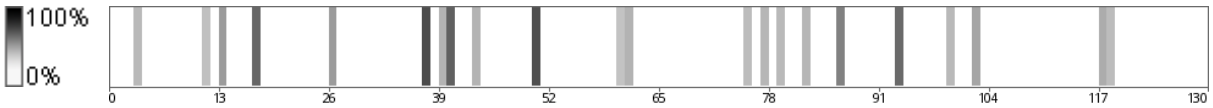
PaperPass旗舰版检测报告
简明打印版

比对结果(相似度):

总　体：13% (总体相似度是指本地库、互联网的综合对比结果)
本地库：13% (本地库相似度是指论文与学术期刊、学位论文、会议论文、图书数据库的对比结果)
期刊库： 5% (期刊库相似度是指论文与学术期刊库的比对结果)
学位库：10% (学位库相似度是指论文与学位论文库的比对结果)
会议库： 0% (会议库相似度是指论文与会议论文库的比对结果)
图书库： 4% (图书库相似度是指论文与图书库的比对结果)
互联网： 0% (互联网相似度是指论文与互联网资源的比对结果)

报告编号：5CBA81FE347E7HPGR
检测版本：旗舰版
论文题目：基于DPDK的高性能IPSec VPN
论文作者：殷悦
论文字数：2959字符(不计空格)
段落个数：91
句子个数：130 句
提交时间：2019-4-20 10:20:46
比对范围：学术期刊、学位论文、会议论文、书籍数据 、互联网资源
查询真伪：http://www.paperpass.com/check

句子相似度分布图:



本地库相似资源列表(学术期刊、学位论文、会议论文、书籍数据):

1.相似度： 1% 篇名：《基于路由器平台的IPSec协议的实现》
来源：学位论文 华中科技大学 2004
2.相似度： 1% 篇名：《基于Openswan的国密IPsecVPN服务器软件设计与实现》
来源：学位论文 西安电子科技大学 2014
3.相似度： 1% 篇名：《浅析IPSec协议及安全联盟》
来源：学术期刊 《大陆桥视野》 2015年24期
4.相似度： 1% 篇名：《IPSec VPN中NAT穿越的研究》
来源：学位论文 重庆邮电大学 2010
5.相似度： 1% 篇名：《基于P2P技术的IPSec VPN的研究与设计》
来源：学位论文 桂林电子科技大学 2007
6.相似度： 1% 篇名：《基于嵌入式系统的PKI技术研究与实现》
来源：学位论文 国防科学技术大学 2005
7.相似度： 1% 篇名：《对虚拟专用网分析、实现与改进》
来源：学位论文 山东大学 2003
8.相似度： 1% 篇名：《快速Internet密钥交换协议（JFK）的改进与实现》
来源：学位论文 重庆大学 2006
9.相似度： 1% 篇名：《IPSec协议中加密算法使用研究》

来源：学术期刊 《计算机工程与应用》 2003年15期
10.相似度： 1% 篇名：《基于IPSec网络安全协议的研究及实现》
来源：学位论文 电子科技大学 2010
11.相似度： 1% 篇名：《基于IPv6的网络安全架构分析与研究》
来源：学位论文 西安科技大学 2008
12.相似度： 1% 篇名：《软交换组网与业务》
来源：书籍数据 人民邮电出版社 2005-9-1
13.相似度： 1% 篇名：《VPN技术在“一卡通”网络中的应用研究与设计》
来源：学位论文 苏州大学 2005
14.相似度： 1% 篇名：《网络安全协议》
来源：书籍数据 电子科技大学出版社 2008-3-1
15.相似度： 1% 篇名：《IPSec和SSL技术在构建VPN中的应用研究》
来源：学位论文 山东大学 2007
16.相似度： 1% 篇名：《基于IPSec的VPN网关设计与实现》
来源：学位论文 国防科学技术大学 2008
17.相似度： 1% 篇名：《网络安全体系结构》
来源：书籍数据 电子科技大学出版社 2006-9-1
18.相似度： 1% 篇名：《IP安全组播密钥管理技术研究》
来源：学位论文 华中科技大学 2008
19.相似度： 1% 篇名：《Red Hat Linux服务器配置与应用》
来源：书籍数据 人民邮电出版社 2006-1-1
20.相似度： 1% 篇名：《Red Hat Linux服务器配置与应用》
来源：书籍数据 人民邮电出版社 2006-1-1
21.相似度： 1% 篇名：《网络安全技术》
来源：书籍数据 西安电子科技大学出版社 2007-2-1
22.相似度： 1% 篇名：《IPSec多播密钥管理协议(GDOI)的改进及其实现》
来源：学位论文 汕头大学 2006
23.相似度： 1% 篇名：《金融软件的系统开发及安全性改进》
来源：学位论文 北京邮电大学 2005
24.相似度： 1% 篇名：《采用统一接口采集Linux内核信息的方法研究》
来源：学术期刊 《计算机应用》 2004年12期
25.相似度： 1% 篇名：《IPSec VPN的研究设计与实现》
来源：学位论文 山东大学 2007
26.相似度： 1% 篇名：《材料研究信息安全传送中IPSec协议的实现》
来源：学位论文 电子科技大学 2001
27.相似度： 1% 篇名：《Linux操作系统实时性研究与应用》
来源：学位论文 南京航空航天大学 2011
28.相似度： 1% 篇名：《Linux用户空间加/解密API的设计与实现》
来源：学术期刊 《计算机应用与软件》 2013年2期
29.相似度： 1% 篇名：《一种改进的IPSec穿越NAT方案》
来源：学术期刊 《计算机技术与发展》 2006年8期

