IPSec 分析与应用

Analysis and application of IPSec protocol

李革新　李虎雄　（温州大学计算机学院 325027）
胡昌杰　（湖北职业技术学院计算机系　432100）

摘要：本文分析了 IPSec 安全体系结构，讨论了 IPSec 工作模式，给出了 IPSec 应用实例。
关键词：IPSec　工作模式　SA

1　IPSec 安全体系结构

IPsec 安全体系由认证头 AH（Authentication Header）协议、封装安全载荷 ESP（Encapsulating Security Payload）协议、密钥交换 IKE（Internet Key Exchange）协议、安全关联 SA（Security Association）以及加密和验证算法共同组成，其安全体系如图 1 所示。

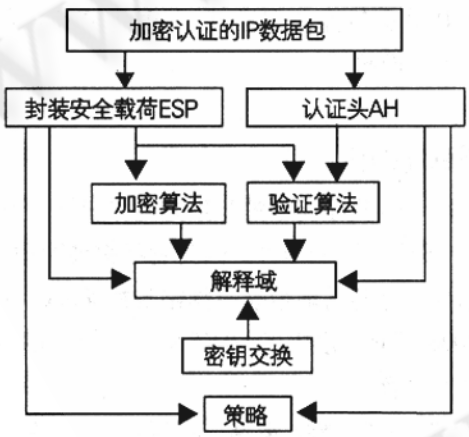

图 1　IPSec 安全体系示意图

（1）AH 协议。AH 协议为数据包提供身份验证、完整性和抗重放功能，并签署整个数据包，但不加密该包，因此不提供机密性。

（2）ESP 协议。ESP 协议提供身份验证、完整性、抗重放及机密性。在传输模式下，只保护数据而不保护 IP 报头。

（3）IKE 协议。IKE 协议是一种实现密钥交换定义的协议，是 Oakley 和 SKEME 协议的一种组合，并在 ISAKMP（Internet Security Association and Key Management Protocol）定义的框架内运作。ISAKMP、Oakley、SKEME 三个协议构成了 IKE 的基础，IKE 沿用了 ISAKMP 的基础、Oakley 的模式及 SKEME 的共享核密钥更新技术，从而定义出验证加密生成技术以及协商共享策略。因此 IKE 可用于在对等端之间认证密钥，并在它们之间建立共享的安全策略。

（4）SA 安全关联。SA 是策略和密钥的结合，用来定义保护端到端通信的安全服务、机制和密钥，它可以看成是两个 IPsec 对等端之间的一条安全隧道，可以为不同类型的流量创建独立的 SA。比如为 TCP 创建独立的 SA，也可为 UDP 创建独立的 SA。

（5）加密和验证算法。为保护通信安全，IKE 执行两个阶段的操作：密钥交换和数据保护。通过在彼此通信的计算机或网关上协商，从而达成一致的加密和身份验证算法，保证机密性和身份验证。在进行密钥安全交换时，用于生成实际密钥的基本密钥材料的组是 Diffie－Hellman 组，可以生成 768 位或 1024 位的主密钥的密钥材料。加密算法有 DES、3DES。完整性算法包括 MD5 和 SHA1。身份验证方式有：Kerberos V5、公钥证书和预共享密钥，其中 Kerberos V5 是 Windows 2000 的默认身份验证方式。

2　IPsec 工作模式

2.1　IPsec 传输模式

传输模式通过 AH 或 ESP 报头对 IP 有效荷载提供保护，其中 TCP 片段、UDP 数据报和 ICMP 消息就是典型的 IP 有效载荷。传输模式下的 AH 报文格式如图 2 所示，在使用此模式时，AH 将对整个数据包提供认证、

完整性与抗重播服务。但是 AH 不对数据进行加密，不提供保密性。数据可以读取，但禁止修改。AH 为了保证数据的完整性，利用身份验证报头对整个数据包进行签名。

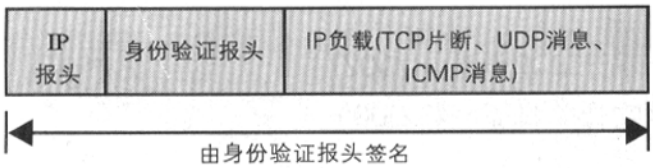

图 2　AH 报文格式

当使用 ESP 传输模式时（传输模式下 ESP 报文格式如图 3 所示），ESP 除了具有身份验证、完整性和抗重播功能外，还可以为 IP 负载（或称载荷）提供机密性。传输模式中的 ESP 不对整个数据包进行签名，只对 ESP 报头、IP 负载和 ESP 尾端进行完整性保护。同时用 ESP 报头对原始 IP 负载及 ESP 尾端加密，保证数据的机密性。

