毕业论文开题答辩

汇报人：殷悦 学号：150120526

目录

01

课题背景

课题背景-概述

应用

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。

原理

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VPN

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。。

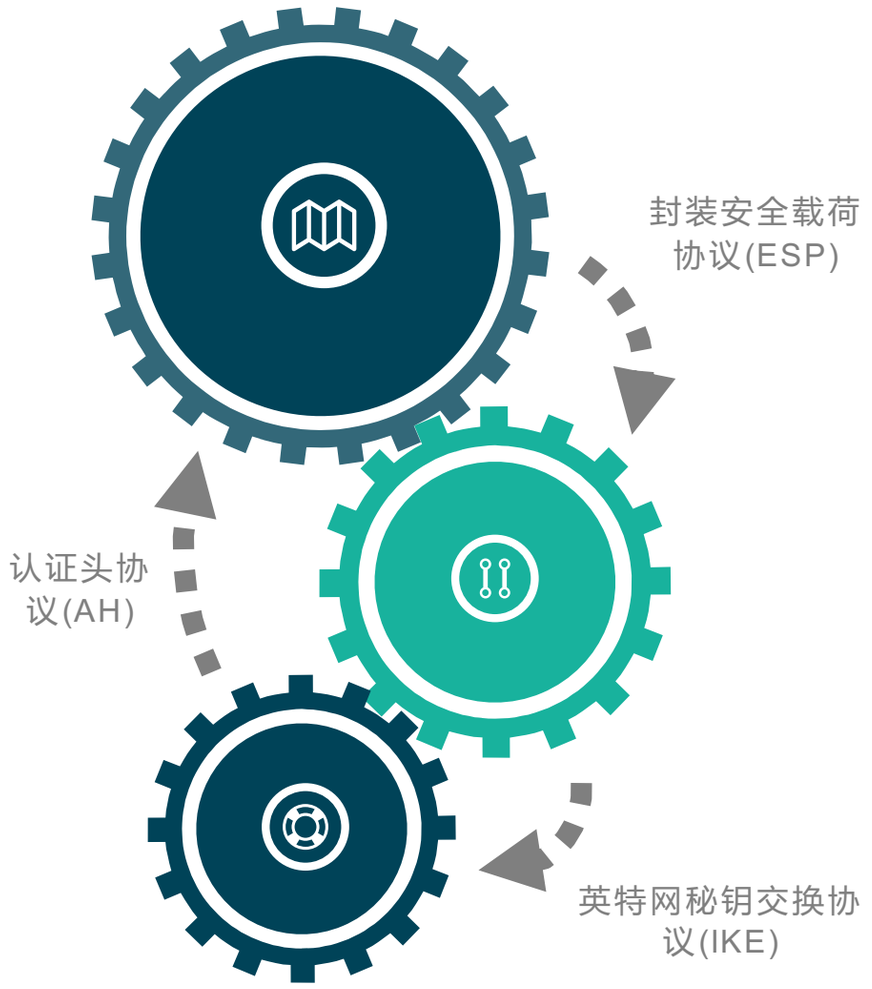
课题背景-IPSec协议

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。



02

现状分析

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。

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。

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。

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

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。

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。

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

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。

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。

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。

03

研究内容

拟解决的关键问题

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。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：

01

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

02

学会调用Linux内核的IPSec，会生成证书，部署IPSec VPN

03

熟悉DPDK编程，了解DPDK原理，学会运用HugePage和NUMA提升程序效率

04

使用并部署DPDK处理IPSec协议中ESP部分，实现简单通信功能

05

将IPSec的IKE和DPDK的SP对接起来

06

实现用户态数据转发网关算法，使其可以完成数据转发

07

如果有能力，可尝试实现基于网卡实现加密算法的offloading

拟采取的研究方法和技术路线

01 阅读论文了解业界的解决方案和技术路线

02 阅读DPDK官方文档、书籍及例子代码，熟悉DPDK编程

04 阅读IPSec协议的rfc文档了解开发原理和实现步骤

03 熟悉IPSec代码，并搭建IPSec环境

05 搭建DPDK开发环境，配置HugePage，绑定网卡

06 尝试调用内核IPSec的ESP部分，学习内核IPSec协议

07 理解IPSec的ESP部分，将内核IPSec协议移植到DPDK

08 将传统协议栈IKE和DPDK的ESP部分对接起来

09 进行性能测试，和基准进行对比，总结性能提升

04

进度安排

课题已具备和所需的条件

所需条件：

支持DPDK的千兆网卡

2核心4G内存支持DPDK的软路由或PC

一台发包性能测试机

课题已具备的条件：

支持DPDK的千兆网卡

2核心4G内存支持DPDK的软路由或PC

一台发包性能测试机

进度安排

12月25日-1月4日

完成开发环境搭建

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

2月20日-3月20日

完成IPSec IKE和ESP对接

3月20日-3月31日

基于网卡实现加密算法的offload

4月 1日-4月10日

完成并发和线速转发性能测试

预期达到的目标


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

THANK YOU

感谢聆听，批评指导