计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
43(3):375~380, 2006

IPSec 和 IP Filter 在路由器中部署策略的研究

王 利 徐明伟 徐 恪
(清华大学计算机科学与技术系 北京 100084)
(wangli@csnet1.cs.tsinghua.edu.cn)

On the Deployment Approach of IPSec and IP Filter in Routers

Wang Li, Xu Mingwei, and Xu Ke
(*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084)

Abstract IPSec and IP Filter are among the most important security modules of IPv6 routers. Similar to the function of IP Filter, the security-association query engine of IPSec also needs filtering and matching the IP packages. The IP packages flowing inside the router could be filtered by IP Filter and IPSec for more than once. Thus, the method of deployment between the two modules will have direct influence on the processing performance of IP packages. In this work, the inter-relationship between the two security modules is given in a perspective of router global security. Moreover, a novel deployment approach is proposed. Compared with the open-source IPv6 protocol stack KAME, the improved processing performance of IPSec is obtained and the negative influence of IP Filter on the IPSec is reduced. Meanwhile, the duplicated IP package filtering within the routers is reduced to improve the processing performance of IP package.

Key words IPSec; IP Filter; router; deployment approach

摘 要 IPSec 和 IP Filter 是 IPv6 路由器中的重要安全部件. IPSec 的安全关联查找引擎具有类似于 IP Filter 的功能,也需要对 IP 包进行过滤和匹配,路由器中流动的 IP 包可能需要经过这两个部件的重复过滤,因此,这两个部件之间的部署策略将会直接影响到 IP 包的处理效率. 从路由器整体安全的角度分析了两个安全部件之间的相互关系,提出了一个新的部署策略. 与国际上著名的开放源码 IPv6 协议栈 KAME 相比较,该部署策略可以提高 IPSec 的处理效率,减轻 IP Filter 对 IPSec 的负面影响,同时,也减少了 IP 包在路由器中的重复过滤,提高了 IP 包的处理效率.

关键词 IPSec;IP Filter;路由器;部署策略
中图法分类号 TP393.08

1 引 言

目前,IPv6 路由器中主要存在两个安全部件:IP Filter 和 IPSec. IP Filter 是路由器中普遍使用的安全部件,它对 IP 包进行准入和准出控制,它由一系列有序的动作——"允许"或"拒绝"——的过滤规则组成,这些规则是基于 IP 包的五元组设置的.

IPSec 是 IETF 制定的一个安全机制,它为 IP 及上层协议提供安全保证[1~3]. IPSec 的处理过程中涉及到一个关键环节,那就是安全关联 SA 的查找[1],本文称之为 SA 查找引擎. 其中,输出 SA 查找引擎类似于 IP Filter,也需要基于 IP 包的五元组对一系列有序的规则(策略选择符)进行过滤和匹配.

IP Filter 和 IPSec 就是位于路由器 IP 通路上的两个 IP 处理部件,所谓"IP 通路",就是指 IP 包在路由器中的流动路径,这样,IP 通路上流动的 IP 包就可能需要经过这两个部件的重复过滤. 我们研究这两个部件在路由器中的部署策略,实际上就是研究这两个部件在 IP 通路上的相对部署位置与相互

收稿日期:2004-11-30 修回日期:2005-05-30
基金项目:国家自然科学基金项目(90104002,60373010);国家"九七三"重点基础研究发展规划基金项目(2003CB314801)

关系,目的就是研究如何实现更佳的部署策略,以实现 IP 包更高效的处理效率,本文不涉及这两个部件的内部具体实现.

