高速边缘路由器中 IPSec 安全引擎实现技术分析

Analysis of Realization of IPSec Security Engine in High Speed Boundary Routers

荣　霓　　荣京东
Rong Ni　　Rong Jingdong

（国防科技大学计算机学院网络所　湖南长沙　410073）
（School of Computer, NUDT, Changsha, Hunan, 410073）

（桂林陆军学院计算中心　桂林　541002）
（Computing Center, Guilin Military Academy, Guilin, 541002）

摘要　在分析高速边缘路由器的功能和 IPSec 协议本身结构的前提下，给出了通用的 IPSec 处理框架，对目前各种基于路由器的 IPSec 实现方式进行了详细的分析，并对今后的技术发展进行了展望。

关键词　高速边缘路由器　IPSec 协议　安全引擎
中图法分类号　TP393.03　A

Abstract　The common processing framework is explained in terms of analysis of the function of high speed boundary routers (HSBR) and the structure of IPSec protocols. The running of current routers based on IPSec are analyzed. The development of IPSec-in-HSBR is outlooked.

Key words　high speed boundary router, IPSec, security engine

高速边缘路由器是指位于 Intranet 和 Internet 之间，担负路由和安全防护的高速路由器。其线速一般可以达到 G bit 级，加密报文占报文总量的 30%甚至更多，安全连接达到几万个以上。路由器作为网络传输过程中的重要设备，对报文安全、正确和快速的转发起着关键性的作用。一方面，网络速度的不断提升直接要求位于网络边缘的路由器具有更高的处理速度；另一方面，安全问题的日趋严重也对边缘路由器的安全性支持提出了更高要求。IPSec 是 IETF 提出的协议级安全框架，它为网络安全问题的解决提供了一个发展方向，成为了网络安全技术领域研究的热点问题。目前，除了各个权威组织对协议标准本身的制定和不断完善外，大量的厂商也投入到以 IPSec 协议为安全引擎的网络设备研制中。由于协议族中的 AH 和 ESP 协议是 IPv6 中安全相关的组成部分，所以，研究 IPSec 的实现，在技术发展上就保证了与下一代网络标准的兼容。随着 IPSec 协议的不断完善发展以及 IPv6 的广泛使用，在边缘路由器上不提供

2002-06-27 收稿。

对 IPSec 的支持将是不可想象的。

1 高速边缘路由器功能

路由器的功能分成两类[1]，一类是数据路径功能，它是一种实时任务，应用于每个到达路由器的分组。主要包括转发决定、通过背板转发和输出链路调度等。另一类是控制功能，为非实时任务，主要包括系统配置、管理和路由表信息的更新，不应用于每个到达路由器的分组，因此与数据路径功能相比其执行是相对不频繁的。设计高速边缘路由器的一个目标是增加分组被路由的速率(特别是使用了 IPSec 加密的报文被路由的速率)，因此急需改进数据路径功能以提高性能。同时，IPSec 处理的引入使得控制功能的改进也需兼顾，包括 IPSec 安全引擎的设置(使用的加密算法、公共密钥生存周期等)以及与其他协议的互操作性处理，如 NAT 等。但主要还是数据路径功能的全面提升。Tom Riordan 将数据路径功能的大部分划分到数据平面内[2]，而把其余的和控制功能一起划分到控制平面中。按照它的分类，数据平面和控制平面的功能被清晰和有序的分隔且更加灵活。

2 IPSec 协议

IPSec 协议是 IETF 针对互联网 TCP/IP 协议的脆弱而从协议级提供的面向安全的解决方案。IETF 于 1998 年 11 月颁布了这个基于 IP 层的安全标准，其目标是为 IP v4 和 IP v6 提供具有较强互操作能力、高质量和基于密码的安全，以及在 IP 层实现包括访问控制、无连接完整性、数据源认证、抗重播、机密性和有限的业务流机密性的多种安全服务。

