



主动防御的网络安全探讨

盛科网络

网络5.0 产业和技术创新工程

网络安全方向的探讨

盛科交换芯片安全特性积
累

交换网络解决方案整体架构

网络解决方案是支撑信息网、视频、语音、WEB服务等网络业务的核心组件
随着SDN技术变革，网络解决方案清晰的形成了芯片，交换机和控制器三个层次

编排器
控制器



交换机NOS
交换机硬件



SDN
交换芯片



SDN交换芯片

- 负责业务流量线速转发
- 卸载大量虚拟化和安全业务功能

交换机软硬件

- 交换硬件核心芯片是交换芯片和CPU
- 交换机NOS运行控制和管理协议，南向管理交换芯片，北向对接控制器

控制器和编排器

- 控制器是网络业务集中式的大脑，对交换机以及交换芯片进行控制
- 编排器灵活的进行业务的管理和调度

被动防御技术难以对抗网络攻击的多变性

网络攻击目标多变

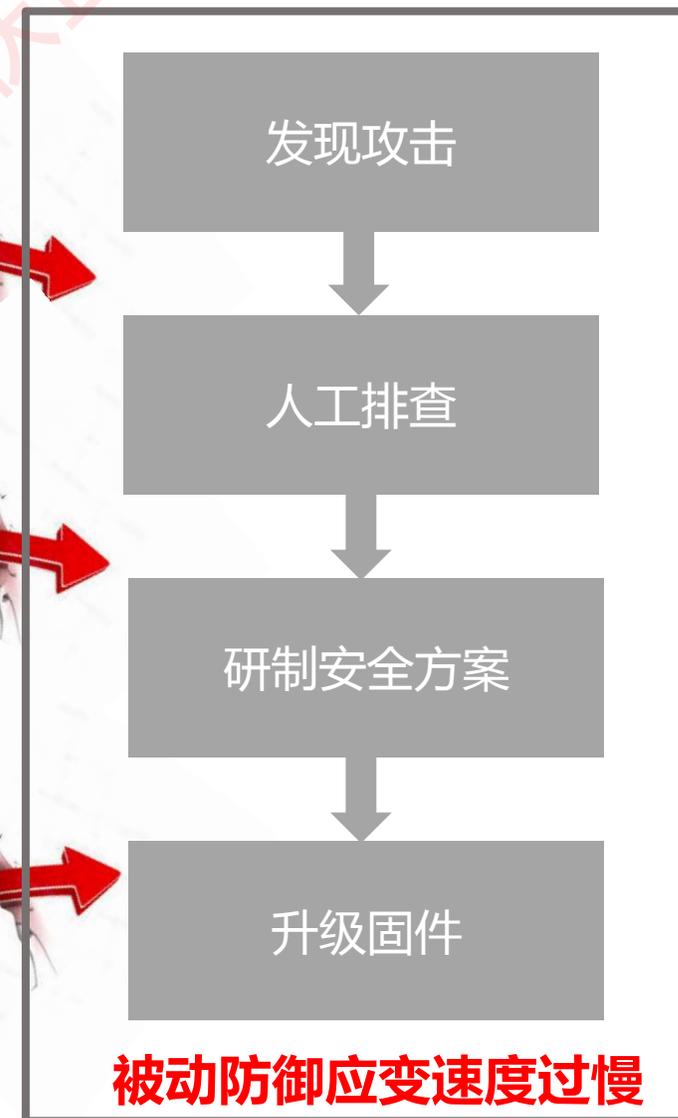
- 网络应用、网络解决方案、用户终端都是可能的被攻击的目标对象

网络攻击目的多变

- 针对不同的目标对象，存在多种攻击目的，包括攻击目标瘫痪、盗取数据信息、伪造终端或者业务等

