Computer Science and Application 计算机科学与应用, 2018, 8(1), 123-129
Published Online January 2018 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2018.81016

Hans汉斯

Research and Implementation of User-Mode IPSec Based on DPDK

Yangyang Feng

China University of Mining & Technology, Beijing
Email: 1119114266@qq.com

Received: Jan. 8th, 2018; accepted: Jan. 23rd, 2018; published: Jan. 30th, 2018

Abstract

This paper aims at the problems of delay, congestion, small throughput caused due to increasing users and more network traffic demand by using IPSec gateway, analyzes the shortcomings during the IPSec solution process, and puts forward the method of implementation of DPDK gateway based on IPSec in user space. Aiming at the problem of large overhead of traditional programs, we propose to build Cisco VPP as a platform and DPDK as a receiving packets tool to build data processing platform. The test results show that the performance of the IPSec solution of user space based on DPDK is improved effectively compared with the traditional solution.

Keywords

IPSec, DPDK, User-Space, Performance Boost

基于DPDK的用户态IPSec网关的研究和实现

冯扬扬

中国矿业大学(北京)，北京
Email: 1119114266@qq.com

收稿日期：2018年1月8日；录用日期：2018年1月23日；发布日期：2018年1月30日

摘　要

本论文针对在使用IPSec网关时由于用户量不断增加、网络流量需求大的情况下所造成的时延、阻塞、吞吐量小等问题，分析了内核态IPSec解决方案处理流程中存在的不足，提出了基于DPDK在用户态实现IPSec网关的方法。针对传统方案处理开销大的问题提出利用思科的VPP作框架，DPDK作收包工具搭建平台实现数据包在用户态的处理。测试结果表明，基于DPDK的用户态IPSec解决方案与传统方案相比，

文章引用: 冯扬扬. 基于 DPDK 的用户态 IPSec 网关的研究和实现[J]. 计算机科学与应用, 2018, 8(1): 123-129.
DOI: 10.12677/csa.2018.81016

性能得到了有效的提升。

关键词

IPSec，DPDK，用户态，性能提升

1. 引言

随着互联网技术的快速发展，智能终端用户量的爆炸式增加，对移动通信业务的覆盖效果要求越来越高。据调查显示，移动通信业务主要集中在车站、住宅区、办公区等室内场所[1]。但目前室内信号存在容纳终端量小、信号不稳定，数据和话音质量差等现象。针对上述现象，室内信号增强的解决方案主要有 femto 基站、路由器、AP 等。Femto 系统是通过固网宽带接入核心网，为用户提供固定移动融合业务，在高性价比实现移动通信室内覆盖、固定移动综合业务平台化提高等方面具有显著优势，已成为主流运营商重点关注的技术方向。Femto 系统是由 Femto AP、安全网关、Femto 网关等组成的，目前 Femto 应用中一般安全网关都是作为独立网元存在的。本文分析的就是安全网关作为独立网元存在的不足，并针对这些不足对独立安全网关进行改进，利用基于 DPDK 实现的用户态 IPSec 网关来改善数据通信处理流程复杂带来的一系列问题，优化安全网关的性能。

2. 架构概述

2.1. Femto 架构概述

Femto 系统架构组成如图 1 所示，包括终端、femto 基站、femto 网关、核心网[2]。Femto 基站通过 Internet 连接到 femto 网关，在 Internet 上传输的数据安全性很容易通过相应的技术手段造成威胁，所以提高 femto 系统的安全性是非常必要的，IPSec 网关技术应运而生[3]。

2.2. IPSec 框架概述

IPSec 安全网关的运行环境是 Linux 系统。如图 2 所示为 IPSec 安全网关的结构框图。其中数据加解密模块、AH (Authentication Header，验证头)/ESP (Encapsulated Security Payload，封装安全载荷)实现模块、SADB (Security Association Database，安全关联数据库)/SPDB (Safety Policy Database，安全策略数据库)等模块都是在内核层实现的，IKE (Internet Key Exchange，因特网密钥交换协议)模块在用户层实现[4]。

