第 8 章　网络传输的安全

我们知道，在 Windows 2000 系统中，可以通过使用访问控制甚至加密的方式来保护本地计算机上的文件系统。但是，当一个授权用户通过网络从另一台计算机上存储文件时，这些文件就要以非保护的形式在网络上传输，这样就会很容易被非授权的用户通过嗅探、中间人劫持等技术手段来进行截获。

本章将分析 Windows 2000 系统中所采用的一些技术，这些技术不但能够保护网络上传输数据的安全，而且可以保护系统和服务免受通过网络进行的非授权访问。它们包括：

- IPSec（IP 安全协议）
- SSL（Secure Socket Layer，安全套接字层）
- VPN（Virtual Private Networks，虚拟专用网络）

8.1　网络的不安全性

网络操作系统使用的许多传统安全机制都是基于用户名和口令的。Windows 增加的几个安全特性，如加密文件系统（EFS）和智能卡身份验证，它们都只能提供本机的安全性，并不能保护在网络上传输的数据。例如，管理员可以通过设置严格的文件访问权限来保护重要的、敏感的文件，但是当一个授权用户通过网络从远程系统上访问其中一个文件的时候，数据在网络传输过程中就完全不受保护。即使文件是经过加密的，服务器在将它发送给客户之前也要先对其进行解密，所以在网络传输的时候并没有任何保护。下面首先描述一下在网络上对数据及正常服务造成危害的几种常用攻击技术。

8.1.1　网络监听

网络监听攻击技术，又称为网络嗅探技术。对攻击者来说，通过嗅探技术能以非常隐蔽的方式攫取网络中传输的大量敏感信息（例如用户账号及口令）。与主动扫描相比，嗅探行为更难被察觉，也更容易操作。网络上以明文方式传输的任何信息（如 POP3 邮件接收、FTP 文件传输、TELNET 远程登录等）在这种攻击面前都是非常脆弱的。

1．共享环境的嗅探技术原理

在以太网的一个冲突域中，通信是基于广播方式传送数据的，所有的物理信号都会被传送到每一个主机节点。而主机是否真正对此数据进行处理，则取决于该则数据帧的真实目的地址。所有网络接口卡（网卡）都可以监听到在物理介质上传输的所有的数据帧。正常情况下，一个网络接口应该只响应如下两种数据帧：

- 与自己的 MAC 地址相匹配的数据帧
- 发向所有机器的广播数据帧

注意：这里的广播数据帧是另外一个概念，其目的地址不是单个的主机 MAC，而是 0xFFFFFFFFFF 这样的值，表示该数据帧应该让所有的接收节点都处理。

但是，网卡可以被设置成混杂接收模式（Promiscuous）。在这种模式下，无论接收到的数据帧目的地址如何，网卡都能够予以接收。这就是共享式网络环境的嗅探技术原理。

2．交换环境的嗅探技术原理

在使用交换机进行连接的网络环境中，交换机不会将发往单个主机的数据包向所有端口发送，从而避免了利用网卡混杂模式进行的嗅探。但是，可以利用 ARP 欺骗等技术来进行网

络嗅探，使得交换机形同虚设。

按照 ARP 协议的设计，为了减少网络上过多的 ARP 数据通信，一台主机，即使收到的 ARP 应答并非自己请求得到的，它也会将其插入到自己的 ARP 缓存表中，这就造成了“ ARP 欺骗 ”的可能。如果攻击者想监听同一网络中两台主机之间的通信（即使是通过交换机相连），他会分别给这两台主机发送一个 ARP 应答包，让两台主机都“ 误 ”以为对方的 MAC 地址是第三方攻击者所在的主机。这样，双方看似“ 直接 ”的通信连接，实际上都是通过黑客所在的主机间接进行的。在这种嗅探方式中，攻击者所在主机不需要设置网卡的混杂模式，因为通信双方的数据包在物理上都是发送给黑客所在的中转主机的，只要将网卡设置为默认转发数据包即可（类似于一台路由器）。

8.1.2 IP 欺骗

TCP/IP 网络上的每个数据包都包含有源 IP 地址和目的 IP 地址。IP 欺骗（Spoofing）技术就是伪造某台主机的 IP 地址的技术。通过 IP 地址的伪装使得某台主机能够伪装另外的一台主机，而这台主机往往具有某种特权或者被另外的主机所信任。

IP 欺骗通常都需要编写程序来实现。通过使用 RawSocket 编程，发送带有假冒的源 IP 地址的数据包，来达到自己的目的。另外，在 Internet 上也有大量的可以发送伪造的 IP 地址的工具包可用，使用它可以任意指定源 IP 地址，避免留下痕迹。

在网络上常常需要经过身份验证，这种验证一般发生在用户连接到网络上去使用某种资源或服务的时候。一般来说，身份的验证往往发生在应用层上，典型的情况如用户在使用 FTP 进行文件的传输的时候或者使用 Telnet 进行远程登录时，用户需要输入用户名和口令，只有用户名和口令相符和的时候才通过了认证。还有另外的验证，一般用户在使用机器的时候并不感觉到验证的发生，如一些不发生在应用层的验证，这时候的验证往往是计算机之间的认证。计算机之间的相互对话完成验证，计算机之间的验证是自动进行的，只有这样不经过人的干预，才有可能发生伪装的事情。

入侵者可以利用 IP 欺骗的技术获得对主机未授权的访问，因为他可以发出这样的 IP 包，声称来自内部地址。当目标主机利用基于 IP 地址的验证来控制对目标系统中的用户访问时，就可以允许攻击者接收到不应该为其接受的文件。这种技术手段甚至可以使得攻击者获取特权或者普通用户的权限。有的系统即使设置了防火墙，但是如果没有设置对本地域中资源 IP 包地址的规律，那么这种欺骗技术依然可以奏效。

8.1.3 拒绝服务攻击

拒绝服务攻击（Denial of Service, DoS）这种攻击手段使得网络上的目标服务器淹没在大量无用的请求信息之中，消耗网络带宽或系统资源，导致网络或系统不胜负荷以至于瘫痪而停止提供正常的网络服务。这是一种最悠久也最常见的攻击形式，是现今威胁网络安全的主要因素之一。从技术角度看，只要网络系统或应用服务还存在漏洞，只要网络协议的实现还存在隐患，甚至只要提供服务的系统仍然具有网络开放的特性，拒绝服务攻击就会存在。

其实，严格来说，拒绝服务攻击并不是某一种具体的攻击方式，而是攻击所表现出来的结果，就像其字面意义那样，黑客可以采用种种手段，最终使得目标系统因遭受某种程度的破坏而不能继续提供正常的服务，甚至导致物理上的瘫痪或崩溃。具体的操作方法可以是多种多样的，可以是单一的手段，也可以是多种方式的组合利用，但归根结底，其最终目的就是导致目标系统无法正常运行或处理正常的服务请求。

具体来说，拒绝服务攻击大致可以分为 4 类：

- 产生大量无用的突发流量，致使目标网络系统整体的网络性能大大降低，丧失与外界通信的能力，许多自动传播的网络蠕虫往往导致这样的结果。

- 利用目标主机提供的网络服务以及网络协议的某些特性，发送超出目标主机处理能力的“正常”服务请求，导致目标主机丧失对其他正常服务请求的响应能力。
- 利用目标主机系统或应用软件实现上的漏洞或缺陷，发送经过特殊构造的数据包，导致目标主机的瘫痪，例如针对 Windows 系统的带外攻击。
- 针对目标系统的特定漏洞，在目标系统本地运行特意编制的破坏程序或特殊形式的系统操作，致使系统崩溃。

8.1.4 应用层攻击

在许多情况下，运行在网络系统上的应用程序的安全性是不完善的，使得攻击者能够通过某些手段损害系统，如修改操作系统、应用程序或数据文件；植入病毒或远程控制程序等非授权软件；破解应用程序或操作系统中的访问控制机制。这种攻击尤其针对 Web 服务器上的应用为多，如由于 ASP、PHP 脚本程序书写得不严谨引发的“SQL Injection”攻击时常发生。

8.2 IPSec

IPSec 是一种安全协议，通过对传输之前的每个 IP 数据包进行加密来保护网络传输。当使用 IPSec 来保护数据时，发送系统先把各个单独的数据包加密，然后再以普通的方式传输。直到数据包到达最终目的地时才进行解密操作。如此，截获网络传输数据的时候只能得到数据的加密形式，这对攻击者来说是毫无用处的。

IPSec 是在网络层上的加密操作。这项技术也意味着转发数据包的中间主机不必支持 IPSec，因此可以通过 WAN 连接 LAN 上部署 IPSec，并且能够在使用拨号或虚拟专用网（VPN）连接的远程访问连接上部署 IPSec。而数据链路层上的加密操作只是保护各个中间链路上的数据，因此处理数据包的每个路由器将不得不对接收端的数据包解密并在转发它们之前重新对其加密，这不但增加了路由器的处理开销而且限制了支持 IPSec 的路由器的使用。网络层加密也意味着对工作站的所有输出业务都进行保护，而不管这些业务是由什么系统或进程产生的。而后面讨论的用来保护 Web 客户/服务器通信的安全套接层（SSL）协议就是工作在 OSI 参考模型的最高层—应用层上，因此客户和服务器应用程序都必须支持该协议，它才能正常的发挥作用。

Windows 2000 IPSec 是一个可靠的 IPSec 版本，Windows 2000 系统通过 Windows 2000 IPSec 简化了网络安全的部署和管理。

8.2.1 IPSec 标准

IPSec 是由 Internet 工程任务组（IETF）作为用于 Internet 协议（IP）的安全体系结构而设计，它建立在 IETF 所批准的一系列标准文档的基础之上。IPSec 定义了 IP 数据包格式和相关基础结构，以便为网络通信提供端对端、加强的身份验证、完整性、反重播和保密性。使用 IETF 定义的 Internet 密钥交换（IKE，在 RFC 2409 中定义），还提供了按需要的安全协商和自动密钥管理服务。

而 Windows 2000 中的 IPSec 实现和相关的服务则是由 Microsoft 和 Cisco Systems, Inc 共同开发的。它们建立在以下一些有关 IPSec 的 RFC 文档基础之上。

- RFC 2401：Security Architecture for the Internet Protocol
- RFC 2402：IP Authentication Header
- RFC 2403：The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404：the Use of HMAC-SHA-1-96 within ESP and AH

- RFC 2405：The ESPDES-CBC Cipher Algorithm With Explicit IV
- RFC 2406：IP Encapsulating Security Payload(ESP)
- RFC 2407：The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408：Internet Security Association and Key Management Protocol(ISAKMP)
- RFC 2409：The Internet Key Exchange(IKE)
- RFC 2410：The NULL Encryption Algorithm and Its Use With IPSec
- RFC 2411：IP Security Document Roadmap
- RFC 2412：The OAKLEY Key Determination Protocol

8.2.2 IPSec 基础

IPSec 使用两种不同的协议向系统提供不同的安全级别：IP 验证报头（AH）和 IP 封装安全载荷（ESP）。IPSec 协议（包括 AH 和 ESP）既可用来保护一个完整的 IP 数据包，也可用来保护某个 IP 数据包的上层协议，这两方面的保护分别是由 IPSec 的两种不同的模式来提供的：传输模式和隧道模式。

1. 传输模式和隧道模式

在 IPSec 的传输模式中，IP 头与上层协议头之间插入一个特殊的 IPSec 头；而在隧道模式中，要保护的整个 IP 包都需加密封装到另一个 IP 数据包里，同时在外部与内部 IP 头之间插入一个 IPSec 头。这两种模式的区别如图 8-1 所示。

