基于 IPSec 的 VPN 技术的应用研究

王凤领
(哈尔滨德强商务学院,黑龙江 哈尔滨 150025)

摘 要:IPSec VPN 是采用 IPSec 协议来实现远程接入的 VPN 技术,极大地提高了 TCP/IP 协议的安全可靠性。文中首先对 VPN、IPSec 技术进行了介绍,分析了 IPSec VPN 的特点,对 IPSec 协议的体系结构、工作模式等进行了研究,给出了 IPSec 的具体实现步骤和方法,并通过 IPSec VPN 技术,提出了一个实现内网跨公网安全可靠传输数据的具体方案,结果证明了该技术的可行性和可靠性。总之,IPSec VPN 保证在 Internet 网络传输数据安全性的基础上,节省了大量的网络费用。

关键词:IPSec;虚拟专用网;验证头;植入安全载荷;安全联盟
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2012)09-0250-04

Study on Application of VPN Technology Based on IPSec

WANG Feng-ling
(Harbin Deqiang Business College, Harbin 150025, China)

Abstract: IPSec VPN is VPN technology which uses the IPSec protocol to realize remote access, greatly improve the safety and reliability of the TCP / IP protocol. Firstly introduced VPN, IPSec technology, analyzed the characteristics of IPSec VPN, IPSec protocol architecture, operating mode and so on, gave the IPSec steps and methods, and through the IPSec VPN technology, presented a network implementation of a safe and reliable transmission of data across a network scheme, the results demonstrate the feasibility and the reliability of the technique. In conclusion, IPSec VPN ensured the data security in Internet network transmission and save a lot of cost.

Key words: IPSec; VPN; AH; ESP; SA

0 引 言

近年来,随着 Internet 技术的迅速发展,企业和部门之间的交流也越来越频繁,当今急需解决的关键性问题是在公司内部和企业之间进行安全可靠的数据传输。实现企业外联网和公司内联网通过传统的租用线路或组建专网来完成,使得公司内部和企业之间的用户进行远程安全可靠的数据传输,但除了高昂的租用专线费用外,还会造成网络的重复建设和投资。于是,企业开始寻求投资低,安全性、可靠性高,扩展性好,易于管理的网络。

IPSec 协议在多种不同网络安全解决方案中,成为目前 VPN 技术开发中使用最广泛的一种安全协议标准就是以其包容广泛的机制和强大的安全性,是在 Internet 上通用的一种安全协议,因此,在公司和企业网络建设中得到了广泛的应用。

收稿日期:2012-01-09;**修回日期**:2012-04-13
基金项目:黑龙江省高等教育学会"十二五"教育科学研究规划课题(HGJXH B2110602)
作者简介:王凤领(1976-),男,山东金乡人,副教授,硕士,主要领域为计算机网络、数据库。

1 VPN 的概述

VPN 虚拟专用网(Virtual Private Network)是指在公用网络上建立一条临时的、安全的、稳定的隧道,利用加密、认证等多种技术通过网络安全协议,形成一个专用的虚拟链路,保证数据在网络上的安全传输[1]。

根据不同要求,可以构造不同类型的 VPN,按照网络服务类型来划分,VPN 通常可分为以下三种类型:(Intranet VPN)企业内部虚拟专用网、(Remote Access VPN)远程访问虚拟专用网和(Extranet VPN)企业扩展虚拟专用网。

企业内部虚拟专用网是公司总部与公司分部拥有一定访问权限的用户之间通过"内部网 VPN"构筑的虚拟专用网,所有端点间的数据传输都要经过加密和身份认证。

远程访问虚拟专用网也称拨号方式的 VPN,即公司员工通过本地的 Internet 服务提供商(ISP)拨号等方式构建的虚拟专用网,在公司内网和所登录的计算机之间建立了一条加密信道。

企业扩展虚拟专用网是不同公司和供应商之间通过公网构筑的虚拟专用网,它能够保证包括 TCP 和 UDP 服务在内的各种应用服务的安全,是一个由加密

算法、认证方案和访问控制功能组成的集成系统[2]。

私有信息在公网上传递最重要的就是提供数据保护的安全性,建设 VPN 经常使用的协议主要有四种类型:PPTP、L2TP、SOCKS v5、IPSec。PPTP、L2TP 被称为第二层隧道协议,是在数据链路层上实现数据封装的协议。SOCKS v5 称为上层协议,是在会话层上实现数据流控制的协议。IPSec 被称为第三层隧道协议,是在网络层上实现数据封装的协议。