网络攻击方法多变

- 网络攻击的方法也具备多变性，包括伪造报文，篡改报文，修改网络设备配置等





主动防御技术动态应对多样网络攻击

网络攻击目标多变

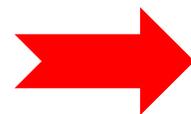
- 网络应用、网络解决方案、用户终端都是可能的被攻击的目标对象

网络攻击目的多变

- 针对不同的目标对象，存在多种攻击目的，包括攻击目标瘫痪、盗取数据信息、伪造终端或者业务等

网络攻击方法多变

- 网络攻击的方法也具备多变性，包括伪造报文，篡改报文，修改网络设备配置等



交换芯片实时可视化
转发行为、状态

攻击模式识别

SDN的方式下发
安全策略

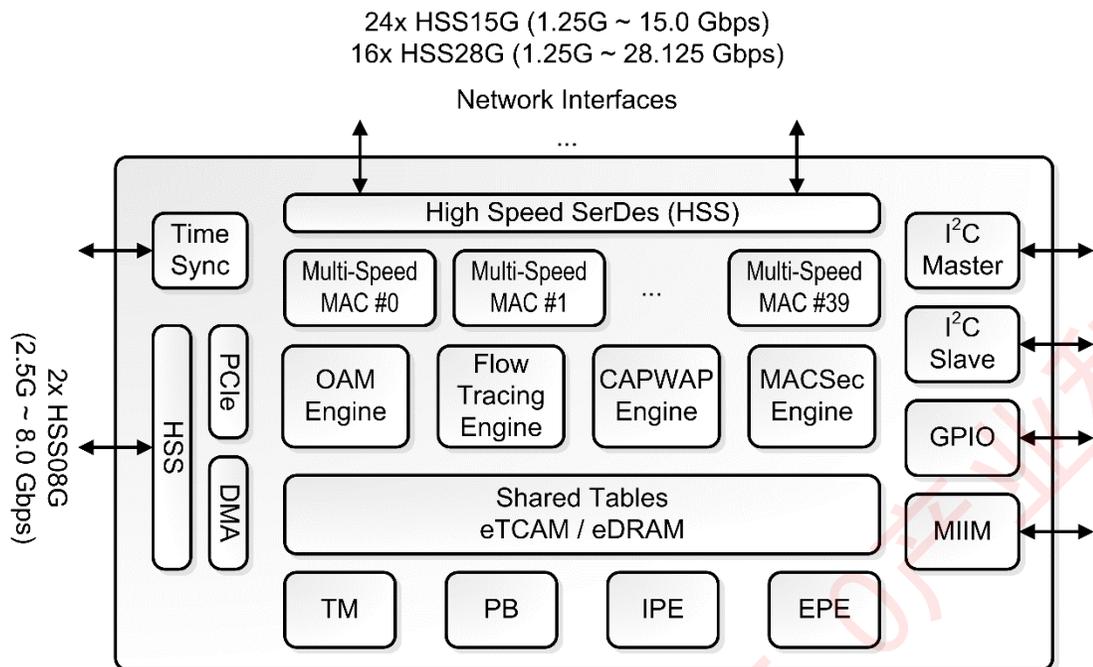
动态加载策略

主动防御实时、高效

主动防御技术背景介绍

交换芯片主动安全特性

交换芯片积累丰富的安全特性



Network SerDes Compliance:
SGMII/ QSGMII/ USXGMII-M/ XFI/ SFI/ 10G-KR/ 40G-KR4/ 100G-KR4/
25G-KR/ 50G-KR2