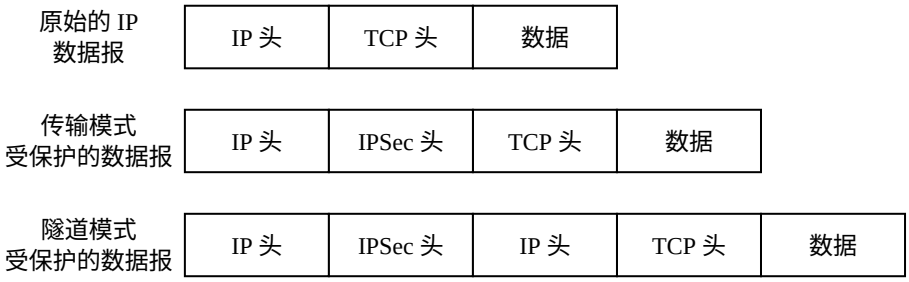

图 8-1　处于传输模式和隧道模式下的受 IPSec 保护的 IP 数据报

两种 IPSec 协议（AH 和 ESP）均能同时以传输模式或者隧道模式工作。

传输模式用来保证在同一 LAN 上或通过专用 WAN 链路连接起来的系统之间的客户对客户的安全性。在传输模式下，两个端的系统都必须支持 IPSec，而中间节点系统不必支持 IPSec，它们只是以普通的方式转发数据包。

隧道模式用于网关对网关的连接，例如通过需要最大安全性的 Internet 连接虚拟专用网络（VPN）的那些连接。在隧道模式下，只有提供安全服务的网关才必须支持 IPSec。隧道通过 Internet 连接两个网络的情况下，数据包的源和目的终端都不必支持 IPSec。产生数据包的系统把数据包传送的本地网络中的一个网关上，此网关把数据包封装到带有 IPSec 安全性的 IP 数据包中，并通过 Internet 把它们传送到另一个网络中的一个网关上。远程网关接收到数据包，解密数据并进行所需的校验，然后用普通的 IP 数据包或任何其他的网络层协议把数据发送到目标系统上，如图 8-2 所示。

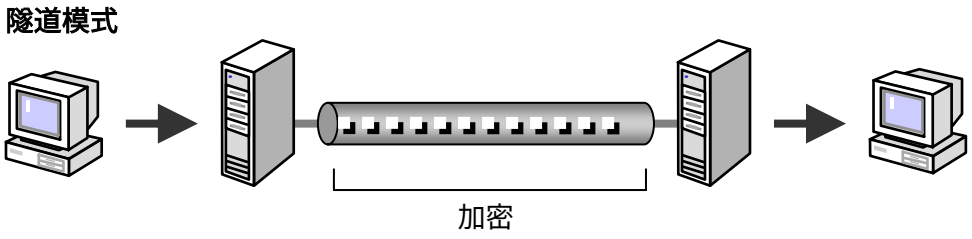

图 8-2 IPSec 的隧道模式

2. 封装安全载荷（ESP）

ESP（Encapsulating Security Payload）是属于 IPSec 的一种协议，可用于确保 IP 数据包的机密性（未被他人看过）、数据的完整性以及对数据源的身份验证。此外，它也要负责对重播攻击的抵抗。

具体的实现原理是在 IP 头（以及任何 IP 选项）之后，要保护的数据（传输层协议以及由创建该数据包的应用程序所产生的数据）之前，插入一个新头，也就是 ESP 头。受保护的数据可以是一个上层协议，或者是整个 IP 数据包（这取决于采用的是传输模式还是隧道模式）。最后，还要在数据包的最后追加一个 ESP 尾，如图 8-3 所示。

图 8-3　受 ESP 保护的 IP 数据包

ESP 是一种新的 IP 协议，对 ESP 数据包的标识是通过 IP 头的协议字段来进行的。假如这个字段的值为 50，就表明这是一个 ESP 包，而且紧接在 IP 头后面的是一个 ESP 头。

3. 验证报头（AH）

与 ESP 类似，AH 也提供了数据完整性、数据源验证以及抗重播攻击的能力，但不能用它来保证数据的机密性。

AH 给标准的 IP 数据包增加了另一个报头，这个 AH 报头接在原来的 IP 报头之后，紧接着下一个报头就是要保护的数据，如图 8-4 所示。

图 8-4　受 AH 保护的 IP 数据包

如果数据包中含有其他的 IPSec 协议（如 ESP），那么这些协议的报头就应该紧跟在 AH 报头之后。IP 报头中的“协议”字段必须标识出现在数据包中的下一个报头。在带有 AH 报头的数据包中，“协议”字段的值为 51，而 AH 报头中的“下一报头”字段值标识了传输层协议报头。

4. 安全联盟（SA）

为了能够正确封装及提取 IPSec 数据包，有必要采取一套专门的方案，将安全服务、密

钥与要保护的通信数据联系到一起，同时要将远程通信实体与要交换密钥的 IPSec 数据传输联系到一起。换言之，要解决如何保护通信数据、保护什么样的通信数据以及由谁来实行保护的问题，这样的构建方案称为安全联盟（Security Association, SA）。

IPSec 的 SA 是单向进行的。也就是说，它仅朝一个方向定义安全服务，要么对通信实体收到的包进行“ 进入 ”保护，要么对实体外发的包进行“ 外出 ”保护。具体采用什么方式，要由三方面的因素决定：第一个是安全参数索引（SPI），该索引存在于 IPSec 协议头内；第二个是 IPSec 协议值；第三个是要向其应用 SA 的目标地址，它同时决定了方向。通常，SA 是以成对的形式存在的，每个朝一个方向。既可人工创建它，亦可采用动态的创建方式。SA 驻留在安全联盟数据库（SADB）内。

IPSec 的基本架构定义了用户能以多高的精度来设定自己的安全策略。这样一来，某些通信便可以统一为其设置某一级的基本安全措施，而对其他通信则可谨慎对待，为其应用完全不同的安全级别。举个例子：管理员可在一个网络安全网关上制订 IPSec 策略，对在其本地保护的子网与远程网关的子网间通信的所有数据，全部采用 DES 加密，并用 HMAC-MD5 进行验证；从远程子网发给一个邮件服务器的所有 Telnet 数据均用 3DES 进行加密，同时用 HMAC-SHA 进行验证；最后对于需要加密的、发给另一个服务器的所有 Web 通信数据，则用 IDEA 满足其加密要求，同时用 HMAC-RIPEMD 进行验证。

IPSec 策略由安全策略数据库（Security Policy Database, SPD）加以维护。在 SPD 这个数据库中，每个条目都定义了要保护的是什么通信、怎样保护它以及和谁共享这种保护。对于进入或离开 IP 堆栈的每个数据包，都必须检索 SPD 数据库，调查可能的安全应用。对一个 SPD 条目来说，它可能定义了这样几种行为：丢弃、绕过以及应用。其中，丢弃表示不让这个包进入或外出；绕过表示不对一个外出的包应用安全服务，也不指望一个进入的包进行了保密处理；而应用是指对外出的包应用安全服务，同时要求进入的包已应用了安全服务。对那些定义了应用行为的 SPD 条目，它们均会指向一个或一套 SA，表示要将其应用于数据包。

IPSec 通信到 IPSec 策略的映射关系是由选择符（Selector）来建立的。选择符标识通信的一部分组件，它既可以是一个粗略的定义，也可以是一个非常细致的定义。IPSec 选择符包括：目标 IP 地址、源 IP 地址、名字、上层协议、源和目标端口以及一个数据敏感级（假如也为数据流的安全提供了一个 IPSec 系统）。这些选择符的值可能是特定的条目、一个范围或者是一个“ 不透明 ”。在策略规范中，选择符之所以可能出现“ 不透明 ”的情况，是由于在那个时刻，相关的信息也许不能提供给系统。举个例子来说，假定一个安全网关同另一个安全网关建立了 IPSec 通道，它可指定在该通道内传输的（部分）数据是网关背后的两个主机之间的 IPSec 通信。在这种情况下，两个网关都不能访问上层协议或端口，因为它们均被终端主机进行了加密。“ 不透明 ”亦可作为一个通配符使用，表明选择符可为任意值。

假定某个 SPD 条目将行为定义为应用，但并不指向 SADB 数据库内已有的任何一个 SA，那么在进行任何实际的通信之前，首先必须创建那些 SA。如果这个规则用于自外入内的进入（Inbound）通信，而且 SA 尚不存在，则按照 IPSec 基本架构的规定，数据包必须丢弃。假如该规则用于自内向外的外出（Outbound）通信，则通过 Internet 密钥交换，便可动态的创建 SA。

IPSec 结构定义了 SPD 和 SADB 这两种数据库之间如何沟通，这是通过 IPSec 处理功能——封装与拆封来实现的。此外，它还定义了不同的 IPSec 实施方案如何共存。然而，它却没有定义基本 IPSec 协议的运作方式。这方面的信息包含在另外两个不同的文件中，一个定义了封装安全载荷（RFC2406），另一个对验证头（RFC2401）进行了说明。

8.2.3 Windows 2000 中的 IPSec

Windows 2000 系统包含了 Internet 工程任务组的 IPSec 协议。Windows 2000 的 IPSec 提供了带防御保护网络关键线路的网络管理器。

大多数传统的 Windows 网络安全策略将重点放在防止来自企业网络外面的攻击。防火墙、安全路由器以及拨号访问的令牌身份验证都是防御外来威胁的管理举措。但加强网络外围并不能抵御来自内部的攻击。事实上，来自员工、辅助人员或承包商的内部攻击，可使单位泄露大量的敏感信息。防火墙对这种内部威胁并不能提供任何保护。

Windows 2000 与 IPSec 协议集成的一个最大优点就是具有保护来自内部和外部攻击的能力。另外，该操作是透明完成的，不会给单个用户增加任何麻烦或额外的开销。Internet 工程任务组（IETF）定义：IPSec 使用身份验证报头（AH）以及封装的安全措施负载（ESP），身份验证报头给数据通信提供了源身份验证和完整性。封装的安全措施负载除提供身份验证和完整性外，还提供保密性。有了 IPSec，只有发送者和接收者知道安全密钥。如果身份验证数据是有效的，那么接收者知道该通信是来自发送者，并且在传输过程中数据没有被更改。Windows 2000 中的 IPSec 建立在 IETF 模型上，它将公钥与私钥加密技术结合起来，并提供自动密钥管理，因而能提供最大的安全性和高速的吞吐量。它可以将身份验证、完整性、反重播以及保密性（可选）结合起来，从而保障安全通信。

由于 Windows IP 安全机制部署在传输层的下面，所以网络管理员（和软件供应商）就不用一次一个应用程序地部署和协调安全，省去了很多麻烦和开销。通过部署 Windows 2000 系统，应用程序可以自动继承 Windows 2000 的安全保障功能，网络管理员也可以给整个网络提供更强大的保护层。Windows IPSec 的加密支持也已扩展到了虚拟专用网络（VPN）之中。

IPSec 与 Windows 2000 的集成由于以下一些因素使得网络及安全管理员从中受益。

- 开放的工业标准：IPSec 提供了一个开放的工业标准方法，替代专用的 IP 加密技术。由此产生的互操作性，使网络管理员从中受益。
- 透明性：IPSec 在传输层下面工作，对应用程序和用户来说都是透明的，这就意味着，当 IPSec 在防火墙或路由器中实现时，无须更改用户桌面上的网络应用程序。
- 身份验证：强大的身份验证服务，可防止使用假冒身份的人员截获数据。
- 保密性：当敏感数据在通信双方之间传输时，保密性服务可防止未经授权的人员访问数据。
- 数据完整性：IP 身份验证报头和散列消息身份验证代码的变化，保证了通信过程中数据的完整性。
- 动态密钥重设：在进行通信的过程中，动态密钥重设有助于保护数据不受攻击。
- 端到端安全链接：Windows IPSec 为企业同一域内以及任何受信任域间的专用网络用户提供了端到端的安全链接。
- 集中管理：网络管理员使用安全策略和筛选器，根据用户、工作组或其他标准，提供相应的安全等级。集中管理降低了管理成本。
- 灵活性：Windows IPSec 提供了很大的灵活性，可允许将策略应用到企业范围内或单个工作站上。

