哈爾濱工業大學

毕业设计（论文）开题报告

题 目：基于 dpdk 的高性能的 IPSec VPN 的研究与实现

专　　业　信息安全

学　　生　殷悦

学　　号　**150120526**

班　　号　**1504201**

指导教师　刘扬

日　　期　**2018 年 1 月 4 日**

1．课题背景及研究的目的和意义

1.1 课题背景

随着网络通信技术的发展，大数据到来，用户和网络都日益增长。而保证网络的高速和安全问题成了重中之重。近几年来，网络安全事故频发，信息的传输受到了严重威胁。

而企业、政府、贸易、学校之间需要频繁通信，拉用专线实现困难，耗资巨大。如果直接在公网上通信，信息的机密性无法得到保障。因而需要一个建立在公网上的高效且安全的连接隧道。

虚拟专用网络(Virtual Private Network)，即 VPN 使用了加密和隧道技术在公共网络中建立了一条虚拟专用的链路，使物理位置相距很远的人通过 VPN 技术也可以像在局域网中一样通信。

常见的 VPN 技术有 PPTP / L2TP 和 IPSec，PPTP 与 L2TP 位于链路层，两种协议均基于 PPP 协议来封装数据包。PPTP 与 L2TP 的区别在于前者仅支持两端点间建立隧道，而后者可以可以支持两端点间建立多条隧道，且后者支持隧道模式下认证。而 IPSec 为目前最流行的 VPN 协议，IPSec 包含了一套英特网秘钥交换协议、认证头协议、封装安全载荷协议。

IPv6 是下一代互联网安全协议,IPSec 作为 IP 层的安全协议,兼容了 IPv4 和 IPv6,为 IP 层数据报文提供了完整性、机密性、抗重放攻击、报文原地址认证。IPSec 可运行于任何支持 IP 协议的设备。作为 IPv6 的一重要组成部分，所有 IPv6 节点均需支持并使用 IPSec 协议,而 IPv4 可使用 IPSec,但并非必须使用 IPSec。除了 IPv4 和 IPv6 本身协议的不同，IPSec 协议在 IPv4 和 IPv6 的作用、功能、结构均相同。

IPSec 由三部分组成：

认证头协议(AH)用于对报文源地址认证和报文完整性检测功能。

封装安全载荷协议(ESP)用于报文内容认证和加密的功能，加密算法常用 AES、DES、3DES 等，完整性校验算法常用 HMAC-SHA1、HMAC-MD5 等。

英特网秘钥交换协议(IKE)用于协商源主机和目的主机间用作保护 IP 报文的 ESP 和 AH 等参数，例如加密秘钥、秘钥生存周期、认证算法、加密算法等。

IPSec 仅指 AH 和 ESP，IKE 使用 UDP 的 500 端口，是应用层协议。

传统的 VPN 吞吐量低，包转发率低，时延大。随着 VPN 通信规模增大，传统的 VPN 在性能上无法满足用户的需求，因此开发一款安全高性能的 VPN 意义重大。

1.2 研究的目的和意义

传统的 VPN 吞吐量低，包转发率低，时延大。协议栈集成于系统内核中，传统协议栈中断频繁，内存间复制多，功能冗余等缺点。通过构建用户态协议栈和 VPN 来弥

补这些缺点，满足高速和高效等性能需求。

随着 VPN 通信规模增大，传统的 VPN 在性能上无法满足用户的需求，因此开发一款安全高性能的 VPN 意义重大。

首先了解传统协议栈在高速网络下遇到的问题，并列出目前主流的协议栈加速方案。其次了解 DPDK 所能解决传统协议栈存在的瓶颈和解决方案，学习用户态协议栈的实现方式，了解数据收发模块、底层驱动模块、转发协议模块、路由算法模块。

