第 3 章 IPSec VPN

IPSec 技术能够保障局域网、各种类型的广域网以及 Internet 环境中各种类型的信息在网络传输过程中的安全。IPSec 技术应用于 IP 层，以数据包为处理对象，实现了高强度的安全性保障，具体表现为对数据源进行全面验证、对处于无连接状态的数据进行完整性检验、对数据开展机密性和抗重放的检查，以及对有限的业务流所具有的机密性实施检验等各种安全性作用。而运行在系统中的各种类型的应用程序都可以得到在 IP 层建立的密钥以及其他安全机制提供的保障，而不需要独立设计和执行各自的安全保护机制，这就使得系统中的密钥协商所需的系统资源大大减少，同时在统一的安全保证下，能够明显降低安全漏洞的出现概率。因此，IPSec VPN 是目前比较流行的 VPN 实现方案。本章将对 IPSec VPN 的原理与实现进行详细讲解，通过对本章的学习，应了解 IPSec 协议族，掌握 IPSec 技术的原理及实现过程。

3.1 IPSec 概述

3.1.1 IPSec 协议族

IPSec(Internet 协议安全性)是 Internet 工程任务组(IETF)制定的一系列协议，以保证在 Internet 上传送数据的安全保密性。特定的通信方之间在 IP 层通过加密与数据源验证来保证数据包在 Internet 上传输时的私有性、完整性和真实性。

IPSec 通过两个安全协议来实现对 IP 数据包或上层协议的保护，在实现过程中不会对用户、主机或其他 Internet 组件造成影响。IPSec 主要依赖密码技术提供认证和加密机制，它是现代密码技术在通信领域的应用范例。

IPSec 作为网络安全的一个重要协议族，定义了在网络层使用的安全服务，其功能体现了网络安全的大部分需求，包括数据加密、对网络单元的访问控制、数据源地址验证、数据完整性检查和防止重放攻击。

3.1.2 IPSec 的体系结构

IPSec 是一个关于开放标准的框架，它给出了应用于 IP 层上的网络数据安全的体系结构，包括 AH(认证头)协议、ESP(封装有效载荷)协议、IKE(密钥管理协议)协议以及用

于用户身份认证和数据加密的一系列算法。IPSec 的体系结构可分为 7 个部分，如图 3-1 所示。

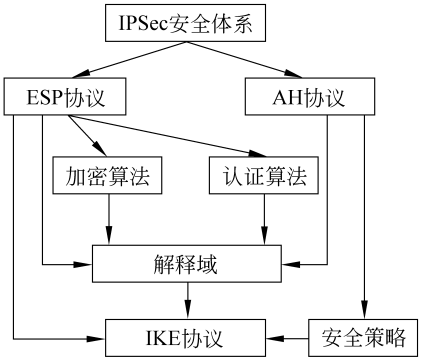


图 3-1　IPSec 体系结构

(1) AH 协议。定义了认证头进行的身份认证、数据包格式及相关的服务。其主要功能有数据源验证、数据完整性校验和防止重放。

(2) ESP 协议。定义了有关数据包加密(可选身份认证)、数据包格式和相关的服务。它除了提供 AH 协议的所有功能之外，还提供 IP 数据包加密功能。

(3) 加密算法。描述如何将 AES、DES、3DES 等加密算法应用于 ESP 协议中。

(4) 认证算法。描述如何将 MAC2MD5、HMAC2SHA21 等各种身份认证算法应用于 AH 协议和 ESP 协议中。

(5) IKE 协议。用于管理两个通信实体之间密钥的生成、分发和更新等。例如，IKE 协议能够实现自动建立加密、认证的安全信道以及密钥的自动安全分发和更新。

(6) 解释域(Domain of Interpretation，DOI)。用于存放密钥管理协议协商的参数，如加密及认证算法的标识符、参数等。

(7) 安全策略(Security Policy，SP)。用于决定两个通信实体之间如何通信。其核心由 3 个部分组成：SA(安全联盟)、SAD(Security Association Database，安全联盟数据库)以及 SPD(Security Policy Database，安全策略数据库)。

在 IPSec 的体系结构中，AH 协议和 ESP 协议是安全处理协议，这两个协议既可以单独使用，又可以同时使用，前者提供数据完整性保护，后者提供数据保密性和数据完整性保护。两个协议都是将一个可变长度的数据包结构插入 IP 头与上层协议之间。AH 协议首先使用协商好的算法和密钥计算整个数据包不变部分的摘要值，然后将此摘要值作为数据包完整性的证据保存在身份认证头结构中。ESP 协议则将原始数据包加密后作为载荷携带在数据包中。此外，ESP 协议也可以实现数据完整性验证，但是与 AH 协议包含的字段不同。表 3-1 给出了这两种协议的比较。这两种协议的实现原理将在 3.2 节详细叙述。

表 3-1 AH 协议与 ESP 协议的比较

安全特性	AH	ESP
网络层的 IP 协议号	51	50
提供数据完整性验证	是	是
提供数据源验证	是	是
提供数据加密	否	是
防止重放	是	是
与 NAT 协议一起工作	否	是
保护 IP 数据包	是	否
只保护数据	否	是

3.1.3 IPSec 的关键概念

本节对 IPSec 的关键概念进行介绍。

(1) 安全联盟(SA)。包括协议、算法、密钥等内容,具体确定了如何对 IP 数据包进行处理。安全联盟是单向的,在两个安全网关之间进行双向通信时,需要两个安全联盟来分别对输入数据流和输出数据流进行安全保护。安全联盟由一个三元组来唯一地标识,这个三元组包括安全参数索引、目的 IP 地址和安全协议号(AH 或 ESP)。

(2) 安全联盟数据库(SAD)。用于存放安全联盟的所有状态数据的存储结构。

(3) 安全参数索引是一个 32b 的数值,在每一个 IPSec 包中都携带该数值。由安全参数索引、目的 IP 地址、安全协议号组成的三元组唯一地标识一个特定的安全联盟。手工配置安全联盟时需要手工指定安全参数索引,为保证安全联盟的唯一性,必须使用不同的安全参数索引来配置安全联盟。IKE 协议产生安全联盟时,使用随机数来生成安全参数索引。

(4) 安全策略,由用户手工配置,规定对什么样的数据流采用什么样的安全措施。一条安全策略由名字和顺序号共同标识。

(5) 安全策略数据库(SPD)。是所有具有相同名字的安全策略的集合,用来指明所有 IP 数据包文应使用何种安全服务以及如何获得这些服务的数据结构。当一个接口需要对外建立多条安全隧道时,必须采用这种形式。使用 SPD 时需要明确一个原则:任何一个端口都只能应用一个安全策略库,任何一个安全策略库也只能应用于一个端口。

(6) 数据封装。是指将 AH 协议或 ESP 协议相关的字段插入原始 IP 数据包中,以实现对数据包的身份认证和加密。

(7) 安全隧道。是点对点的安全连接。通过在安全隧道的两端(本端和对端)配置(或自动生成)对应的安全联盟,实现 IP 数据包的本端加密和对端解密。安全隧道可以跨越多台路由器和网络,只有安全隧道的两端共享了秘密;对于隧道中间的路由器和网络,所有的加密数据包和普通数据包一样被透明地转发。