Windows 2000 充分利用了强大的工业标准的加密算法和身份验证技术。其中包括：

- Diffie-Hellman 技术：因其发明人 Whitfield Diffie 和 Martin Hellman 而得名，它是一个公钥加密算法，允许两个通信实体协商确定一个共享的密钥。Diffie-Hellman 以交换公共信息的两个通信实体开始。每个实体将另一个实体的公共信息与自己的私有信息结合起来，生成一个共享的密钥值。
- 散列消息身份验证代码（HMAC）及变体：HMAC 是一个提供完整性和身份验证

的密钥算法。使用加密散列的身份验证给数据包生成一个数字签名，这个数字签名可以由接收者验证。如果消息在传输过程中发生改变，散列值也会改变，IP 数据包就会被拒绝。

- HMAC-MD5：是一个产生 128 位值的散列函数。
- HMAC-SHA：是一个产生 160 位值的散列函数。尽管 HMAC-SHA 比 HMAC-MD5 稍慢，但它比 HMAC-MD5 更安全。
- DES-CBC：数据加密标准（DES）—密码块链（CBC）是一个保证保密性的密钥算法。它生成一个随机数，此随机数与密钥一起使用来给数据加密。

8.2.4 Windows 2000 的 IPSec 组件

Windows 2000 的 IPSec 建立于 IETF 的 IPSec 体系结构之上，与 Windows 2000 域和活动目录（Active Directory）服务集成。活动目录使用组策略为 Windows 2000 域成员提供 IPSec 策略的分配和分发，提供基于策略的、支持目录的网络。

Windows 2000 系统中的 IPSec 结构如图 8-5 所示：

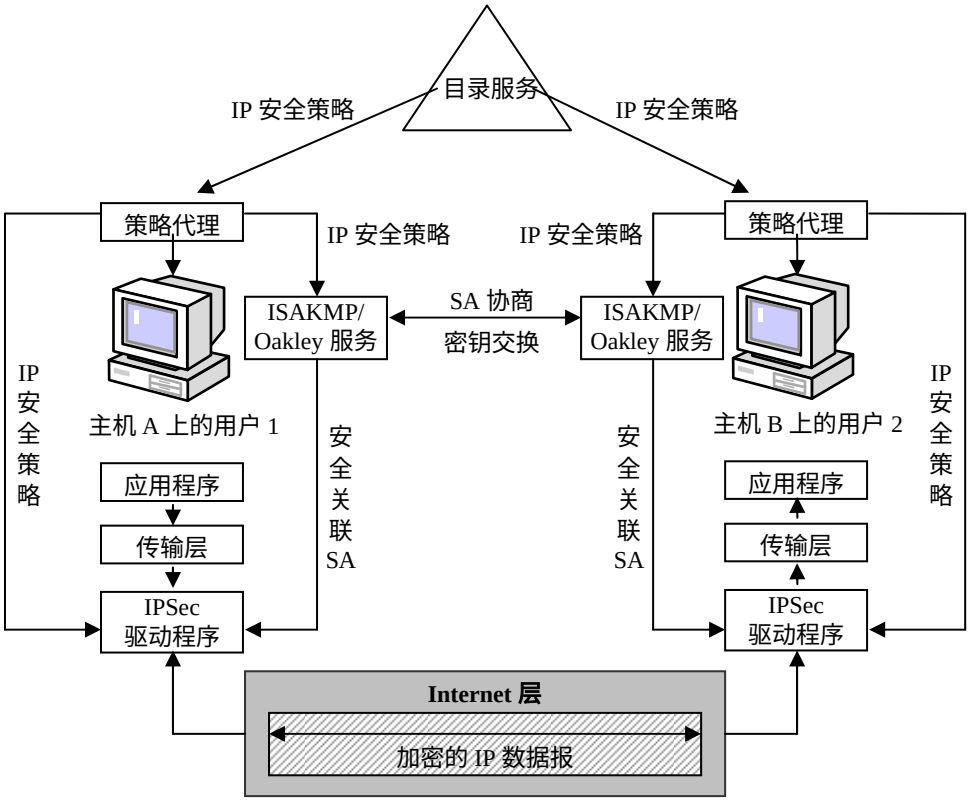

图 8-5 Windows 2000 IPSec 结构图

IPSec 结构中包括以下组件。

1. IPSec 策略

IPSec 使用策略来存储它所提供的各种安全服务的配置信息。这些策略使得管理员能够通过选择允许的通信类型以及决定如何保护哪些通信来实现 IPSec 安全。然后，管理员可以把策略与用户、组或其他的活动目录服务的结构对象关联起来。

2. IPSec 策略管理（IPSec Policy Management）

这是用于 Microsoft 管理控制台（MMC）应用的一个管理单元，通过这个管理单元可以建立和管理 IPSec 策略。

3. IPSec 策略代理服务

在支持 IPSec 的各个系统上运行的这一服务，访问存储在活动目录或本地系统注册表中的 IPSec 策略信息并把这些信息转发到 IPSec 驱动程序中。

4. Internet 密钥交换（IKE）

简而言之，IKE 是一种建立 SA 和在两个系统之间交换密钥的协议。RFC2409 为 IKE 定义了一个两阶段的过程。第一阶段包括建立第一阶段的 SA，即系统之间的一个安全身份验证方法的协商，经验证的通信隧道。建立第一阶段的 SA 包括对系统将要使用的加密算法、散列算法和身份验证方法的协商，接下来便是身份验证过程本身。第二阶段是为 IPSec 服务建立两个 IPSec 协议（AH 和/或 ESP）、散列算法（MD5 或 SHA1）和加密算法（DES 或 3DES）的协商，以及身份验证和加密密钥的交换与刷新。

IKE 的实现提供三个基于 IETF 标准的身份验证方法以在计算机之间建立信任。

- 基于 Windows 2000 域基础结构提供的 Kerberos v5 身份验证，用于在一个域中或在几个受信任域中的计算机之间部署安全通信。
- 使用证书的公钥/私钥签名，与多个证书系统兼容，包括 Microsoft、Entrust、VeriSign 和 Netscape。
- 密码，用术语表示为“预先共享的身份验证密钥”，严格用于建立信任—不用于应用程序数据包保护。

一旦对等计算机互相进行了身份验证，它们就会产生大量密钥以便对应用程序数据包加密。这些密钥只为这两台计算机所知，因此它们的数据能得到很好的保护，免受可能在网络上的攻击者的修改或破译。每一台对等计算机都使用 IKE 来协商使用什么类型和强度的密钥，以及采用什么安全方式来保护应用程序通信。这些密钥根据 IPSec 策略的设置自动刷新以在管理员的控制下提供固定的保护。

5. IPSec 驱动程序

驱动程序接收来自当前有效的并且监视网络通信的 IPSec 策略的过滤清单。当驱动程序检测到与过滤清单中的某一项相匹配的出站数据包时，驱动程序就命令 IKE 开始与目标系统进行密钥交换。一旦与其他系统建立了 SA，驱动程序就在 IPSec 协议报头中插入适当的值，并执行任何必要的加密任务。对于入站的数据包，如果必要的话，驱动程序就通过重复发送系统所执行的计算来校验签名，并且解密包数据。

所以，一旦 IPSec 策略发挥作用，一个典型的数据交换就会按照下列步骤进行：

（1）工作站 A 上的用户产生一个报文并把它发送给工作站 B 上某一特定用户的应用程序中。

（2）工作站 A 上的 IPSec 驱动程序将报文的目的 IP 地址或协议与当前有效的 IPSec 策略中的 IP 过滤清单中相比较。

（3）如果 IPSec 策略规定系统间的通信是安全的，那么 IPSec 驱动程序就指示 IKE 开始与工作站 B 协商。

（4）工作站 B 的 IKE 收到一条来自工作站 A 的 IKE 请求安全协商的报文。

（5）两个系统协商第一阶段的 SA 和第二阶段的两个 SA（入站 SA 和出站 SA）。

（6）工作站 A 上的 IPSec 驱动程序使用为第二阶段出站 SA 而商定的参数，为输出数据计算完整性签名，加密数据，并通过给 IP 数据包增加适当的报头字段来构造 IPSec 数据包。

（7）工作站 A 把完成的数据包传送到工作站 B，工作站 B 再把它们传给自己的 IPSec 驱动程序。

（8）工作站 B 的 IPSec 驱动程序使用入站 SA 的参数，解密数据，并通过重复计算签名和比较签名与数据包中的结果来验证数据包的完整性。

（9）工作站 B 上的 IPSec 驱动程序把解密过的数据传送到 TCP/IP 协议栈，TCP/IP 协议栈再依次把它上传到报文原来的目的地，即应用程序。

8.2.5 实现 Windows 2000 的 IPSec

1. 估计攻击者

无论对于大型的域还是小型的工作组，实现 IPSec 就意味着在使大量用户容易使用信息和防止对敏感数据进行未授权访问之间达到平衡。下面是正确找到平衡要求的方法：

- 评估风险并为本组织确定正确的安全级别
- 标识重要的信息
- 定义使用风险管理标准和保护标识信息的安全策略
- 决定在现存组织中实现策略的最佳方式
- 确保管理和技术要求到位

根据用户的需要，为所有用户提供对适当资源安全而有效的访问。

使用计算机的方式也会影响安全考虑事项。例如，所需的安全可能会有所不同，这取决于计算机是域控制器、Web 服务器、远程访问服务器、文件服务器、数据库服务器、Intranet 客户还是远程客户。Windows 2000 安全构架可以完成最苛刻的安全要求。但是，如果没有认真的计划和评估、有效的安全指导方针、强制性、审核和明智的安全策略设计和分配，仅靠软件的实现效果不大。

2. 确定安全级别

定义标准安全没有明确的尺度。根据组织的策略和基础结构，可能会有很大的区别。可以将下列安全级别作为计划 IPSec 配置的一般基础。

（1）最低安全性

计算机不交换敏感的数据。默认情况下，IPSec 不活动，需要禁用 IPSec 的管理措施。

（2）标准安全

计算机（尤其是文件服务器）用来存储有价值的数据。安全必须平衡，使其不会阻碍验证试图执行任务的用户的合法性。Windows 2000 提供预定义的保护数据的 IPSec 策略，但不需要最高的安全级别：客户（仅响应）和服务器（请求安全设置）。这些策略以及类似的自定义策略将优化效率，而且不会危及安全。

（3）高安全性

包含高度敏感数据的计算机存在数据失窃、意外或恶意破坏系统（尤其在远程拨号方案中）或任何公共网络通信的危险。“ 安全服务器 ”（要求安全）是预定义的策略，它要求对发送或接收的所有交通进行保护。“ 安全服务器 ”（要求安全）包括强大的机密性和完整性算法、完整转寄保密、密钥生存期和限制、强大的 Diffie-Hellman 组。不支持 IPSec 的计算机导致通信不安全，失败的安全协商被阻塞。

3. 预定义的 IP 安全策略

Windows 2000 提供了一套预定义的 IPSec 策略，如图 8-6 所示。默认情况下，所有预定义的策略都是为 Windows 2000 域成员计算机设计的。预定义的策略无须进一步操作就可以指派，也可以对其进行修改，或者将其用作自定义策略的模板。

