

Network Service Optimization with VPP Platform

阿里云 镜清

目标

听完本次演讲后，你将能够：

1. 了解阿里云使用VPP做产品的出发点
2. 了解阿里云对VPP做了哪些选择和优化

目录

1. 概述

1.1 项目背景

1.2 我们的选择和做的工作

2. IP & IPSec分组片

3. Linux Self报文支持

4. 进程间通信

5. IKE问题及解决方案

6. 4G支持

概述 – 项目背景

项目背景

- 实现一款商业的VPN网关 – 智能接入网关
- 简单方便打通线下办公室和线上阿里云
- 加电就上阿里云

需要具备的基本功能

- 支持IKE
- 支持route-based IPSec VPN
- 支持IP转发和VRF
- 有比较高的吞吐能力和比较好的扩展性

概述 – 我们选择和做的工作

我们的基线版本：18.01

- IP & IPSec分组片支持
- Linux self报文支持
- 进程间通信机制
- 专业IKE协商软件和VPP的集成
- 4G支持

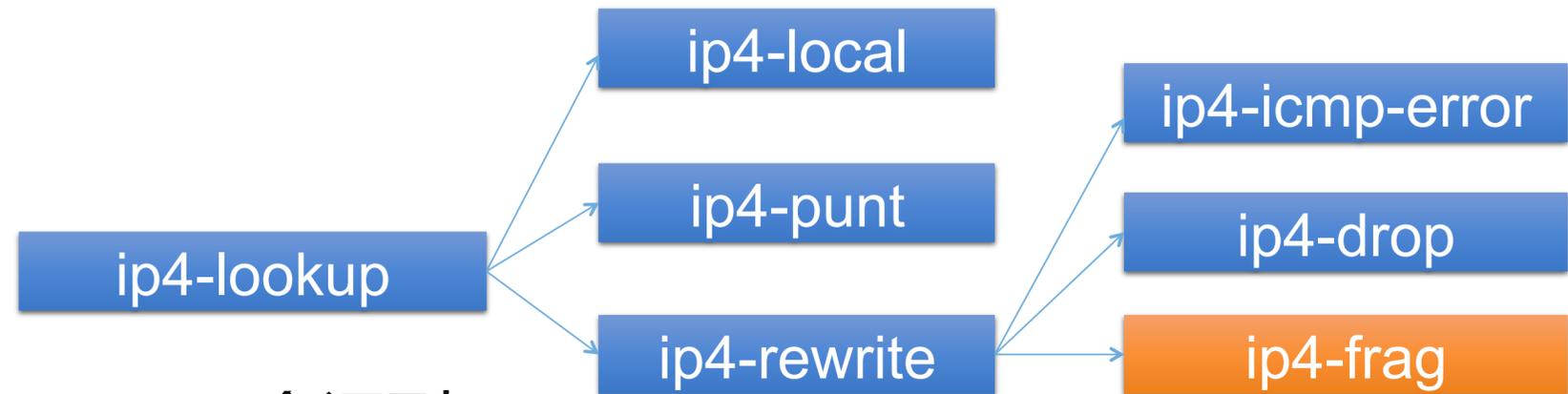
目录

1. 概述
2. IP & IPSec分组片
 - 2.1 IP分组片支持
 - 2.2 IPSec分组片支持
3. Linux Self报文支持
4. 进程间通信
5. IKE问题及解决方案
6. 4G支持

IP & IPSec分片 – IP

IP分片

- VPP 18.01有分片功能，但是只有ip4-map会调到
- 我们在ip4-rewrite node后增加了ip4-frag



IP组片

- 18.01没有通用的组片feature，但是有一个待合并的gerrit
- <https://gerrit.fd.io/r/#/c/9532/>
- 18.04已经合并进来



IP & IPSec分组片 – IPSec

IPSec分片

- 先分片后加密？先加密后分片？

IPSec组片

- 分片报文必须组片后解密，通过IP组片解决
- 多个buffer支持

目录

1. 概述
2. IP & IPSec分组片
3. Linux Self报文支持
 - 3.1 为什么需要支持self报文
 - 3.2 发送和接收self报文
4. 进程间通信
5. IKE问题及解决方案
6. 4G支持

