IPSec 网络安全与实现*

赵雪梅
(盐城工学院 教务处,江苏 盐城　224003)

摘　要:随着网络应用的普及,网络安全问题更加突出,已受到人们的普遍重视。着重对 IPSec 技术以及安全套接层(SSL)、数据链路层加密等网络安全技术进行了研究,并给出 IPSec 在 Windows 2000 和 Cisco 中的实现方法。

关键词:IPSec;Windows 2000;Cisco;SSL;网络安全
中图分类号:TP393.08　　**文献标识码**:A　　**文章编号**:1671 - 5322(2002)03 - 0025 - 04

随着计算机信息技术的飞速发展,网络技术已经成为社会发展的支柱。各个行业尤其是政府部门、教育机构、商业组织、金融部门和军事部门等通过网络将分散在不同地域的组织联系在一起。

计算机网络之间互联可以通过专用线路和 Internet 等连接。通过专用线路连接的网络系统构成了一个物理专用网,采用从物理上隔离来防止外来的入侵。一般银行和军事部门都采用此种网络,但成本较高,需要投入大量的人力、财力和物力,一般企业都难以承受。因此,对于一般的企事业来说,Internet 是网络互联的首选。Internet 是个开放式的网络,给用户的接入和网络的拓展带来了很多方便,但同时网络安全也受到严重威胁。为此,对安全性要求高的数据传输往往采用访问控制、数据鉴别和数据加密等技术来保证通信的安全。

1　当前安全技术

1.1　安全套接层协议(SSL)

SSL 安全套接层协议,是一个用来保证安全传输文件的协议。这种由 Netscape 公司开发的协议是通过在浏览器软件(比如 Internet Explorer、Netscape Navigator)和 WWW 服务器间建立一条安全通道,从而实现文件在 Internet 中传输保密。起初 SSL 只是用作 http 超文本协议的数据加密。现在 SSL 在许多通信软件中也有广泛应用。但是 SSL 只能保护每个安装 SSL 软件的应用程序发送的数据,而对其它的数据传送则不提供加密。因此要对所有数据加密,则需要对每个系统和应用程序都安装 SSL。

1.2　数据链路加密

数据链路层加密是美国国防部等美国国家机构多年来采用的一种加密方式。数据链路层加密,即将数据在线路传输前后分别对其进行加密和解密,这样可以减少在传输线路上被窃听的危险,但付出的代价是使网络运行和传输速度变慢。它的每条通信链路都必须采用一对加密设备,即链路的每端各配备一台。虽然这种方式能够提供高效的安全保护,但却非常难于实现和管理。对于目前日益庞大复杂的 Internet,可能根本就无法工作。

1.3　IP 安全协议(IPSec)

IPSec 为 IP 安全协议,用以保证 IP 网上私有通信的安全。IPSec 提供了 IP 网上的数据完整、可靠性和保密性(加密)。IPSec 为 IPV4 和 IPV6 提供可操作性。对于 IPV4 来说,IPSec 是可选择的。对于 IPV6 来说,IPSec 是必备功能。随着网络安全越来越被重视,IPSec 比 IPV6 推广应用更快。因为现在的各种操作系统都相继支持 IPSec。IPSec 已在 Windows2000、FreeBSD、Linux、Solaris、HP-UX、IBM、AIX 等几乎所有商业操作系统中实

* 收稿日期:2002 - 06 - 17
作者简介:赵雪梅(1975-),女,江苏盐城市人,盐城工学院助教。

现。另外 IPSec 还在一些网络专用设备 Cisco、Lucent、Intel、3COM、Juniper 的路由器中由硬件或软件实现。IPSec 已成为网络安全全新的协议[1]。

2 IP 安全协议(IPSec)的基础原理

IPSec 协议的工作原理如图 1 所示:当 IP 通信模块收到数据包时,通过查询安全策略数据库 SPD(Security Policy Database),以决定对这个数据包的处理:丢失、IPSec 转发或 IPSec 处理,通过查询安全数据库 SAD(Security Association Database),以获取安全连接所需的参数。

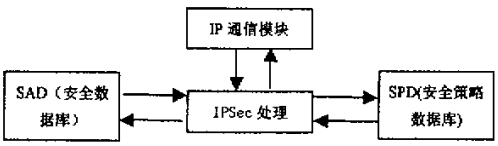

图 1 IPSec 协议的工作原理图

Fig.1 The basic principle of IPSec protocol

IPSec 协议通过鉴别头(AH)和安全负载(ESP)协议来提供 IP 层的安全服务。鉴别头(AH)模式提供了对 IP 头和 IP 包中负载的鉴别。这是通过在共享密钥值中使用带主键的哈希运算来实现的。AH 服务保护了外部 IP 头和负载。它提供对所有在传输过程中不发生改变的 IP 头区域的保护。安全负载封装(ESP)提供在 IP 层的负载加密[2]。