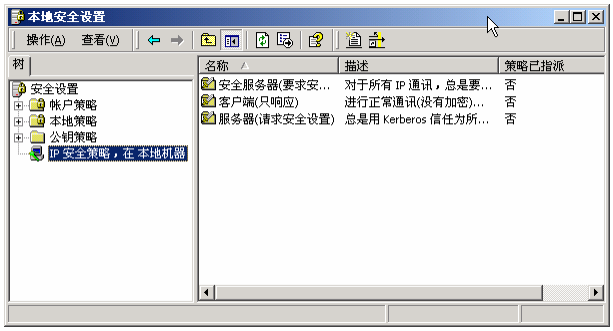

图 8-6　预定义的 IPSec 策略

- 客户端（只响应）

该策略用于在大部分时间都不能保证通信的计算机。例如，企业内部网客户可能不需要 IPSec，除非另一台计算机发出请求。该策略允许在它活动的计算机上正确响应安全通信请求。该策略包含一个默认的响应规则，该规则允许与请求 IPSec 的计算机进行协商。对于该通信，只有被请求的协议和端口传输才是安全的。

- 服务器（请求安全性）

该策略用于应在大多数时间保证通信的

计算机。该策略的一个例子就是传输敏感数据的服务器。在该策略中，计算机接受不安全的传输，但总是通过从原始发送者那里请求安全性来试图保护其他的通信。如果另一台计算机没有启用 IPSec，则该策略允许整个通信都是不安全的。

- 安全服务器（需要安全性）

该策略用于始终需要安全通信的计算机。该策略的一个例子就是传输高度敏感数据的服务器，或者保护内部网不受外界侵犯的安全性网关。该策略拒绝不安全的传入通信，并且传出的数据始终都是安全的。不允许不安全的通信，即使对方没有启用 IPSec。

4. IP 安全策略的管理

管理员可以通过 Microsoft 管理控制台（MMC）来创建、配置和指派 IPSec 策略。既可以集中管理策略（针对 Active Directory 客户）、在本地管理策略（正在运行该管理单元的计算机），也可以远程管理计算机或域策略，如图 8-7 所示。

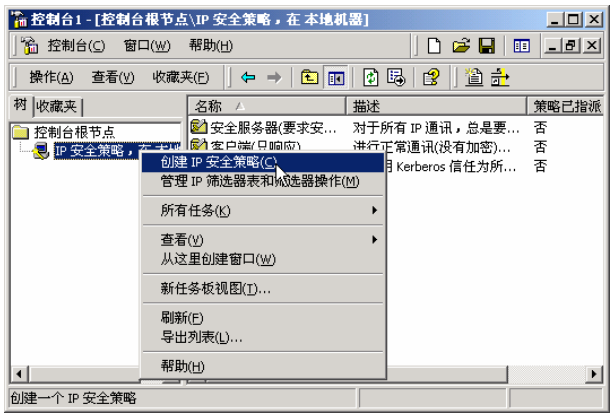

图 8-7　IPSec 策略的管理

对于存储在活动目录（Active Directory）中的策略，“ 组策略 ” 对象定义账户和资源的访问、配置和使用设置。IPSec 策略可以指派给计算机账户、站点、域或组织单位的 “ 组策略 ” 对象。IPSec 策略应用于 Active Directory 对象的 “ 组策略 ” 对象时，该 IPSec 策略传播到所有受该 “ 组策略 ” 影响的计算机账户。

下面是在活动目录中指派 IPSec 策略时要注意的一些事项。

- 如果计算机是域的成员，则应用于域的 IPSec 安全策略将优先于本地的活动 IPSec 策略。
- 指派给 Active Directory 中组织单位的 IPSec 策略将覆盖该组织单位中所有成员的域级策略，最低级组织单位 IPSec 策略将替代该组织单位中所有成员的较高级别组织单位的 IPSec 策略，而不是合并。
- 指派最高可能级别的策略可以提供最大的影响范围，并且对管理的影响最小。
- 即使在指派使用 IPSec 策略的“组策略”对象删除后，IPSec 策略仍将保持活动。在删除策略对象前必须未指派 IPSec 策略。如果删除策略对象并指派了策略，则 IPSec 策略代理将只是假设你不能找到策略并使用缓存的副本。
- 备份和还原 Active Directory 中的组策略时，必须包括 IPSec 策略才能确保一致性。
- IPSec 策略代理仅检查 Active Directory 中更新为活动或指派的策略。如果在 Active Directory 中创建了“新的”IPSec 策略，或者 IPSec 策略已经改变，并指派给某个客户计算机，Winlogon 服务将在其下一个轮询组策略变化周期中发现这些变化，并通知 IPSec 策略代理，然后将这些改变应用于客户计算机。

而对于单独的计算机来说，每个运行 Windows 2000 的计算机都只有一个组策略对象，通常称为本地计算机策略。通过该本地组策略对象，无论是在 Active Directory 环境中，还是在网络环境中，组策略设置都可存储在单个计算机中。因为其设置可被与站点、域或组织单位关联的组策略对象覆盖，所以本地组策略对象是 Active Directory 中影响力最小的一个。在非网络环境中（或没有 Windows 2000 域控制器的网络环境中），本地组策略对象设置较为重要，因为没有其他组策略对象可以覆盖它。

5. IP 安全策略的规则

IP 安全策略由多条规则所组成。而每条规则是由 IP 筛选器列表和 IP 筛选器操作所组合而成的（还包括身份验证方法、隧道设置、连接类型等设置），如图 8-8 所示。

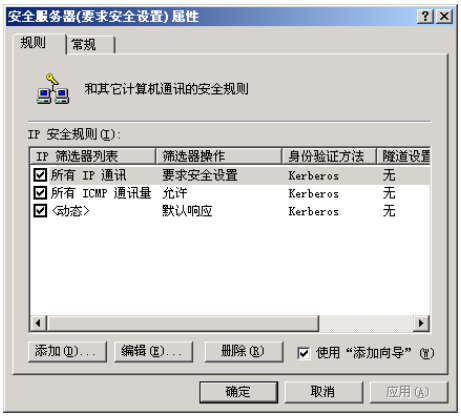

图 8-8 IPSec 策略的组成

每个 IP 安全策略都有预定义的规则，即默认响应的规则。所提供的默认响应规则无须进一步操作即可激活，也可以对其进行修改，以满足特定的需要。它被添加到每一个新创建的策略中，但并不自动激活。它用于任何不需要安全性，但在其他的计算机请求安全通信时必须能够正确响应的计算机。

与预定义的规则相似，也有预定义的 IP 筛选器操作。所提供的预定义筛选器操作无需进一步的操作即可激活，也可以对其进行修改，或者作为定义自定义筛选器操作的模板。它们在任何新建的和现有的规则中都可以被激活。

6. IP 筛选器列表

IP 筛选器列表触发建立在与源、目标及 IP 传输类型匹配的基础上的安全协商，如图 8-9 所示。这种类型的 IP 包筛选允许网络管理员准确定义哪些 IP 传输将受到保护。每个 IP 筛选器列表包含一个或多个 IP 筛选器，它定义了 IP 地址和传输类型。所以，一个 IP 筛选器列表可用于多个通信的情形。

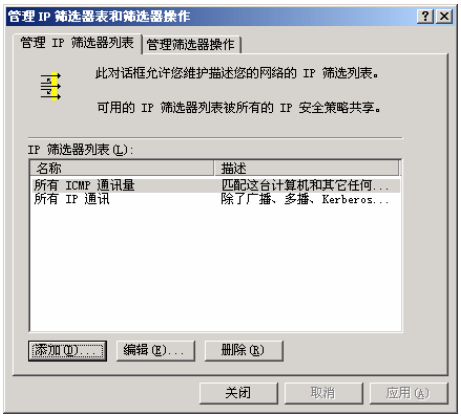

图 8-9　管理 IP 筛选器列表

IPSec 需要在筛选器列表中指定的计算机之间同时有入站和出站筛选器。入站筛选器适用于传入的通信，并允许接收端的计算机响应安全通信请求，或者按照 IP 筛选器列表匹配通信。出站筛选器适用于传出的通信，并触发一个在通信发送之前进行的安全协商。例如，如果计算机 A 要与计算机 B 安全地交换数据：

- 计算机 A 上的活动 IPSec 策略必须有针对计算机 B 的任何出站包的筛选器。Source=A 且 Destination=B。
- 计算机 A 上的活动 IPSec 策略必须有针对计算机 B 的任何入站包的筛选器。Source=B 且 Destination=A。

每一方都必须有反向的筛选器：

- 计算机 B 上的活动 IPSec 策略必须有针对计算机 A 的任何入站包的筛选器。Source=A 且 Destination=B。
- 计算机 B 上的活动 IPSec 策略必须有针对计算机 A 的任何出站包的筛选器。Source=B 且 Destination=A。

每个 IP 筛选器列表是由多个 IP 筛选器所组成的，如图 8-9 所示。

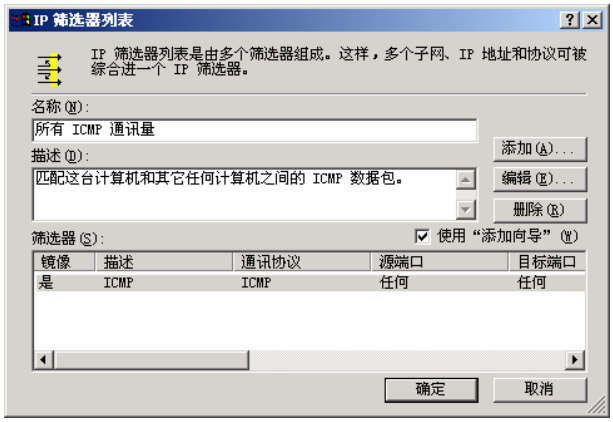

图 8-10　IP 筛选器列表的组成

每个筛选器定义一个应受保护的入站和出站网络通信子集。必须有一个筛选器包含任何相关规则都适用的通信。筛选器包含如下设置。

- IP 数据包的源和目的地址。它可以在单节点级配置，使用一个 IP 地址或 DNS 名称，或者使用一组地址、子网或网络。

- 正在传输的数据包所使用的传输协议。它自动默认包含 TCP/IP 协议簇中的所有协议。然而，可将其配置为单个协议级以满足特殊的需要，包括客户端协议。
- TCP 和 UDP 协议的源和目的端口。默认情况下，所有的端口都包含在内，但是它可以被配置为只适用于一个特定的端口。

7. 筛选器操作

筛选器操作用来定义数据传输的安全需求。筛选器操作可以配置为：

- 用作通过策略（“ 许可 ”）。它不允许安全通信协商。IPSec 简单忽略在这种情况下的通信。这对于来自像 Web 视频服务器这样根本不必保护的单向广播通信是合适的。在实际操作中，应将 IP 筛选器列表限定在最小的范围内。
- 阻塞通信（“ 阻止 ”）。这将阻塞来自未授权的计算机的通信。在实际操作中，应将 IP 筛选器列表限定在最小的范围内。
- 允许与未启用 IPSec 的计算机进行通信（“ 接受不安全通信，但响应时总使用 IPSec ” 和 “ 允许与不识别 IPSec 的计算机进行不安全通信 ”）。这是一个在必要时将回到不安全通信的筛选器操作。在实际操作中，应将 IP 筛选器列表限定在最小的范围内。否则，如果协商失败，任何一个受该筛选器操作所在的规则影响的通信都有可能导致数据被不安全传输。
- 启用会话密钥的完整转寄保密（PFS），它将决定如何生成新的密钥。启用 PFS 可以保证用来保护传输的密钥不被用来生成任何其他的密钥。另外，密钥的密钥材料不能用来生成任何新的密钥。会话密钥 PFS 并不需要重新验证，因而使用的资源比主密钥 PFS 要少。当启用了会话密钥 PFS 时，新的密钥交换将被执行以便在新的会话密钥生成之前积聚新的密钥材料。
- 指定安全要求（“ 使用这些安全设置 ”）。需进行协商的安全需求列表称为 “ 安全方法 ”。每种方法都定义了需协商的算法、安全协议和密钥的生命期。