2 相关工作

KAME 是国际上一个著名的基于 BSD 系 Unix 操作系统的开放源码的 IPv6 协议栈开发项目[4,5]. KAME 的 IPv6/IPSec 协议栈已被多个公司所采用(如:Juniper,Hitachi 和 Fujitsu 等)[5]. 通过观察 KAME 的开放源码和阅读相关文档,我们知道,在 KAME 的实现中,IPSec 和 IP Filter 在路由器中的部署如图 1 所示:

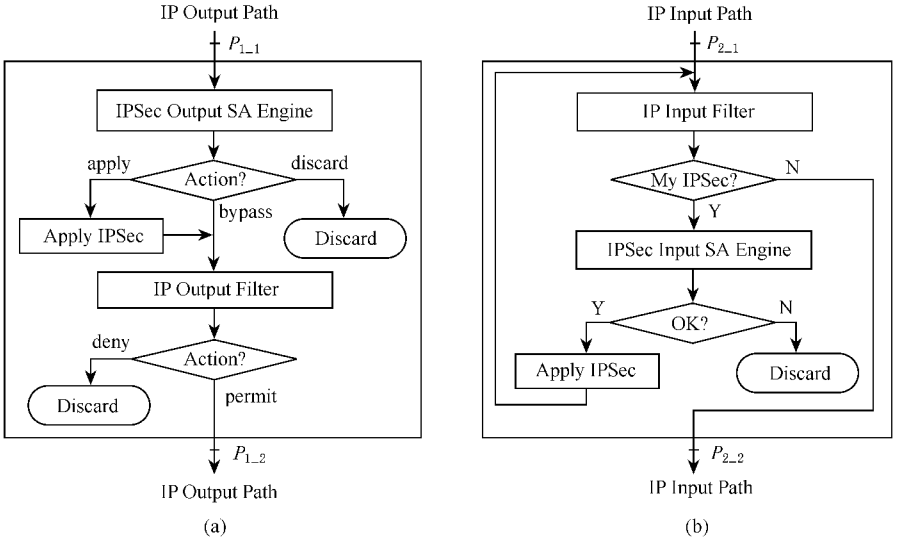

Fig. 1 The deployment approach of KAME. (a) The deployment approach on the IP output path and (b) The deployment approach on the IP input path.

图 1 KAME 方案中的部署策略. (a)IP 输出路径上的部署策略;(b) IP 输入路径上的部署策略

如图 1(a)所示,IP 输出路径上两个部件的部署策略如下:

(1) IPSec 输出 SA 查找引擎部署在 IP 输出 Filter 的前面. 路由器即将输出的 IP 包均要首先经过输出 SA 查找引擎的过滤,然后,从输出 SA 查找引擎出来的所有 IP 包均需要送入 IP 输出 Filter 进行过滤.

(2) IP 输出 Filter 必须兼容 IPSec 安全策略. IP 输出 Filter 必须设置相应的规则以允许 IPSec 产生的新 IPSec 包通过路由器.

如图 1(b)所示,IP 输入路径上两个部件的部署策略如下:

(1) IP 输入 Filter 部署在 IPSec 输入 SA 查找引擎的前面. 路由器接收到的任何 IP 包均需要首先经过 IP 输入 Filter 的过滤,然后,目的地址为本机的 IPSec 包才送入 IPSec 输入 SA 查找引擎进行处理. 经过输入 SA 查找引擎匹配成功的输入 IPSec 包被剥离掉 IPSec 头以后,仍需要再送入 IP 输入 Filter 中进行过滤.

(2) IP 输入 Filter 必须兼容 IPSec 安全策略. IP 输入 Filter 必须设置相应的规则以允许目的地址为本机的 IPSec 包通过.

KAME 认为 IP 包在经过 IPSec 隧道模式的输出处理以后,新 IP 包的源和目的 IP 地址均要改变,路由器需要对该新 IP 包进行准出控制;同时,KAME 认为任何进入路由器的 IP 包均必须首先进行准入控制,而且,IPSec 还原出来的新 IP 包,也必须进行准入控制[4,5].

此外,在国际上另外一个著名的基于 Linux 内核的 IPv6 协议栈开发项目 USAGI 中,两个部件的部署策略也是与 KAME 中的相同[6,7],在此就不做介绍了.

3 本文提出的部署策略——04 方案

在介绍本文提出的部署策略以前,我们先探讨两个部件融合的部署策略是否可行.