(8) 安全网关。是指具有 IPSec 功能的网关设备(安全加密路由器)。安全网关之间

可以利用 IPSec 对数据进行安全保护，以保证数据不被偷窥或篡改。

3.1.4　IPSec 的工作模式

IPSec 在对数据进行封装时有两种模式，AH 协议和 ESP 协议都支持这两种封装模式，即传输模式和隧道模式。前者在原始 IP 头与上层协议之间插入 AH 协议头或 ESP 协议头，后者则是增加新的 IP 头，将原始 IP 头和原始 IP 数据包本身都作为载荷。

1. 传输模式

传输(transport)模式下的安全协议主要用于保护上层协议数据包，仅传输层数据用来计算安全协议头，生成的安全协议头以及加密的用户数据(仅针对 ESP 封装)被放置在原 IP 头后面。即在传输模式下，不对原始数据包进行重封装，只是把新添加的认证头当成原始 IP 数据包的数据部分进行传输。传输模式封装的 IP 数据包结构如图 3-2 所示。

图 3-2　传输模式封装的 IP 数据包结构

当要求端对端(end-to-end)的安全保障，即数据包进行安全传输的起点和终点为数据包的实际起点和终点时才可以使用传输模式，因为此时不用对用户发送的 IP 数据包进行重封装，只需要实现端对端的通信即可。IPSec 的传输模式如图 3-3 所示。

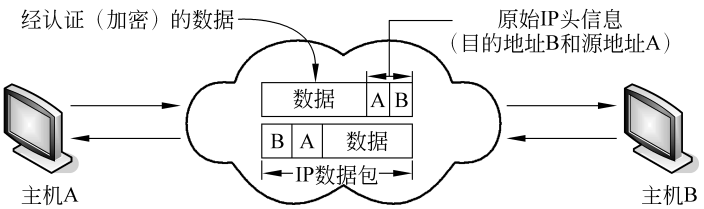
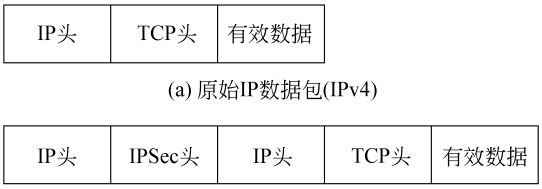


图 3-3　IPSec 的传输模式

2. 隧道模式

隧道(tunnel)模式下的安全协议用于保护整个 IP 数据包，即用户的整个 IP 数据包都被用来计算安全协议头，生成的安全协议头以及加密的用户数据被封装在一个新的 IP 数据包中。也就是在隧道模式下，封装后的数据包有内、外两个 IP 头，其中的内部 IP 头为原 IP 头(Raw IP Header)，外部 IP 头(New IP Header)是新增加的 IP 头。隧道模式封装的 IP 数据包结构如图 3-4 所示。

在隧道模式中，如果采用了 AH 协议，就无法实现 NAT 穿越。这是因为，如果有



(a) 原始IP数据包(IPv4)

(b) 隧道模式封装的IP数据包(IPv4)

图 3-4　隧道模式封装的 IP 数据包

NAT 设备，最外层 IP 头的地址信息一定会发生变化。AH 协议的认证范围是整个新生成的 IP 数据包，只要发生了数据变化则会导致认证失败。而如果单独采用 ESP 协议，认证范围则不包括“新 IP 头”和“ESP 认证数据”这两个字段，原始 IP 头信息不会发生变化，所以单独采用 ESP 作为安全协议时是可以穿越 NAT 的。

隧道模式在两台主机点对点(site-to-site)连接的情况下，原始 IP 头放在了 AH 或 ESP 头之后，隐藏了内网主机的私网 IP 地址，可保护整个原始数据包传输的安全。隧道模式通常用于保护两个安全网关之间的数据，实现点对点的安全连接。IPSec 的隧道模式如图 3-5 所示。

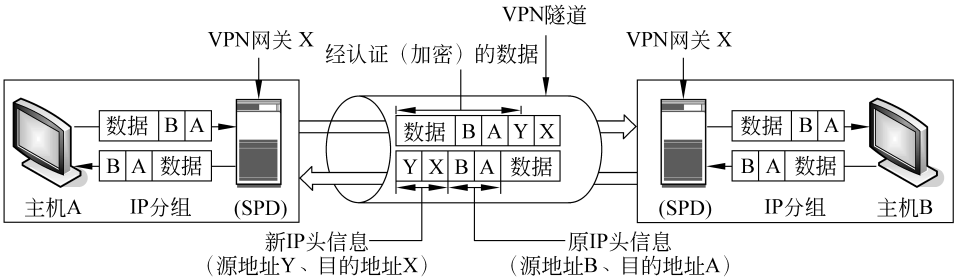


图 3-5　IPSec 的隧道模式

3. 两种模式的比较

从安全性来讲，隧道模式优于传输模式，因为隧道模式可以完全地对原始 IP 数据包进行认证和加密，隐藏客户机的私网 IP 地址，而传输模式中的数据加密不包括原始 IP 头。

从性能来讲，因为隧道模式有一个额外的 IP 头，所以它将比传输模式占用更多带宽，有效传输率较低。

从应用场景来讲，传输模式在 AH 协议或 ESP 协议处理前后 IP 头保持不变，主要用于端对端的应用场景，适用于主机到主机方式数据包的处理；隧道模式在 AH 协议或 ESP 协议处理之后再封装一个外网 IP 头，主要用于点对点的应用场景，适用于转发设备上作为封装处理的场景。

此外，使用传输模式有以下充要条件：要保护的数据流必须完全在发起方和响应方的 IP 地址范围内。因此，可以使用传输模式的情况受到较大的限制。

3.2 IPSec VPN 技术

3.2.1 IPSec 加密传输

1. IPSec 对 IP 数据包的处理

1）对发送数据包的处理流程

在操作系统的 IP 协议栈中，在数据包被从网络设备发送出去之前截取 IP 数据包，然后从中提取选择符信息，据此搜索 SPD 可能会产生如下结果：

（1）安全策略决定丢弃此数据包，则直接丢弃，或向源主机发送 ICMP 信息。

（2）安全策略决定放行，则直接将数据包投放到网络设备的发送队列。

（3）安全策略决定应用 IPSec。此时安全策略指向一个 SA，可以根据它进行安全处理；如果需要的 SA 不存在，则触发 IKE 模块协商建立 SA，在协商周期内，数据包进入等待队列，等待协商完成，若协商超时，也会丢弃该数据包。

2）对接收数据包的处理流程

系统收到 IP 数据包后，从 IP 头及 TCP/UDP 头中提取选择符信息，搜索 SPD。如果该 IP 数据包不是 IPSec 数据包，则直接进行网络转发处理或者交给上层协议处理；如果它是 IPSec 数据包，则依照如下流程处理：

（1）从 IP 数据包中提取出三元组（SPI、目的 IP 地址和安全协议号），并查找 SAD，定位 SA。如果没有 SA，则丢弃该 IP 数据包，并记录日志。

（2）由上一步获得的 SA 进行 IPSec 处理。

（3）由 SA 指向的 SP 确定对 IP 数据包的处理，决定交给上层协议处理还是继续转发。

其中，第（1）、（2）步会循环处理，直到处理到上层协议（TCP/UDP），或者内部 IP 数据包为非本地目的地址，需要转发该 IP 数据包。

2. IPSec 加密传输流程

一个 IP 数据包到达安全加密路由器的端口 1 后，路由器首先根据此数据包的源 IP 地址和目的 IP 地址、端口号、协议号查询本端口引用的访问控制列表，以确定是否允许其通过，然后查询路由表，最后将此数据包送到端口 2。