2.1 协议组成

IPSec 由一系列协议组成，包括 Security Architecture for the Internet Protocol (RFC2401)[3]，IP Authentication Header (RFC2402)[4]，IP Encapsulating Security Payload (ESP) (RFC2406)[5]，Internet Security Association and Key Management Protocol (ISAKMP) (RFC2408)[6]，The Internet Key Exchange (IKE) (RFC2409)[7]等。

在组成 IPSec 的一系列协议中，主要有 3 个主要模块：认证头部(Authentication Header，AH)、封装安全负载(Encapsulating Security Payload，ESP)和密钥交换(Internet Key Exchange)。其简单结构图如图 1：

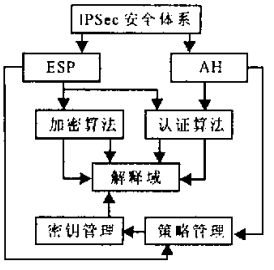

图 1 IPSec 体系结构

2.2 基本处理流程

IPSec 的基本处理思想是通讯双方通过 IKE 协议在不安全的网络上协商密钥和进行认证，然后使用协商好的密钥建立安全联盟(SA)。通过 SA 建立起通信双方的通道后，后续的报文通过 AH 和 ESP 协议进行变换(主要是加密)和封装后利用已经建立的通道进行传输。通讯期间所涉及的安全连接、密钥和认证信息等由 IPSec 协议族中的不同协议分别管理。

2.2.1 出站 IP 报文处理

第一步：选择一个 SA 或 SA 束。每个出站报文都与 SPD 相比较以决定如何处理该报文。如果报文被丢弃或者被允许绕过 IPSec 处理，则直接操作。如果要求使用 IPSec 处理，那么该报文影射到现存的某个 SA(或 SA 束)，或者为该报文建立一个新的 SA(或 SA 束)。由于一个

报文的选择符或许会匹配到多个策略或多个现存的 SA，而且 SPD 是有序的，SAD 却是无序的，所以必须执行特定的算法加以处理。

第二步：建立隧道模式的头。外部 IP 报头的源地址和目的地址定义了隧道的端点（封装者和解封装者），内部报头的源地址和目的地址则分别定义了数据的最初发送者和最终接受者。在隧道内传输时，内部 IP 报头一般不会改变，除非为了缩减 TTL。封装的数据报在通过隧道时，内部报头的 IP 可选项或扩展报头也不会改变。其他协议报头比如 IP 认证报头在需要时可能插在外部和内部的 IP 报头之间。在建立隧道时，须按具体的方法对不同的头/选项域加以处理。

2.2.2　入站 IP 报文处理

在处理 AH 或 ESP 之前，先将 IP 分段报文重组起来，每个将进行 IPSec 处理的入站 IP 报文都由 IP 下一协议域标识出 AH 或 ESP 的值。

第一步：选择 SA 或 SA 束。由于在 AH 或 ESP 头中有 SPI，使得将 IP 报文映射到合适的 SA 被简化。对选择符的检验将在内部报头而不是外部报头的基础上进行。步骤如下：

利用报文的目的地址（外部 IP 头）、IPSec 协议和 SPI 在 SPD 中来查询 SA。

使用上一步中找到的 SA 来进行 IPSec 的认证和加密处理。

在 SPD 中寻找一个匹配该报文的入站策略，可以通过 SA 到 SPD 的回调指针来完成，也可以通过报文选择符与 SPD 的策略相匹配来进行。

检测所要求的 IPSec 处理是否已经进行。

上述步骤结束后，将结果报文传递给传输层或转发报文。这些步骤中的任何 IPSec 头都可能被改变，但是已使用了的 SA 及其使用的顺序等信息可能会在接下来的 IPSec 或防火墙处理中需要。

第二步：处理 AH 和 ESP 隧道。内部和外部 IP 报头、扩展头、AH 和 ESP 的可选项的执行和前面出站报文的一样。

3　路由器实现 IPSec 的现状分析

3.1　通用实施结构分析

目前的一般实施方案都把以下模块作单独定义：

协议引擎模块：该模块主要处理 AH 和 ESP 协议。其主要功能包括处理相关报头、与策略和 SA 管理模块交互以确定安全策略的使用，以及解决关于报文分段和 PMTU 等问题。

