安全系统架构设计

一、安全系统概述

1.1 网络攻击理解

任何一种攻击都是带有目的性或者价值性，在这里倾向于将主流网络攻击分为“打”、“骗”，“偷”。

- 打（让系统不能提供服务，进行勒索）：DDOS攻击将服务器带宽打满，CC攻击将服务器资源打尽等。
- 骗（骗取用户信息）：DNS缓存偷毒将域名解析到钓鱼网站，CSRF使用COOKIE模拟正常用户操作等。
- 偷（偷取有价值信息）：中马后隐蔽隧道传输机密文件，SQL注入后窃取数据库数据等。

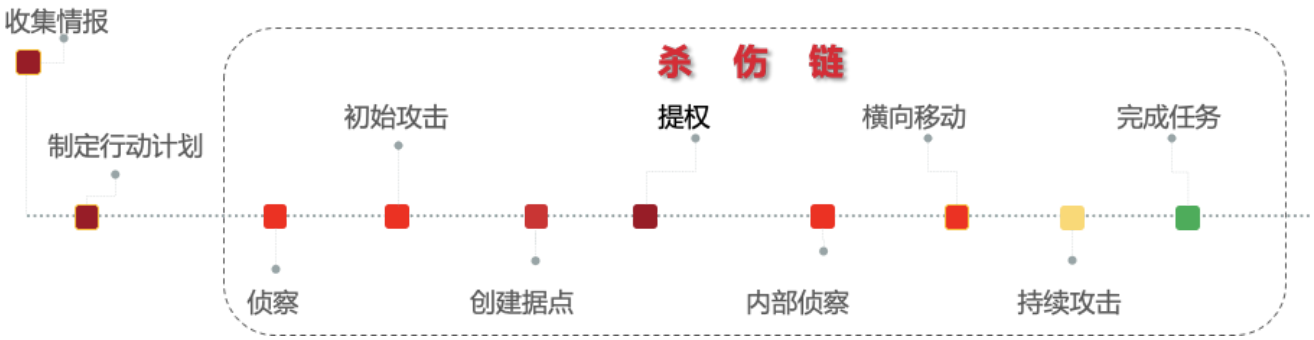
1.2 攻击过程

干活就得有工具，过程要能流程化，完活还要看产出，最后还得能复盘，所以这里以这几部分为维度进行简单描述。

1、工具：（黑客资产）

2、产出：（目标资产）

3、拿一次完整的窃取商业资料的攻击过程为例进行各阶段说明：



1.收集情报：收集情报是一个常态化工作，根据特定任务集中管理相关情报信息；

2.制定行动计划:确定任务目标，配置木马、阵地、漏洞等攻击资产

3.侦察：收集凭证、测绘可访问网络、扫描设备;

4.初始攻击:在应用数据文件中添加可利用点、建立跳板、预置载荷，利用漏洞进行攻击;