数据包到达此加密路由器端口 2 后，将数据包的 IP 头提取出来与访问控制列表对照，如果发现此数据包需要加密，便将其交给 IPSec 来处理。IPSec 加密传输流程如图 3-6 所示。

IPSec 首先根据查询访问控制列表的结果，将对应的 SA 的信息与 IP 头放到 IPSec 队列中，逐一处理。然后，IPSec 将根据该数据包指定的 SA 的配置进行如下操作：

（1）检查此 SA 所用的封装模式。如果是隧道模式，则将原 IP 数据包整个当作数据进行加密；如果是传输模式，则将 IP 头提取出来，只对数据段进行加密。

（2）不论是隧道模式还是传输模式，加密数据的方式都是一致的。此阶段有两种方

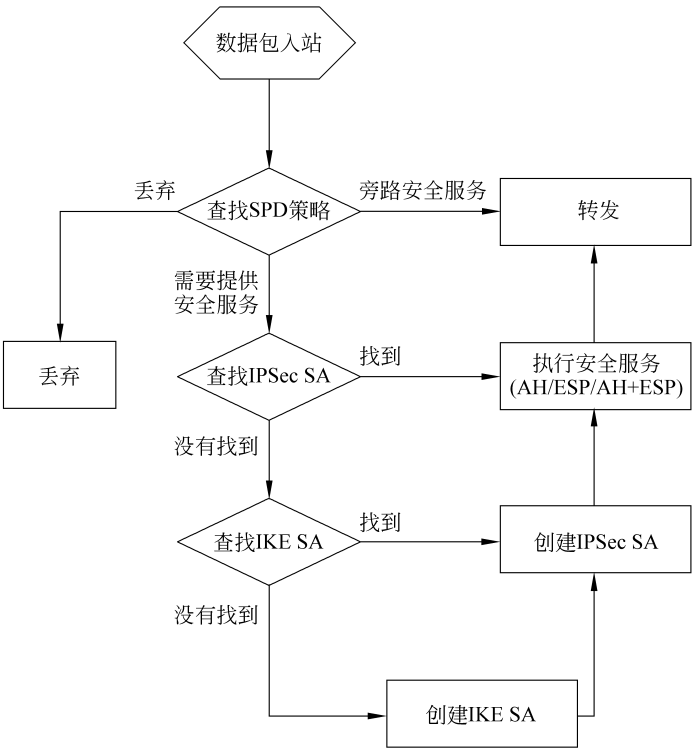


图 3-6　IPSec 加密传输流程

式(由 SA 引用的转换方式配置决定)：一种是 AH 协议方式，另一种是 ESP 协议方式。

(3) 加密完成后，IPSec 根据转换方式(隧道模式或传输模式)为新的数据加上新的 IP 头。对于隧道模式，IPSec 会将 SA 配置中设置的隧道入口和出口的 IP 地址作为新的源 IP 地址和目的 IP 地址，根据使用的协议产生一个新的 IP 头；对于传输模式，IPSec 会将原来的 IP 头直接放在数据的前面，但安全协议号已经修改成了 AH 或者 ESP。

至此发送端的工作完成。接收端的工作与之类似，只是处理的方式相反，后面将对此进行详细讲述。

3.2.2　AH 协议的原理及运行方式

1. AH 协议

AH 协议主要提供 3 个安全功能：数据完整性服务、数据验证、防止数据重放攻击。

AH 的工作原理是在每一个数据包上添加一个身份认证头。这个身份认证头包含一个带密钥的散列值(可以将其当作数字签名，但不使用证书)，此散列值在整个数据包中计算，因此对数据的任何更改都将导致散列值无效，因此该过程提供了完整性保护。

AH 头位置在 IP 头和传输层协议头之间。AH 协议由 IP 协议号 51 标识，该值包含在 AH 头之前的协议头(如 IP 头)中。AH 可以单独使用，也可以与 ESP 协议结合使用。ESP 协议也提供可选择的认证服务，AH 协议与 ESP 协议的认证服务的差别在于它们计

算时所覆盖的范围不同。

AH 头结构如图 3-7 所示。

图 3-7　AH 头结构

在 AH 头结构中，各个字段的含义如下。

(1) 下一个头：指定被封装的数据的协议，协议号是由 Internet 数字分配机构(Internet Assigned Numbers Authority，IANA)定义的。

(2) 有效载荷长度：定义了 AH 头的长度，不包括其外面的 IP 头和封装的数据长度。

(3) 保留字段当前没有使用。

(4) 安全参数索引：由接收端的设备为单向连接分配的一个数字，它可以区分从这台设备的一个连接和另一个连接或是其他端对端设备出去的流量。这个字段长为 4B。

(5) 序列号：指定通过数据连接的每一个数据包的独立的号码，该字段可用于检测重放攻击。

(6) 验证数据：包含 ICV(Integrity Check Value，完整性校验值)和其他数据，其中 ICV 为数据包提供了验证信息，它是利用 MD5 或 SHA-1 HMAC 功能产生的数字签名。

对于 AH 协议的功能有以下两点需要注意：

(1) AH 的保护服务中不包括数据加密，因此 AH 通常使用在内部网络中。

(2) AH 不能与 NAT 联合工作的原因是：NAT 改变了源 IP 地址与目的 IP 地址，但是 AH 在建立 ICV 时需要使用这些字段。

2. 传输模式下 AH 的封装

AH 用于传输模式时，提供基于主机到主机的安全通信。AH 头紧跟在 IP 头之后、上层协议头(如 TCP 头)之前，对这个数据包进行保护。传输模式下 AH 的封装结构的对比如图 3-8 所示。

3. 隧道模式下 AH 的封装

AH 用于隧道模式时，提供基于网关和主机的安全通信。在隧道模式下，AH 协议封装整个 IP 数据包，并在 AH 头外部再封装一个 IP 头，内部 IP 头的源 IP 地址和目的 IP 地址是最终的通信两端的 IP 地址，而外部 IP 头的源 IP 地址和目的 IP 地址是隧道的起止端点的 IP 地址。在隧道模式下，AH 协议保护了整个内层 IP 数据包。与传输模式类

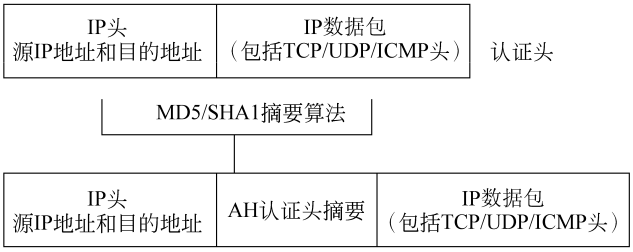


图 3-8　传输模式下 AH 的封装结构

似，AH 头的位置也是紧接在最外面的 IP 头之后。隧道模式下 AH 的封装结构如图 3-9 所示。

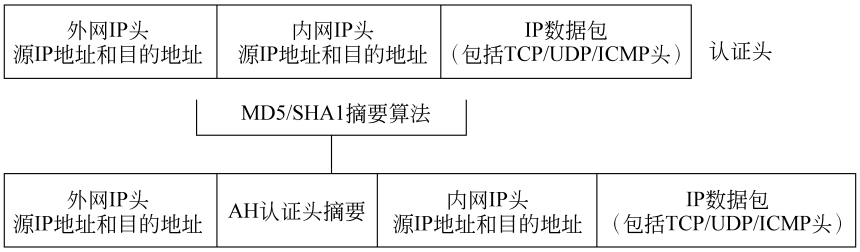


图 3-9　隧道模式下 AH 的封装结构

4. AH 处理流程

AH 的工作主要涵盖了对于数据包的发送处理和接收处理，在发送的时候主要添加相应的 AH 头，而在接收的时候主要进行相应的数据解码处理。

1）对发送数据包的处理流程

AH 的验证数据包产生一个完整性验证值（ICV）。在接收方，通过重新计算 ICV 并与收到的发送方计算的 ICV 进行比较，判断 AH 提供保护的数据是否遭到篡改。