互联网相似资源列表：
暂无互联网相似资源

全文简明报告:

2.1 VPN 原理概述

2.2 IPSec 综述

2.2.1 IPSec 处理

{44%：由于IP协议设计之初没有安全保护，数据在传输中有可能被监听或篡改，存在安全隐患。} 而IPSec是一套完整的加密系统，IPSec有协议提供每个IP数据包的认证，完整性校验（保证传输中未被篡改），机密性（数据包加密）

IPSec技术主要有AH，ESP，IKE，ISAKMP/Oakley和算法组成。

AH协议： 有完整性校验功能，但不能加密数据。

ESP协议： 有完整性校验功能和加密功能。

IKE协议： {42%：主用于秘钥管理，完成设备间会话秘钥协商和交换。}

加密认证算法： {53%：建立连接时需要确定加密和认证的算法，加密常用AES、3DES等算法，认证常用SHA-1和MD5算法。}

SA协议： 用于在不同设备间算法协商和秘钥匙交换的概念。

2.2.2 ESP(封装安全载荷)与AH(验证头)

{69%：ESP主要提供数据加密和完整性校验}

ESP协议：

加密前数据包： IP HDR Data

加密后数据包： New IP HDR Auth(ESP HDR Enc(IP HDR Data) ESP Trailer ESP Auth)

隧道和传输模式：

传输模式：

IP HDR Auth(ESP HDR Enc(Data) ESP Trailer ESP Auth)

{53%：仅对IP头部以上的数据进行加密，不对IP头进行加密，主要用于基于IPSec的点对点通用路由协议}

隧道模式：

New IP Header Auth(ESP HDR Enc(IP HDR Data) ESP Trailer ESP Auth)

首先加密原有数据包，然后加入新头部

2.2.3 IKE(Internet密钥交换)

IKE由三部分组成：

ISAKMP： 使用了UDP的500端口，定义了信息交换的体系结构

SKEME： 实现公钥加密认证体制

Oakley： {77%：提供了IPSec对等体间达成相同加密密钥的基本模式机制。}

SA(SecurityAssocation，安全联盟)： {46%：用于协商实体通信建立的一种协约，协定了IPSec协议、密钥、转码方式、密钥有效期等。} {71%：IPSec会构建一个SA数据库（SADB）用来维护IPSec协议保障数据安全。}

SA是单向的： 两设备通过 ESP进行通信，则设备则需要 SA（ IN）和 SA（ OUT）， {46%： SA（ OUT）用作处理发出的数据包， SA（ IN）用作处理接受的数据包，} SA（ IN）和对方的 SA（ OUT）使用相同的加密参数（密钥等）。

SA还区分协议，若AH和ESP同时生效，AH和ESP会产生不同的SA。

SA有两种：

IKE（ISAKMP） SA： 用于协商IKE数据流加密及对等体认证的算法（对密钥加密和peer认证），只能有一个。

IPSec SA： {76%：用于协商对等体之间的IP数据流进行的加密算法，可以有多个。}

IKE交换模式（主模式）

Peer1Peer2

SA交换（用于确认对方使用的算法）

发送本地IKE策略---发起方发送策略--]

接受对端确认的策略[--接收方确认策略---查找匹配的策略

密钥交换（产生密钥）

---发起方的密钥生成信息--]密钥生成

密钥生成[--接收方的密钥生成信息---

ID交换及验证（验证对方身份）

{41%：---发起方身份和验证数据--]身份验证和交换过程验证}

{46%：身份验证和交换过程验证[--接收方身份和验证数据---}

IKE的交换模式（野蛮模式）

Peer1Peer2

SA交换，密钥生成(确认对方使用的算法，产生密钥)

