IPSec在MPLS VPN中的应用

罗恒洋
(安徽财经大学 信息工程学院 计算机系,安徽 蚌埠 233041)

摘 要:随着MPLS技术在骨干网上的广泛使用,网络服务商向用户提供基于MPLS技术的虚拟专用网服务。基于MPLS网络的VPN服务在传输用户数据时存在一定的安全漏洞,文中分析了MPLS VPN的结构及存在的安全缺陷,提出一种方法,把IPSec应用在MPLS VPN中以加强用户数据传输的安全性。对IPSec的安全功能及应用场合进行了研究,给出在用户管理的网络边缘设备CE上配置IPSec的方法。实现了VPN用户数据分组进入骨干网之前的安全保护措施,并对IPSec分组的工作过程做了解释。

关键词:IPSec;多协议标签交换;VPN安全;数据安全
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2009)03-0168-04

Application of IPSec in MPLS VPN

LUO Heng-yang
(Department of Computer, School of Information and Engineering,
Anhui University of Finance & Economics, Bengbu 233041, China)

Abstract: As the technology of MPLS was widely used on backbone network, the Internet service providers provide the services of VPN based on MPLS for VPN users. There are a lot of security leaks in sevices of VPN based on MPLS while data packets are transported in it. Analyzes the structure of MPLS VPN and security defects existing in the VPN. Proposes a method by which IPSec is applied to MPLS VPN to enhance the security of user data. Studies the security functions and application ranges of IPSec. Put forward how to config the IPSec protocol in client edge devices of user's network. Realizes the protection of VPN user's data before the data enter into the backbone network and explains the working mechanism of IPSec packet.

Key words: IPSec; MPLS; VPN security; data security

0 引 言

VPN技术是一种在公共传输网络上通过隧道技术完成专用数据信息传输的技术,随着网络技术的不断发展,VPN技术也不断发生变化。用户对互连网的链路带宽、服务分类、服务质量等要求越来越高,这种情况下推动了MPLS技术在IP骨干网上广泛地使用,MPLS技术本身对组建VPN有着独到的优势[1]。采用MPLS技术组建VPN时,与采用PPTP、L2TP、PPTP、L2F、IPSec和GRE技术相比,在服务质量、服务分类及流量工程方面前者有强大的优势。从用户的安全角度看,尽管MPLS采用严格的路由信息隔离措施,相对于传统IP数据交换有一定安全性,但MPLS VPN在路由信息交换及数据传输时仍存在被攻击的可能[2]。文中提出一种方案,采用IPSec与MPLS技术相结合的办法实现用户数据信息在VPN中更加可靠、安全地传输。

1 MPLS VPN结构及安全性分析

MPLS VPN基本结构如图1所示,图1所示的MPLS VPN主要由以下基本元素组成:

骨干网边缘路由器(PE)用于存储虚拟路由转发表(VRF),处理VPN-IPv4路由。用户网边缘路由器(CE)用于接收和分发用户网络路由。骨干网核心路由器(P)负责MPLS分组的转发。多协议扩展BGP(MP-BGP)承载携带标签的VPN-IPv4路由,在骨干网内或骨干网之间分布路由和VPN成员信息。PE-CE路由协议在PE和CE之间传递用户网络路由。标签分发协议(LDP)在PE之间建立LSP,PE路由器和P路由器都要支持。VPN是若干个用户站点的集合,站点之间通过骨干网相互连通,在PE上一个站点由一个虚拟路由转发实例(VRF)来表示,它包含了与

收稿日期:2008-06-24
基金项目:安徽省自然科学研究项目(KJ2007C302ZC)
作者简介:罗恒洋(1970-),男,山东滕州人,讲师,硕士,研究方向为计算机网络与信息安全。

一个用户站点相关的路由表、转发表、接口(子接口)、路由实例以及路由策略等。PE 上的接口(子接口)可以绑定到唯一一个 VRF 上去，这样 PE 可以根据分组进入的接口(子接口)来区分其所属的站点，一个 VRF 可以被绑定到多个接口(子接口)上。