AH ICV 的计算数据包括 IP 头中的值（这些值必须满足的条件是传输中不变或在 AH 处理前的变化可预测）、AH 头中的数据、可能有的填充字节和高层协议数据。

按照 AH 头中各字段的出现顺序，对各字段的构造、处理过程说明如下：

（1）下一个头字段的取值来自跟在 AH 头后的数据的协议号。有效载荷长度代表从序列号字段开始的 AH 头长度（以 32b 为单位）。安全参数索引的值来自 AH SA 中的 SPI。

（2）创建一个外出 SA 时，发送方的计数器被清零（初始化），每次利用这个 SA 构造一个 AH 之前，发送方将计数器加 1 并将新值填入序列号字段，这样就能保证每个 AH 头中的序列号是唯一的、单调递增的。根据是否提供防重放服务，发送方对序列号的溢出处理不同。若接收方允许防重放功能（默认），则发送方在计数器溢出之前要创建新的 SA；若接收方禁止防重放功能，则发送方只需将计数器递增，在序列号等于最大值（$2^{32}-1$）后，将计数器重新清零。

（3）在进行 ICV 计算之前，AH 头中的验证数据字段必须被清零。因为与 ESP 相

比，AH 将验证服务覆盖范围扩展到之前的 IP 头，因此必须将 IP 头中取值不定的字段清零，这样，在传输过程中，中间设备对这些字段的修改不会影响数据包中数据的完整性。

(4) 在需要填充的情况下，填充可分为隐式和显式两种。根据验证算法的需要，在 ICV 计算之前，隐式填充数据被添加到数据包的尾部，填充长度由算法决定，内容必须清零，并且不随数据包一起传输；而显式填充的长度取决于 ICV 的长度和 IP 协议版本(IPv4 或 IPv6)。填充的内容可以任意选择，位于验证数据之后的这些填充包含在 ICV 计算中，并且随数据包一起传送。

(5) 计算好的 ICV 被复制到 AH 头中的验证数据字段。至此 AH 处理结束，处理后的数据包可以继续进行下一步处理。

2) 对接收数据包的处理流程

在 AH 处理之前，可能需要重组收到的 IP 数据包。对于接收方 AH 而言，必须丢弃需要处理的 IP 数据包的分片。根据 AH 处理之前检索到的 AH SA，具体的处理过程如下：

(1) 若接收方指定这个 SA 禁止防重放服务，则无须对序列号进行检查；反之，对接收到的每个数据包，必须首先验证其序列号，确保在该 SA 的作用时间内该序列号没有重复出现。使用滑动接收串口和位掩码检查重复的数据包。若检查失败，则这个数据包被丢弃。

(2) 对通过序列号检查的数据包进行 ICV 验证。第一步，将数据包中的验证数据字段中的 ICV 保存下来，然后将该字段清零。第二步，接收方根据 AH SA 指定的验证算法，选择与发送方一致的计算范围(可能需要隐式填充)进行 ICV 计算，将计算的结果与保存的 ICV 值相比较。若两者不一致，则接收方丢弃这个无效的 IP 数据包；否则，表明 ICV 检查成功，接收方更新接收窗口。

(3) ICV 验证完成之后，应比较 SA 对应的 SPD 条目所采用的安全策略和这一数据包所采取的保护方式之间的异同，完成对两种安全方式的一致性检验。

3.2.3　ESP 协议的原理及运行方式

1. ESP 协议

ESP 协议提供了对数据的第 3 层保护。它提供了与 AH 协议同类型的服务，但有以下两点例外：

(1) ESP 提供对用户数据的加密服务。

(2) ESP 的数据验证和完整性服务只包括 ESP 头和有效载荷，不包括外部的 IP 头。因此，如果外部 IP 头被破坏，ESP 无法检测到，而 AH 可以检测到。

ESP 协议包结构如图 3-10 所示。

(1) 安全参数索引(SPI)：标识一个安全连接，与 AH 头中的 SPI 字段相同。需要指出的是，SPI 本身可以被验证，但不会被加密，否则无法处理。

(2) 序列号：一个单调递增的计数器的值，同 AH 头中的序列号字段相同，主要为了抵抗重放攻击。同样，序列号也不会被加密。

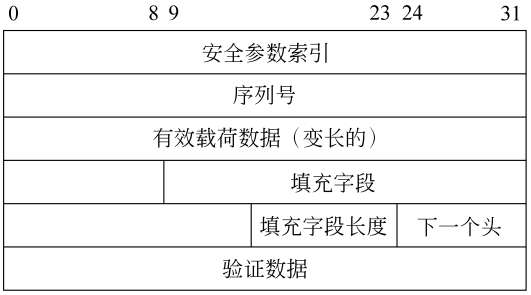


图 3-10　ESP 协议包结构

（3）有效载荷数据：长度可变，为加密的传输数据。

（4）填充字段：长度为 0～255B，用于将明文扩充到规定的长度，以保证边界的正确，同时隐藏有效载荷数据的实际长度。

（5）填充字段长度：表示填充字段填充的字节数。

（6）下一个头：标识下一个头的类型，从而表示有效载荷数据的类型。在传输模式下，该字段是处于保护中的 IP 上层协议（如 UDP 或 TCP）的协议类型值；在隧道模式下，该字段的值为 4。

（7）验证数据：与 AH 头中的验证数据字段相同，ICV 的长度必须是 32b 的整数倍，是在前面字段基础上计算的完整性校验值。

2. 传输模式下 ESP 的封装

ESP 用于传输模式时，只能用于基于主机到主机的 IP 网络安全通信，且此时只能保护 IP 网络层之上的协议（如 TCP）数据，而不包括 IP 头。传输模式下的 ESP 封装头紧接在 IP 头之后、上层协议头之前（在协议嵌套模式下，则位于其他 IPSec 协议头之前）。传输模式下 ESP 的封装结构如图 3-11 所示。