发送本地IKE策略，密钥生成信息

---发起方策略，密钥生成信息--]

查找匹配的策略，密钥生成

[--接收方的密钥生成信息，身份和验证数据---

接收对端确认的策略，密钥生成

ID交换及验证（验证对方身份）

--发起方身份和验证数据--]

身份验证和交换过程验证

点对点IPSec VPN协商过程有两个阶段，两设备间建立安全的传输连接需要先协商使用的加密算法、密钥、封装技术。

第一步： {43%：两设备间建立安全的管理连接，用作保护加密第二阶段协商过程。}

第二步： {45%：协商安全连接的参数，两设备间形成安全连接。}

接下来就可以使用该安全连接来传输数据。

{44%：阶段一ISAKMP SA提供了后续协商的安全，阶段二IPSec SA协商在第一阶段加密保护下进行，IPSec SA为后续传输数据加密。}

阶段一： 进行ISAKMP SA协商

{45%：1.协商对等体间认证的方式（共享密钥或数字证书）}

2.协商加密使用的算法（DES或3DES等）

3.协商认证使用的算法（MD5或SHA）

4.协商Diffie-Hellman密钥组

{61%：5.协商协商模式（主模式或野蛮模式）}

6.协商SA生存期

阶段二： 进行IPSec SA协商

1.协商双方封装技术（ESP或AH）

2.协商加密算法

3.协商HMAC方式（MD5或SHA）

{68%：4.协商传输模式（传输模式或隧道模式）}

5.协商SA生存期

2.3 XFRM 框架

XFRM是Linux引入的一种基于策略的高扩展性网络安全架构。 在Linux2.6内核中包含了PF_KEY，2.4内核需要打补丁实现。 根据RFC2367的定义，内核PF_KEY实现了安全联

盟(SA)和安全策略(SP)的数据库以及用户空间接口。 {44%：不同系统的SA和SP实现管理不同，在Linux内核中则通过xfrm库来实现。}

IPSec的SP：

SPD用来存放 IPSec哪些流量需要走 IPSec的规则表，表中包含目的 IP，源 IP，执行协议(AH或 ESP或 AH和 ESP并存)， {50%：源端口，目的端口，工作模式(传输模式或隧道模式)。} 当主机有数据通过VPN发出的时候，数据包会根据SPD规则进行匹配，只有匹配到，数据包才会通过AH或ESP处理。

IPSec的SA：

SAD用来存安全信息， SAD数据库中包含的信息有 SPI值，目的端 IP， AH或ESP， AH验证算法， AH验证加密密钥， ESP验证算法， ESP验证加密密钥， ESP加密算法， ESP加密密钥，隧道或传输模式。 SPI索引值是双方用于索引数据库，手动指定或随机生成的一个值。

2.4 DPDK 平台介绍

2.4.1 DPDK简介

DPDK(Data planedevelopment kit)是一个用于处理和加速网络数据包的软件库，相比于传统的Linux操作系统协议栈，DPDK有五个特点：

1.轮询模式处理数据包： 轮训检查是否有数据到达，避免了因为中断导致上下文切换的开销，提升了收发报文的效率。 虽然该方式会导致CPU一直处于满负荷运行，但却很适合处理不间断大量数据包。 当然在特定情况下仍然支持中断。

2.用户态驱动： 传统协议栈在内核态实现，用户态和内核态交换数据需要内存拷贝和系统调用，不必要的消耗很大。 {48%：使用DPDK可以实现用户态驱动，避免了内存拷贝和系统调用。} {43%：但用户需自行实现协议栈对数据进行处理和解析。}

3.独占与亲和性： 为避免不同核间线程的频繁切换，可以指定某个核心的特定任务，保证cache的更高命中率

4.降低访问存开销： 传统协议栈未充分利用cache和内存，使用Hugepage可以降低TLB miss，使用内存多通道交错访问提高内存访问有效带宽

5.软件调优： 数据预取利用了程序的时间和空间局部性原理，软件预先取， cache行对齐及和 burst批量处理多元数据， 可以一次将8个、16个甚至32个报文一次处理，这样可以降低访存次数，提高收发包效率。

2.4.2 DPDK加密加速技术

2.4.3 用户态协议栈

2.5 基于DPDK的高性能IPSec VPN架构设计

2.6 本章小节