现有的 IPSec 安全网关技术是使用 IPSec 隧道对数据进行加解密处理，这种方式会增加额外的带宽，对数据的传输速率产生很大的影响，因此需要寻求方法来提升安全网关的性能。提升 IPSec 安全网关性能的方法有三种：第一，优化 IPSec 加解密算法；第二，利用加速硬件来处理加解密流程；第三，内核协议栈中 IPSec 数据的处理流程的内存拷贝、系统调用、中断的开销比较大，而用户态只有一些上层应用程序，我们可以把协议栈放在用户态减少上述开销，在用户态实现 IPSec 功能。基于上述三种方法的对比和衡量，本文采用在用户态实现 IPSec 功能来优化安全网关的性能。

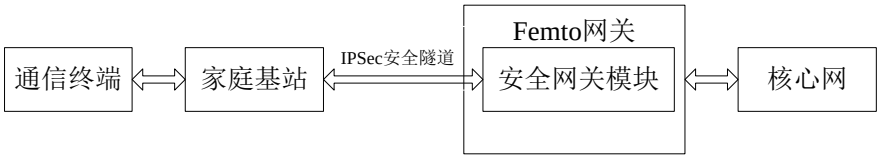

Figure 1. Femto system
图 1. Femto 系统

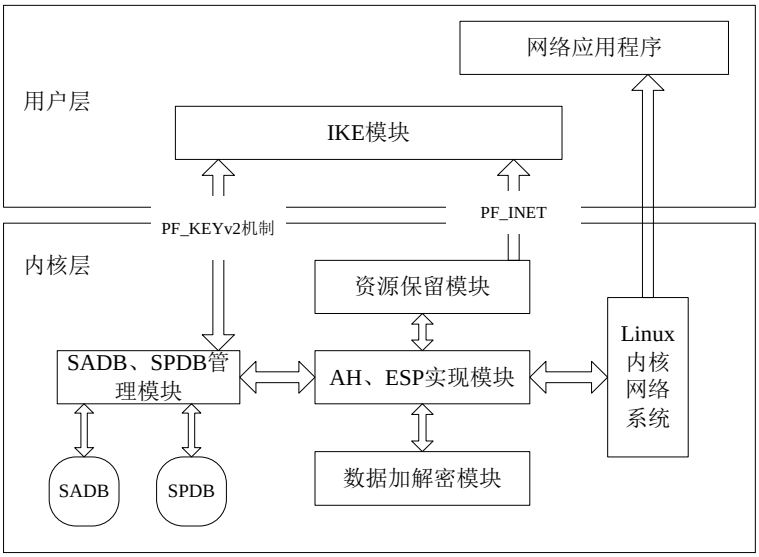

Figure 2. The structure diagram of IP Security gateway
图 2. IPSec 网关的结构框图

3. 解决方案

通过大量的调研和学习，本文提出了一种基于 DPDK (Data Plane Development Kit，数据平面开发套件)实现用户态 IPSec 网关功能的方法。即利用基于 VPP (Vector Packet Processing，向量报文处理)框架实现的 DPDK 模块、协议栈处理模块和 IPSec 模块来提升安全网关的性能，如图 3 所示。

首先介绍一下 DPDK，DPDK 是 Intel 推出的运行在用户空间上利用自身提供的数据平面库来实现数据包快速收发的套件，绕过了 Linux 内核协议栈对数据包进行相应的处理[5]。DPDK 主要有两个功能：底层驱动和数据收发。

DPDK 在底层驱动模块实现了多核处理和分布式存储分配方式。DPDK 改变了传统处理方式不支持多核环境的缺点，实现了多核环境，把所有的逻辑核分为主核和次核两部分，主核负责初始化次核、内存池的初始化、共享变量的建立、硬件的检测以及任务的分发等。次核负责执行主核分发的任务。同时为了避免分发的任务在多个逻辑核之间频繁的迁移，DPDK 通过 CPU 亲和性将任务固定分发到某一个次核。次核的任务执行由主核完全控制，不能被其他应用程序抢占，因此在整个应用程序的执行期间，处理器核都是被独占的。