策略和 SA 管理模块：直接控制 SAD 和 SPD 的模块，其功能包括策略的表示、修改，对密码算法的调用，以及一些通用设置操作。它对 SA 的管理主要是非 IKE 功能的操作，如生存时间等方面的管理。

SPD 模块：SPD 保存着对报文分组所应该实施的安全策略，工作中报文分组都需要通过对 SPD 的查询以决定其对应的处理。对于外出报文，IPSec 需要查询 SPD 以决定是否对该报文进行安全保护；而对于进入报文，IPSec 也需要查询 SPD 以判断该报文已经受到的安全保护是否与策略配置的相符。

SAD 模块：SAD 保存着活动的 SA 列表，表中的每一项都对应着一个 SA 的连接。所有的 SA 通过 IKE 协议生成，并有着相应的生存时间（在此我们省略了对手工分发密钥 MKM 的描述，毕竟在 HSBR 上使用手工分发密钥不应该被强调）。

IKE 模块:IKE 是一个存在于嵌入式路由器操作系统映象空间的进程,一般在系统自举时被引导,然后就处于休眠状态直至被激活。IKE 通过与策略和 SA 管理模块的合作,管理 SA 的建立和重新建立。

密码算法模块:作为各模块使用的密码算法的管理和实现模块,一般应采用硬件实现以加快处理速度。

通用的实施结构见图 2。

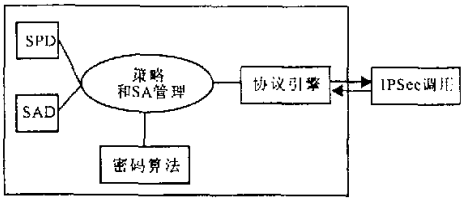

图 2 通用 IPSec 实现结构

3.2 纯软件实现结构

采用纯软件 IPSec 协议引擎和"look-aside"机制对 IPSec 报文进行处理。也就是说,当路由器系统碰到 IPSec 报文时,不再按一般 IP 报文进行处理,而是将报文传递到 IPSec 的处理模块(软件),由该模块完成 IPSec 协议的相应操作。目前一些中、低端的路由器采用这种实现方案的较多。该软件优点是可移植性好,开发简单。由于这是一种集中式的软件实现方案,其明显缺点是速度慢,开销大,无法适应高速边缘路由器的需要。

3.3 线缆中的块(BITW)实施结构

在这种实施方案中,IPSec 安全引擎被置于一个独立的设备(线卡)上,该设备直接连到路由器的物理接口上。一般来说,该设备不会运行任何的路由算法,只用来进行 IPSec 的相应处理。

对于 BITW 实现的评价,其优点是独立的设备使得 IPSec 的实现可以和路由器其他部分分开,通过在该独立设备上使用快速的加密芯片,可以提高 IPSec 报文分组的处理速度。缺点是该设备无法连接到路由器的每一个接口,各接口流入的 IPSec 报文分组都必须通过另外的总线传递到该设备上,严重影响路由器本身的处理效率。

3.4 FlowThrough 实现结构

NetOctave 公司的 FlowThrough 安全体系结构是一种比较快速的基于硬件的 IPSec 实现方式。它允许安全处理芯片直接连接到数据通路上,这样就消除了"look aside"实现方式的低效[8]。

FlowThrough 技术的评价,优点是速度快,结构简单(路由器)。由于这是一种集中式的硬件实现方式,缺点是通用性差,整个路由器的数据带宽受到 FlowThrough 芯片的限制,成为整个系统的瓶颈,扩展性差,因为所有报文全部流过 IPSec 芯片没有必要的。