5.创建据点：利用初始攻击成果建立据点，进程隐藏、网络连接隐藏、文件隐藏；

6.提权：利用操作系统漏洞，获取令牌、修改安全策略、获取权限；

7.内部侦察：获取系统信息、获取网络信息、枚举账号和权限、枚举文件系统、枚举操作系统和软件、枚举进程、测绘可访问网络、嗅探网络；

8.横向移动：端口映射、内网渗透、网络嗅探、远程执行、摆渡攻击、创建用户；

9.持续攻击：键盘记录、下载执行、系统密码窃取、数据加密打包、网络通信回传、文件窃取、账号窃取、流量隐藏、固件植入、传回目标资产

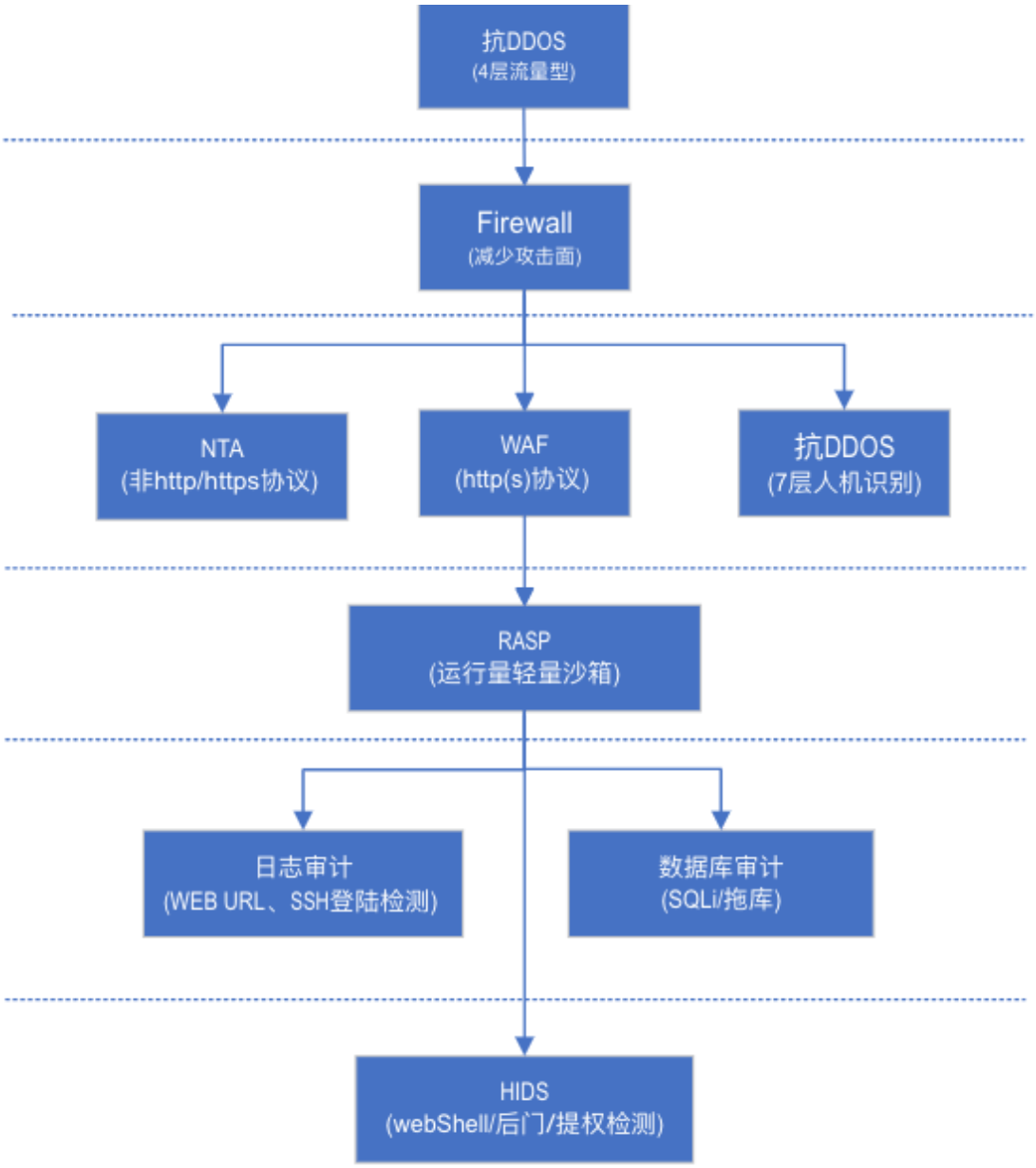
10.完成任务：清理痕迹；

1.3网络安全防御

魔高一尺，道高一丈，有攻就有防，所以催生了很多种类网络安全设备。

单一的网络安全设备可能只对某些类型的攻击有效，所以目前企业级的安全，需要各种网络安全设备进行有效组合和联动来达成防御的目的。

下图是从抽象的纯视角进行展示：



1、对于企业的生产网络而言，最外围的威胁主要包括：4层flood+链路劫持。对应最外层的主要防御手段是抗DDOS。来保证后续的所有网络安全设备能正常工作。

2、抗之后的第一道防御模型是快速收敛入口，减小攻击面，通常的手段是4层，5元组ACL过滤或利用服务的反向代理只对外开放 80，443等主要服务端口，这里主要是防火墙的功能。

3、在4层协议过滤之后，攻防模型进入第7层应用层协议对抗，

1）HTTP(S)协议，防御手段是WAF；

2）非HTTP(S)协议，主要使用NTA做全流量分析（如果没有部署WAF，NTA也支持HTTP协议分析）

3）应用层flood攻击，CC攻击等，使用7层的抗做人机识别的源认证。

4、在7层协议的后面是应用代码的运行时状态检测，在比较大规模的生产环境中，一般以检测为主，在小规模环境下可以采取相对重度的方式用模块检测OWASP TOP 10（注入、失效的身份认证、敏感数据泄露、XXE、失效的访问控制、安全配置错误、XSS、不安全的反序列化、使用含有已知漏洞的组件、不足的日志记录和监控）中适合本企业的模型进行检测。