下面说明了添加或编辑筛选器的操作：

（1）进入 “ 管理 IP 筛选器表和筛选器操作 ” 的 “ 管理筛选器操作 ” 界面，如图 8-11 所示。

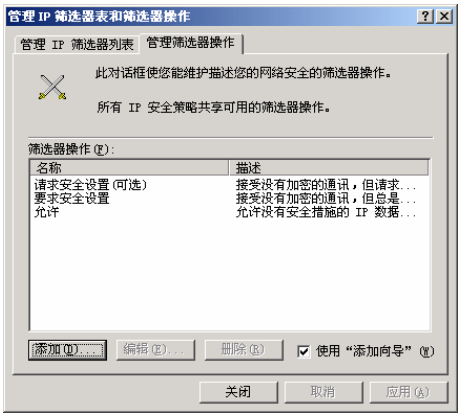

图 8-11 添加 “ 筛选器操作 ”

（2）点击 “ 添加 ” 按钮，请确认选中了 “ 使用添加向导 ” 复选框。

（3）使用 “ 添加筛选器操作 ” 向导进行操作。

（4）输入筛选器操作的名称，如图 8-12 所示。

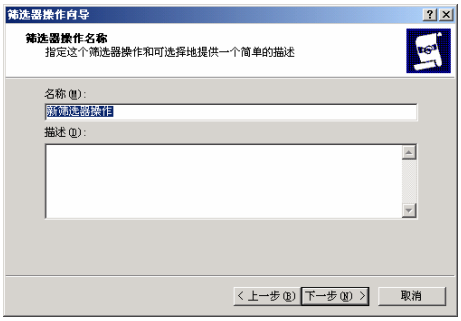

图 8-12　输入筛选器操作的名称

（5）选择筛选器操作，如图 8-13 所示。

- 单击“ 许可 ”允许以明文发送或接收数据包。这些数据包将不请求安全性。
- 单击“ 阻止 ”强制立即丢弃符合筛选器条件的数据包。这些数据包将不请求安全性。
- 单击“ 协商安全 ”使用“ 安全方法首选顺序 ”中的安全方法列表为符合筛选器的数据包提供安全性。这些数据包将来的安全请求将被接受。

图 8-13　设置筛选器操作的行为

（6）设置完筛选器操作后，双击该 IP 筛选器操作的条目，弹出该筛选器操作的属性对话框，如图 8-14 所示。

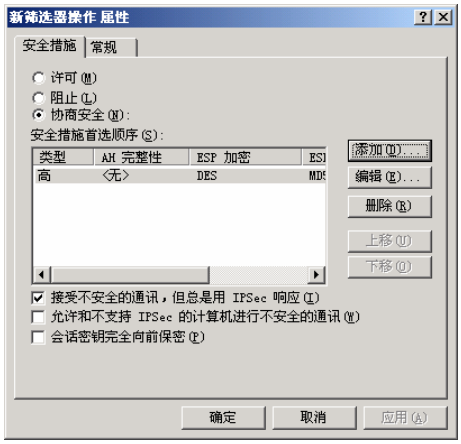

图 8-14 更改筛选器操作的属性

（7）如果不想阻塞传入的不安全通信，但想确保保护传出的通信和后续的双向通信，请选中“ 接受不安全的通信，但总是用 IPSec 响应 ”复选框。

（8）如果想允许与其他不支持 IPSec 的计算机通信，并想确保在没有 IPSec 协商响应的情况下能够继续通信，请选中“ 允许和不支持 IPSec 的计算机进行不安全的通信 ”复选框。如果 IPSec 协商在某一端失败后，该选项将禁用这一端的 IPSec 一段时间。

（9）选中“ 会话密钥完全向前保密 ”复选框，保证不重复使用主密钥或主密钥材料生成

会话密钥。

(10) 在“ 常规 ”选项卡中，可以更改该筛选器操作的名称，也可以更改对该筛选器操作的说明。例如，可以输入该筛选器操作所代表的安全级别

需要说明的是：“ 允许和不支持 IPsec 的计算机进行不安全的通信 ”和“ 接受不安全的通信，但总是用 IPsec 响应 ”在“ 默认响应 ”规则中是不可用的。“ 会话密钥完全向前保密 ”将在每个会话重加密操作期间创建新的密钥。这是最常见的安全设置。但是，该设置将给服务器增加相当可观的负担，而且会导致完成重加密操作所需的时间增加。发起方和响应方都必须配置相同的设置才能成功协商。而且，在使用该功能时，与其他产品的互通将受到影响。

8. 创建自定义的 IPSec 策略

要定义计算机的 IPSec 策略，必须要有访问“ 组策略 ”的适当管理员权限，或者是本地系统 Administrators 组的成员。

基本的操作步骤如下。

（1）在“ IP 安全策略管理 ”中，选择要定义新策略还是编辑当前的策略。

（2）如果需要创建新的策略，则在控制台树中，右击“ IP 安全策略，在本地机器 ”，然后在弹出的菜单中选择“ 创建 IP 安全策略 ”命令。

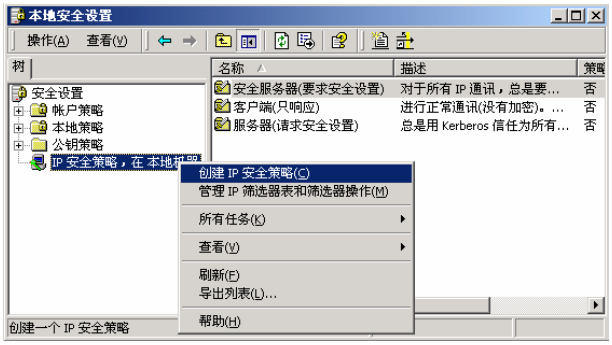

图 8-15 创建 IP 安全策略

（3）根据“ IP 安全策略向导 ”中的提示进行逐步的设置，直到出现新策略的“ 属性 ”对话框。

（4）如果需要编辑已有的策略，则右击该策略，然后选择“ 属性 ”命令。

（5）打开“ 常规 ”选项卡，在“ 名称 ”中输入惟一的名称，在“ 描述 ”中，输入关于安全策略的说明，例如它将影响的组或域。

（6）如果该计算机是域的一部分，那么，要指定策略代理检查组策略以便进行更新的时间间隔，可在“ 检查策略更改间隔 ”中键入以分钟为单位的值。

（7）如果对密钥交换的安全性有特殊要求，可单击“ 高级 ”按钮。

（8）打开“ 规则 ”选项卡，并为策略创建任何需要的规则。

如果正创建新策略，并且新策略没有显示在控制台树中，则可右击“ IP 安全策略，在本地机器 ”，然后选择“ 刷新 ”命令。

以下说明添加或编辑规则的基本操作过程：

（1）在“ IP 安全策略管理 ”中，右击要修改的策略，然后选择“ 属性 ”命令。

（2）决定是否使用添加向导：

- 要使用“ 安全规则 ”向导添加规则，请确保选中“ 使用添加向导 ”复选框，单击“ 下一步 ”按钮，然后按照指令进行操作。
- 要手动添加或编辑规则，请确保清除“ 使用添加向导 ”复选框，然后单击“ 添加 ”或“ 编辑 ”按钮继续该过程。

（3）定义“ IP 筛选器列表 ”、“ 筛选器操作 ”、“ 连接类型 ”、“ 身份验证方法 ” 和 “ 隧道设置 ” 属性。

需要注意的是：新的规则将自动应用于正在创建或编辑的策略；每个新的 IPSec 策略中会自动添加 “ 默认响应 ” 规则（而且如果选择就激活）。如果不想让此规则成为策略的一部分，请取消激活该规则（不能删除预定义规则）。

以下说明定义 IPSec 身份验证方法的基本过程。

（1）在 “ IP 安全策略管理 ” 中，右击要修改的策略，然后选择 “ 属性 ” 命令。

（2）单击要修改的规则，然后单击 “ 编辑 ” 按钮。

（3）在 “ 身份验证方法 ” 选项卡中，单击 “ 添加 ” 按钮。或者，如果正重新配置现有的方法，请单击身份验证方法，然后单击 “ 编辑 ” 按钮。

（4）定义身份验证方法：

- 如果该规则适用于已被 Windows 2000 受信域验证的计算机，请单击“ Windows 2000 默认值（Kerberos V5 协议）”使 Kerberos V5 安全协议用于身份验证服务。
- 要使公钥证书用于身份验证服务，请单击 “ 使用此证书颁发机构（CA）颁发的证书 ”。如果选择使用证书，请单击 “ 浏览 ” 选择根 CA。
- 要指定使用自己的密钥进行身份验证，可单击“ 此字串用来保护密钥交换（预共享密钥）”。

以下说明指定 IPSec 连接类型的基本过程。

（1） 在 “ IP 安全策略管理 ” 中，右击要修改的策略，然后选择 “ 属性 ” 命令。

（2） 单击要修改的规则，然后单击 “ 编辑 ” 按钮。

（3） 在 “ 连接类型 ” 选项卡中，选择将应用此规则的连接类型：

- 要将此规则应用到在该计算机中创建的所有网络连接，可单击 “ 所有网络连接 ”。
- 要将此规则应用到在该计算机中创建的所有 LAN 连接，可单击 “ 局域网（LAN）”。
- 要将此规则应用到在该计算机中创建的所有远程或拨号连接，可单击“ 远程访问 ”。

以下说明指定 IPSec 隧道的基本过程。

（1）在 “ IP 安全策略管理 ” 的详细信息窗格中，右击要修改的策略，然后选择 “ 属性 ” 命令。

（2）选定要修改的规则，然后单击 “ 编辑 ” 按钮。

（3）在 “ 隧道设置 ” 选项卡中，指定要作为隧道终结点的计算机：

- 若禁用该规则的隧道，单击 “ 此规则不指定 IPSEC 隧道 ”。
- 若对特定的计算机使用隧道通信，单击 “ 隧道终结点由此 IP 地址指定 ”。

9. 使用 IPSec 策略的注意事项

IPSec 为传出和传入的数据包加密，代价是操作系统实施加密时增加了 CPU 的负担。在很多部署中，客户机和服务器都有相当多的可用 CPU 资源，因此 IPSec 加密不会对性能产生明显影响。对于同时支持许多网络连接或向其他服务器传输大量数据的服务器而言，加密产生的额外成本是显著的。基于上述原因，在部署 IPSec 之前应使用模拟网络传输进行测试。如果使用第三方硬件或软件产品提供 IP 安全，测试也很重要。

Windows 2000 提供设备接口，允许使用智能网卡实现硬件加速 IPSec 每个数据包的加密过程。网卡供货商可能会提供几种版本的客户机和服务器卡，也可能不支持所有 IPSec 安全措施的组合。

管理员可以考虑在下列场合下使用 IPSec：

- 单位内部网的对等通信
- 远程访问（拨号或虚拟专用网络）通信
- 安全的路由器——路由器 WAN 通信

管理可以为每个域或部门定义 IPSec，也可以在没有指派域 IPSec 策略的计算机上定义本地 IPSec 策略。管理员可以给下列各项配置 IPSec 策略：

- 指定 IPSec 客户间所要求的身份验证和机密性等级
- 指定 IPSec 已知客户间允许通信的最低安全等级
- 允许或阻止与 IPSec 未知客户的通信
- 出于机密性考虑要求所有通信加密或允许明文通信
- 考虑使用 IPSec 为下列应用程序提供安全措施