传统安全特性

- 有线业务的硬件ASE128/256加解
- 无线业务的DTLS加解密度
- 协议报文防攻击技术
- 集成ARM交换芯片支持TrustZone

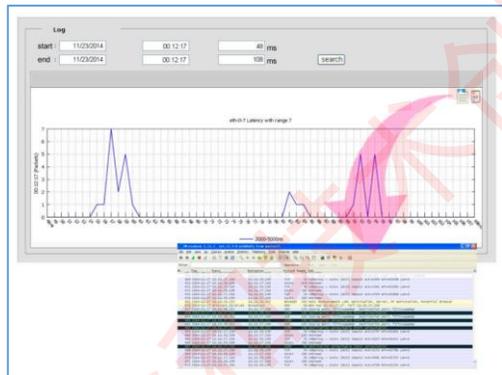
主动防御技术

- 芯片缓存状态可视化
- 芯片会话状态可视化
- 芯片级别大象流识别功能
- 拟态安全认证功能
- SDN灵活的业务流水线
- 基于大象流和老鼠流的动态策略

主动防御特性 – 发现攻击阶段



动态安全防御需要具备动态分析网络流量转发的行为,状态的能力为后续判断是否出现网络攻击提供基础



交换芯片状态监控
基于端口，芯片全局的缓存和时延监控



交换芯片流量会话监控
Netflow功能，基于会话的粒度对报文转发行为状态进行监控

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
|----- globalSrcPort[15:0] |----- residenceTime[47:32] |-----| |
|----- residenceTime[31:0] |-----|