5、再往后的攻击模型，介于应用层攻击到系统层攻击之间，包括：直达的恶意攻击、暴力破解，直接调用系统命令但仍未获得完全系统权限的指令执行，对应的防御模型抽象为数据库审计、日志审计。

6、在攻击链的末端，最后一层攻击模型是获取系统权限，防御者模型则是检测提权和rootkit，对应的解决方案通常是HIDS。

同时国家也出台了网络安全保护2.0规范（简称等保2.0），信息系统以及基础设置，2级以上都需要经过等保测评才能对外开放，所以可见网络安全越来越受到国家层面的重视。

信息系统安全等级保护的定级准则和等级划分			
等保等级	备案	适用信息系统及行业	信息系统破坏后侵害程度
第一级（自主保护级）	无需备案，对测评周期无要求。	一般适用于小型私营、个体企业、中小学，乡镇所属信息系统、县级单位中一般的信息统。	信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成一般损害，但不损害国家安全、社会秩序和公共利益。
第二级（指导保护级）	公安部门备案，建议两年测评一次。	一般适用于县级其些单位中的重要信息系统；地市级以上国家机关、企事业单位内部一般的信息系统。例如非涉及工作秘密、商业秘密、敏感信息的办公系统和管理系统等。	信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成一般损害，但不损害国家安全。
第三级（监督保护级）	公安部门备案，要求每年测评一次。	一般适用于地市级以上国家机关、企业、事业单位内部重要的信息系统，例如涉及工作秘密、商业秘密、敏感信息的办公系统和管理系统；跨省或全国联网运行的用于生产、调度、管理、指挥、作业、控制等方面的重要信息系统以及这类系统在省、地市的分支系统；中央各部委、省（区、市）门户网站和重要网站；跨省连接的网络系统等。	信息系统受到破坏后，会对国家安全、社会秩序造成损害，对公共利益造成严重损害，对公民、法人和其他组织的合法权益造成特别严重的损害。
第四级（强制保护级）	公安部门备案，要求半年一次。	一般适用于国家重要领域、重要部门中的特别重要系统以及核心系统。例如电力、电信、广电、铁路、民航、银行、税务等重要、部门的生产、调度、指挥等涉及国家安全、国	信息系统受到破坏后，会对国家安全造成严重损害，对社会秩序、公共利益造成特别严重损害。

		计民生的核心系统。	
第五级（专控保护级）	公安部门备案，依据特殊安全需求进行。	一般适用于国家重要领域、重要部门中的极端重要系统。	信息系统受到破坏后，会对国家安全造成特别严重损害。

二、业务、工程和技术的折衷

2.1 业务优先

很多人问过一个问题，“既然是纵深防御，好像检测告警居多，而防护的部分比较少”，这确实是目前大型安全体系的现状。因为安全手段要适应业务，必须有所妥协，而不能只以安全效果最大化来衡量。所以本着为业务让路的原则，最后就变成检测手段很多，阻断手段一般不轻易用。所以在很多场景下大型互联网公司阻断的安全手段就变成了WAF。

客观一点说，如果熟悉甲方的安全建设，阻断也并不只有WAF这个单一的角色，所谓防护是由一系列手段叠加后的效果。

2.2 工程裁剪

上述1.4介绍的“全套”设计对于大多数场景而言还是太贵了，在业务规模和安全投入没有达到理想化水平之前，需要做一些妥协和裁剪，但是这种裁剪还是要追求有限安全总投入（钱、人员编制，内部支撑团队）水平下的最大安全效果。

裁剪最大的决定因子是：IDC规模，因为它决定安全的总投入，极端一点说：

- 小的网站弄个modsecurity或naxsi，装个OSSEC就完事了，哪还用得着这么复杂。
- 大的机房例如AWS云，安全手段和措施多么复杂都是有必要的。

裁剪的另一个决定因子是：业务类型，因为他决定哪些网络能力需要重点建设，极端一点说：

- 如果业务流量几乎全部都是http(s)，那么应该重点投入WAF的。
- 如果业务中含有大量非HTTP协议的标准协议，则应该重点建设NTA。
- 如果消息接口、远程过程调用、数据缓存和持久化中私有协议占多数，则应该重点建设HIDS。