对于网络安全部署规划中的 IPSec 可考虑以下策略：

- 对使用 IPSec 通信的客户机和服务器进行标识
- 标识客户身份验证是基于 Kerberos 信任还是数字证书
- 描述每台计算机如何最初接收适当的 IPSec 策略并继续接收策略更新
- 描述每个 IPSec 策略内部的安全规则。考虑如何需要证书服务通过数字证书支持客户身份验证
- 描述为计算机注册 IPSec 证书的登记过程和策略

8.3 SSL

8.3.1 SSL 概述

SSL（Secure Socket Layer，安全套接字层）是 Netscape 公司率先采用的网络安全协议，是在传输通信协议（TCP）上实现的一种安全协议，它采用公开密钥技术。SSL 协议的目标是提供两个应用间通信的保密和可靠性，可在服务器和客户机端同时实现支持。SSL 可提供 3 种基本的安全服务：信息加密、信息完整性、相互认证。

SSL 实际上由两层协议所组成。

- SSL 记录协议：用于封装不同的上层协议。它涉及应用程序提供的信息的分段、压缩、数据认证和加密。SSL v3 提供对数据认证用的 MD5 和 SHA 以及对数据加密用的 R4 和 DES 等的支持，用来对数据进行认证和加密的密钥可以 SSL 的握手协议来协商。
- SSL 握手协议：用来在服务器和客户机在传输应用数据之前，交换版本号、协商加密算法、（相互）身份认证并交换密钥。SSL v3 提供对 Deffie-Hellman 密钥交换算法、基于 RSA 的密钥交换机制和另一种实现在 Fortezza Chip 上的密钥交换机制的支持。

客户机提出自己能支持的全部算法清单，由服务器来选择最适合它的算法。

Netscape 公司已经推出了 SSL 的参考实现（称为 SSLref），而另一免费的 SSL 实现叫做 SSLeay。SSLref 和 SSLeay 均可为任何 TCP/IP 应用提供 SSL 功能。Internet 号码分配当局（IANA）已经为具备 SSL 功能的应用分配了固定的端口号，例如，带 SSL 的 HTTP（https）被分配的端口号是 443，带 SSL 的 SMTP（ssmtp）被分配的端口号是 465，带 SSL 的 NNTP（snntp）被分配的端口号是 563 等。

由于 SSL 独立于应用协议，因而上层应用可能叠加在 SSL 协议上。S-HTTP（安全超文文本传输协议）是 HTTP 协议的扩展，允许客户机与服务器协定基于公钥加密的多级安全性，

提供加密、鉴别等功能。S-HTTP 和 SSL 是从不同的角度提供对 Web 的安全服务：S-HTTP 对单个文件做“ 私人/签名 ”之区分，而 SSL 则把参与通信的相应进程之间的数据通道按“ 私用 ”和“ 已认证 ”进行监管，主要集中在它的握手协议上。两者可以融合成一个统一的协议。

8.3.2 SSL 的典型应用

在使用 SSL 安全机制的时候，客户端与服务器建立连接，服务器把它的数字证书与公共密钥一并发送给客户端，客户端随机生成会话密钥，用从服务器得到的公共密钥对会话密钥进行加密，并把会话密钥在网络上传递给服务器，而会话密钥只有在服务器端用私人密钥才能解密，这样，客户端和服务器端就建立了一个惟一的安全通道。

SSL 通常用于 Web 站点，比如银行及电子商务站点，这些站点通常都需要客户端传输敏感数据。默认情况下我们所使用的 HTTP 协议是没有任何加密措施的，所有的消息全部都是以明文形式在网络上传送的，恶意的攻击者可以通过安装监听程序来获得我们和服务器之间的通信内容。这点危害在一些企业内部网络中尤其比较大，对于使用 HUB 的企业内网来说简直就是没有任何安全可讲。因为任何人都可以在一台电脑上看到其他人在网络中的活动，对于使用交换机来组网的网络来说虽然安全威胁性要小很多，但很多时候还是会有安全突破口，比如没有更改交换机的默认用户和口令，攻击者可以登录上去把自己的网络接口设置为侦听口，依然可以监视整个网络的所有活动。

所以可以利用 SSL 来加密 HTTP 通道。在 Web 站点上建立了 SSL 安全机制后，只有 SSL 允许的客户才能与该 Web 站点进行通信。此时在使用 URL 资源定位器时，输入的是“ https:// ”，而不是“ http:// ”。

8.3.3 使用 SSL 保护 Web 站点

要在 Windows 2000 的 Web 站点上使用 SSL，必须首先获取一个服务器证书，它可以验证服务器的身份并且包含用于加密服务器所传输的数据的公钥。可以从多个第三方公司获取一个证书，也可以使用 Windows 2000 的证书服务和 IIS 中的“ 服务器证书向导 ”来自己颁发一个证书。

具体的操作步骤如下：

（1）在本机或者网络上能够到达的一台计算机上安装证书服务器。

（2）安装完成之后，在本地启动“ Internet 服务管理器 ”来申请一个服务器数字证书。在“ Internet 服务管理器 ”中选择需要配置的 Web 站点。

（3）选择 Web 站点属性里的“ 目录安全性→安全通信→服务器证书 ”，如图 8-16 所示。

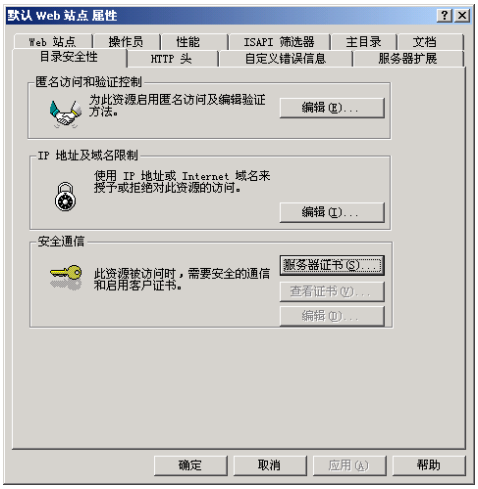

图 8-16 Web 站点安全通信中的服务器证书

（4）如果是第一次配置，就选择创建一个新的证书，如图 8-17 所示。

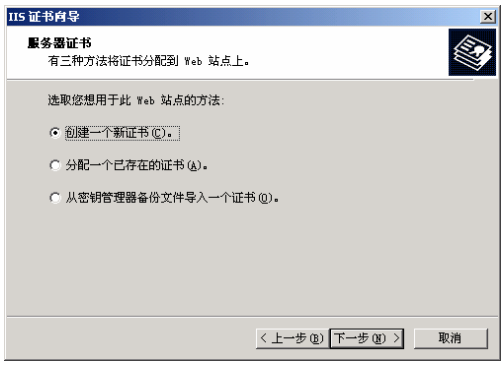

图 8-17　创建一个新的证书

（5）按照“ IIS 证书向导 ”的提示，设置默认的站点名称和加密位长，填写组织信息，填写站点公用名称，填写地理信息，输入证书请求的本地保存文件名（如 C:\certreq.txt）。

（6）完成以上设置之后，需要把刚生成的服务器证书请求提交给证书服务器（在第（1）步操作中安装的证书服务器）。在默认情况下证书服务器安装完成之后会在证书服务器的 Web 站点里面创建几个虚拟目录。在本地打开 URL 链接：http:// 证书服务器地址 /CertSrv/default.asp。

（7）选择申请证书，如图 8-18 所示。

图 8-18　通过 Web 浏览器申请证书

（8）在选择申请类型的时候，选择高级申请，如图 8-19 所示。

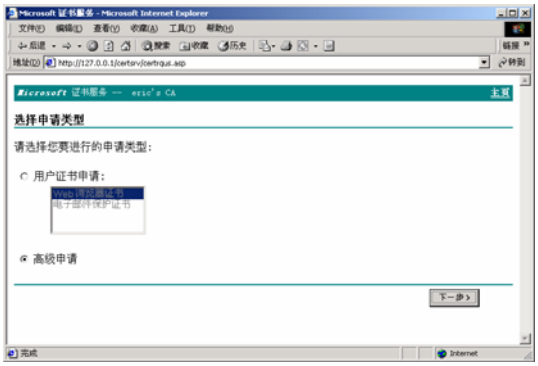

图 8-19　使用高级申请的类型申请证书

（9）选择使用 base64 的编码方式来提交证书申请。

(10) 在证书申请的地方把前面生成的证书请求文件 certreq.txt 的内容复制进去，然后单击“ 提交 ”按钮，如图 8-20 所示。

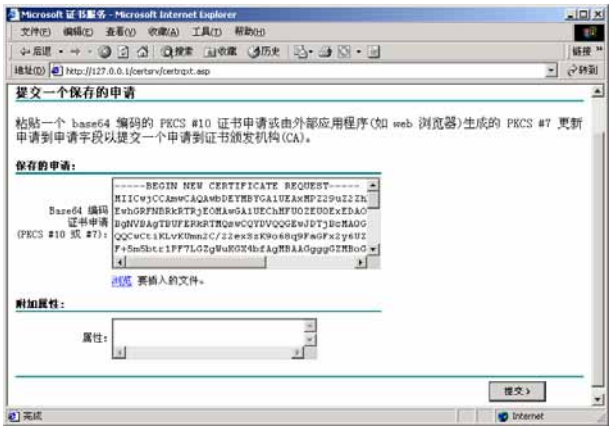

图 8-20　提交证书申请

(11) 提交成功以后就是证书的挂起状态，也就是等待 CA 中心来颁发这个证书了。

(12) 在证书服务器上启动“ 管理工具 ”里的“ 证书颁发机构 ”，在待定申请中右击刚才的申请条目，然后选择“ 颁发 ”命令，如图 8-21 所示。

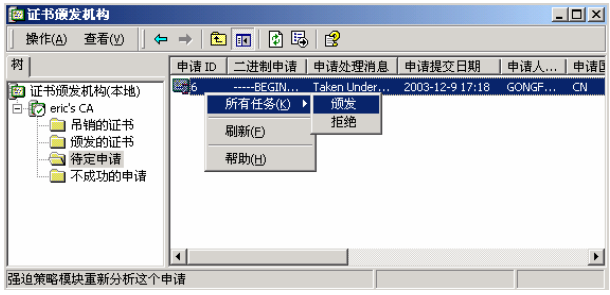

图 8-21　在证书服务器上颁发证书

(13) 颁发成功以后，在颁发的证书里找到刚才所颁发的证书，双击其“ 属性 ”栏目，然后在其“ 详细信息 ”里选择将证书复制到文件，如图 8-22 所示。

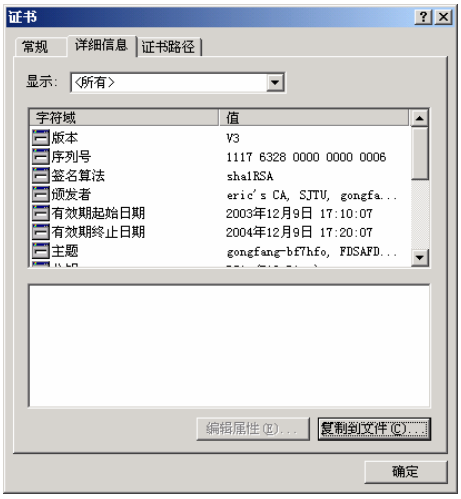

图 8-22　导出证书

(14) 将该颁发的证书导出到一个文件中，如 c:\ eric.cer。

(15) 回到本地的 IIS Web 管理界面，再次选择“ 证书申请 ”，此时就会出现“ 挂起的证书请求 ”，如图 8-23 所示。

(16) 选择刚才导出的证书文件 eric.cer。

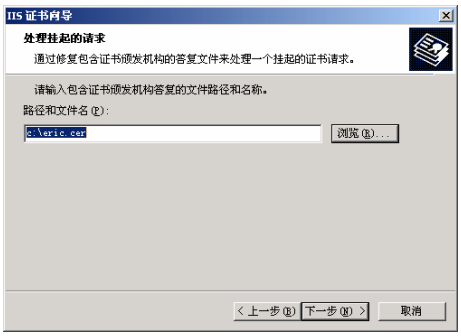

图 8-23 导入证书

(17) 确定一切信息无误之后，单击“ 下一步 ”按钮完成 SSL 的安装。

此时就能通过 https（默认使用 443 端口）的方式进入该站点。而且在第一次进入时会提示下载客户端证书。此后所有访问该 Web 站点的信息都是以加密的方式在网络上传输的了，任何人都无法轻易了解其中的内容了。