3.1 两个部件融合的部署策略是否可行

如果对 IP Filter 进行改进,使每条规则的动作由"允许"和"拒绝",改为"允许并使用 IPSec"、"允许并绕过 IPSec"和"拒绝",那么,就能实现两个部件的融合. 将两者融合的部署策略在理论上是一个

不错的方案,但是,本文认为在路由器的实际配置、管理和维护中,两者的融合并不是一个可行的方法,原因如下:

(1) 两者是两个解决不同安全问题的安全部件. IP Filter 解决的是"IP 包能否通过的问题",而 IPSec 解决的不仅是"IP 包是否需要进行安全保护"的问题,而且还解决"使用什么安全策略进行安全保护"的问题. 例如:两个顺序相邻的"允许"规则 R1 和 R2,当把它们作为 IP Filter 的规则时,其先后顺序对 IP Filter 没有影响;但是,当作为 IPSec 选择符时,其先后顺序对 IPSec 的结果就可能有影响,因为 IPSec 可能要求匹配 R1 的 IP 包使用策略 SP1 进行安全保护,匹配 R2 的 IP 包使用策略 SP2 进行安全保护.

(2) 两者是两个不同安全等级的安全部件,它们的配置需要不同的安全知识. IP Filter 是路由器中最基本的安全部件,而 IPSec 是目前路由器中所支持的最高等级的安全部件,它的配置需要更多的安全知识.

(3) IPSec 功能的加载和卸载对 IP Filter 的影响. 当两者融合到一体后,若需要卸载 IPSec,那些动作为"允许并使用 IPSec"的规则不能简单地进行删除,而是应该转换为"允许并绕过 IPSec"的规则,这样,就可能产生许多冗余的规则. 若需要加载 IPSec 时,新配置的"允许并使用 IPSec"的规则就需要添加到一有序序列的规则中的适当位置,而不能简单的添加到最后,这样,就增加了规则配置和维护的难度.

(4) IPSec 的配置需要考虑对端安全网关的情况. IPSec 策略选择符的配置一方面需要考虑本端的情况,另一方面还需要考虑对端安全网关策略选择符的配置情况. 因为 IPSec 要求两个安全网关上配置的策略选择符应该尽可能形成"镜像"关系[8~11],这样,才能使密钥交换协议 IKEv1 的协商成功率更高,并为尽可能多的 IP 流提供安全保护.

3.2　方案的指导原则

本文提出了一个新的概念——路由器整体安全.无论路由器内部具有怎样的安全部件,以及安全部件的数量和关系如何,对于路由器外部的网络而言,这些部件表现出来的安全功能必须是作为一个和谐、统一的整体而存在的,并作为一个安全整体为网络提供安全保护的,这些安全部件不应表现出相互矛盾的安全功能.

基于路由器整体安全的概念,我们提出了如下的指导原则:

(1) 高安全等级原则. 本文认为 IPSec 比 IP Filter 具有更高的安全等级,或者说 IPSec 是目前路由器中所支持的最高等级的安全功能. 它的高安全等级就体现在它是对合法和可信任的 IP 包提供安全保证,因为 IPSec 要保护的 IP 包必须匹配 IPSec 的安全策略[1]. 因此,低安全等级的 IP Filter 应该且必须兼容于高安全等级的 IPSec 的安全策略,它不应该阻断高安全等级的 IPSec 的工作.

(2) 策略一致性原则. 本文认为 IPSec 的安全策略和 IP Filter 的安全意图在本质上是和谐的、一致的,这是由路由器的整体安全所决定的. 本文认为不存在必须使用 IP Filter 对 IPSec 进行阻断的情况,否则,就可能存在路由器花费了宝贵的计算资源对 IP 包进行加密或解密处理后的新 IP 包被 IP Filter 阻断的矛盾情况,若存在该现象,本文就认为 IP Filter 的安全意图违背了路由器的整体安全.

3.3　04 方案

本文提出了一种新的部署策略,我们称之为 04 方案,如图 2 所示.