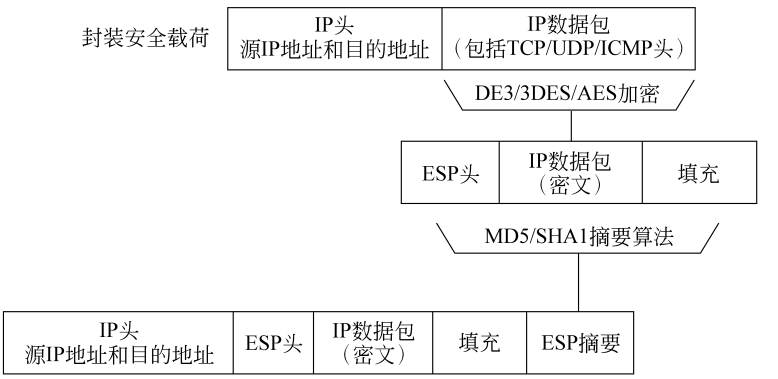


图 3-11　传输模式下 ESP 的封装结构

3. 隧道模式下 ESP 的封装

当 ESP 协议应用于网关时，必须使用隧道模式。此时，ESP 封装整个 IP 数据包，并

在 ESP 头外部再封装一个 IP 头。内网 IP 头的源 IP 地址和目的 IP 地址是最终通信两端的 IP 地址，而外网 IP 头的源 IP 地址和目的 IP 地址是隧道的起止端点的 IP 地址，内网 IP 头和外网 IP 头中的 IP 地址可以是不同的。此时，ESP 对内网的整个 IP 数据包进行保护。隧道模式下 ESP 的封装结构如图 3-12 所示。

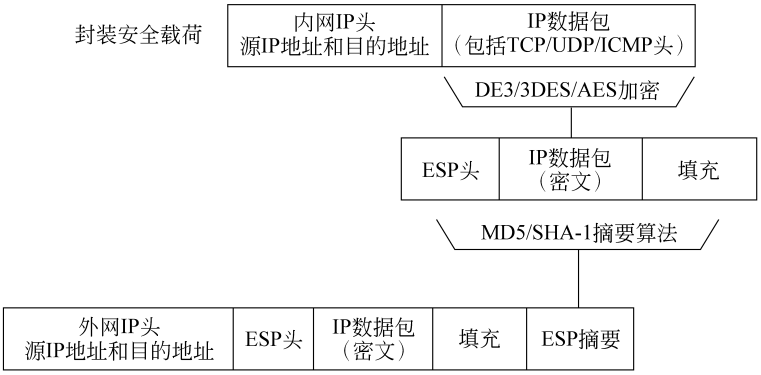


图 3-12　隧道模式下 ESP 的封装结构

4. ESP 处理过程

ESP 对发送的 IP 数据包主要进行加密处理，而对接收的 IP 数据包主要进行验证处理。

1）对发送数据包的处理流程

ESP 对发送数据包的处理可以分为 3 部分：序列号生成、数据包加密和 ICV 计算。若 ESP SA 不提供加密服务，则可忽略加密处理。具体步骤如下。

（1）对于发送数据包中序列号的处理，ESP 与 AH 完全相同。

（2）加密处理前，发送方首先构造 ESP 数据包，将 SA 中的 SPI 复制到 SPI 字段，将 ESP SA 中的计数器加 1 后的新值填入序列号字段。根据 SA 工作模式的不同，封装在 ESP 有效载荷数据字段中的数据也不同：传输模式下是原始的高层协议信息，下一个头字段取自 IP 头中的协议字段；而隧道模式下是整个原始的 IP 数据包，下一个头的可能取值为 4（IPv4 环境）或 41（IPv6 环境）。此外，隧道模式下，一个新的 IP 头插在 ESP 数据包的前面，新 IP 头中各字段的取值遵照本地的 IP 协议版本的规定。对于 IPv4 头，源 IP 地址和目的 IP 地址依赖于 ESP SA。若数据包被转发，则取值遵照封装前后 TTL 协议版本的规定。对于 IPv4 头，源 IP 地址和目的 IP 地址依赖于 ESP SA。若数据包被转发，封装前后 TTL 值需减 1。

（3）根据需要，可能要添加填充数据。填充内容可以不同，但填充长度字段必须赋值。

（4）加密处理则利用 ESP SA 指定的加密密钥、加密算法、加密模式和可能的初始化矢量加密上述操作后的结果，包括有效载荷数据、填充、填充长度、下一个头 4 个字段。若 ESP SA 同时提供验证服务，则先进行加密，后进行验证，验证数据没有被加密，这样的安排便于接收方及时发现、拒绝重放或伪造的数据包。

(5) 发送方对 ESP 数据包中去除验证数据后剩下的部分进行 ICV 计算,因此安全参数索引、序列号和加密的有效载荷数据、可能出现的填充、填充长度、下一个头字段均包含在 ICV 计算中。ICV 被复制到 ESP 尾部的验证数据字段中。

2) 对接收数据包的处理流程

ESP 在处理之前可能需要对数据包的分片进行重组,对每个接收数据包的处理大致可以分为 3 部分:序列号验证、ICV 验证和数据包解密。序列号要在 ICV 提供的完整性保护下工作,因此,对一个 ESP SA 而言,如果不提供验证服务,那么提供防重放服务是没有任何意义的。具体步骤如下:

(1) 若接收方禁止防重放服务,则无须对 ESP 数据包中的序列号进行检查,否则,需要检查序列号是否重复,检查采用的方法与 AH 协议相同。若 ESP 数据包中包含有效序列号,则进行 ICV 验证,若验证失败,接收方丢掉这个无效的 IP 数据包。

(2) 若 ESP SA 同时提供验证服务,则接收方利用 SA 指定的验证算法,对不包含验证数据的 ESP 数据包进行 ICV 计算,并将结果和 ESP 数据包中包含的验证数据相比较。若重新计算的 ICV 和接收到的 ICV 相同,则认为数据有效,可以接受;否则丢弃整个数据包。

(3) 直到此时,接收方才利用 ESP SA 指定的密钥、加密算法、算法模式等对有效载荷数据、填充、填充长度、下一个头字段进行解密,得到明文。然后处理加密算法规范可能使用的填充数据。最后重构原始的 IP 数据包。在传输模式下,利用原始的 IP 头和 ESP 有效载荷数据字段中的原始高层协议信息重构 IP 数据包;在隧道模式下,则利用 ESP 有效载荷数据字段中的 IP 数据包和隧道外的 IP 头重构 IP 数据包。

(4) 如果 SA 同时提供解密和验证服务,解密和验证操作可以并行执行,此时验证操作必须在解密数据包进入下一步处理之前完成。在某些情况下,解密操作不一定会成功,此时后续协议负责处理解密后的数据包。判断解密的结果是否正确。

3.2.4 IKE 协议

1. IKE 协议概述

IPSec 的安全联盟(SA)可以通过手工配置的方式建立,但是当网络中的节点较多时,手工配置将非常困难,而且难以保证安全性。这时就要使用 IKE 协议自动地进行安全联盟建立与密钥交换的过程。

IKE 协议是建立在由 Internet 安全联盟和密钥管理协议(Internet Security Association and Key Management Protocol,ISAKMP)定义的框架上,沿用 Oakley 的模式以及 SKEME 的共享和密钥更新技术定义的秘密材料(包括验证材料和加密材料)生成技术和密钥协商策略。作为混合协议,IKE 协议的功能是在保护方式下协商 SA,并为 SA 提供经验证的秘密材料。IKE 协议不仅可用于协商 VPN,而且可用于远程用户接入安全主机和网络。IKE 协议同样支持客户协商,在这种模式下,终端实体的身份信息是隐藏的。

IKE 协议利用 Diffie-Hellman 密钥交换算法和各种身份认证方法(如数字签名)可以在一条不保密的、不受信任的通信信道(如 Internet)上为交换密钥的双方建立一个安全