为了解决传统处理方式中硬件中断所带来的负载严重不均衡问题，以最快的速度处理数据包，DPDK 采用轮询模式从网卡获取数据包，每一个逻辑核可以分配一个发送和接收队列，将收到的数据包平均放在网卡的接收队列中，以此实现负载均衡。另外不断的检查每一个逻辑核的发送队列，将要发送的数据包发送出去[5]。通过上述方式，有效减少了数据收发的开销，实现数据包的快速收发。

接下来介绍的是用户态的框架 VPP。VPP 是 Cisco 开发的一套基于 DPDK 实现的运行在用户空间的

可扩展框架。它是个延展性很高的应用，一个应用在 VPP 里以连起来的若干节点(Graph Node)组成，每个节点包含上述的一个或多个功能。网络帧在 VPP 中被储存在网络帧向量 Packet Vector 中，它也是节点的唯一处理对象，节点也会根据处理结果来决定网络帧的下一个目的地节点。它的功能非常强大，提供了完整的 IPsec 协议栈支持：ESP，Transport 和 Tunnel 模式，以及 IKEV2，将 VPP IPSec 和 DPDK Cryptodev 进行了融合，在 VPP IPSec 中成功启用了 DPDK Cryptodev 来负责所有的 Crypto 工作，让两者之间有了强烈的化学反应。VPP DPDK IPsec 工作流如图 4 所示，可以看到，在 interface-output 节点处，程序发现网络帧是 ESP 协议帧后，将其组成 Packet Vector 传递给 ipsec-if-output 节点，再将其交给 DPDK Cryptodev 加持的 dpdk-esp-encrypt 和 dpdk-esp-decrypt 做 Crypto 工作。然后再传递给 dpdk-crypto-input 轮询节点，dequeue 处理完的工作流。接下来的 dpdk-esp-encrypt-post/dpdk-esp-decrypt-post 负责网络帧的再封装[6]。

4. 测试及分析

为了比较用户态 IPSec 网关与传统方案的性能，搭建如图 5 所示的测试环境。其中网关 A 和 B 是两

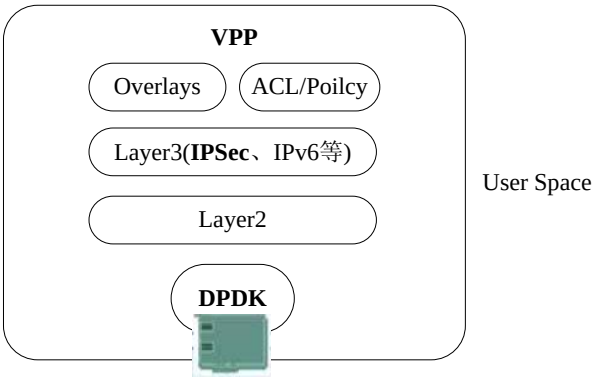

Figure 3. The structure diagram of VPPDPDK IPSec in User Space
图 3. VPPDPDK IPSec 在用户态的结构框图