如图 2(a)所示,IP 输出路径上两个部件的部署策略如下:

(1) IPSec 输出 SA 查找引擎部署在 IP 输出 Filter 的前面. 路由器即将输出的 IP 包均首先经过 IPSec 输出 SA 查找引擎的过滤,然后,只有 IPSec 不需要处理的 IP 包才需要送入 IP 输出 Filter 进行过滤,IPSec 处理以后的新 IP 包不需要经过 IP 输出 Filter 的处理.

(2) IP 输出 Filter 的规则不需要兼顾 IPSec 安全策略.

我们之所以在 IP 输出路径上采用这样的部署策略,原因除了上述两个原则以外,我们还认为:

(1) 经过 IPSec 输出处理后产生的新 IP 包,其源和目的 IP 地址由 SA 指定. 而 SA 是可信任的,它即可手工配置,也可通过 IKE 协议协商产生;因此,对该新 IP 包进行准出控制没有必要.

(2) IP 输出 Filter 对本路由器产生的 IP 包(如:OSPF 路由协议包)不需要进行准出控制,但是,此类 IP 包却仍然需要进行 IPSec 输出 SA 查找引擎的处理,因为路由器可能需要对这些 IP 包进行安全保护. 这样,将输出 SA 查找引擎部署在 IP 输出 Filter 的前面,有利于对本路由器自身产生的 IP 包的安全保护.

如图 2(b)所示,IP 输入路径上两个部件的部署策略如下:

(1) IP 输入 SA 查找引擎与 IP 输入 Filter 并列部署. 路由器接收到的任何 IP 包首先判断它是否为"目的地址是本机的 IPSec 包",若不是,就将它送到 IP 输入 Filter 进行处理;若是,就送到 IPSec 输入 SA 查找引擎进行处理.

(2) IP 输入 Filter 的规则不需要兼顾 IPSec 安全策略.

我们之所以在 IP 输入路径上采用这样的部署策略,原因除了上述两个原则以外,我们还认为:

(1) IPSec 输入 SA 查找引擎对输入 IPSec 包的匹配就已经完全具备了 IP 输入 Filter 的功能,而且还具备重传检测(可选)和完整性检查功能. 输入 SA 查找引擎是根据 IPSec 包的"目的 IP 地址、协议号和安全参数索引 SPI"进行 SA 查找的,若查找失败,就将 IPSec 包丢弃;若成功,IPSec 还需要进行源 IP 地址检测、重传检测(可选)和完整性检查.

(2) IPSec 输入安全处理后还原出来的新 IP 包也没有必要再送入 IP 输入 Filter 中进行准入控制. 因为,IPSec 已经对该包按照安全策略进行了策略验证.

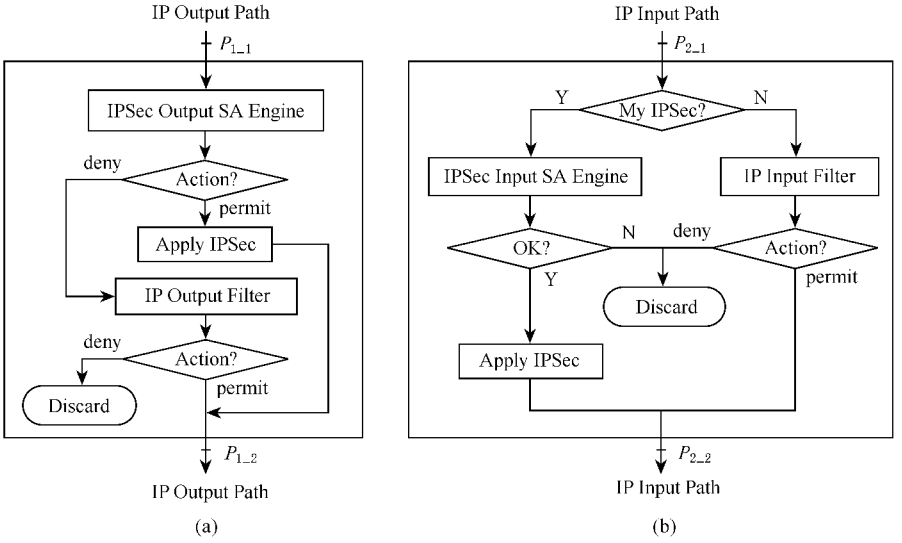

Fig. 2 The deployment approach of 04 Solution. (a) The deployment approach on the IP output path and (b) The deployment approach on the IP input path.