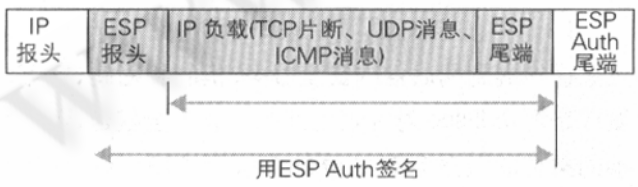

图 3　AH 报文格式

2.2 IPSec 隧道模式

隧道模式提供对整个 IP 数据包的保护。使用隧道模式时，将 AH 报头或 ESP 报头插在新的 IP 报头和整个 IP 数据包之间。新 IP 报头的 IP 地址就是隧道终结点，源 IP 数据包中 IP 报头的 IP 地址是有效载荷的源地址与目标地址。

在 AH 隧道模式中（隧道模式下 AH 报文格式如图 4 所示），使用 AH 与 IP 报头来封装 IP 数据包并对整个数据包进行签名以求完整性并进行验证。

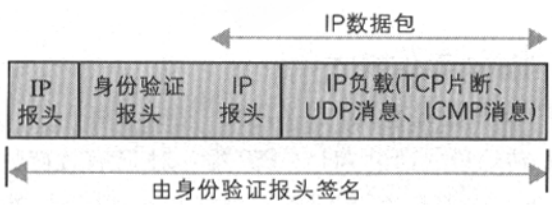

图 4　隧道模式下 AH 报文格式

隧道模式下 ESP 报文格式如图 5 所示，IPSec 采用 ESP 报头与新 IP 报头以及 ESP AUTH 尾端来封装 IP 数据包。

图 5　隧道模式下 ESP 报文格式

系统使用 ESP 报头对 IP 数据包（即原 IP 头、IP 载荷）与 ESP 尾端加密，保证原 IP 数据包的安全与机密性，即使被截取也无法被识别。同时用 ESP AUTH 尾端对 ESP 报头、IP 数据包及 ESP 尾端进行签名，以保证数据的完整性。然后，IPsec 将整个 ESP 载荷封装在未加密的新的隧道 IP 报头内。新隧道 IP 报头内的信息只是用来表示路由从源地址到目标地址的数据包。

在进行隧道操作时，ESP 与 AH 可组合使用，从而为隧道 IP 数据包提供保密性，同时为整个数据包提供完整性和身份验证。

3　IPSec 应用

IPSec 作为安全网络的长期方向，是基于密码学的保护服务和安全协议的套件。因为它不需要更改应用程序或协议，用户可容易地给现有网络实施 IPSec。现以 Windows 2000 环境为依托，介绍 IPSec 在 LAN 中的具体应用。

3.1 实施步骤

（1）建立新 IPSec 策略。在源主机上，依次选择开始、程序、管理工具、本地安全策略，打开本地安全设置对话框，右单击“IP 安全策略，在本地机器”，选择创建 IP 安全策略，使用 IP 策略安全向导，单击下一步，在弹出的对话框中填写 IP 安全策略的名称，单击下一步，接受对话框中“默认的响应”复选项，单击下一步，接受默认的选项“Windows”，单击下一步，选择编辑属性复选项，单击完成按钮完成 IPSec 的初步配置。

（2）添加 IP 筛选器。在不选择使用添加向导的情况下，单击添加按钮，在出现新规则属性对话框中，单击添加按钮，出现 IP 筛选器列表对话框，此时可为新的 IP 筛选器列表命名并填写描述。并单击添加按钮，出现筛选器属性对话框。单击寻址标签，选定“一个特

定的 IP 地址"作为源地址，并输入源主机 A 的 IP 地址。将目标地址选定为"一个特定的 IP 地址"，并输入目标主机的 IP 地址。同时选取镜像复选项。单击协议标签，选择协议类型为 ICMP（以便在测试 IPSec 时使用 Ping 命令）。单击确定按钮，返回 IP 筛选器列表对话框，单击关闭按钮回到新规则属性对话框，选中单选钮激活新设置的 IP 筛选器。