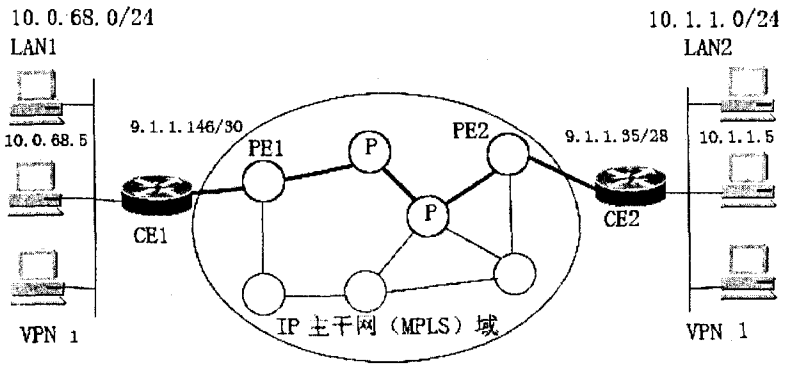

图 1　MPLS VPN 结构

通过命令行或网管工具来配置 VRF，主要的参数包括路由区分符(RD)、入路由目标、出路由目标以及接口(子接口)表等。用户接入 MPLS VPN 的方式是每个站点提供一个或多个 CE 同骨干网的 PE 连接，在 PE 上为这个站点配置 VRF，将连接 PE－CE 的接口(子接口)绑定到 VRF 上。PE 与 CE 间可通过 RIP、OSPF、BGP 协议交换路由信息，PE 间通过 BGP 协议交换路由信息[3]。由 PE 和 P 设备组成的 MPLS 骨干网是网络服务提供商管理的，为所有的 VPN 客户提供网络服务，是 VPN 客户共享的骨干网络，PE 路由器之间通过 BGP 协议交换路由信息，中间经过多个 P 路由器，容易使非法用户与 PE 路由器建立连接，获取 VPN 用户信息，导致用户 VPN 信息泄漏，因此网络服务提供商要采用安全认证机制，控制与 PE 路由器的连接请求。CE 设备属于客户网络设备，客户的 VPN 通过 CE 设备与网络服务提供商的 PE 设备连接，接入 MPLS 骨干网，CE 设备与 PE 设备通过 RIP、OSPF 或 BGP 协议交换路由和数据信息时仍面临非法用户攻击的危险[2,3]，如非法用户可以与 PE 或 CE 连接窃取 VPN 路由信息，监听 VPN 用户的数据信息。网络服务提供商管理的 MPLS 骨干网为很多用户提供网络服务，其提供的安全措施是一般的认证、数据完整性和机密性方法，不一定能够满足特定用户的 VPN 安全需要，如果用户需要加强自己 VPN 的安全性，一定要在用户管理的网络内采取安全措施。在用户管理的网络内引进 IPSec 协议实现用户 VPN 的安全性。

2　IPSec 的安全功能

IPSec 工作在 IP 层，为 IP 层及其以上层协议提供保护，IPSsec 提供访问控制、无连接的完整性、数据来源验证、防重放保护、保密性、自动密钥管理等安全服务[4,5]。IPSec 主要由认证头(AH)协议、封装安全载荷(ESP)协议及因特网密钥交换(IKE)协议。

AH 协议为 IP 分组提供无连接的数据完整性和数据源身份认证，同时具有防重放攻击的能力。数据完整性校验通过消息认证码产生的校验值来保证；数据源身份认证通过在待认证的数据中加入一个共享密钥来实现；AH 报头中的序列号可以防止重放攻击。

ESP 为 IP 分组提供数据的保密性、无连接的数据完整性、数据源身份认证以及防重放保护，与 AH 相比，数据保密性是 ESP 的新增功能，其他功能 AH 都可以实现。AH 和 ESP 可以单独使用，也可以配合使用，通过这些组合方式，可以在两台主机、两台安全网关或主机与安全网关之间配置多种灵活的安全机制。

密钥管理包括 IKE 协议和安全关联(SA)等部分，IKE 在通信系统之间建立安全关联，提供密钥确定、密钥管理的机制，是一个产生和交换密钥材料并协调 IPSec 参数的框架，IKE 将密钥的协商结果保留在 SA 中，供 AH 和 ESP 以后通信时使用。IKE 协议的主要功能是建立和维护 SA，SA 是两个通信实体经过协商建立起来的一种简单“连接”，规定用来保护数据的 IPSec 协议类型、加密算法、认证方式、加密和认证密钥、密钥的生存时间以及防重放攻击的序列号等，SA 可以手工建立，也可以使用 IKE 协议自动建立，SA 驻留在安全关联数据库 SAD 内。