在 Web 站点安全通信的属性设置（通过 Web 站点属性里的“ 目录安全性→安全通信→编辑 ”进入）中，可以设置不同的选项来对客户端进行不同的要求，如图 8-24 所示。

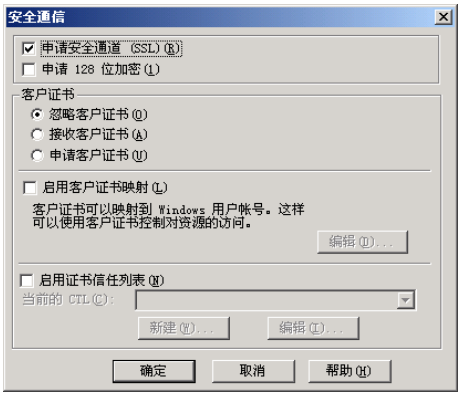

图 8-24 Web 站点安全通信的属性设置

如果不选择“ 申请安全通道（SSL） ”，则允许客户端选择是否使用 SSL 加密传输，即客户可以使用加密的方式访问“ https://x.x.x.x ”，也可以使用非加密的方式访问“ https://x.x.x.x ”。如果选择“ 申请安全通道（SSL） ”，那么就要求客户端必须使用 SSL 加密传输，即必须使用“ https://x.x.x.x ”的形式。

如果选择“ 申请 128 位加密 ”，则要求客户端的浏览器必须支持 128 位的加密程度。建议不要选择该项，因为一般的浏览器支持的都是 56 位的加密强度。

如果选择“ 申请客户证书 ”（在选择了“ 申请安全通道（SSL） ”的前提下），那么当客户以 https 的形式访问该 Web 站点时，会被提醒需要选择一个已经安装的客户证书，如果没有客户证书或者没有服务器信任的客户证书，那么就不能访问。客户证书是服务器判断客户端是否可信任的依据，用来防止不被信任的客户端访问该服务器。

8.4 VPN

VPN（Virtual Private Networks，虚拟专用网络）能够利用 Internet 或其他公共互联网络的基础设施为经过相互授权的用户创建通信隧道，并通过加密传输来提供与专用网络一样的安全和功能保障。VPN 可用于政府、企事业单位总部与分支机构内部联网（Intranet-VPN），为用户提供高速、安全、可靠、可管理、高质量的服务。

虚拟专用网络允许远程通信方、销售人员或企业分支机构使用 Internet 等公共互联网络

的路由基础设施以安全的方式与位于企业局域网端的企业服务器建立连接。虚拟专用网络对用户端透明，用户好像使用一条专用线路那样在客户计算机和企业服务器之间建立点对点连接，进行数据的传输，如图 8-25 所示。

虚拟专用网络技术同样支持企业通过 Internet 等公共互联网络与分支机构或其他公司建立连接，进行安全的通信。这种跨越 Internet 建立的 VPN 连接逻辑上等同于两地之间使用广域网建立的连接。虽然 VPN 通信建立在公共互联网络的基础上，但是用户在使用 VPN 时感觉如同在使用专用网络进行通信，这也是“虚拟专用网络”这个名称的由来。

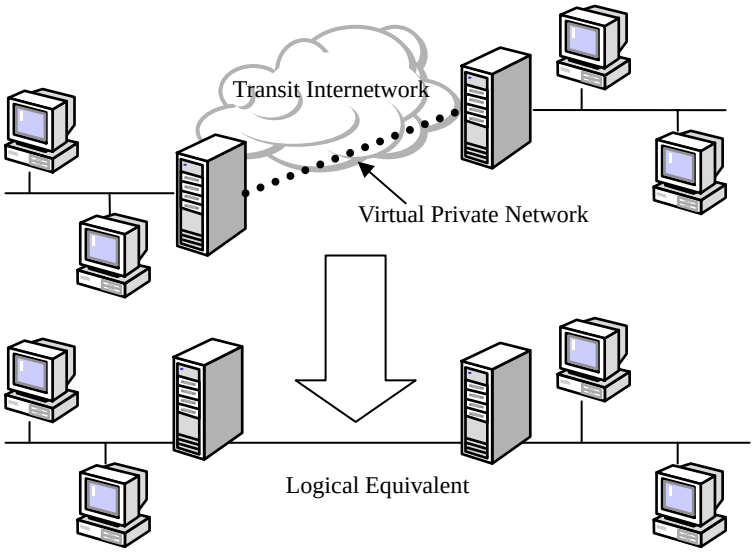

图 8-25　虚拟专用网络

8.4.1　VPN 基础

客户端和服务器通过 Internet 这样的公共网络进行专用网络通信的问题就是安全性。要保证传输数据的保密性，就需要一个保证数据安全的机制。VPN 使用的方式就是“隧道操作”（Tunneling）。

1. 隧道操作

隧道操作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。隧道协议将这些其他协议的数据帧或包重新封装在新的包头中发送。新的包头提供了路由信息，从而使封装的负载数据能够通过互联网络传递。被封装的数据包在隧道的两个端点之间通过公共互联网络进行路由。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。一旦到达网络终点，数据将被解包并转发到最终目的地，如图 8-26 所示。

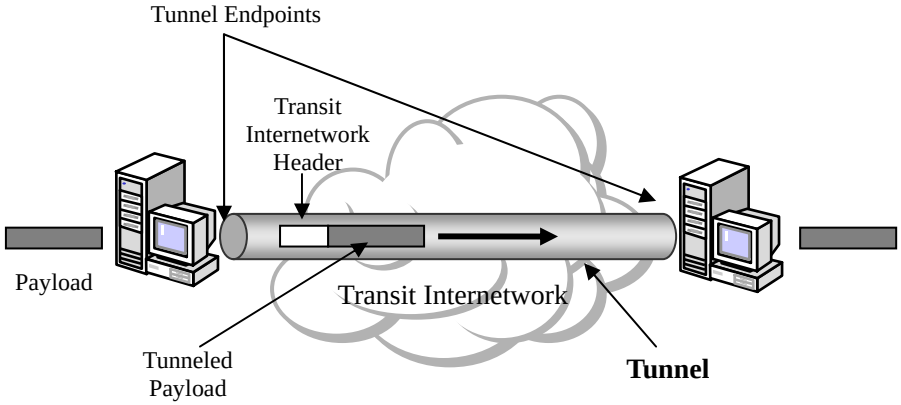

图 8-26　VPN 隧道

包括数据封装、传输和解包在内的全过程就是“ 隧道操作 ”。而封装过的数据包在中转互联网络上经过的逻辑路径称作“ 隧道 ”。

2. VPN 隧道协议

为创建隧道，隧道的客户机和服务器双方必须使用相同的隧道协议。用于 VPN 的最常用的隧道协议如下。

- 点对点隧道协议（Point to Point Tunnel Protocol, PPTP）

PPTP 是 PPP 的一个扩展，它增加了一个新的安全等级，并且可以通过 Internet 进行多协议通信，它支持通过公共网络（如 Internet）建立按需的、多协议的、虚拟专用网络。PPTP 可以建立隧道或将 IP、IPX 或 NetBEUI 协议封装在 PPP 数据包内，因此允许用户远程运行依赖特定网络协议的应用程序。PPTP 在基于 TCP/IP 协议的数据网络上创建 VPN 连接，实现从远程计算机到专用服务器的安全数据传输。VPN 服务器执行所有的安全检查和验证，并启用数据加密，使得在不安全的网络上发送信息变得更加安全。尤其是使用 EAP 后，通过启用 PPTP 的 VPN 传输数据就像在企业的一个局域网内那样安全。另外还可以使用 PPTP 建立专用 LAN 到 LAN 的网络。PPTP 是 Microsoft 和其他厂家支持的标准。

- 第二层隧道协议（Layer2 Tunneling Protocol, L2TP）

除了 Microsoft 之外，另有一些厂家也做了许多开发工作。PPTP 能支持 Macintosh 和 Unix，而 Cisco 的 L2F（Layer2 Forwarding）就是又一个隧道协议。Microsoft、Cisco 和其他一些网络厂商将 L2F 与 PPTP 融合在一起形成了新的 L2TP 协议。PPTP 和 L2TP 十分相似，因为 L2TP 有一部分就是采用 PPTP 协议。L2TP 也会压缩 PPP 的帧，从而压缩 IP、IPX 或 NetBEUI 协议，同样允许用户远程运行依赖特定网络协议的应用程序。与 PPTP 不同的是，L2TP 使用新的 IPSec 来进行身份验证和数据加密。目前 L2TP 只支持通过 IP 网络建立隧道，不支持通过 X.25、帧中继或 ATM 网络的本地隧道。

- IP 协议安全（Internet Protocol Security, IPSec）

在前面已经详细叙述过 IPSec 了。当使用 IPSec 且处于隧道模式时，完整的 IP 数据包是由 ESP 来进行封装和加密的，然后结果会被封装（使用明文的 IP 数据头），并在中转互联网络上进行传输。

8.4.2　VPN 的基本应用

1. 通过 Internet 实现远程用户访问

虚拟专用网络支持以安全的方式通过公共互联网络远程访问企业资源，如图 8-27 所示。

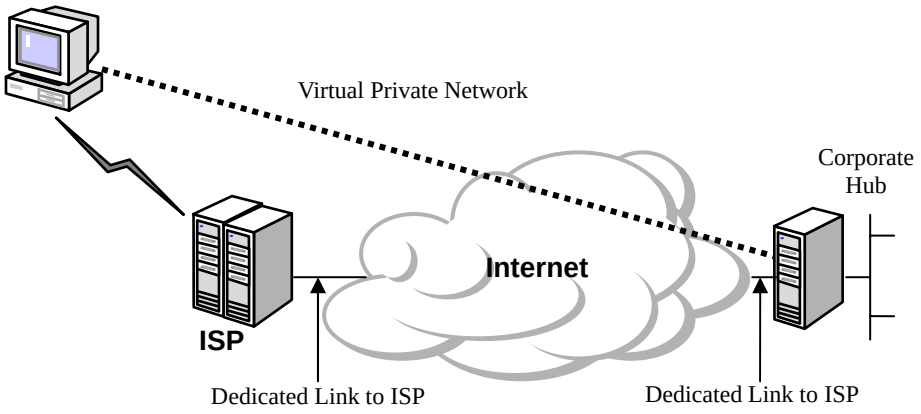

图 8-27　通过 Internet 进行远程访问

可以采用以下两种方式使用 VPN 连接远程局域网络。

（1）使用专线连接分支机构和企业局域网

不需要使用价格昂贵的长距离专用电路，分支机构和企业端路由器可以使用各自本地的专用线路通过本地的 ISP 连通 Internet。VPN 软件使用与当本地 ISP 建立的连接和 Internet 网络在分支机构和企业端路由器之间创建一个虚拟专用网络。