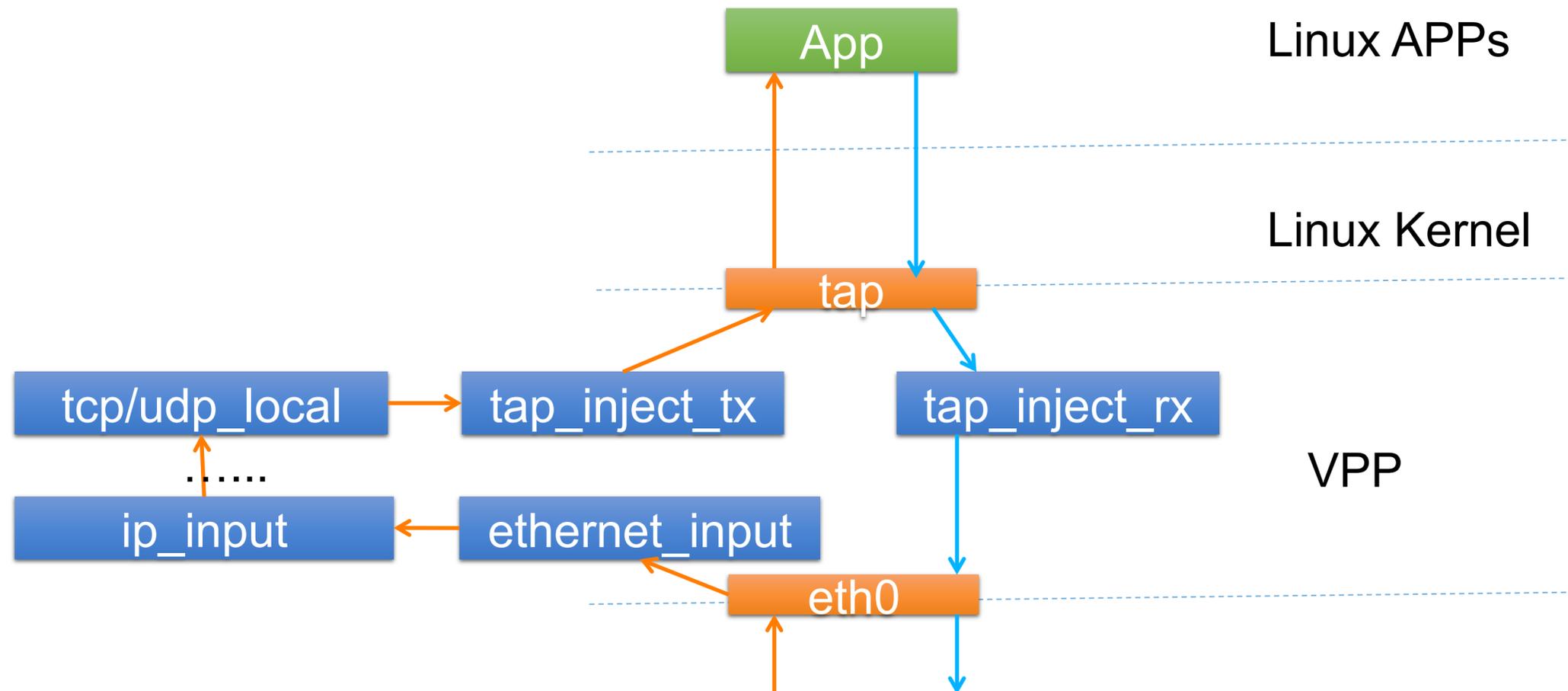
Linux self报文支持

为什么需要支持self报文

- IKE
- 动态路由协议
- DHCP Server
- SSH/Telnet

接收发送self报文

- router plugin(tap-inject)?
- <https://gerrit.fd.io/r/vppsb.git>



目录

1. 概述
2. IP & IPSec分组片
3. Linux Self报文支持
4. 进程间通信
 - 4.1 原因
 - 4.2 如何实现
5. IKE问题及解决方案
6. 4G支持

进程间通信

原因

- VPP和其他应用比如IKED、agent之间需要信息同步
- IKED和Agent之间也需要信息同步

解决方案

- unix socket/netlink
- TIPC/nanomsg

目录

1. 概述
2. IP & IPSec分组片
3. Linux Self报文支持
4. 进程间通信
5. IKE问题及解决方案
 - 5.1 VPP IKE问题
 - 5.2 我们的解决方案
6. 4G支持