2　IPSec 技术的概述

IPSec 是 IETF 制定的,它定义了在公网时实现安全传输的规范,保证 IP 数据包的完整性、私有性和真实性及采用的加密方法通过在 IP 数据包中增加字段的方式来完成。实现主机和安全网关、安全网关与安全网关或主机与主机之间的数据保护通过 AH、ESP、IKE 协议来完成。为确保建立一个安全可靠的通信隧道,IPsec 协议集合了多种安全技术。

2.1　AH 协议

AH 验证头[3](Authentication Header)能提供数据源身份认证、数据的完整性以及重放保护能力,不能提供数据加密功能,为确保被修改的数据包可以被安全检查出来,只能为 IP 数据流提供较高强度的密码认证,是一种 IPSec 的安全认证协议。AH 报头中的序列号是为了防止重放攻击而加入的;通过在待认证数据中加入一个共享密钥来实现数据源身份认证;通过由消息认证码(MD5)产生的校验来保证数据完整性。AH 既可以单独使用,也可在隧道模式下和 ESP 联用。

2.2　ESP 协议

ESP 植入安全载荷[4](Encapsulating Security Payload)为保证数据的机密可靠性,IPSec 协议是将用户数据进行加密后封装到 IP 数据包中的,作为可选项,为保证报文的完整性和真实性,用户可选择使用带有密钥的哈希算法来实现,是 IPSec 的另一种安全认证协议。只有 ESP 能提供数据加密,ESP 与 AH 都能提供数据源身份认证、数据完整性和重放保护能力。当要实现数据源身份认证、数据完整性校验和数据保密性时,必须采用 ESP 协议来封装 IP 数据包来完成。ESP 规范规定要强制实现 56 位的 DES 加密算法来保证数据通信中的互操作性,同时 ESP 几乎可以支持各种对称密钥的加密算法,与具体的加密算法间是相互独立的,加密算法缺省是 DES-CBC。

2.3　IKE

IKE 密钥管理协议[5](IPsec Key Exchange)主要是用于动态验证 IPSec 通信双方之间协商安全服务和建立安全关联,以及生成安全密钥。无论用 ESP 或是 AH 协议来封装数据包之前,必须先建立一个安全关联,安全关联可通过协议动态生成或者手工创建。

2.4　IPSec SA

SA 安全联盟(Security Association)是一个双方协定,是构成 IPSec 的基础,包括密钥、算法和协议等内容,一个 SA 由 3 个参数(IP 目的地址,SPI,安全协议标识符)唯一指定,IPSec 对数据提供安全服务通过 SA 来完成。IP 目的地址是 IPSec 协议的对方地址,可以是用户末端系统,路由器或防火墙;SPI(Security Parameter Index,安全参数索引)在每一个 IPSec 报文中都携带有该值,是用一个 32 比特数值来表示的;安全协议标识符是标识该关联是 AH 安全关联或者是 ESP 安全关联。

2.5　ISAKMP

ISAKMP(Internet Security Association and Key Management Protocol)是应用层上的协议[6],采用密钥管理协议作为管理协议的框架。ISAKMP 协议定义了通信双方的认证过程,安全联结的建立、删除和修改过程以及相应的报文格式。它不仅可管理 IPSec 协议所辖的密钥和安全联结,也适用于其他网络的安全协议。一次 ISAKMP 会话可分为两个阶段:会话双方通过协商建立一个 ISAKMP 的安全关联,用来保护自身的通信。通过基于公钥加密算法的数字签名来完成会话双方相互之间的认证。ISAKMP 定义一个认证时应遵循的报文格式,具体认证步骤是由相应的认证协议来规定;会话双方协商建立其他安全关联。IPSec 使用 Internet 密钥交换协议 IKE 来完成会话密钥的生成[7]。

3　IPSec 的应用研究

3.1　IPSec 的定义

IPSec(Internet Protocol Security)即 Intenet 安全协议,它是 IETF 于 1998 年 11 月提供 Internet 网络安全通信的规范,是提供私有信息通过公网传输的一种安全保障。IPSec 对于 IPv6 是强制性的,对于 IPv4 是可选的,由于 IPSec 是在 TCP/IP 协议的 IP 层实现的,因此可用它为 IP 及上层协议提供安全保证。IPSec 可以为 IPv6 和 IPv4 提供基于加密的互操作性强高质量的安全机制,通过使用密码学的方法来支持数据的保密和认证服务,使用户具有选择地使用,并达到所期望的一种安全服务[8]。IPSec 协议是目前 VPN 技术开发中使用最广泛的一种安全协议,它在未来将成为 IP VPN 的一个标准。

3.2　IPSec VPN 特点

IPSec VPN 技术保证了在用公网上传送内部数据的安全可靠性。目前,世界许多知名企业构建企业虚拟业务网,已经把 VPN 技术作为移动用户和远端分支连接的主要手段[9]。