图 2 04 方案中的部署策略. (a) IP 输出路径上的部署策略;(b) IP 输入路径上的部署策略

4 性能评价

我们设计了如图 3 所示的网络环境. 路由器 A 是一台 CPU 为 Intel Pentium 166MHz,内存为 64MB,有两块 10Mbps 网卡的计算机,它运行的是我们自己实现的路由器协议栈软件. 路由器 B 是一台 CISCO2600,它运行的 IOS 是 c2600-ik8o3s-mz.122-11.T2.bin. 我们在两个路由器之间建立起一个 ESP 加密隧道,该隧道对主机 A 和 B 之间的 PING 包使用 DES 算法进行 ESP 安全保护.

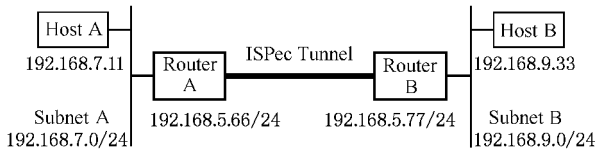

Fig. 3 The simulation network.

图 3 模拟网络环境

我们通过主机 A 向主机 B 发送大小为 1000KB 的 PING 包,如图 4 所示,我们测量 PING 包在 IP 通路上的 P_{2_1} 和 P_{1_2} 这两个测试点之间的处理延迟. 因此,处理延迟就反映了不同部署策略对 IP 包处理效率的影响.

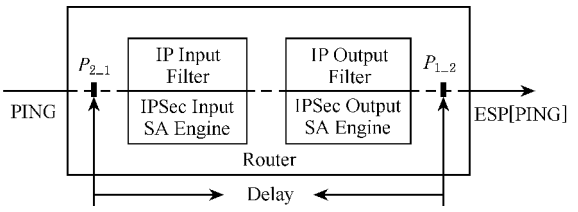

Fig. 4 The delay of the PING packets between P_{2_1} and P_{1_2}.

图 4 PING 包在两个测试点 P_{2_1} 和 P_{1_2} 之间的处理延迟

我们的测试分为两类:一类是测试"IPSec 需要进行安全保护的"IP 包的处理延迟;另一类是测试"不需要 IPSec 进行安全保护的"IP 包的处理延迟,

其方法是将主机 Host A 的 IP 地址改变为 192.168.7.22/24,这样,PING 包就不需要 IPSec 的安全保护.

图 5 显示的是部署策略对"需要 IPSec 安全保护的 IP 包"的处理延迟的影响. 由图 5(a),我们得出结论:04 方案对 IPSec 需要进行安全保护的 IP 包的处理延迟不会随着 IP Filter 数量的增加而变化,因为 04 方案中需要进行 IPSec 处理的 IP 包不需要经过 IP Filter 的处理;而 KAME 方案中的处理延迟会随着 IP Filter 数量的增加而增加. 由图 5(b),我们得出结论:两个方案对需要 IPSec 安全保护的 IP 包的处理延迟均会随着 IPSec 安全策略选择符的增加而增加,两者的处理延迟相同.