的、共享秘密的会话，通过管理安全联盟来实现对密钥的管理。

Diffie-Hellman 密钥交换算法是早期的密钥交换算法之一，它使得通信的双方能在非安全的信道中安全地交换密钥，用于加密后续的通信消息。

2. IKE 与 IPSec 的关系

IKE 是 IPSec 协议族中的一种，IKE 与 IPSec 的关系如图 3-13 所示。

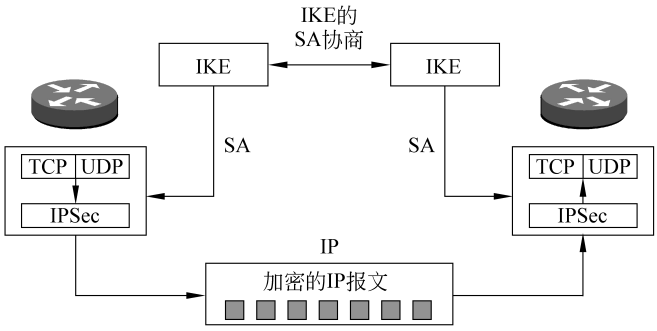


图 3-13　IKE 与 IPSec 的关系

IKE 是 UDP 上的一个应用层协议。IKE 为 IPSec 协商建立 SA，并将建立的参数及生成的密钥交给 IPSec。IPSec 使用 IKE 建立的 SA 对 IP 数据包进行加密或验证处理。

IKE 在 IPSec 中的作用包括以下几点：

- 降低手工配置的复杂度。
- 定时更新 SA。
- 定时更新密钥。
- 允许 IPSec 提供反重放服务。
- 允许在端与端之间进行动态认证。

3. IKE 的两个阶段

IKE 使用了两个阶段的 ISAKMP 分别建立 IKE SA 和 IPSec SA。其中，IPSec SA 受 IKE SA 的保护，IKE SA 为 IPSec SA 提供交换服务。整个协商过程分为两个阶段。

第一阶段的实施过程如图 3-14 所示。

在第一阶段，双方协商建立一个安全的、经过相互身份认证的数据通道，称之为 IKE SA。IKE SA 保存着双方继续协商 IPSec SA 所需的加密算法、密钥等安全参数。在第一阶段协商中可以采用两种模式：即主模式(main mode)和激进模式(aggressive mode)。

主模式执行 3 步双向交换过程，总共 6 个数据包。3 步双向交换是指：协商安全策略用于管理连接、使用 Diffie-Hellman 算法对上一步中协商的加密算法和 HMAC 功能产生密钥，使用预共享密钥、RSA 加密的随机数或者 RSA 签名(数字证书)执行设备验证。

主模式有一个好处：设备验证的步骤发生在安全的管理连接中。因为这个连接是在前两步中构建的，所以两个对等体发送给对方的任何实体信息都可以免受窃听攻击。

在激进模式中，发生两步交换。第一步交换含有一些用于保护管理连接的策略、Diffie-Hellman 算法建立的公钥/私钥对的公钥、实体信息及其验证(例如签名)。所有这

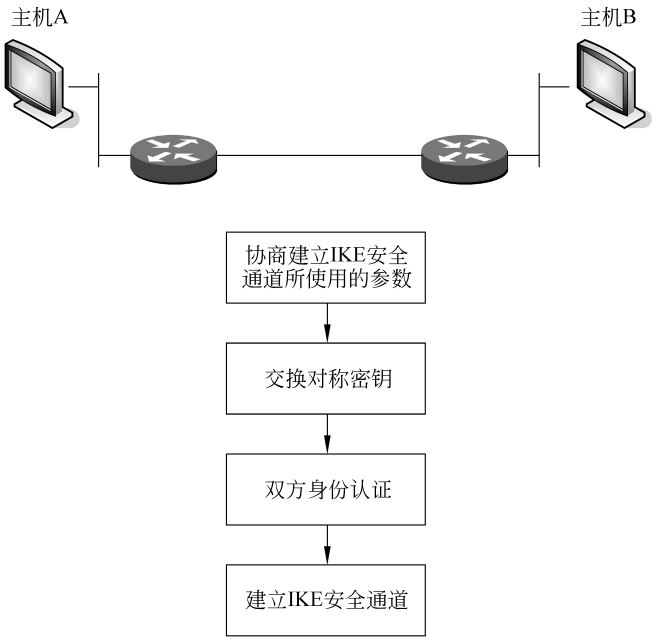


图 3-14　第一阶段的实施过程

些信息都放入一个数据包中。第二步交换是对收到的上述数据包进行确认，共享加密的密钥(由 Diffie-Hellman 算法生成)，并检查管理连接是否已成功地建立。

激进模式与主模式相比的一个主要的优点是建立管理连接的速度较快。激进模式的缺点是任何发送的实体信息都是明文的，所以如果某人在正在传输过程中实施窃听攻击，就会看见用于建立设备验证的签名的实体信息。

这两种模式主要的区别在于是否对用户的身份载荷(ID payload)进行认证，它们需要交换的数据包的数量也不同。密钥协商过程中一共可以采用 4 种身份认证方法，即数字签名、公钥加密算法、改进的密钥算法和预共享密钥。

第一阶段的实施过程如图 3-15 所示。

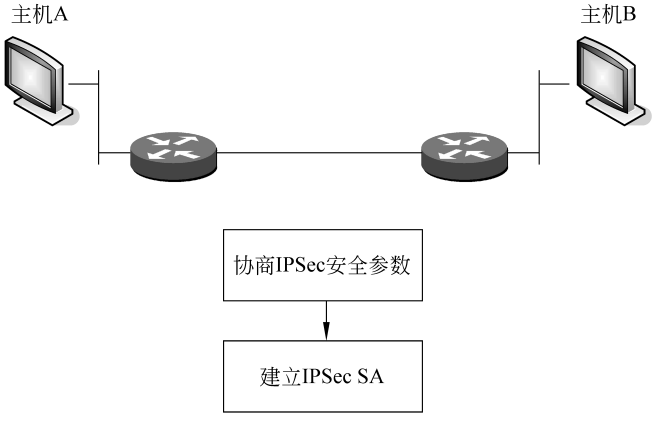


图 3-15　第二阶段的实施过程

在第二阶段，双方使用第一阶段产生的 IKE SA，协商产生用于上层应用的 IPSec SA，使用快速模式(quick mode)来实现。

快速模式有两个主要功能：

- 协商安全参数来保护数据连接。
- 周期性地对数据连接更新密钥信息。

第二阶段实际上是在两个对等体之间构建两个单向数据连接。例如，主机 A 有一个到主机 B 的单向数据连接，主机 B 有一个到主机 A 的单向数据连接。由于两个数据连接均是单向的，所以在两个对等体之间协商的安全参数可能是不同的。例如，主机 A 到主机 B 的数据连接可能使用 3DES 算法进行加密，而主机 B 到主机 A 的数据连接可能使用 DES 算法进行加密。

第二阶段构建数据连接的过程中可以使用一个或者两个安全协议来保护传输的数据，即 AH 协议和 ESP 协议。

安全协议的连接模式也有两种，即传输模式和隧道模式(若同时使用了 AH 协议和 ESP 协议，则需要对它们使用同一种连接模式)。

在传输模式中，用户数据的实际源 IP 地址和目的 IP 地址启用保护服务，当使用这种连接模式添加的设备越来越多时，就会变得非常难以管理。这种模式通常用于在两台设备之间保护特定的流量，例如 TFTP 传输配置文件或者系统日志传输日志消息。