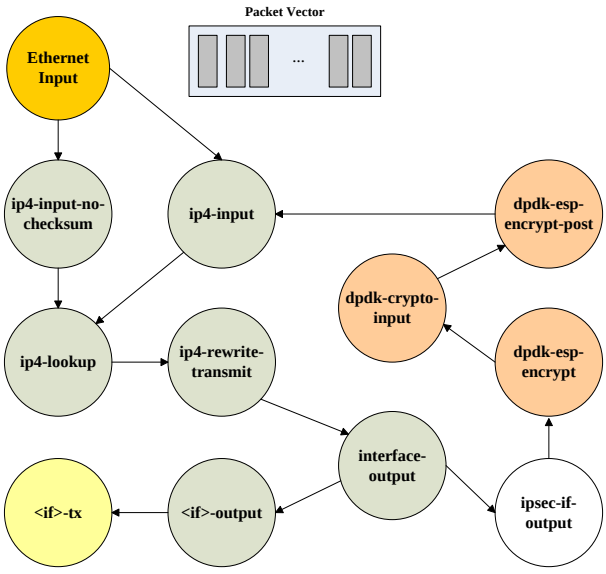

Figure 4. VPP DPDK IPsec workflow
图 4. VPP DPDK IPsec 工作流

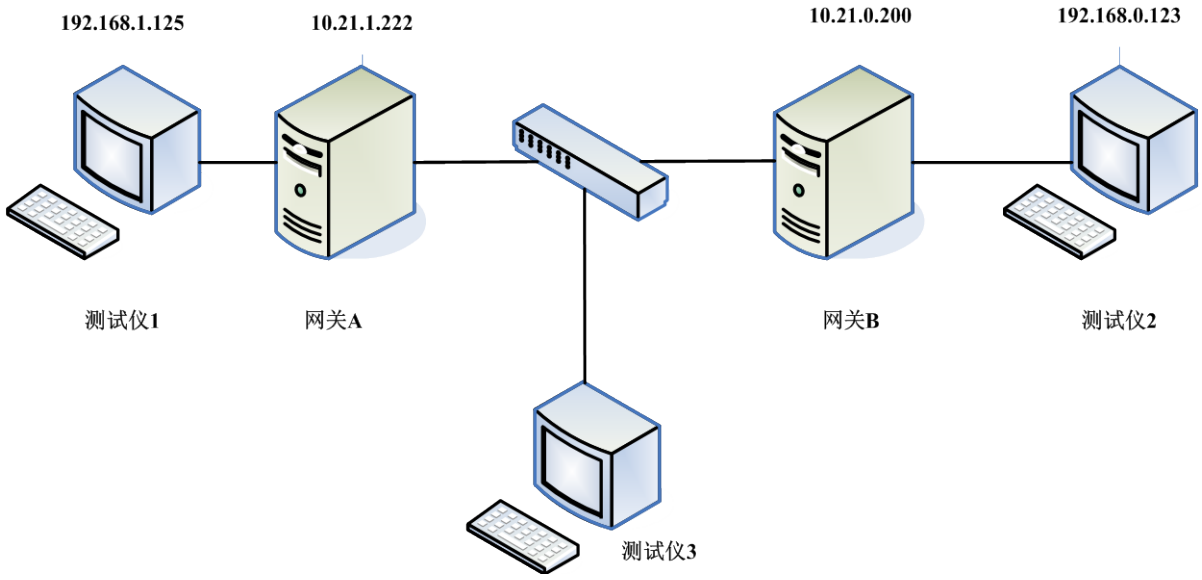

Figure 5. Test architecture
图 5. 测试架构

台 Dell PowerEdge R620 (型号)服务器，两个处理器，12 个物理核，24 个逻辑核，NUMA 架构，32 G 内存，Ubuntu14.04(64 位)操作系统，万兆光口。测试仪 1、2、3 用的是 IXIA 测试仪。其中测试仪 1 表示的是发出数据包的速度；测试仪 2 表示接收数据包的速度；测试仪 3 表示网关 A 发出数据包的速度。

4.1. VPP 安装步骤

1) 下载源码：git clone https://gerrit.fd.io/r/vpp；
2) 安装依赖：make install-dep；
3) 安装：执行./build-root/vagrant/build.sh；
4) 生成 Makefiles 文件：gitpull；cd build-root/；make distclean；./bootstrap.sh；
5) 进行编译：make V = 0 PLATFORM = vpp TAG = vpp install-deb；
6) 包安装：ls *.deb；dpkg–i *.deb；
7) 启动 VPP：start vpp [7]。

4.2. DPDK 安装步骤

1) 下载源码：git clone git://dpdk.org/dpdk
2) 设置环境变量：进入 dpdk 目录：cd~/dpdk
编辑一个环境变量文件名字为 dpdkrc，内容为：
export RTE_SDK = “pwd”；
export RTE_TARGET = x86_64-native-linuxapp-gcc；
然后执行 sourcedpkdrc 命令；
3) 编译 dpdk
makeconfig T = x86_64-native-linuxapp-gcc；
make install T = x86_64-native-linuxapp-gcc；

