应的数据链路层报头和报尾。

PPTP 的封装如图 1-11 所示。

数据链路层报头	IP报头	GRE报头	PPP报头	加密PPP有效载荷	数据链路层报尾

图1-11　PPTP的封装

2）PPTP 数据包的接收处理

PPTP 客户机或 PPTP 服务器在接收到 PPTP 数据包后，将做如下处理：

① 处理并去除数据链路层报头和报尾。

② 处理并去除 IP 报头。

③ 处理并去除 GRE 和 PPP 报头。

④ 对 PPP 有效载荷即传输数据进行解密或解压缩。

⑤ 对传输数据进行接收或转发处理。

3）PPTP 协议的特性

① 使用 MPPC 微软点对点隧道协议。

② 使用 MPPE 协议。

③ 用户认证：PAP 口令认证协议 /CHAP 挑战握手认证协议；EAP 可扩展认证协议；微软私有 MS-CHAP V1/V2 协议 。

④ 多协议支持：为 PPP 协议的扩展，能分装 IP、IPX 数据（HDLC 只能分装 IP，PPP 能分装 IP、IPX）。

3．隧道协议 L2TP

L2TP 协议也是基于第二层协议 PPP 进行的扩展，它结合了点对点隧道协议 PPTP 和第二层转发协议 L2F 协议的优点，基于 UDP 协议实现，协议的额外开销较少。其报文分为数据消息和控制消息两类。数据消息用于投递 PPP 帧，该帧作为 L2TP 报文的数据区。L2TP 不保证数据消息的可靠投递，若数据报文丢失，不予重传，不支持对数据消息的流量控制和拥塞控制。控制消息用以建立、维护和终止控制连接及会话，L2TP 确保其可靠投递，并支持对控制消息的流量控制和拥塞控制。

L2TP 可以提供包头压缩。当压缩包头时，系统开销（overhead）占用 4 字节，而 PPTP 协议下要占用 6 字节。

L2TP 可以提供隧道验证，而 PPTP 则不支持隧道验证。但是当 L2TP 或 PPTP 与 IPSec 共同使用时，可以由 IPSec 提供隧道验证，不需要在第二层协议上验证隧道。

L2TP 支持的协议有 IP 协议、IPX 协议和 NetBEUI 协议。

4．隧道协议 IPSec

“Internet 协议安全性（IPSec）”是一种开放标准的框架结构，通过使用加密的安全服务以确保在 Internet 协议（IP）网络上进行保密而安全的通信。

IPSec 通过三个要素进行安全保护：验证头 AH、封装安全载荷 ESP、互联网密钥管理协议 IKMP。

提供三种功能：加密、认证和完整性。IPSec 使用的加密算法包括：对称算法（DES、3DES、AES）和非对称算法（RSA）；消息摘要算法 MD5/SHA1，带密钥的消息摘要算法 HMAC、HMAC-MD5、HMAC-SHA1 等。

IPSec 不是一个单独的协议，而是一组协议，IPSec 协议的定义文件包括了 12 个 RFC 文件和几十个 Internet 草案，已经成为工业标准的网络安全协议。

1）最重要的三个协议

AH、ESP：这是真正对 IP 包进行处理的 IPSec 协议。

IKE：应用层协议，用于协商 SA（安全联盟），不用于处理 IP 包。

AH 只验证数据完整性，没有加密功能；ESP 既能实现数据加密又能实现数据完整性验证。

2 ）IPSec 运行模式

传输模式（Transport Mode）：保护的内容是 IP 包的载荷。可能是 TCP/UDP 等传输层协议，也可能是 ICMP 协议，还可能是 AH 或者 ESP 协议。为上层协议提供安全保护。通常情况下传输模式只用于两台主机之间的安全通信。

隧道模式（Tunnel Mode）：保护的内容是整个原始 IP 包，隧道模式为 IP 协议提供安全保护。只要 IPSec 双方有一方是安全网关或路由器，就必须使用隧道模式。