IPSec 定义了用户能以多大的粒度来设定自己的安全策略，由选择符来控制粒度的大小，安全策略由安全策略数据库 SPD 维护。对于流出 IP 分组，IPSec 协议先查询 SPD，确定该数据包应使用的安全策略，如果检索到的安全策略是应用 IPSec，则再查询 SAD 来确定是否存在有效的 SA，若存在有效的 SA，则取出相应的参数，将分组封装，然后发送；若未建立 SA，则启动或触发 IKE 协商，协商成功后再对分组封装、发送，不成功则将分组丢弃，并记录出错信息；若存在 SA 但无效，则将此信息向 IKE 通告，请求协商新的 SA，协商成功后再将分组进行安全封装和发送，不成功则丢弃分组并记录出错信息。对于流入 IP 分组，IPSec 协议先查询 SAD，如得到有效的 SA，则对分组进行解封装，再查询 SPD，验证为该分组提供的安全保护是否与所配置的策略相符，如相符则将还原后的分组交给 TCP 层，或做转发；如不相符，则将分组丢弃，并记录出错信

息。

IPSec 提供的标准安全机制可保障主机之间、网络安全网关(路由器或防火墙)之间或主机与安全网关之间的 IP 分组安全,它有一套默认的、强制实施的算法,以确保不同的实施方案之间的互通。使用 IPSec 协议中的 AH 协议和 ESP 协议,可以对 IP 分组或上层协议(如 UDP 和 TCP)进行保护,这种保护由 IPSec 两种不同的工作模式来提供,即传输模式和隧道模式。传输模式为上层协议提供安全保护,保护的是 IP 分组的有效载荷或者说保护的是上层协议,如 TCP、UDP 和 ICMP。隧道模式为整个 IP 分组提供保护,隧道模式先为原始 IP 分组增加 AH 或 ESP 字段,然后再在外部增加一个新的 IP 分组头。所有原始的或内部分组通过这个隧道从 IP 网络的一端传递到另一端,沿途的路由器只检查最外面的 IP 分组头部,不检查内部原来的 IP 分组头部,这种模式适用于路由器。无论采用哪种模式,IPSec 能够为穿越边缘设备的通信提供强有力的安全保障,不会对内部网的通信及骨干网产生负面影响。

3 IPSec 分组的处理

IPSec 的实现必须使用安全策略数据库 SPD 和安全关联数据库 SAD[5]。SPD 中的策略条目表示策略,使用一个或多个选择符来指定其涵盖的 IP 数据流。每个条目都包含一个指示器,指出让与该策略匹配的数据流通过、丢弃还是进行 IPSec 处理。如果是进行 IPSec 处理,条目中将包含一个 SA(或 SA 束)说明,其中列出了要使用的 IPSec 协议、模式和算法。SAD 中的每个条目都定义了与一个 SA 相关联的参数,创建 IPSec SA 时,将使用该 SA 的所有参数更新 SAD。对于流入 IPSec 分组将使用外部 IP 报头中的目标 IP 地址、SPI 和 IPSec 安全协议作为索引,在 SAD 中查找相应的 SA 条目;对于流出 IPSec 分组,将使用 SPD 中指向 SAD 的指针来获取相应的 SA 条目。图 1 中的用户边缘路由器 CE1 和 CE2 假定是 Cisco 路由器,以 Cisco 路由器为例分析 IPSec 分组的处理及配置。CE1 的配置如下:

```
hostname ce1
!
!
ip domain - name cisco.com
!
!
crypto isakmp policy 1
authentication pre - share
crypto isakmp key cisco address 9.1.1.35
!
!
crypto IPSec transform - set test esp - 3des esp - sha - hmac
!
crypto map vpn 1 IPSec - isakmp
set peer 9.1.1.35
set transform - set test
match address 100
!
!
!
interface Serial0/0
ip address 9.1.1.146 255.255.255.252
crypto map vpn
!
interface Ethernet0/1
ip address 10.0.68.1 255.255.255.0
half - duplex
!
ip classless
ip route 0.0.0.0 0.0.0.0 9.1.1.146
!
!
access - list 100 permit ip 10.0.68.0 0.0.0.255 10.1.1.0 0.0.0.255
!
!
line con 0
line aux 0
line vty 0 4
login
!
!
end
```

路由器 CE2 的配置:

```
hostname ce2
!
!
ip cef
ip audit notify log
ip audit po max - events 100
!
cryto isakmp policy 1
authentication pre - share
crypto isakmp key cisco address 9.1.1.146
!
!
cryto IPSec transform - set test esp - 3des esp - sha - hmac
!
crypto map vpn 1 IPSec - isakmp
```

```
description CE1
set peer 9.1.1.146
set transform-set test
match address 100
!
!
controller ISA 1/1
!
!
interface FastEthernet4/0
ip address 10.1.1.1 255.255.255.0
duplex full
no cdp enable
!
interface FastEthernet5/0
ip address 9.1.1.35 255.255.255.240
duplex full
no cdp enable
crypto map vpn
!
ip classless
ip route 0.0.0.0 0.0.0.0 9.1.1.33
!
!
access list 100 permit ip 10.1.1.0 0.0.0.255 10.0.68.0 0.0.0.255
!
!
line con 0
line aux 0
line vty 0 4
login
!
!
end
```