最后测试出用户态协议栈和传统内核协议栈在高速网络环境下的性能差距，以及测试环境对测试结果的影响。总结该论文的工作与不足，列出未来的研究方向。

2. 国内外在该方向的研究现状及分析

2.1 国外现状及分析

人们通常通过展开研究 VPN 网关的功能，例如改进安全协议、提高加密速度改进网关架构等等。随着网络的发展，人们发现服务器内核在处理高速报文的瓶颈。

国外思科是互联网解决方案的领先提供者，其设备和软件产品主要用于连接计算机网络系统。Cisco Cataltsy 6500 和 Cisco 7600 系列互联网路由器上的端点位置提供了经济有效的 IPSec VPN。该系列模块提供了最新的加密硬件加速技术，支持多种 PKI，自动登记证书以及全套通道支持。可为大型分组提供 1.9Gpbs 的 3DES 流量，为普通大小的分组提供 1.6Gpbs 的 3DES 流量，可同时端接 8000 条 IPSec 通道。

零拷贝技术可以减少数据在用户空间和内核空间的相互拷贝技术，避免因数据拷贝引起的上下文切换，该技术应用于协议栈，可较大程度提升性能。数据通过 DMA 技术直接从网卡到内存，避免了 CPU 参与拷贝任务，也减少了数据对 IO 依赖。

华盛顿大学学者设计了 Alipine，它解决了传统应用移植到用户栈改动较多的问题，将内核空间虚拟化为用户空间协议栈。

加拿大埃里克恩格尔克大学学者设计了 Wattcap。它实现了传输层协议栈的相互交互和网络层数据包的重组分片功能。

2.2 国内现状及分析

清华大学学者设计了通过用户态通信的协议 RCP。RCP 绕过系统内核和网络直接通信，减少了数据包的复制，提高了效率。

国内深信服和天融信的 IPSec VPN 近年来取得了很大的成功,天融信 IPSec VPN 系统采用了 TOS 安全操作系统，采用了全模块化设计并使用了中间层概念，减少了系统对硬件的依赖性，使用了先进的多核并行技术。

为应对内核效率低的问题，通常人们采用两种解决方案：

1.通过硬件来加速协议栈处理速度，TOE 即 TCP/IP 卸载引擎，是常用的一种加速方案，将协议栈交给 GPU 或 FUPGA，但因存在调试复杂，对硬件要求高，成本高昂而较少使用

2.使用内核协议或高性能报文收发平台，广泛使用的框架有 DPDK，PF_RING 和 netmap。netmap 性能较低，PF_RING ZV 开发人员较少，而 DPDK 加入了 Linux 基金项目，开发人员多，因此本文采用 DPDK 框架进行研究。

3．研究内容及拟解决的关键问题

3.1 研究内容

本文研究利用IPSec通信协议，使用IKE进行证书认证及协商会话秘钥，对流经的数据使用ESP进行加密，通过DPDK平台提高通信数据包处理低效问题。

3.2 拟解决的关键问题

DPDK是用户态驱动，并且输出的是链路层报文。为了实现该需求，需要完成：

1. 熟悉IPSec协议，了解IPSec的每个步骤及其作用，熟悉IKE通信过程，熟悉ESP数据结构和IKE数据结构，了解IKEv1和IKEv2的异同
2. 学会调用Linux内核的IPSec，会生成证书，部署IPSec VPN
3. 熟悉DPDK编程，了解DPDK原理，学会运用HugePage和NUMA提升程序效率
4. 使用并部署DPDK处理IPSec协议中ESP部分，实现简单通信功能
5. 将StrongSwan的IKE和DSP对接起来
6. 实现用户态数据转发网关算法，使其可以完成数据转发
7. 如果有能力，可尝试实现基于网卡实现加密算法的offloading

4. 拟采取的研究方法和技术路线、进度安排、预期达到的目标

4.1 拟采取的研究方法和技术路线

1. 阅读论文了解业界的解决方案和技术路线
2. 阅读 DPDK 官方文档、书籍及例子代码，熟悉 DPDK 编程
3. 阅读 IPSec 协议的 rfc 文档了解开发原理和实现步骤
4. 熟悉 IPSec 代码，并搭建 IPSec 环境
5. 搭建 DPDK 开发环境，配置 HugePage，绑定网卡
6. 尝试调用内核 IPSec 的 ESP 部分，学习内核 IPSec 协议
7. 理解 IPSec 的 ESP 部分，将内核 IPSec 协议移植到 DPDK