3）利用 IPSecVPN 通信的过程

①对路由器 A、B 进行配置。

②路由器 A、B 协商 IKE SA，该 SA 用于保护后续通信。

③路由器 A、B 在 IKE SA 的保护下，协商第二阶段 SA，即最终的 IPSec SA。

④主机 A、B 在 IPSec SA 的保护下，经过 IPSec 通道进行通信。

4）IPSec 隧道模式具有如下功能和局限

①只能支持 IP 数据流。

②工作在 IP 栈的底层，因此，应用程序和高层协议可以继承 IPSec 的行为。

5．隧道协议 SSL

SSL（安全套接层）协议是目前广泛应用于浏览器与服务器之间的身份认证和加密数据传输的安全协议。 SSL 协议采用对称加密技术进行对传输数据加密，采用非对称加密技术进行身份认证和交换对称加密密钥。

SSL 协议在协议栈中的位置如图 1-12 所示。

<table>
<tr><td>SSL握手协议</td><td>SSL修改密文规约协议</td><td>SSL告警协议</td><td>HTTP</td></tr>
<tr><td colspan="4">SSL记录协议</td></tr>
<tr><td colspan="4">TCP</td></tr>
<tr><td colspan="4">IP</td></tr>
</table>

图1-12　SSL在协议栈中的位置

SSL 记录协议（SSL Record Protocol）建立在可靠的传输协议（如 TCP）之上，为高层协议提供数据封装、压缩、加密等基本功能的支持。SSL 记录协议接受传输层的应用报文，将数据分片成可管理的块，可选地压缩数据，应用 MAC，加密，增加首部，在 TCP 报文段中传输结果单元，被接受的数据被解密、验证、解压和重新装配，然后交给更上层应用。