在隧道模式中，中间设备通常执行用户数据的保护服务。这种连接模式用于点对点和远程访问连接，因为原始的 IP 数据包被保护，嵌入 AH/ESP 中，外面添加了一个 IP 头，内部的 IP 数据包可以包含私有的 IP 地址。如果使用 ESP 进行加密，那用户数据实际的源 IP 地址和目的 IP 地址对于窃听者是隐藏的。

与传输模式相比，隧道模式的主要优点是保护服务的功能可以集中在少量设备上，减少了配置和管理工作量。

3.2.5　IPSec SA

1. 安全联盟和密钥管理协议

ISAKMP 协议定义了 SA 建立过程中的协商、修改、删除的过程以及通信的消息结构。ISAKMP 为密钥的传输和数据的认证提供了统一的协议框架结构，而该框架独立于具体的密钥产生算法、加密算法和认证机制。

一个 ISAKMP 消息由一个消息头和多个消息载荷构成。当一个 ISAKMP 消息有多个消息载荷时，这些消息载荷利用 ISAKMP 消息头和各个消息载荷头的下一个载荷字段(指针)构成一个消息载荷数据串。

2. IKE SA 的建立

IKE SA 的建立是通过第一阶段的 ISAKMP 交换来实现的。ISAKMP 第一阶段交换的目的是建立一个保密的已验证的通信信道(IKE SA)，并生成密钥，为双方的 IKE 通信提供机密性、消息的完整性以及消息源验证服务，IKE SA 用于保护 IKE 阶段的消息交换和第二阶段 IPSec SA 的建立，IKE SA 主要包括加密算法(如 DES、3DES 等)、散列算

法(如 MD5、SHA-1 等)、认证方法和 SA 的生命周期等安全属性。IKE 第一阶段有两种模式:主模式和激进模式。

在主模式下,IKE SA 的建立需要在发起者和响应者之间交换 6 条消息。

(1) 第 1、2 条消息用于协商安全联盟特性,以明文方式传输,不进行身份认证。

(2) 第 3、4 条消息用于交换随机数和 Diffie-Hellman 的公开值,它们也以明文方式传输。

(3) 第 5、6 条消息用于交换通信双方相互认证所需要的信息,其内容由前 4 条消息建立的加密算法和密钥来保护。

经上述 6 条消息的交换后,发起者和响应者就分别建立了各自的 IKE SA,并在各自的 IKE SA 数据库中增加一条记录。

3. IPSec SA 的建立

IPSec SA 的建立阶段在已经建立的 IKE SA 保护下进行,通信双方协商拟定 IPSec 的各项特征,包括 IPSec 协议类型(如 AH、ESP)、加密算法(如 DES、3DES)、散列算法(如 MD5、SHA-1)、加密模式和安全联盟生存周期等,并为它们生成密钥。

在 IPSec SA 的建立阶段,通过使用来自 IKE SA 的 SKEYID_a 作为认证密钥,对快速交换模式的整个消息进行验证,该验证除了提供数据完整性保护服务外,还提供数据源身份认证服务;通过使用来自 IKE SA 的 SKEYID_e 对交换的消息进行加密,以保证消息的机密性。

IPSec SA 的建立共交换 3 条消息。

(1) 第 1 条消息用于发起者向响应者提交认证信息。

(2) 第 2 条消息是响应者对第一条消息的响应。

(3) 第 3 条消息用于发起者向响应者证明自己的活性。

3.3 IPSec VPN 系统

3.3.1 IPSec VPN 概述

IPSec 协议族由 ESP 协议、AH 协议和 IKE 协议组成。

AH 协议提供验证和可选的防重放保护两种安全服务。若要提供 AH 保护,需要在原始内容前添加额外的载荷——AH 头。AH 头的格式比较简单,较适合在加密服务受限的场合提供快速安全服务。

与 AH 协议相比,ESP 协议功能更为强大,提供加密服务、验证服务、抗重放保护服务和有限的流量保密服务。采用 ESP 协议保护的数据需要添加更多的载荷,如 ESP 头、ESP 尾。

AH 协议和 ESP 协议提供的安全服务依靠 IKE 协议产生、更新会话密钥。基于公私钥密码系统,IKE 协议实际上是 IPSec 协议族中的信令协议,提供了自动化的安全密钥协商手段。

IPSec 的作用实际上体现为对数据包的处理。按照处理流程的不同，IPSec 对数据包的处理分为发送数据包的处理和接收数据包的处理。对发送数据包采用 IPSec 处理的目的是添加对数据包的保护；处理接收数据包时则采用相反流程，去除数据包中的 IPSec 载荷。

由于 IPSec 实施在 IP 层，具有对应用完全透明的优点，所以很适合构建 IPSec VPN。基于采用 IPSec 组建 VPN 大致有 3 种模式：基本模式、嵌套模式和链式模式。3 种模式各有特点：基本模式是基础；嵌套模式提供多级安全保护；链式模式采用集中控制方式，强化对隧道的管理。IPSec VPN 还可在远程拨号接入环境下对数据传输安全提供保护。

3.3.2　IPSec VPN 的基本模式

IPSec 保护的对象是 IP 数据包本身，因此 IPSec 安全保护可连续或嵌套使用，并且支持轴辐(hub-and-spoken)模式。

支持安全拨号接入的 IPSec VPN 实例如图 3-16 所示。在 3 个安全网关 gw_a、gw_b、gw_c 上安装 IPSec 的某种实现，安全网关同时具备将内部网络接入公共网络(Internet)的功能。通过将位于不同安全网关之后的多个子网间的数据通信置于各网关提供的 IPSec 保护之下，可以构建一个虚拟专用网。VPN 一般假设网关与公共网络的连接是不安全的，与内部网络/主机间的连接是安全的。子网 2 和子网 3 之间的数据流到达各自的网关设备后，通过隧道在公共网络中安全地传输。在隧道终点——远方安全网关，控制数据被剥离，原始的数据通过网关后的内部网络抵达最终目的地。如果安全网关为受保护的对象提供加密服务，则隧道中的数据是加密的，没有会话密钥的任何公共网络上的任何中间设备均无法获知传输内容。若提供验证服务，则对 IP 数据包的任何篡改都会因为无法通过接收端对数据的完整性检查而被接收端发现。利用单调递增的序列号，还可以检测重播的数据包，在一定程度上可抵御拒绝服务(Denial of Service，DoS)攻击。