IPSec VPN 的特点归纳有如下几点：

1. 灵活性。IPSec VPN 可以使公司随时安全的与全球用户传递信息。

2. 节省费用。公司不用再另外承担租用固定线路的费用。

3. 广泛性。IPSec VPN 可以连接少量或者连接众多的分支机构。

4. 强大的安全性。IPSec 提供数据的源身份认证、加密性、完整性以及抗重放能力，保证了 TCP/IP 协议的安全性。在 VPN 交换机上，通过 LDAP、RADIUS 和 SecurID 来实现授权等多种方式保证安全，也通过支持所有领先的通道协议、过滤/防火墙、数据加密来保证安全。

5. 多业务性。远程的视频业务和 IP 话音连通数据业务一起可传送到远端分支和移动用户，节省了大量的长途话费，为现代化办公提供了便利条件。

6. 冗余性。VPN 设备通过提供冗余机制来保证设备和链路的可靠性。

7. 动、静态路由。RIP 和 OSPF 协议使得 VPN 设备间像路由器一样连接和扩展，并且动态路由协议可在加密隧道中支持，适于网络规模的不断扩大，用户和路由都需要路由协议的支持使得整个网络的地址管理方便有效。

8. 通道分离性。VPN 交换机的分离通道特性为 IPSec 客户端提供了有利保障，支持本地网络、Internet、Extranet 的访问。

9. 易于管理。通过使用管理软件可以实现对远端节点的管理来完成远程配置数据。

3.3 IPSec 协议体系结构

IPSec 是一种协议套件[10]，主要包括：AH、ESP、IKE、ISAKMp/Oakley 以及转码，图 1 描述了这些组件之间的关系和交互方式。

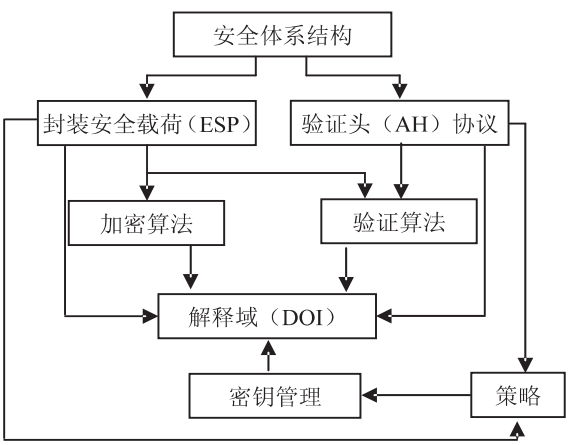

图 1 IPSec 的安全体系结构

1. IPSec 体系结构：包含需求、概念、定义和定义 IPSec 的技术机制；

2. 验证头（AH）：它包含使用 AH 进行包身份验证相关的包格式，是用于为 IP 提供数据源身份验证、数据完整性，不加密所保护的数据包；

3. 封装安全载荷（ESP）：通过将整个上层协议或 IP 分组部分封装到一个 ESP 载荷中，对载荷进行相应的安全处理，如加密等，是用于保护 IP 数据包的机密性；

4. 验证算法：描述如何用于 AH 中和 ESP 身份验证选项的各种身份验证算法；

5. 加密算法：描述如何用于 ESP 中的各种加密算法；

6. 解释域：彼此相关各部分的标识符及运作参数；

7. 密钥管理：IKE 为默认的密钥自动交换协议，用于动态建立安全关联以及交换密钥；

8. 策略：其核心由三部分组成：SAD，SA，SPD。决定两实体间能否通信以及如何通信。SAD 是进入和外出包处理维持一个活动的 SA 列表；SA 包括 SPI、应用协议、源/目的地址、所用算法/密钥/长度，表示策略实施的具体细节；SPD 决定整个 VPN 的安全需求。

3.4 IPSec 工作模式

IPSec 规范可分为传输模式和隧道模式两种，传输模式是上层协议头与 IP 头之间插入 IPSec 头；而隧道模式是外部 IP 头与内部 IP 头之间插入 IPSec 头，要保护整个 IP 包被加密封装到另一个 IP 数据包里。

1. 传输模式。

传输模式的目的是为了保护端到端的安全通信[11]。在传输模式中，所有解密、加密和协商操作均由端系统自行完成，两个需要通信的终端计算机彼此之间要直接运行 IPSec 协议，不加入任何 IPSec 过程，网络设备只执行正常的路由转发，不关心协议或此类过程。

2. 隧道模式。

隧道模式的目的是为了保护站点之间的特定或全部数据。在隧道模式中，安全网关与安全网关之间运行 IPSec 协议，所有解密、加密和协商均由安全网关来完成，安全网关对其来自端系统的数据进行保护，AH 或 ESP 头和加密用户数据被封装在一个新的 IP 包中，用户的整个 IP 包被用来计算 AH 或 ESP 头。产生数据包的系统把数据包发送到本地网关上，然后网关对其进行处理后通过 Internet 把它发送到另一个网关上，并将接到数据包对数据进行解密、校验后，再用普通的 IP 包格式将数据发送到目的终端。