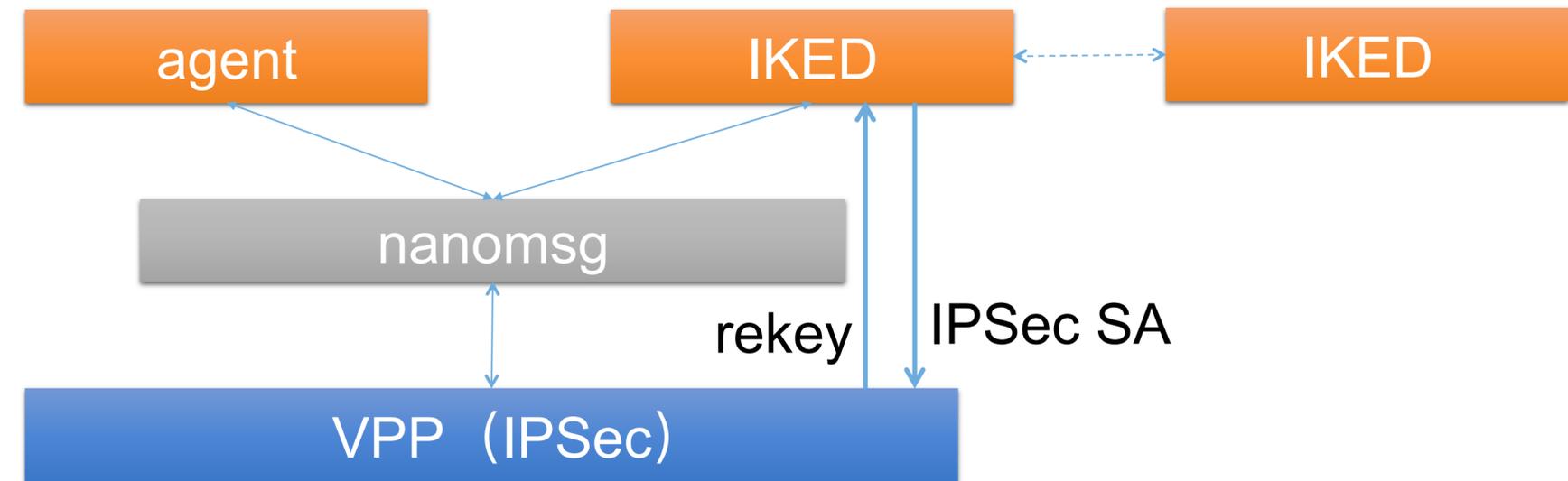
VPP IKE问题

VPP IKE的问题

- 只支持IKEv2
- 只支持IKEv2的responder
- VPP也不适合集成复杂的IKE协商过程

解决方案

- 用专门的IKE软件做协商 – strongswan、freeswan or others
- 协商后通过API把密钥注入到VPP中
- ipsec接口index在VPP、IKED和agent之间同步



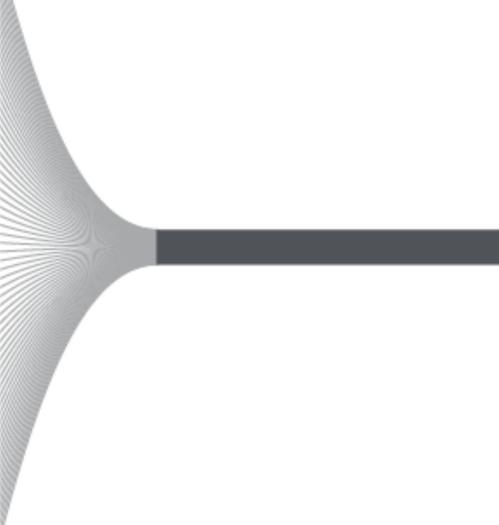
目录

1. 概述
2. IP & IPSec分组片
3. Linux Self报文支持
4. 进程间通信
5. IKE问题及解决方案
6. 4G支持
 - 6.1 解决方案

4G支持

解决方案

- AF_PACKET
 - VPP已经支持
 - 性能一般
- 支持DPDK的驱动
 - 改动难度大
 - 性能比较高



各位小伙伴，我们在招人

欢迎加入阿里云，一起玩转VPP

简历投递到：jingqing.cjy@alibaba-inc.com

为了无法计算的价值 |  阿里云