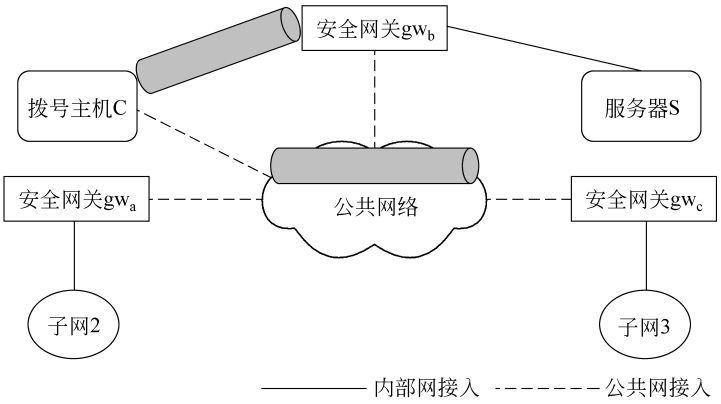


图 3-16　支持安全拨号接入的 IPSec VPN 实例

隧道正常工作的前提是：内部子网在设置路由时将默认网关指向本地安全网关，在子网 2 和子网 3 中，默认网关分别被设为安全网关 gw_a、gw_c。

在图 3-16 所示的实例中，拨号主机 C 也可以安全远程接入安全网关 gw_b后的服务器

S，即支持漫游接入。这里的拨号主机必须是实现 IPSec 的主机，通过拨号等方式接入公共网络。当需要访问服务器 S 上的资源时，拨号主机 C 与安全网关 gw_b 先协商建立隧道，然后对服务器 S 的访问在协商好的 SA 的保护下进行。与一般的端对端的 IPSec 应用不同，安全网关 gw_b 代表服务器 S 对来自拨号主机 C 的数据包进行 SA 处理，而在拨号主机端，C 负责本地发送数据包和接收数据包的 IPSec 处理。

在 VPN 和漫游接入这两种应用中，一般需要创建隧道模式的 SA。根据需求的不同，可使用 SA 的不同组合；若只需要验证保护，则可使用 AH SA 或只提供验证服务的 ESP SA；若还需要加密保护，可联合应用只提供机密服务的 ESP SA 和 AH SA 或应用同时提供加密和验证两种服务的 ESP SA。

3.3.3 IPSec VPN 的嵌套模式

在图 3-16 的示例中，IPSec 协议提供的安全保护范围只限于公共网络。在某些情况下，可能还需要对内部网络的保护，这样引入了多级网络安全保护的概念。图 3-16 中，若拨号主机 C 访问的服务器 S 在内部网络中属于某些关键部门，则通过隧道终点——网关 gw_b 后，访问数据包以明文形式在内部网络中传输，也面临严重的安全威胁——机密信息泄露。

IPSec 提出的嵌套隧道(iterated tunneling)技术可很好地解决这个问题。嵌套隧道是指同时应用多级安全协议，这些协议通过 IP 隧道技术联系在一起而生效。根据两条隧道端点之间的关系，典型的嵌套隧道可分为 3 种：两条隧道的两个端点完全一致；两条隧道有一个共同的端点；两个隧道的端点完全不同。每条隧道可使用不同的安全协议(AH 或 ESP)、不同的加密算法/验证算法。

应用嵌套隧道技术可以构建嵌套 VPN。以图 3-16 中的网络为例，如果在服务器 S 前放置一台安全网关 $gw_{b'}$，则可保证在内部网络中拨号主机 C 对服务器 S 的安全访问。拨号主机 C 在访问服务器 S 之前需要建立两条隧道：隧道 1 作用于拨号主机 C 和 $gw_{b'}$ 之间的传输路径；隧道 2 跨过安全网关 $gw_{b'}$，将对数据的保护扩展到 gw_c。拨号主机 C 选用这两条隧道保护的先后顺序不能颠倒：隧道 2 在前，隧道 1 在后。与之类似，子网 2 和子网 3 中的主机间通信若需要端对端安全保护，也可利用嵌套隧道技术，在需要跨网通信的主机上安装 IPSec 模块。在通信之前，首先建立两台主机间的隧道，然后在两台主机各自的安全网关上分别建立另一条隧道。这两条隧道联合作用，为主机间的数据流提供灵活的多级安全保护。

3.3.4 IPSec VPN 的链式模式

基于 IPSec 构建的 VPN 还可以采用轴辐模式，与链路级保护类似，这种模式下隧道的建立是在中心安全网关的控制下进行的。除中心安全网关之外，其他任意两个安全网关之间都不能直接建立隧道，必须分别与中心安全网关单独建立一条隧道，再由这两条隧道搭建成目的隧道。

轴辐模式 VPN 的应用示例如图 3-17 所示。如果要通过安全网关 gw_a、gw_c 为子网 2 和子网 3 建立隧道，必须采取如下步骤：在安全网关 gw_a 和 gw_b(中心控制网关)之间建

立隧道 1；在 gw_c 和 gw_b 之间建立隧道 2。在中心安全网关 gw_b 的控制下，gw_a、gw_c 利用隧道 1 和隧道 2 来保护子网 2 和子网 3 间的数据通信。

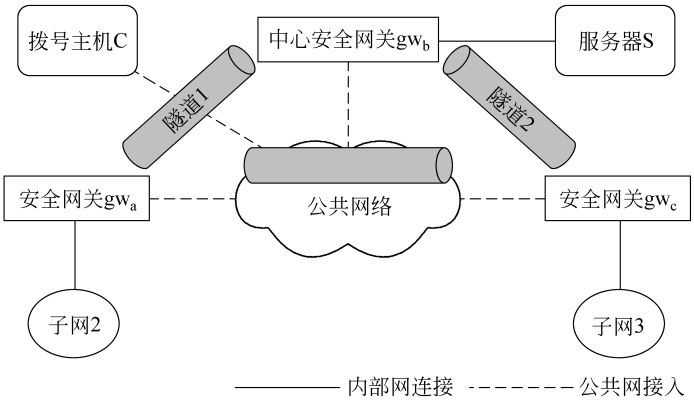


图 3-17　轴辐模式 VPN 的应用示例

如果子网 2 中某台主机想访问子网 3 中的服务器，则访问数据在经过安全网关 gw_a 时，被封装在隧道 1 中送往中心安全网关 gw_b；gw_b 对其进行解密、验证后将原始请求包从隧道 1 中剥离，因为请求包的目的地位于安全网关 gw_c 后的子网 3 中，gw_b 利用隧道 2 将请求包再一次封装，送往 gw_c；在隧道 2 的终点，封装的数据被验证、解密，然后从隧道 2 中剥离，原始的请求包最终被安全网关 gw_c 送往目的地。对访问请求的响应包的传输路径正好相反。

在轴辐模式下，拨号主机对 VPN 内子网的访问也需通过中心安全网关进行。即拨号主机先与中心安全网关建立一条隧道，然后中心安全网关与访问目标处的安全网关建立另一条隧道，这样，远程接入就受到这两条隧道的保护。

与一般 VPN 相比，轴辐模式系统性能欠佳，这是因为同一个数据包被多次加密、解密，在繁忙的公共网络上的延迟时间可能很长。其优点在于易于管理，便于大规模部署。中心安全网关是整个 VPN 系统的核心，可为不同的链接定制灵活的安全策略并分发。新增的 IPSec 设备对其他安全网关的影响很小，新增的设备只需与中心网关建立隧道，利用这条隧道形成与其他所有安全网关间的隧道。

3.4　IPSec VPN 的应用

IPSec VPN 是 IPSec 的一种应用方式，其目的是为 IP 远程通信提供高安全性特性。IPSec VPN 的应用场景分为以下 3 种。

（1）点对点。例如，企业的多个机构分布在互联网的多个不同的地方，各使用一个应用层网关相互建立 VPN 隧道，企业各分机构内网用户之间的数据通过这些网关建立的 VPN 隧道实现安全传输。

（2）端对端。两个位于不同网络的 PC 之间的通信由两个 PC 之间的 IPSec 会话保