无论如何追求性价比的裁剪，在生产网络的安全管理中，都必须有一个安全底线：

- 保证正常用户可以访问服务。
- 保证恶意攻击者不能随意操纵数据户和用户数据。
- 保证敏感数据不能随意外传出去。

2.3 技术考虑

1、在系统设计中，需要考虑高内聚低耦合，通用的方式为：

同时还需要考虑6种设计约束，以及3大类23种设计模式（因为我们设计系统需要尽可能的复用，以及方便后期的功能扩展和他人维护）。

2、单一网络安全系统的通用设计分为：

- 流量捕获：这个是所有处理的前提，作为输入源，对于网络层大流量检测设备一般会使用DPDK或者pfring的方式来提高性能。
- 规则：例如DDOS的4层flood攻击是基于统计规则，防火墙是基于ACL/黑名名单规则，NTA/WAF的检测是基于攻击特征库和攻击行为建模、7层抗D是基于协议交互模型、RASP是基于安全保护代码嵌入、日志审计和数据库审计是基于用户行为规则，HIDS是基于快照/异常检查/入侵检测规则。
- 动作：对于疑似攻击的流量研判的动作，作为输出结果，通常分为：告警（提示当时访问有安全问题）、阻断（禁止当前用户访问）、加入黑名单（对于源IP的访问按照3元组或者5元组在一定时间内全部禁止。）。

3、系统设计需要同步考虑3个主要要素：

- 算法：采用何种算法可以使得我们设计的系统准确性和性能达到极限.

  在程序设计中，提升准确性：

  a. 如何保证重点流量重点检测：引入IP信誉机制
  b. 如何保证自定义端口协议的检测（例如把http端口定义成8888）：引入端口学习机制
  c. 如何保证正则匹配的准确性：引入hyperscan匹配机制
  d. 如何保证规则的准确性：引入运营数据分析加白机制
  e. 如何保证DDOS阈值的准确性：引入动态基线学习机制
  f. ……

在程序设计中，提升性能：

a. 如何无锁化：采用RSS分流、RTC运行模式、CAS无锁队列，每个核心一个数据副本。
b. 如何减少TLB MISS：采用大页内存
c. 如何保证cache命中率最高：采用cacheline对齐机制、prefetch预取机制。
d. 如何保证内存访问效率最高：采用NUMA本地内存机制
e. 如何保证CPU的效率充分利用：采用向量编程机制充分利用流水线原理。
f. ……

- 算力：评估采用物理机或云主机的CPU资源，内存资源，IO资源等。
  a. 如何保证在有限的资源下，进行全流量检测：引入黑白名单机制。
  b. 如何适应低IO强计算的场景：打开CPU超线程。
  c. 如何让每个CPU单独跑一个线程，不接受系统调度：使用CPU亲和性以及CPU隔离技术。
  d. 如何保证每个CPU尽量跑满：区分快慢流程，根据比例分配算力资源。
  e. 如何保证没有NUMA MISS：每个NUMA节点下有一份内存拷贝。
  f. ……
- 算据：既我们要处理的数据，需要先评估业务模型得出数据模型。
  a. 网络层IPV4、IPV6的流量占比？
  b. 传输层TCP/UDP/ICMP流量占比？
  c. 应用层http/https/dns/其它协议流量占比？
  d. 外部客户访问字节流量/字节主动外连流量/字节内部通信的流量占比？
  e. 同一个会话的来回数据是否在网络中能hash到同一个网口？
  f. ……