4 典型应用

4.1 IPSec 实现的步骤

1. 当 VPN 设备发现数据需要被保护时，启用安全

协议 IPSec。

2. 密钥管理协议阶段 1 验证 IPSec 对等方,在该阶段中协商 IKE 安全关联,为阶段 2 中的协商 IPSec 安全关联创建一条安全的通信信道。

3. 密钥管理协议阶段 2 协商 IPSec 安全关联参数,创建的安全参数则用来保护端点之间交换的信息和数据,在对等方中创建匹配 IPSec 安全关联。

4. 数据传输发生存储在安全关联数据库中的密钥和基于 IPSec 参数的 IPSec 对等方。

5. 通过超时发生或删除安全关联终止 IPSec 隧道[12]。

4.2 基于 IPSec 的 VPN 技术的具体应用实例

基于 IPSec 的 VPN 技术的具体应用实例如下:

1. 在某 A 企业的总部放置一台 IPSec VPN 网关,各分部的局域网可用放置一台 IPSec VPN 终端设备作为代理服务器来进行上网。

2. 总部采用 10M 专线来接入 Internet,各分部可根据网络资源的实际情况采用 ADSL/2M/LAN 专线等方式实现 Internet 的接入方式。APN 硬件设备具有防火墙、路由器和数据加密的功能,为提高安全性和节约成本,不需要再装专业的防火墙等设备,比较适合于接入单位内网等场所。

3. 采用一个 B 类私有 IP 地址,统一划分 IP 地址的分配,如 172.16.X.X,每个分部分配一个 C 类的地址,如分部 192.168.2.X、总部 192.168.1.X,子网掩码均设置为 255.255.255.0。

4. 新建一台财务软件服务器、视频会议服务器、OA 服务器,各分配一个私网地址,如视频会议服务器 192.168.100.11、财务软件服务器 192.168.100.12、OA 服务器 192.168.100.10。

5. IPSec VPN 网关可以进行远程统一更新防火墙或其他设置策略,可以用来管理和查看各 VPN 终端的状况。

5 结束语

IPSec 加强了 Internet 传输数据的安全性,对 IP 数据包的安全性提供了可靠保护,降低了网络费用,为 VPN 的建立提供了有利保障。虽然 IPSec 在现今性能比较稳定,应用的相对比较广泛,但作为新的安全协议,在实际应用和理论上仍需要进一步的改进创新,相信 IPSec VPN 技术将会有更广、更好的发展前景。

参考文献:

[1] 沈俊霞. 基于 IPSec 的 VPN 的研究与实现[D]. 上海:上海交通大学,2008.

[2] 梁 军,聂瑞华. 基于 IPSec 的 VPN 技术的研究[J]. 计算机与现代化,2009(11):57-59.

[3] Kent S, Atkinson R. IP Authentication Header[S]. RFC2402 IETF,1998.

[4] Kent S, Atkinson R. IP Encapsulating Security Payload[S]. RFC2406 IETF,1998.

[5] Kent S, Atkinson R. The Internet Key Exchange[S]. RFC2409 IETF,1998.

[6] Maughan D, Schertler M, Schneider M. Internet Security Association and key Management Protocol (ISAKMP)[S]. RFC 2408, IETF,1998.

[7] 郭旭展. 基于 IPSec 的 VPN 安全技术研究[J]. 电脑知识与技术,2009(8):6652-6654.

[8] 郑 博. 基于 IPSec 的 VPN 技术及应用[J]. 数字技术与应用,2011(9):53-54.

[9] 时 晨,申普兵,杨 瑾,等. IPv6 校园网环境下 IPSec VPN 的安全性研究[J]. 计算机技术与发展,2010,20(10):167-170.

[10] 蓝集明,陈 林. 对 IPSec 中 AH 和 ESP 协议的分析与建议[J]. 计算机技术与发展,2009,19(11):15-17.

[11] 冀 强. IPSec VPN 技术研究及应用[D]. 北京:北京邮电大学,2009.

[12] 颜 凯,杨 宁,李育强,等. 思科网络技术学院教程 CCNP 2 远程接入[M]. 北京:人民邮电出版社, 2004.

基于 IPSec 的 VPN 技术的应用研究

作者：王风领
作者单位：哈尔滨德强商务学院,黑龙江 哈尔滨 150025
刊名：计算机技术与发展
英文刊名：Computer Technology and Development
年，卷(期)：2012(9)