IPSec 有两种实现的方式:传输模式和隧道模式,如图 2 所示。

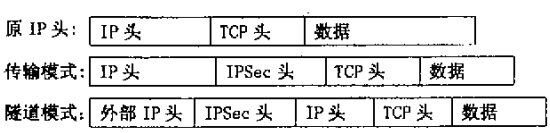

图 2 IPSec 协议的两种实现方式

Fig.2 The realization mode of IPSec protocol

在传输模式中,只有 IP 负载被加密,IP 头才保持加密。在隧道模式中,整个 IP 包被加密并成为一个新 IP 包的负载。新的 IP 头包含了它的 IPSec 的对等体的目标地址。IP 包的所有信息受到了保护,包括 IP 头[3]。

3 IPSec 的实现

3.1 IPSec 在 Windows 2000 中的实现

Windows 2000 操作系统是微软公司开发的网络操作系统平台,不管是 Windows 2000 Professor、Windows 2000 Server 还是 Windows 2000 Advanced Server 都能够很好的支持 IPSec 协议,而 Windows 以前的版本,如 Win98 与 WINNT 都不支持 IPSec。在 Windows 2000 的网络中局域网、广域网都可以使用 IPSec 来保证网络安全。现在随着技术的推动,Windwos 2000 平台已进入一般用户的家庭,可以通过操作系统内置的安全平台来保证整个网络通讯的安全。

3.1.1 Windows 2000 自带的 3 种安全策略

3.1.1.1 安全服务器

安全服务器是内置安全策略中要求最严格的。它要求所有的 IP 通讯都必须采取 IPSec 认证及加密通讯。不允许不受信任的客户端与之通信。

3.1.1.2 服务器(请求安全设置)

服务器(请求安全设置)是安全定义仅次于安全服务器策略的安全策略。它定义了所有的 IP 通讯,先要求计算机进行安全通讯,如果对方计算机不支持安全通讯,没有启用 IPSec 安全策略,也与这台计算机进行正常通讯。但整个通讯过程是不安全的。

3.1.1.3 客户端(只响应)

客户端(只响应)是内置策略中安全级别最低的一种。它定义只有当对方计算机与本机要求安全通讯时,才能启用此策略。如果对方计算机没有要求,则采用正常的通讯。而本机与其它机通讯时,则直接与其进行正常通讯。

3.1.2 Windows 2000 支持的 3 种身份验证方式

3.1.2.1 Kerberos v5 协议

Kerberos v5 是标准网络身份验证协议,该协议由麻省理工学院起草,旨在给计算机网络提供“身份验证”。Microsoft 发布此信息是为了使第三方能够验证 Windows 2000 安全模型,使企业客户、开发人员和业界用户都从中受益。该认证方法适用于任何运行 Kerberos v5 协议的客户机(无论该客户机是否基于 Windows)。一般作为域成员的客户机上运行 Kerberos,认证有效。

3.1.2.2 证书

证书通常是一个签名文档,标记特定对象的公开密钥,由 CA(Certificate Authority,认证机构)签发,CA 具有权威性,是一个普遍可信的第三方。CA 的主要功能:证书的颁发、更新、查询、作废和归档等。当通信双方都信任同一个 CA 时,两者就可以得到对方的公开密钥,从而进行安全通信、签名和检验。

3.1.2.3　预置共享密钥

预置共享的密钥,是个比较简单的方法,严格用于在计算机之间建立信任的密码。就好像两个人之间通进行加密通话,首先通过预先说定的暗号进行身份验证。然后再共同导出通讯加密密钥。

以上 3 种方法都有实际的应用。Kerberos 主要是用在域成员间进行安全通讯时的身份认证。证书现在在一些大型的机构中用得比较多。而对于一般的用户来说,运用共享密钥比较方便,特别是当 2 台机通过 Internet 进行通讯时,可以通过设定密钥来保证传输的安全。

3.2　IPSec 在 Cisco 中的实现

思科(Cisco)系统公司是全球领先的互联网解决方案提供者,其设备和软件产品主要用于连接计算机网络系统。思科设备能全面支持 IPSec 技术。使用路由器来实现 IPSec,对客户端来说是完全透明的,用户端的系统平台、通讯方式都与它没有关系。

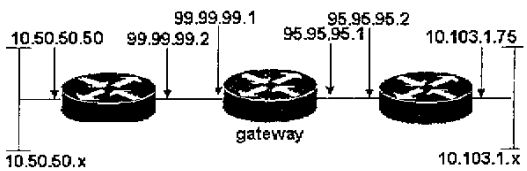

图 3　路由器 A 与路由器 B IPSec 的实现

Fig.3　Realization of IPSec between router A and router B

思科实现 IPSec 有以下 5 个步骤,我们通过图 3 的网络拓扑进行解释:

(1)创建 IKE 加密策略

IKE 用来在路由器之间创建安全联系(SA)。加密算法、哈希算法、以及验证方法、diffe-hellman 组件和生存期都是根据 IKE 策略来配置。

A 路由器配置:

```
crypto isakmp policy 1authentication pre-share
crypto isakmp key cisco123 address 95.95.95.2
```

以上 3 条命令创建 IKE 的整个过程。整个配置都是在配置模式下进行的。第 1 条命令定义一个 IKE 策略;第 2 条命令定义认证方法为 pre-share(预共享);第 3 条命令设置共享密钥,这里要注意 A、B 路由器之间定义的共享密钥必须相同,IP 地址为对等体路由器的 IP 地址。对等体路由器也就是指要与本身实现 IPSec 传输的另一台路由器。

B 路由器的配置与 A 路由器基本相同,只是对等体路由器的 IP 地址 95.95.95.2 改为 99.99.99.2

(2)定义加密的转换算法

如果 SA 创建安全联系成功,则必须定义加密转换。Cisco 所支持的加密转换有:ah-md5-hmac、ah-sha-hmac、comp-lzs、esp-3des 等。

A 路由器的配置:

```
crypto IPSec transform-set rtpset esp-des
```

其中 rtpset 是设置加密转换的名称。Esp-des 是加密算法。

B 路由器的配置与 A 相同。

(3)定义保护的流量

要实现对数据的加密,路由器必须使用 CPU 进行数据处理。这样对整个路由器的处理效率肯定有一定的影响。因此,不赞同对所有的数据包都进行加密处理。只对需要加密的数据进行加密处理。正常情况下,一般都是通过路由器的扩展访问列表来实现的。

A 路由器:access-list 115 permit ip 10.50.50.0 0.0.0.255　　10.103.1.0 0.0.0.255

通过上面这条路由器命令可以实现只对数据包从 A 网络访问 B 网络数据进行加密。当然还需要 IPSec 与访问列表相配置。

B 路由器的配置可以参考 A 路由器进行配置。

(4)定义密码映射

定义密映射也是 IPSec 设置中比较关键的一步。因为刚才定义的访问列表没有与 IPSec 相关联。必须进行定义。

A 路由器的配置:

```
crypto map rtp 1 IPSec-isakmp
set peer 95.95.95.2
set transform-set rtpset
match address 115
```

第 1 条命令定义密码映射,rtp 为映射名。第 2 个是设置对等 IPSec 服务路由器 IP 地址。第 3 条命令中 rtpset 是刚才所设置的转换算法。第 4 条命令与刚才定义的访问列表匹配。定义网络 A 到 B 网络 IP 通信进行加密。

B 路由器的配置可以参考 A 路由器的配置。

(5)将密码映射用于一个接口

在此接口能够提供 IPSec 服务前,必须将刚

才定义的密码映射设置用于此端口。A 路由器的配置：

```
crypto map rtp
```

其实 rtp 与刚才定义的密码映射名对应。B 路由器的配置可以参考 A 路由器的配置。

4 结束语

随着网络应用的普及，网络安全问题将更加突出，已得到了人们的普遍重视，许多国家的网络技术人员都在积极地探索与研究网络安全技术。作为目前比较成熟的网络安全技术的 IPSec，由于其提供了网络层 IP 的安全机制，大大加强了网络信息传输的安全性，因此越来越多的厂家生产的产品都支持 IPSec 服务。

参考文献：

[1] 桂玲. Internet 安全技术-IPSec[J]. 铁道通信信号，2000，(6)：26 – 28.
[2] 徐竹兵. IPSec 网络安全构架[J]. 应用技术，2000，(10)：33 – 36.
[3] 许进. IPSec 设计及实现[J]. 北京航空航天大学学报，2001，(8)：386 – 390.

IPSec network security and realization

ZHAO Xui-mei
(Department of Studies of Yancheng Institute of Technology，Jiangsu Yancheng 224003，China)

Abstract：With popularization of network application，the network safety problem has been getting more outstanding，and has been already set store widely by people. This paper put great emphasis on research on IPSec，ssl，data link layer encryption ，etc. And the realization methods to IPSec were given out in Windows 2000 and Cisco networks.
Keywords：IPSec；Windows 2000；Cisco；SSL；network security

(上接第 13 页)
加强。

参考文献：

[1] Richard Annderson，Chrisblexnud. ASP 3 高级编程[M]. 刘福太译. 北京：机械工业出版社，2000.
[2] 武延军，赵彬. 精通 ASP 网络编程[M]. 北京：人民邮电出版社，2000.

Application of Session Object in Elective System

HUANG Shu-rong
(Department of Computer Engineering of Yancheng Institute of Technology，Jiangsu Yancheng 224003，China)

Abstract：Active Server Pages (ASP) is an active Web development technology of Microsoft，which allows to create server-side applications that can be used by a variety of browsers. The Session is one of the most important built-in objects of ASP，which can be used by individuals. The application of session object in elective system based on relational database technology is presented in this paper.
Keywords：ASP；Session；elective system