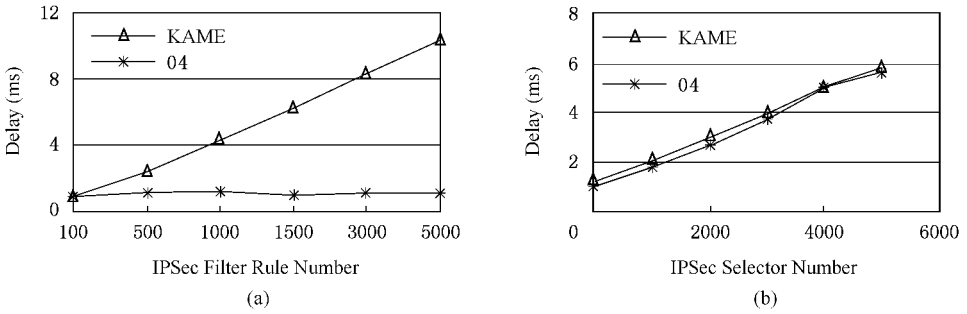

Fig. 5　The delay of the"IP packets requesting IPSec protection". (a) The influence of IP Filter rule number on the processing delay when the number of IPSec policy selector is fixed and (b) The influence of IPSec policy selector number on the processing delay when the number of IP Filter rule is fixed.

图 5　"需要 IPSec 安全保护的 IP 包"的处理延迟. (a) 当 IPSec 策略选择符数量固定时,IP Filter 规则数量对处理延迟的影响;(b) 当 IP Filter 规则数量固定时,IPSec 策略选择符数量对处理延迟的影响

图 6 显示的是部署策略对"不需要 IPSec 安全保护的 IP 包"的处理延迟的影响. 可以看出,在此情况下,两个方案对在 IP Filter 规则和 IPSec 策略选择符数量变化时的处理延迟是相同的.

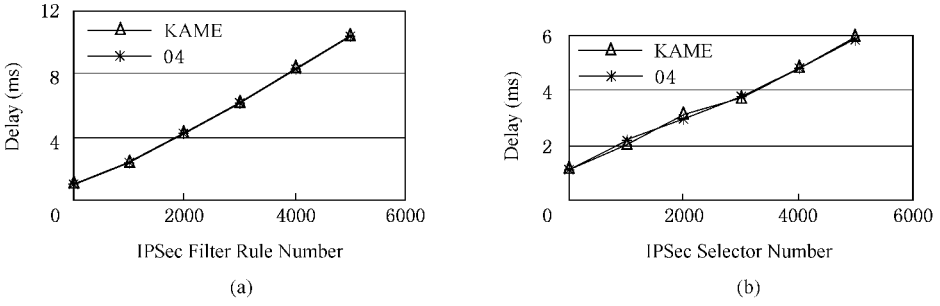

Fig. 6　The delay of the IP packets"not necessary to be protected by IPSec". (a) The influence of IP Filter rule number on the processing delay when the number of IPSec policy selector is fixed and (b) The influence of IPSec policy selector number on the processing delay when the number of IP Filter rule is fixed.

图 6　"不需要 IPSec 安全保护的 IP 包"的处理延迟. (a) 当 IPSec 策略选择符数量固定时,IP Filter 规则数量对处理延迟的影响;(b) 当 IP Filter 规则数量固定时,IPSec 策略选择符数量对处理延迟的影响

由此,我们认为 04 方案的部署策略比 KAME 具有更高的处理效率,它一方面提高了"需要 IPSec 保护的"IP 包的处理效率,避免了 IP Filter 对"需要 IPSec 保护的"IP 包的处理效率的影响;另一方面,对"不需要 IPSec 保护的"IP 包的处理效率与 KAME 方案相同.

5　结束语

本文研究了 IPSec 和 IP Filter 这两个安全部件在路由器中的部署策略. 本文认为两者的部署策略如何,将影响到 IP 包在路由器中的处理效率.

本文提出的部署策略提高了 IPSec 的处理效率,最大程度地排除了 IP Filter 对 IPSec 处理效率的负面影响,提高了 IP 包的处理效率. 同时,方案减少了 IP Filter 规则配置的复杂度,即 IP Filter 在进行规则配置时,不需要兼顾 IPSec 的安全策略. 本文提出的部署策略还有一个特点:就是尽可能消除了 IP 通路上 IP 包的重复过滤,IP 输入路径上的 IP

包就完全消除了重复过滤;IP 输出路径上的 IP 包,也部分地消除了重复过滤.