3.5 基于网络处理器(NP)和 ASIC 的实现技术

使用 NP 和 ASIC 是目前路由器硬件设计中应用日趋广泛的技术。ASIC 的使用是因为虽然转发引擎结构极大地提高了效率,但由于传入快速通路的数据越来越多,对线卡上通用 CPU 的处理能力提出了更高的要求,超过了通用 CPU 的能力。这样,线卡上的通用 CPU 就被更加高速、功能固定的 ASIC 所取代。通过采用高速、专用 ASIC,大大减少了 CPU 的负担,这样,大部分 IP 报文就可以使用快速通路通过系统,而只有控制包和异常包需经慢速通路转发至 CPU。但采用固定的 ASIC,在提高效率的同时,付出的代价是降低通用 CPU 固有的可编程能力,于是网络处理器(NP)应运而生。它既可用于线卡的快速通路中,类似于固定功能 ASIC;又具有较好的可编程能力,类似于通用 CPU 的功能。NP 的特点使它被越来越广泛地被使用

于高速路由器的设计中[9]。不同的 NP 具有不同的处理速度和可编程性。其基本功能是以线速转发数据包。NP 将根据用户编程规则对输入的数据包进行封装，并根据用户编制的算法校正输入的数据，然后，对数据包进行处理，根据相关协议规则转发数据包，并提供给用户相应的统计结果，以便用户跟踪分析快速通路的流量。

高速路由器一般采用分布方式实现数据通路的功能。在高速路由器中，CPU 只负责控制通路处理，将中低端路由器中用 CPU 实现的数据通路功能转移到各网络接口卡上或功能部件上。高端路由器接口逻辑上由网络处理器和网络接口组成。网络处理器可以采用商用网络处理器或者专门设计的网络处理器。具体实现中物理上采用两种形式，一种是网络处理器与接口分离，代表产品有 Cisco 12008 系列，特点是转发性能可以根据需要配置；另一种是一对一地集成，代表产品如银河玉衡 9108 核心路由器，特点是转发性能随接口数量自动增加。我们的高速边缘路由器的结构主要基于后一种形式。目前我们正在进行以 NP 为基础，采用 ASIC 设计的 IPSec 安全引擎的体系结构的研究和设计，集成了 NP 和 IPSec 安全引擎的 SE-1 产品就是其研发的成果。

4　总结和展望

IPSec 的高速边缘路由器实现是一个在理论和工程上都有较大意义的领域。本文对目前的多种实现机制和对以网络处理器为基础集成 ASIC 专用芯片的实现形式进行了比较详细的分析。目前，网络技术的发展速度很快，许多 Switch Fabric 的制造商已经在其产品中采用了一种称为 SERDES 的接口来连接位于线卡上的 TM 单元和交换板上的 Crossbar。SERDES 接口是一种类似 SDH 标准的接口，在其数据帧中分开销和净荷两部分，其中开销字节传输的是一些请求信息或流控信息。在交换板上，各输入端口的同步通过 SERDES 数据帧中传递的同步时钟来保证。SERDES 接口虽然现在还没有被 NP 论坛接受为一种通用的接口标准，但它的出现为以后实现线卡与交换单元的光连接打下了基础。随着当前一代的网络处理器和现有的微处理器之间的不断融合，以及大量专用的 ASIC 的出现，高速边缘路由器将向着超标量、超流水的方向发展，可以提供更快的报文处理速度和更丰富的功能。

参考文献

1　彭元喜．高速 IP 分组分类算法和实现技术的研究(博士论文)．清华大学，2002．3．
2　Tom Riordan．网络用处理能力：网络应用之微处理器的演变．EDN China，2002．2．
3　Security Architecture for the Internet Protocol(RFC2401)．
4　IP Authentication Header(RFC2402)．
5　IP Encapsulating Security Payload (ESP) (RFC2406)．
6　Internet Security Association and Key Management Protocol (ISAKMP) (RFC2408)．
7　The Internet Key Exchange (IKE) (RFC2409)．
8　NetOctave NSP4200 Security Processor，NetOctave 公司，2001．
9　苏金树．超高性能路由器．中兴通讯技术，2001．8．

(责任编辑：蒋汉明)