（2）使用拨号线路连接分支机构和企业局域网

不同于传统的使用连接分支机构路由器的专线拨打长途或电话连接企业 NAS 的方式，分支机构端的路由器可以通过拨号方式连接本地 ISP。VPN 软件使用与本地 ISP 建立起的连接在分支机构和企业端路由器之间创建一个跨越 Internet 的虚拟专用网络，如图 8-28 所示。

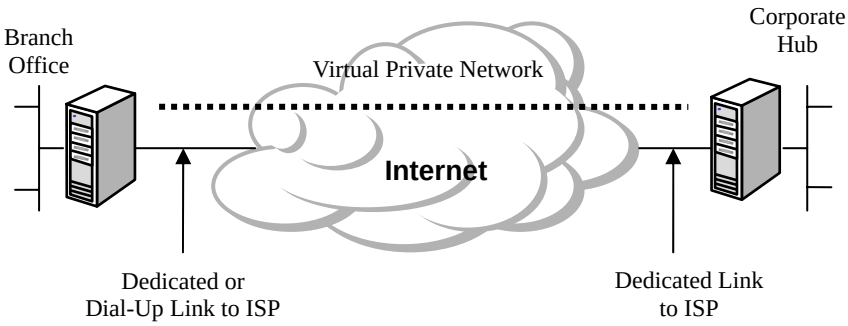

图 8-28　Internet 上的一个 VPN

应当注意在以上两种方式中，是通过使用本地设备在分支机构和企业部门与 Internet 之间建立连接。无论是在客户端还是服务器端都是通过拨打本地接入电话建立连接，因此 VPN 可以大大节省连接的费用。建议作为 VPN 服务器的企业端路由器使用专线连接本地 ISP。VPN 服务器必须一天 24 小时对 VPN 数据流进行监听。

2. 连接企业内部网络计算机

在企业的内部网络中，考虑到一些部门可能存储有重要数据，为确保数据的安全性，传统的方式只能是把这些部门同整个企业网络断开形成孤立的小网络。这样做虽然保护了部门的重要信息，但是由于物理上的中断，使其他部门的用户无法访问，造成通信上的困难。

采用 VPN 方案，通过使用一台 VPN 服务器既能够实现与整个企业网络的连接，又可以保证保密数据的安全性。路由器虽然也能够实现网络之间的互联，但是并不能对流向敏感网络的数据进行限制。而企业网络管理人员通过使用 VPN 服务器，可以指定只有符合特定身份要求的用户才能连接 VPN 服务器获得访问敏感信息的权限。此外，可以对所有 VPN 数据

进行加密，从而确保数据的安全性。没有访问权限的用户无法访问部门的局域网络。

8.4.3 在 Windows 2000 中实现 VPN

1. 配置并启用 VPN 服务器

在 Windows 2000 系统中，可参照以下基本步骤来配置并启用一个 VPN 服务器：

（1）打开“管理工具”中的“路由和远程访问”控制台。

（2）在控制台树中右击服务器的节点，从弹出的菜单中选择“配置并启用路由和远程访问”命令，如图 8-29 所示。

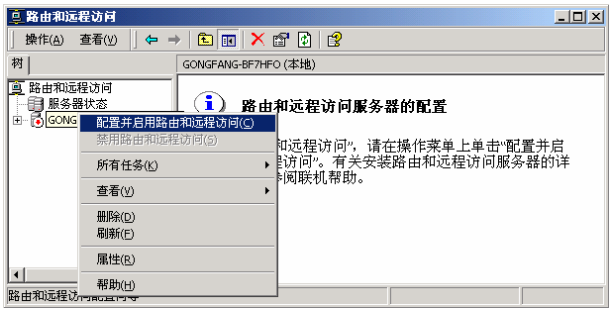

图 8-29 配置并启用路由和远程访问

（3）根据“路由和远程访问服务器设置向导”中的提示进行操作。

（4）在“公共设置”界面中，选择“虚拟专用网络（VPN）服务器”，如图 8-30 所示。

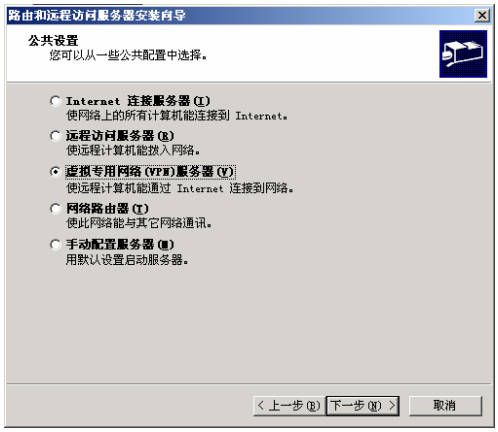

图 8-30 配置 VPN（虚拟专用网络）服务器

（5）在“远程客户协议”界面中确认 TCP/IP 已出现在协议列表中。

（6）在“Internet 连接”界面中选择“无 Internet 连接”。

（7）在“IP 地址指定”界面中选择“自动”选项。

（8）在“管理多个远程服务器”界面中选择“不，我现在不想设置此服务器使用 RADIUS”。

（9）完成“路由和远程服务器安装向导”所提供的设置，会出现“路由和远程访问”的消息窗口，提示必须配置一个 DHCP 消息中继以支持来自远程访问客户端的 DHCP 消息中继传输。

(10) 刚安装的路由和远程访问服务（类型为 VPN 服务器）会默认启动。

此时，该 VPN 服务器还无法访问，因为还没有向任何用户授予过远程访问权限。可以参照以下步骤对用户授予远程访问的权限：

（1）如果远程访问服务器在 Windows 2000 域中，则打开 Active Directory 用户和计算机；

如果是独立服务器或是成员服务器，则打开“ 计算机管理 ”。

（2）在控制台目录树中，单击“ 用户 ”。在详细信息窗口中，右击用户名，然后选择“ 属性 ”命令。

（3）在“ 拨入 ”选项卡中的“ 远程访问权限（拨入或 VPN） ”下，选择“ 允许访问 ”或者“ 通过远程访问策略控制访问 ”，然后单击“ 确定 ”按钮，如图 8-31 所示。

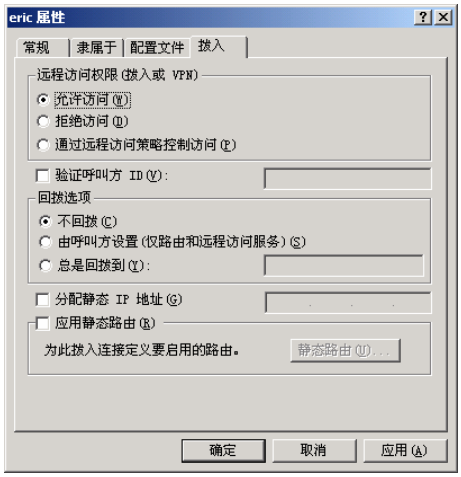

图 8-31　授予用户远程访问的权限

2. 配置 VPN 客户端

在 Windows 2000 系统中，可参照以下基本步骤将工作站配置为一个 VPN 客户端：

（1）在“ 网络和拨号连接 ”窗口中，双击“ 新建连接 ”。

（2）根据“ 网络连接向导 ”中的提示进行操作。

（3）在“ 网络连接类型 ”、界面中选择“ 通过 Internet 连接到专用网络 ”。

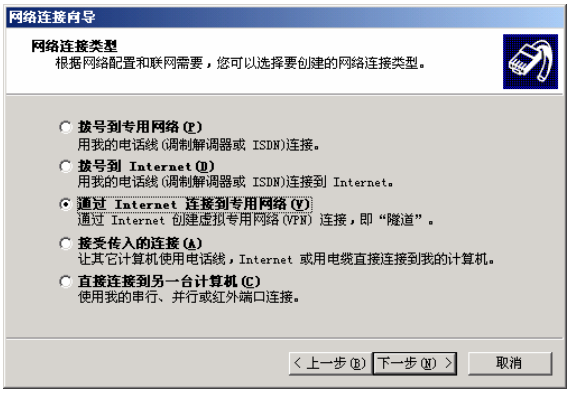

图 8-32　通过 Internet 连接到虚拟专用网络

（4）如果已经在该工作站上配置过一个拨号连接，则向导会显示“ 公用网络 ”界面，如图 8-32 所示，在其中可以选择建立 VPN 连接之前计算机应当拨叫的连接。当客户端通过 Internet 进行连接时需要进行此步骤，但对于本地 VPN 连接的情况则不必。

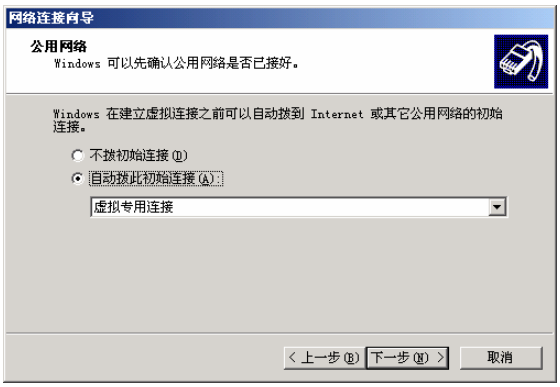

图 8-33 “ 公用网络 ” 界面

（5）在 “ 目标地址 ” 页中输入 VPN 服务器的 IP 地址，如图 8-34 所示。

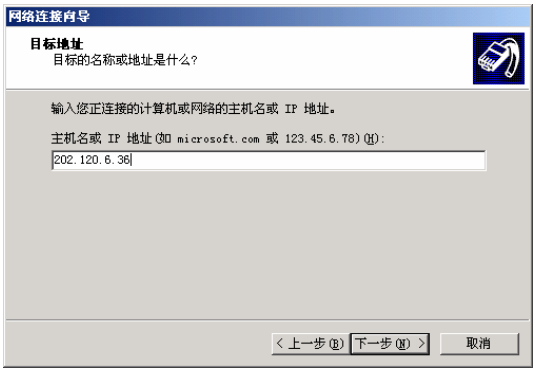

图 8-34 VPN 服务器的目标地址

（6）在 “ 可用连接 ” 界面中选择可以使用该连接的用户是否包括系统中的所有用户。

（7）完成 “ 网络连接向导 ” 以创建该连接。

3. 连接 VPN 服务器

（1）在 “ 网络和拨号连接 ” 窗口中，双击刚才添加的 “ 虚拟专用连接 ” 。

（2）输入正确的用户名和密码，单击 “ 连接 ” 按钮，开始尝试连接远程的 VPN 服务器，如图 8-35 所示。

图 8-35 连接 VPN 服务器

（3）连接成功后，在 VPN 服务器上，可以在 “ 路由和远程访问 ” 控制台中扩展 “ 远程访问控制端 ” 节点，则可以对远程连接的信息进行查看。通过双击某项连接可以查看包括服务器发送、接收的字节和数据帧的数目在内的统计信息。

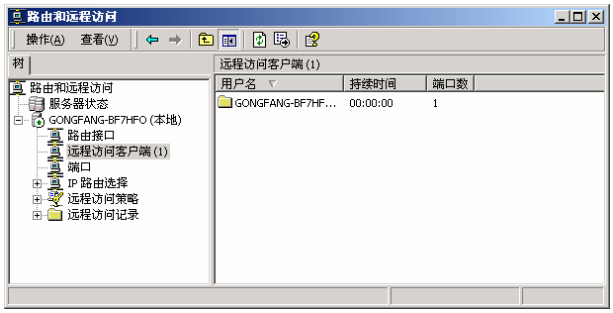

图 8-36　查看远程访问客户端的信息