在这个实例中，CE1 所在的 LAN(10.0.0.68/24)中的一台设备(10.0.68.5)同 CE2 所在的 LAN(10.1.1.0/24)中的设备(10.1.1.5)通信，这两台设备属于 VPN1，通信方从 CE1 到 CE2。IP 分组由 LAN1 到达 CE1，CE1 的路由选择配置判断出应将分组从串行接口 0/0 路由出去，从串行接口 0/0 将分组传输出去之前，发现该接口配置了一个加密映射，要使用 IPSec 对该分组进行处理，接下来路由器 CE1 查询 SPD，看其中是否有该分组的配置策略(源地址为 10.0.68.5，目标地址为 10.1.1.5)，访问列表 100 是加密映射中配置的策略[6]，它与源地址位于网络 10.0.68.0/24 且目标地址位于网络 10.1.1.0/24 中的所有分组都匹配，这个分组与该策略匹配，对它要执行 IPSec 保护。如果分组不与该访问列表匹配，将直接发送它，不做 IPSec 处理。根据 CE1 的配置对该分组使用安全协议 ESP，用 3DES 进行加密，用 SHA-HMAC 确保数据完整性，使用隧道模式来封装分组。下一步检查是否建立了 IPSec 对等体的 IKE SA 和 IPSec SA，如果未建立对等体之间执行 IKE Phase 1 协商，以建立 IKE/ISAKMP SA，建立 IKE/ISAKMP SA 之前，CE1 中所有与策略匹配的分组被加入队列。建立 IKE/ISAKMP SA 后，在 IPSec 隧道模式下使用 ESP 报头封装原始 IP 分组，在 IPSec 封装报头中，使用源 IP 地址 9.1.1.146 和目标 IP 地址 9.1.1.35。然后将该分组交给常规 IP 转发例程进行处理，即转发到 PE1 上，识别该分组属于 VPN1，进入到 MPLS 域内在骨干网上转发。接下来，加密的 IPSec 分组到达 CE2，VPN1 中的目的用户边缘路由器，该分组中的 IPSec 报头表明，路由器 CE2 必须对其进行 IPSec 处理，使用目标地址 9.1.1.35、安全协议 ESP 和 ESP 报头中的 SPI 作为索引，在 SAD 中查找该分组的 SA，找到匹配的 SA 后，使用合适的变换对分组进行验证和解密，将分组解密后对分组执行相应的策略检查，检查正确，CE2 对分组进行常规处理，将分组交给 VPN1 的目的主机 10.1.1.5。

从上述过程中可以看出在网络服务商提供的 MPLS VPN 中，VPN 的管理由网络服务提供商管理，VPN 用户想要增强 VPN 的安全性，可以在用户管理的边缘设备 CE 上增加安全措施，确保用户数据在公用网络上的安全。

4　结束语

基于 MPLS 网络的 VPN 中，网络服务提供商向用户提供 VPN 的管理及服务，在一些应用场合，用户对其数据传输的安全性有特殊要求，如电子商务应用、金融行业的应用，单纯依靠网络服务提供商提供的网络服务存在一定的安全漏洞，用户必须在自己管理的网络范围内采取一定的安全措施，这样做虽然会增加用户管理和配置网络的复杂性，但换回的是更加安全可靠的网络服务，把 IPSec 引入用户管理的边缘设备 CE 中是一种可行的保护用户数据安全方法。

参考文献：

[1] 吴　炜，谢冬青. 一种基于隧道性能分析的 VPN 分类方法[J]. 计算技术与自动化，2005(3)：83-84.

[2] 吴英挺. MPLS VPN 安全问题探讨[J]. 现代电信科技，2005(8)：14-19.

(下转第 174 页)

端对应的字符下标分别是 $d_1 = i + \mathrm{dist}(T_i)$ 和 $d_2 = i + 1 + \mathrm{dist}(T_{i+1})$，再比较 d_1 和 d_2 的大小。如果 $d_1 < d_2$，将模式末端右移至 T_{d2} 字符处进行新一轮匹配；如果 $d_1 > d_2$，则须判断 T_{i+1} 在模式中出现的次数，若不出现或只出现一次，则直接右移 $m+1$ 个字符，若 T_{i+1} 在模式中出现多于一次，则将模式末端右移至 T_{d1} 字符处再进行下一轮匹配。用 flag 函数判断 T_{i+1} 在模式中出现的次数，定义如下：

$$\mathrm{flag}(c) = \begin{cases} 1; \text{字符 } c \text{ 在模式中只出现一次} \\ 0; \text{字符 } c \text{ 在模式中出现多于一次} \end{cases}$$