三、设计的例子

在第3节课已经讲过WAF系统的搭建，这里我们以NTA为例简述安全系统设计。

3.1NTA目标

监控字节内部机房的网络质量，尽可能发现网络层次的攻击，敏感数据是否会被泄漏。

3.2业务方

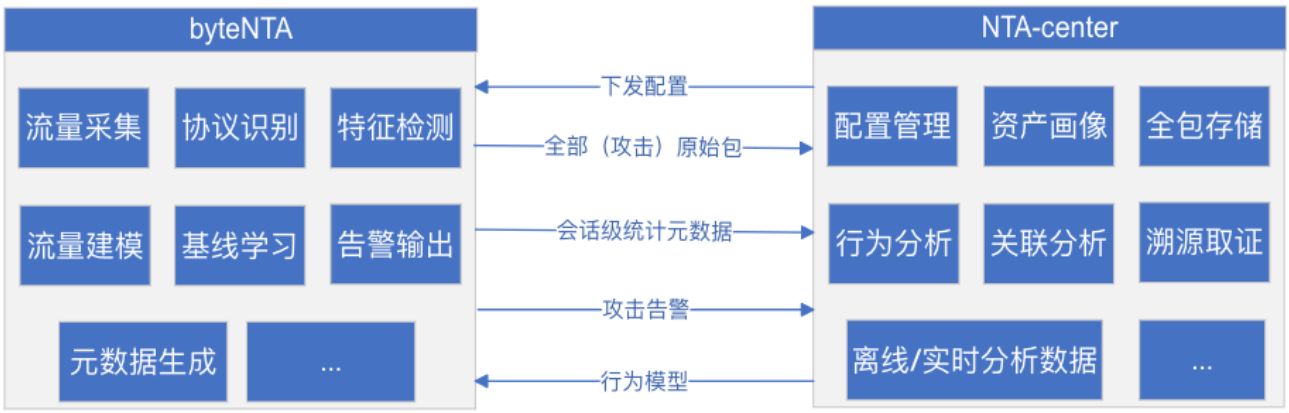
需要和字节内部其它服务共享资源，在发现攻击，根据研判是告警还是阻断。

3.3工程

部署在字节所有机房的入口处，整体流量每秒超过10T，需要考虑高性能。

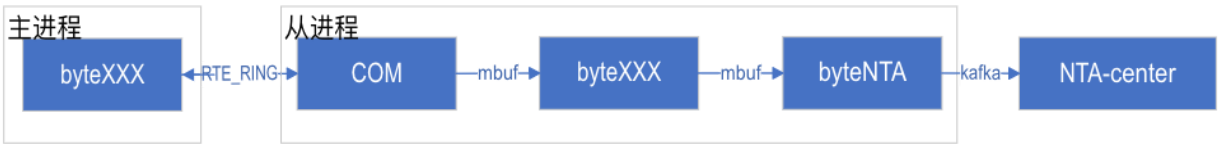
3.4技术架构设计

1、逻辑架构：

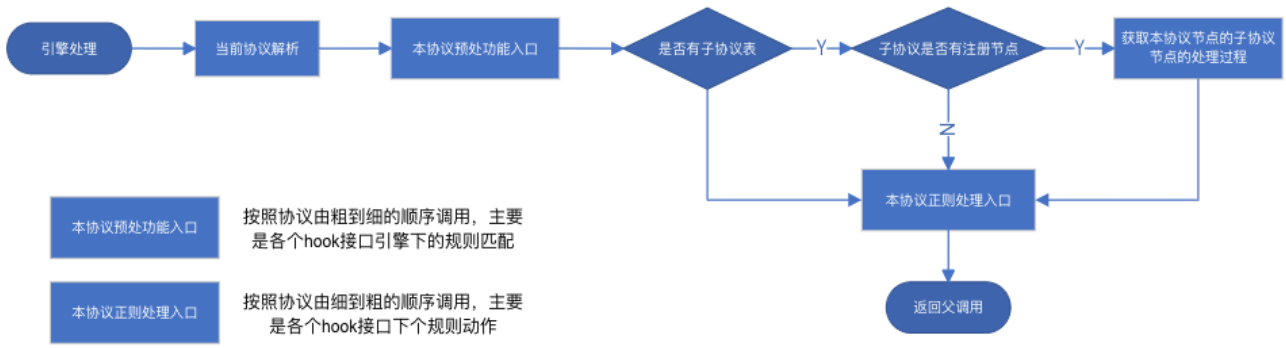


- 模块划分：前端探针(byteNTA)+后端管理平台（NTA-CENTER）。
- 接口定义：配置接口，原始包发送接口，统计元数据下发接口，攻击告警接口，行为模型接口
- 领域模型：规则检测、正常行为模型检测（流量基线学习），恶意行为模型检测（恶意邮件检测、病毒文件检测、隐匿通道检测等）