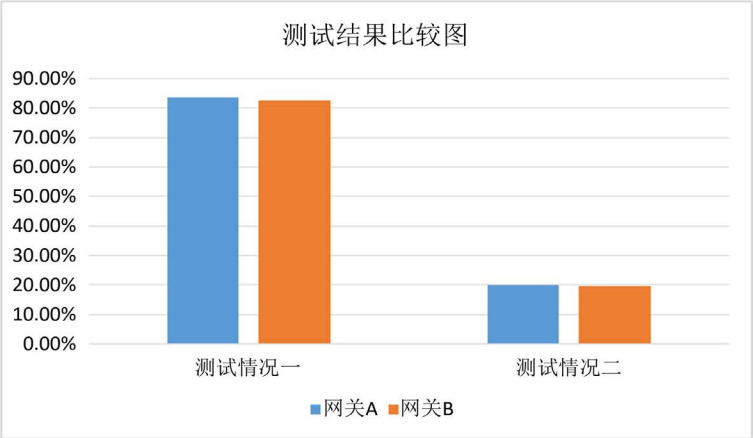

Figure 6. Test result diagram
图 6. 测试结果图

4) 配置 hugepages

mkdir-p/mnt/huge；

mount-t hugetlbfsnodev/mnt/huge；

echo 1024 > /sys/devices/system/node/node0/hugepages/hugepages-2048kB/nr_hugepages；

5) 加载驱动模块

cd tools；

./dpdk-devbind.py –status (查看网络端口状态)；

modprobeuio；

cd x86_64-native-linuxapp-gcc/kmod；

insmodigb_uio.ko；

6) 绑定网卡

./dpdk-devbind.py –bind = igb_uioethx；

./dpdk-devbind.py –status；

7) 解绑命令

./dpdk-devbind.py –u 02:06.0 02:07.0；

./dpdk-devbind.py –status [8]。

经过上述步骤，完成运行在用户态的 VPP 和 DPDK 环境的搭建，要在 VPP 上实现 IPSec 和 IKEV2 的功能，还需要经过一系列的配置才能实现，在这里就不详细进行介绍了，环境搭建好之后，基于 DPDK 实现的 IPSec 网关就可以成功实现数据包在用户态的安全传输。

4.3. 测试结果分析

从测试仪 1 以 20 Gbit/s 的极限速度向测试仪 2 发送数据，单核转发，测试情况分为以下两种：一、网关 A、B 均为 VPP DPDK IPSec；二、网关 A、B 均为标准 IPSec (strongswan5.3.3)。使用百分比来表示此刻速率达到的最大吞吐量程度，100%表示 20 Gbit/s。测试结果如图 6 所示。从测试结果图可知，在用户态实现的 VPP DPDK IPSec 网关比传统方案性能提升了很多，说明本方案是可行且有效的。

5. 总结

根据传统 IPSec 网关的不足，本文提出了一种基于 DPDK 的用户态 IPSec 网关的解决方案，并在 Linux

环境下实现了此方案。测试结果表明，VPP DPDK IPSec 与传统方案相比，性能得到了有效的提升。

参考文献 (References)

[1] 陈文雄. Femto 系统独立安全网关改造方案[J]. 移动通信, 2014(23): 29-32.

[2] 中国移动 GSM TD-SCDMA TD-LTE_Femto_Nanocell_网关设备技术规范 V1.0.0[Z]. 中国移动通信公司, 2012.

[3] 殷瑞祥, 谢小梅. 一种快速加解密的 Femto 安全网关系统[J]. 信息技术, 2015(3): 85-88.

[4] Korona, M., Skowron, K., Trzepiński, M. and Rawski, M. (2017) FPGA Implementation of IPsec Protocol Suite for Multigigabit Networks. 2017 *International Conference on Systems, Signals and Image Processing* (*IWSSIP*), May 22-24 2017, Poznan. https://doi.org/10.1109/IWSSIP.2017.7965619

[5] 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.

[6] VPP IPSec Implementation Using DPDK Cryptodev API. https://docs.fd.io/vpp/17.01/dpdk_crypto_ipsec_doc.html

[7] VPP/Build, Install, and Test Images. https://wiki.fd.io/view/VPP/Build,_install,_and_test_images

[8] http://dpdk.org/doc/guides/linux_gsg/index.html