（3）规定筛选器操作。单击新规则属性对话框中的"筛选器操作"标签，在不选择使用向导的情况下单击添加按钮，出现新筛选器操作属性对话框。选择协商安全单选框，并单击添加按钮选择安全措施，如果选择"加密并保持完整性"，即使用 ESP 协议，它可提供具有"三重数据加密标准（3DES）"算法的数据加密、具有"安全散列算法 1（SHA1）"的数据完整性和身份验证，以及默认密钥寿命（100 MB/小时）。传送的数据被加密，验证为可信的并且没有被更改。单击确定返回新筛选器操作属性对话框，再次单击添加按钮选择安全措施，选择"仅保持完整性"，即使用 AH 协议，使得传送的数据将被验证为可信并没有被更改，同时数据不被加密。或者选择"自定义"单选框，进行高级 IPSec 策略的配置。返回到新筛选器操作属性对话框，利用上移或下移按钮来确定安全措施的首选顺序。并确保不选择"允许和不支持 IPSec 的计算机进行不安全的通信"，单击确定返回到筛选器操作标签。并单击单选按钮激活新设置的筛选器操作。

（4）设置身份验证方法。单击新规则属性对话框中的身份验证方法标签。单击添加按钮，出现新身份验证方法属性对话框。选择"此字串用来保护密钥交换（预共享密钥）"单选框，并输入预共享密钥字串"LIGEXIN"。单击确定返回身份验证方法标签，并单击上移按钮使"预共享的密钥"成为首选。

（5）设置隧道。单击新规则属性对话框中的隧道设置标签，由于 IPSec 隧道模式作为一种高级特性，仅在网关到网关（也叫作路由器到路由器）隧道环境、服务器到服务器或服务器到网关配置中使用。所以此处选择"此规则不指定 IPSec 隧道"。

（6）设置连接类型。单击新规则属性对话框中的连接类型标签，选择所有网络连接，单击确定返回到新 IP 安全策略属性对话框，单击关闭按钮回到本地安全策略窗口。

按以上步骤，对 LAN 中的目标主机做同样的配置。

3.2 测试 IPSec

进行 IPSec 测试时，从三个方面进行，在以下执行"Ping 对方 IP 地址 -t"命令时，需要密切注意观察屏幕上的提示。

（1）不激活源主机和目标主机测试 IPSec。在不激活源、目标主机上执行 Ping 命令时会发现相互能 Ping 通。

（2）只激活一方主机的 IPSec。首先在源主机新建的 IP 安全策略上单击鼠标右键，并选择"指派"，激活该 IP 安全策略。其次在源主机上执行"Ping 目标主机的 IP 地址 -t"，屏幕上显示"Negotiating IP Security"信息，说明从激活的主机发送数据包时寻求协商安全。最后在未激活 IP 安全策略的目标主机上 Ping 源主机时，并不能 Ping 不通。

（3）同时激活双方主机上的 IPSec。首先在已激活的源主机上执行命令"Ping 目标主机的 IP 地址 -t"，其次在目标主机新建立的 IP 安全策略上单击鼠标右键，并选择"指派"，激活目标主机上的 IP 安全策略，最后执行带参数 t 的 Ping 命令。密切观察屏幕提示"Negotiating IP Security"，发现源主机和目标主机间保持持续的安全协商过程。

4 结束语

本文虽然只介绍了 LAN 中两台计算机间应用 IPsec 的方法，但是该协议也可应用于 Intranet 及 Internet 上，为计算机或网关之间提供安全通信。

参考文献

1 Kent, S., "IP Encapsulating Security Payload (ESP)", draft - ietf - ipsec - esp - v3 - 09 (work in progress), October 2004.

2 Kent, S., "IP Authentication Header", draft - ietf - ipsec - rfc2402bis - 08 (work in progress), October 2004.

3 Aboba, B. and W. Dixon, "IPsec - Network Address Translation Compatibility Requirements", RFC 3715, March 2004.

4 [美] Doraswamy N, Harkins D. IPSec 新一代因特网安全标准，机械工业出版社，2000。