SSL 记录协议加密流程如下。

① 分片：每个上层报文分成 16KB，或更小。

② 压缩：可选，前提是不能丢失信息，并且增加的内容长度不能超过 1024 字节，SSLv3 中缺省的压缩算法为空。

③ 增加 MAC 码：需要共享密钥。

④ 加密：使用同步加密算法对压缩报文和 MAC 码进行加密。可选的加密算法（P210）。

⑤ 增加 SSL 首部（内容类型 8b，主要版本 8b，次要版本 8b，压缩长度 16b。）

SSL 握手协议建立在 SSL 记录协议之上，用于在实际的数据传输开始前，通信双方进行身份认证、协商加密算法、交换加密密钥等。SSL 握手协议分为 4 个阶段。

阶段 1：建立安全功能，包括协议版本、会话 ID、密文族、压缩方法和初始随机数。

阶段 2：服务器认证和密钥交换。

阶段 3：客户认证和密钥交换

SSL 客户端只需在浏览器的 Internet 选项中进行设置，即可以支持 SSL 协议，如图 1-13 所示。

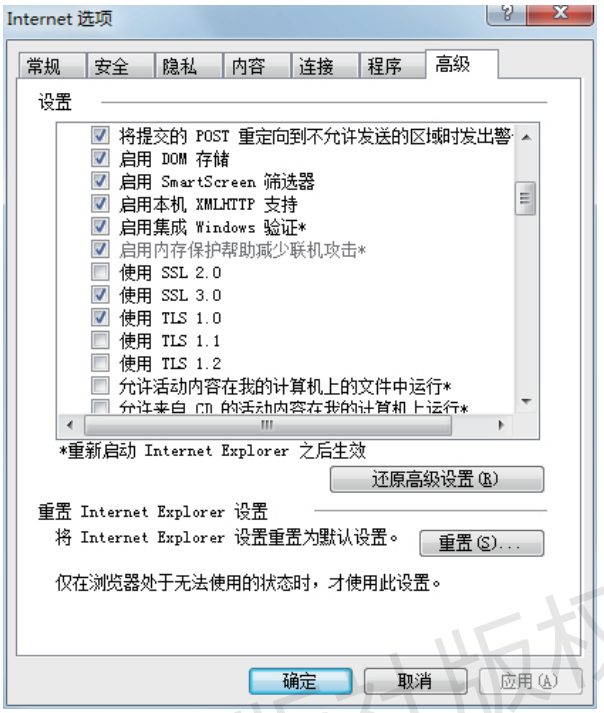


图1-13　SSL客户端设置

SSL VPN 即指采用 SSL 协议来实现远程接入的一种新型 VPN 技术。它包括：服务器认证、客户认证（可选）、SSL 链路上的数据完整性和 SSL 链路上的数据保密性。对于内、外部应用来说，使用 SSL 可保证信息的真实性、完整性和保密性。正因为 SSL 协议被内置于 IE 等浏览器中，使用 SSL 协议进行认证和数据加密的 SSL VPN 就可以免于安装客户端。相对于传统的 IPSec VPN 而言，SSL VPN 具有部署简单、无客户端、维护成本低、网络适应强等特点。

一般而言，SSL VPN 必须满足最基本的两个要求：

（1）使用 SSL 协议进行认证和加密；没有采用 SSL 协议的 VPN 产品自然不能称为 SSL VPN，其安全性也需要进一步考证。

（2）直接使用浏览器完成操作，无须安装独立的客户端。

思考练习

一、填空题

1. 根据 VPN 的用途，可将它分为 _____，_____，_____ 三种应用类型。

2. 消息的原始形式称为 _____，已加密的形式称为 _____。这个变换处理过程称为 _____ 过程，它的逆过程称为 _____ 过程。

3. VPN 的实现技术包括 _____，_____，_____，_____。

4. SSL 协议工作于网络的 _____ 层，是由 _____、_____

两个子协议构成的。

5. 对称密码体制的代表算法有 _____、_____；非对称（公钥）密码体制的最常用的算法是 _____、_____。

二、单项选择题

1. 严格的口令策略应当包含哪些要素（　　）？

A. 同时包含数字、字母和特殊字符　　B. 系统强制要求定期更改口令

C. 用户可以设置空口令　　D. 满足一定的长度，比如 8 位以上

2. 以下关于非对称密钥加密说法正确的是（　　）

A．加密方和解密方使用的是不同的算法　B．加密密钥和解密密钥是不同的

C．加密密钥和解密密钥是相同的　　D．加密密钥和解密密钥没有任何关系

3. 实现数字签名，发送方使用（　　）进行数字签名。

A．签名人的私钥　　B．签名人的公钥

C．接收人的私钥　　D．接收人的公钥

4. 以下关于对称密钥加密说法正确的是（　　）

A．加密方和解密方使用的是不同的算法　B．加密密钥和解密密钥是不同的

C．加密密钥和解密密钥是相同的　　D．加密密钥和解密密钥没有任何关系

5. MD5 算法得出的摘要大小是（　　）。

A．128 位　　B．160 位　　C．128 字节　　D．160 字节

6. SHA-1 算法得出的摘要大小是（　　）

A．128 位　　B．160 位　　C．128 字节　　D．160 字节

7. PPTP、L2TP 和 L2F 隧道协议属于（　　）协议。

A. 第一层隧道　　B. 第二层隧道　　C. 第三层隧道　　D. 第四层隧道

8. VPN 技术的实现过程综合应用了多项技术，其中不包括（　　）

A．隧道技术　　B．加密技术　　C．身份认证技术　　D．访问控制技术

9. IPSec 隧道协议属于（　　）协议。

A. 第一层隧道　　B. 第二层隧道　　C. 第三层隧道　　D. 第四层隧道

三、问答题

1. 哪些情况不适用 VPN 技术？

2. IPSec VPN 和 SSL VPN 进行比较。

3. 常用的消息摘要算法有哪些？

4. 两种加密体制各自的优缺点有哪些？