|----- timestamp[63:32] |-----|
|0|X|----- timestamp[29:0] |-----|
```

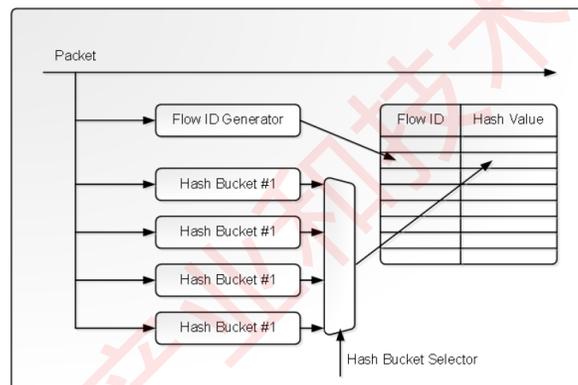
交换芯片报文监控
逐跳叠加报文添加ERSPAN header，包含时间戳，交换机ID，源端口，时延等信息，发送至远端的分析服务器



主动防御特性 – 攻击模式识别阶段

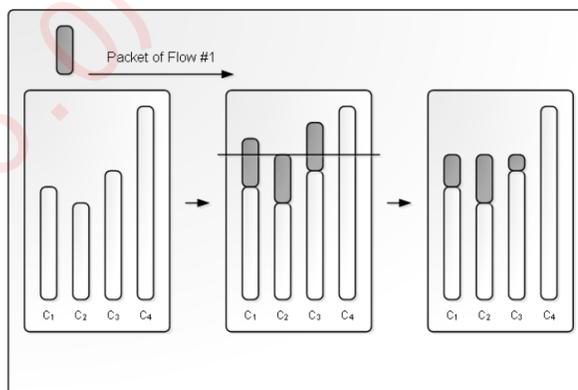


- 控制器和编排器可以通过可视化得到的数据进行分析，通过病毒库训练，人工智能学习等方式识别攻击流量
- 交换芯片也集成了部分模式识别能力，可以自主识别可能的DDoS流量攻击



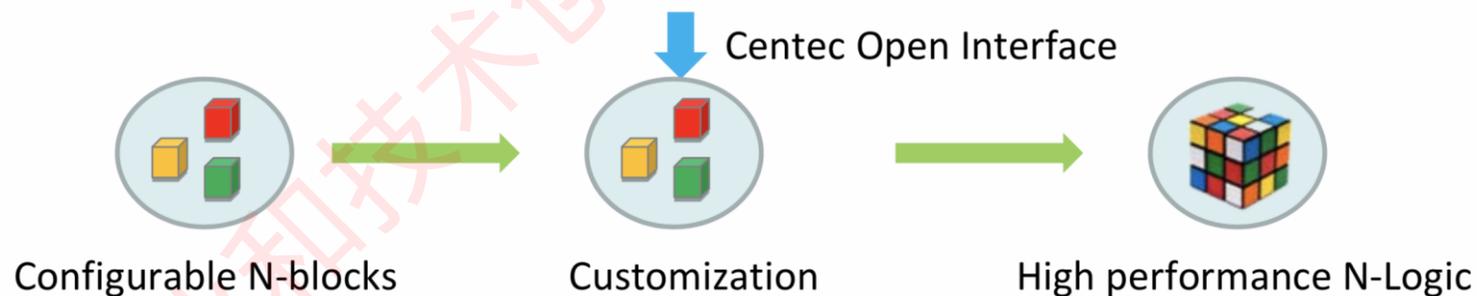
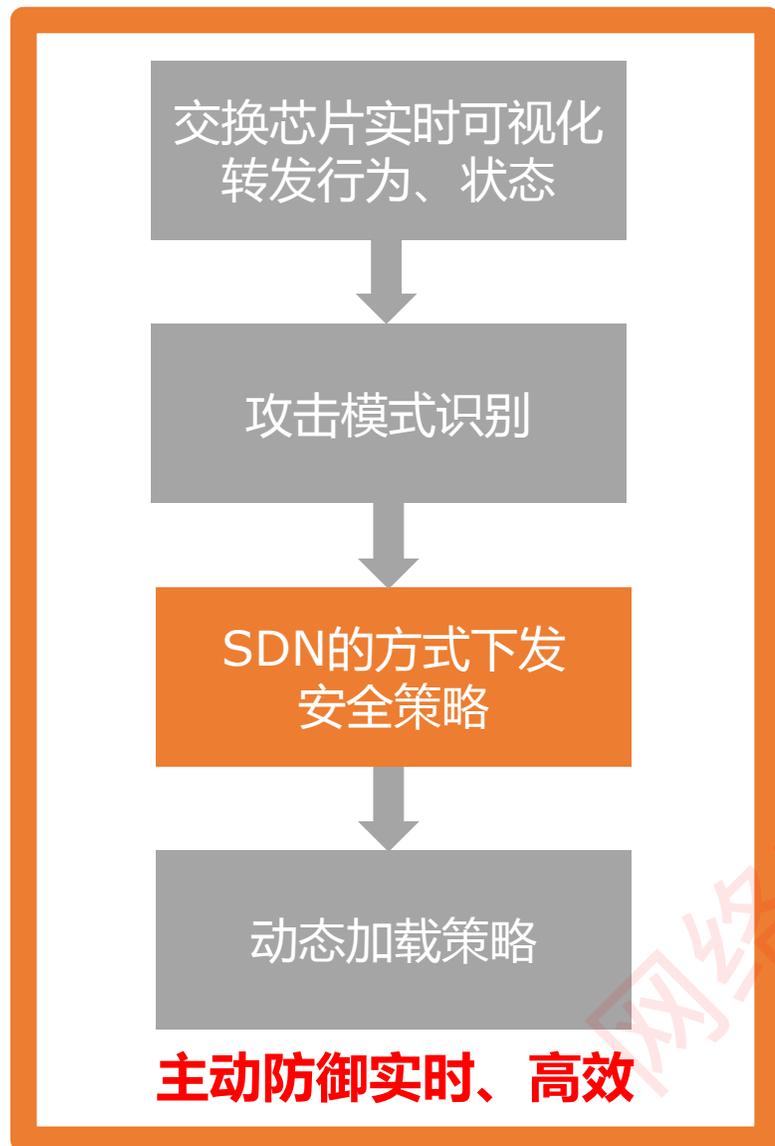
交换芯片大象流识别算法

- 大象流在芯片中指定直接内报文字节达到阈值的特征流
- 比如某一流量10s内超过200M，可以被芯片的大象流匹配



盛科芯片可以将匹配的异常大象流通过交换机NOS送至控制编码器，进一步确认是否为攻击流量