表 3 改进的 BM 算法移动过程

substringjklgsmearchalgorithm
algorithm
algorithm
algorithm

给定文本串：substringjklgmsearchalgorithm 和模式串：algorithm，分别用 BM 算法、BMH 算法和改进的 BM 算法进行匹配，匹配次数分别为 5 次、4 次、3 次，一次最大的移动量分别为 m、m、$m+1$ 个字符，可见该改进算法从匹配次数和最大移动量都取得了优势。匹配次数的多少和一次最大移动量以及最大移动量产生的概率有关，BM 算法产生最大位移量的情况是和模式串末端对齐的文本字符不在模式中，BMH 算法产生最大位移量的情况是和模式串末端对齐的文本字符不在模式中或该字符仅出现在模式末端，文中改进的 BM 算法产生最大位移量的情况是下一位字符不在模式串中或该字符在模式串中惟一且失配字符决定的移动量比该字符决定的移动量大两种情况，所以该算法产生最大位移量的概率比 BM 算法和 BMH 算法都要大。表 3 的移动过程也说明了这一点，在三次匹配中都实现了最大位移，极大提高了匹配效率。

3 实验结果

BM 算法的预处理阶段的空间复杂度是 $O(m+\sigma)$，σ 是与文本和模式相关的有限字符集的长度，查找阶段的最坏时间复杂度为 $O(mn)$，而其平均时间复杂度是亚线性的，最好情况下的性能是 $O(n/m)$[3]。BMH 算法的时间复杂度为 $O(n/m)$，改进算法的时间复杂度为 $O(n/m+1)$，可见比 BMH 算法的时间复杂度略优。选取 10M 的英文字母做文本，选取长度为 5、8、10、20、30 的英文字符串为模式串，分别用 BM、BMH 和改进算法进行匹配，结果见图 3，可见改进算法在匹配时间上优于原 BM 算法。

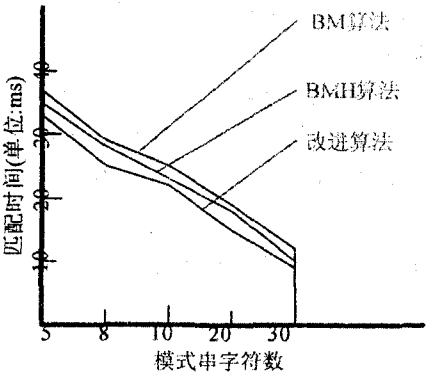

图 3 BM、BMH、改进算法比较

4 结束语

网络新应用的不断出现以及网络带宽的不断增加，使得目前的网络入侵检测系统的处理性能开始不能适应大流量网络环境的要求，这就迫切需要提高 IDS 的处理性能[6]。

文中对模式匹配算法 BH 和 BMH 作了简要的分析，并提出了一种改进算法，从理论分析和实验结果看，该算法减少了匹配次数，缩短了匹配时间，将其应用到入侵检测系统的检测引擎中，可以提高系统检测效率，改善系统性能。

参考文献：

[1] 彭 波. 数据结构[M]. 北京：清华大学出版社，2004.
[2] 傅清祥，黄晓东. 算法与数据结构[M]. 北京：电子工业出版社，2001.
[3] Boyer R S, Moore J S. A fast string searching algorithm[J]. Communications of the ACM, 1977, 20(10): 762－772.
[4] Navarro G, Raffinot M. 柔性字符串匹配[M]. 北京：电子工业出版社，2007: 19－23.
[5] Daniel M S. A very fast substring search algorithm[J]. Communications of the ACM, 1990, 33(8): 132－142.
[6] 伊 静，刘培玉. 入侵检测中模式匹配算法的研究[J]. 计算机应用与软件，2005, 22(1): 112－114.

(上接第 171 页)

[3] 何宝宏. IP 虚拟专用网技术[M]. 北京：人民邮电出版社，2002.
[4] 徐家臻，陈莘萌. 基于 IPSec 与基于 SSL 的 VPN 的比较与分析[J]. 计算机工程与设计，2004(4): 586－587.
[5] Bollapragada V, Khalid M, Wainner S. IPSec VPN 设计[M]. 袁国忠译. 北京：人民邮电出版社，2006.
[6] Metz C Y. IP 交换技术协议与体系结构[M]. 吴 靖等译. 北京：机械工业出版社，1999.