本文是使用线性查找算法对 KAME 方案和我们的 04 方案进行分析、比较和模拟的,在未来的工作中,我们将研究两种部署策略针对不同查找算法的性能差异.

参 考 文 献

1 S. Kent, R. Atkinson. Security architecture for the Internet protocol. RFC 2401, 1998

2 S. Kent, R. Atkinson. IP authentication header. RFC 2402, 1998

3 S. Kent, R. Atkinson. IP encapsulating security payload (ESP). RFC 2406, 1998

4 http://www.kame.net, 2004-09-16/2004-10-25

5 J. Hagino. Implementing IPv6: Experiences at KAME project. In: Proc. 2003 IEEE Symposium on Applications and the Internet (SAINT2003) Workshop. Los Alamitos: IEEE Computer Society Press, 2003. 218~221

6 Mitsuru Kanda, Kazunori Miyazawa, Hiroshi Esaki. USAGI IPv6 IPSec development for Linux, 2004 IEEE Symposium on Applications and the Internet (SAINT2004) Workshop, Tokyo, 2004

7 http://www.linux-ipv6.org, 2004-09-12/2004-10-20

8 D. Piper. The Internet IP security domain of interpretation for ISAKMP. RFC 2407, 1998

9 D. Maughan, M. Schertler, M. Schneider, *et al*. Internet security association and key management protocol (ISAKMP). RFC 2408, 1998

10 D. Harkins, D. Carrel. The Internet key exchange (IKE). RFC 2409, 1998

11 http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/ipsec.pdf, 2004-08-19/2004-10-17

Wang Li, born in 1969. Since 2002, he has been a master degree candidate in the Department of Computer Science of Tsinghua University. His main research interests include network security.

王利,1969 年生,硕士研究生,主要研究方向为网络安全.

Xu Mingwei, born in 1971. Received his Ph. D. degree in computer science from Tsinghua University, China in 1998. Currently he is an associate professor in the Department of Computer Science of Tsinghua University. His main research interests include the architecture of computer network, high-speed router architecture and protocol testing.

徐明伟,1971 年生,博士,副教授,主要研究方向为计算机网络体系结构、高速路由器体系结构、协议测试等.

Xu Ke, born in 1974. Received his Ph. D. degree in computer science from Tsinghua University in 2001. Currently he is an associate professor in the Department of Computer Science of Tsinghua University. His main research interests include next generation Internet, switch and router architecture, peer-to-peer network and QoS control. He is a member of IEEE and IEEE Communication Society.

徐恪,1974 年生,博士,副教授,主要研究方向为新一代互联网体系结构、交换机和路由器体系结构、应用层网络和网络服务质量控制.

Research Background

IPv6 router has two important IP security modules—IPSec and IP Filter. IP Filter is a usual security module used in routers, which provides the input and output admission control for IP packets. IPSec is an IP security protocol suite, and it provides various forms of security guarantee. Similar to the function of IP Filter, the security-association query engine of IPSec also needs filtering and matching the IP packages. IP Filter and IPSec are a couple of IP processing modules in the IP paths of routers. The term IP path we mention here is referred to the IP packet flow path within the routers. Since IP Filter and IPSec all filter the IP packets, the IP packages flowing inside the router could be filtered by the two modules for more than once. Thus, the method of deployment between the two IP security modules will have direct influence on the processing performance of IP packages. In this work, the inter-relationship between the two security modules is given in a perspective of router global security. Moreover, a novel deployment approach is proposed as well. Compared with the open-source IPv6 protocol stack KAME, the improved processing performance of IPSec is obtained and the negative influence of IP Filter on the IPSec is reduced. Meanwhile, the duplicated IP package filtering within the routers is reduced to improve the processing performance of IP package. This work is supported by the National Natural Science Foundation of China (90104002, 60373010) and the National Key Fundamental Research Plan (973) of China (2003CB314801).