8. 将传统协议栈 IKE 和 DPDK 的 ESP 部分对接起来

9. 进行性能测试，和基准进行对比，总结性能提升

4.2 进度安排

1．12 月 25 日-1 月 4 日完成开发环境搭建

2． 1 月 4 日-2 月 19 日完成 DPDK 处理 IPSec 中 ESP 处理部分及网关数据转发功能

3．2 月 20 日-3 月 20 日完成 IPSec IKE 和 ESP 对接

4． 3 月 20 日-3 月 31 日完成基于网卡实现加密算法的 offload

5．4 月 1 日-4 月 10 日完成并发和线速转发性能测试

4.3 预期达到的目标

1. 熟悉业界常用操作系统协议栈优化的方式

2. 熟练使用 DPDK 开发程序

3. 了解 IPSec 原理和每个包的构造及其原理

4. 了解传统协议栈的不足之处，并理解 DPDK 优化的原理

5. 熟练操作 DPDK 开发环境的配置

6. 完成基于 IPSec 的 DPDK ESP 包处理

7. 完成 DPDK 的路由算法，完成包的转发

8. 完成 IKE 秘钥协商和 IPSec ESP 部分在 DPDK 上的对接

9. 并测试出并发和线速性能

5．课题已具备和所需的条件

所需条件：

1. 支持 DPDK 的千兆网卡

2. 2 核心 4G 内存支持 DPDK 的软路由或 PC

3. 一台发包性能测试机

课题已具备的条件：

1. 支持 DPDK 的千兆网卡

2. 2 核心 4G 内存支持 DPDK 的软路由

3. 一台发包性能测试机

6. 研究过程中可能遇到的困难和问题，解决的措施

问题：

1. StrongSwan 代码结构难以理清，代码难以看懂

2. IPSec 协议难以理清

3. DPDK 上手困难

4. 基于网卡的 Offload 的加密算法难以实现

解决措施：

1. 阅读 StrongSwan 官方文档

2. 阅读 IPSec 有关 rfc

3. 阅读 DPDK 相关书籍和示例程序

7. 参考文献

[1] RFC4301, Security Architecture for the Internet Protocol [S]. USA: S. Kent,K. Seo 2015.12

[2] RFC4303, IP Encapsulating Security Payload (ESP) [S]. USA: S. Kent. 2015.12

[3] RFC3602, The AES-CBC Cipher Algorithm and Its Use with IPsec [S]. USA: S. Frankel,R. Glenn,NIST,S. Kelly,Airespace 2003,9

[4] RFC2404, The Use of HMAC-SHA-1-96 within ESP and AH [S]. USA: C. Madson,Cisco Systems Inc,R. Glenn,NIST 1998,11

[5] RFC2367, PF_KEY Key Management API, Version 2 [S]. USA: D. McDonald,C. Metz,B. Phan 1998,7

[6] 阚闯,栾新,戚玮玮. 基于 Linux 的 XFRM 框架下 IPSec VPN 的研究[J]. 计算机工程. 2008(20)

[7] 孙云霄. 面向企业用户的高性能 VPN 系统的设计与实现[D]: [硕士毕业论文]. 威海: 哈尔滨工业大学(威海). 2015.

[8] 穆瑞超. 基于DPDK的高性能VPN网关的研究与实现[D]:[硕士毕业论文]. 威海: 哈尔滨工业大学(威海). 2017.

[9] 吴承. 用户态 IPSec 协议栈的研究与实现[D]:[硕士毕业论文]. 西安: 西安电子科技大学. 2014.

[10] 唐宏,柴桌原,任平,王勇. DPDK 应用基础[J]. 电信科学. 2016(09)

[11] 朱河清. 深入浅出 DPDK[M]. 机械工业出版社. 2016

[12] 王冠群. IPSec 中间人攻击检测方法与防御策略[D]:[硕士毕业论文]. 威海: 哈尔滨工业大学(威海). 2018.

[13] 廖悦欣. IPSec 协议实现技术研究[D]:[硕士论文]. 华南理工大学. 2013.

指导教师评语：_____

_____

_____

_____

_____

指导教师签字：_____ 检查日期：_____