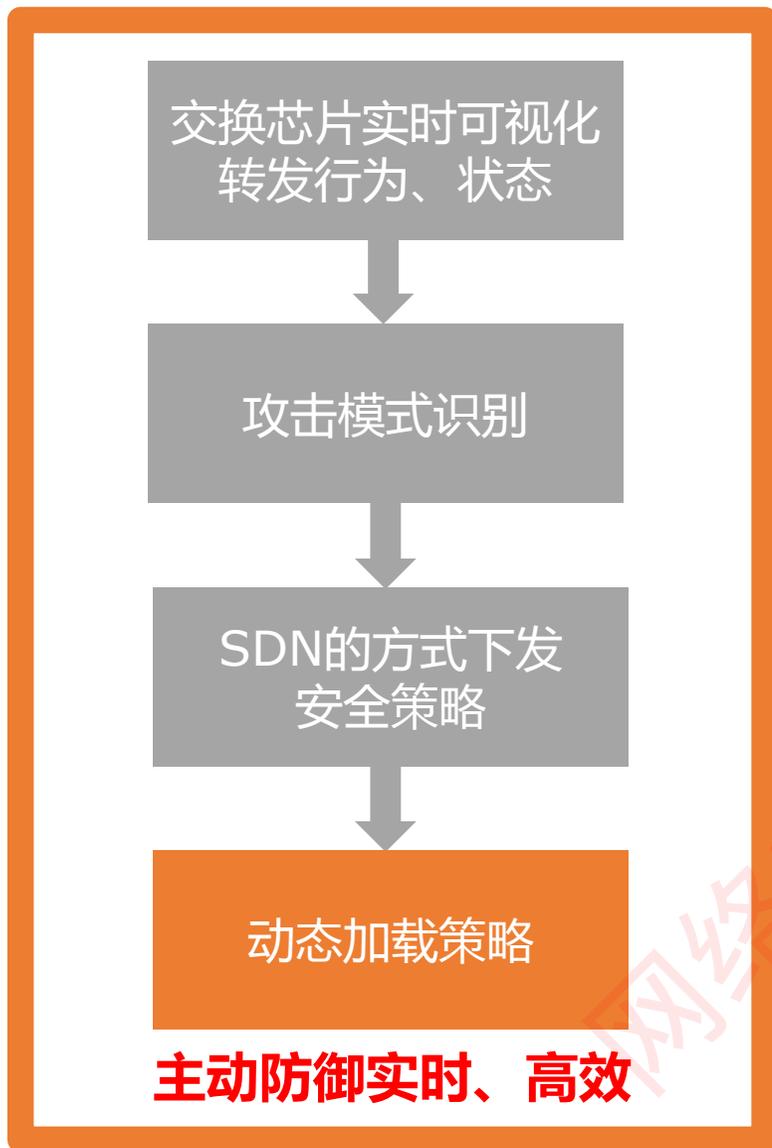
主动防御特性 – 形成安全策略阶段



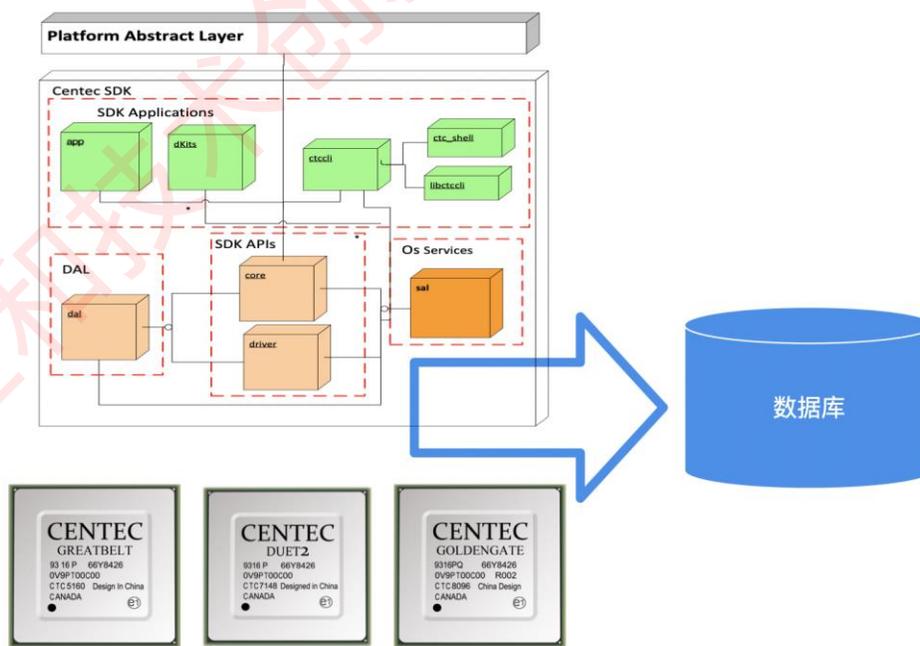
交换芯片N-Flow技术

SDN芯片流水线具备非常强的灵活性，并提供Openflow，NetConf的开放的SDN配置接口，为控制器、编排器提供可编程能力

主动防御特性 - 安全策略加载阶段



- 大部分安全策略可以通过流策略的方式动态下发
- 还有一部分安全策略的加载需要交换机软件进行升级



交换芯片Warm-reboot技术

将SDK和芯片的状态实时同步到数据库，NOS重启后交换芯片进行复位，继续转发，可以实现动态不断流的方式进行NOS升级

基于交换芯片的主动防御总结



交换芯片主动防御特性





THANK YOU

Centec Networks (Suzhou) Co., Ltd.

Website: www.centecnetworks.com

Tel: 86-512-62885358

Email: sales@centecnetworks.com