2、开发架构：

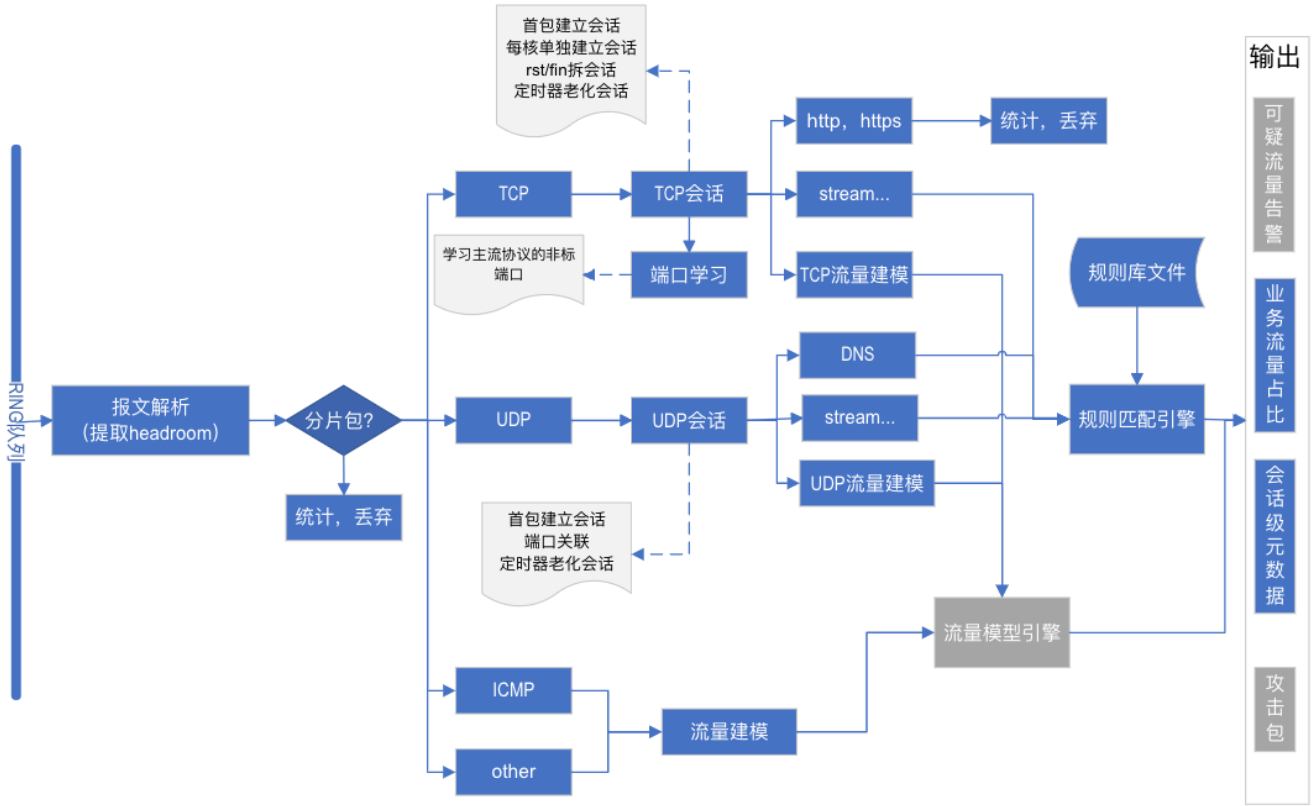


引擎架构（专利2017109922003）：使得每个协议不需要关注自己何时被调用，以及可以根据业务调整动态注册和反注册



- 技术选型：使用DPDK主从进程模型，因为和业务方进行配合，所以需要两者耦合性低。
- 文件划分：COM子目录（流量收发、协议解码、会话处理），引擎子目录（hyperscan正则匹配和回调处理），proto子目录（应用层协议解码子目录），detect（模型检测子目录）、rules（规则库子目录）、output（输出子目录）等。
- 编译关系：所有依赖库使用动态连接库，依赖DPDK驱动和网卡驱动，databus发送库，区分DEBUG版和发布版。

3、运行架构：



技术选型：使用无锁队列（RTE_RING进行传递），正则匹配使用hyperscan，规则语法采用snort语法，开发语言为探针端C语言，发送agent端go语言，探针和agent交互采用本机unix socket，agent发送采用databus进行发送。

控制流划分：分为输入：（根据业务模型，分片包不处理，传输层采用TCP、UDP、ICMP建立会话），处理（因性能需求，对每条会话前N个包进行基于规则的攻击检测，对于不同协议进行不同的流量建模，来发现隐蔽隧道，DGA域名等攻击行为），输出（告警信息，业务流量占比，取证信息，元数据信息）。

同步关系：前端采用RSS分流，RING队列采用多生产者单消费者，每个核采用RTC的方式独占核运行（为不使用锁放弃核间交互），数据发送由所有数据核上报的管理核，进行统一发送。

4、物理架构：

硬件分布：在核心机房入口交换机通过分光，将流量全部拉取一份。

软件部署：每个网卡处理单独一个进程，每个进程根据硬件配置启动多个线程，达到内存最优的NUMA命中和CACHE命中。

方案优化：网卡多队列机制，实现（CPU-网口-队列-内存）的唯一绑定。

5、数据架构：

技术选型：采用hive存储，数据存储有效周期30天，存储容量1PB。

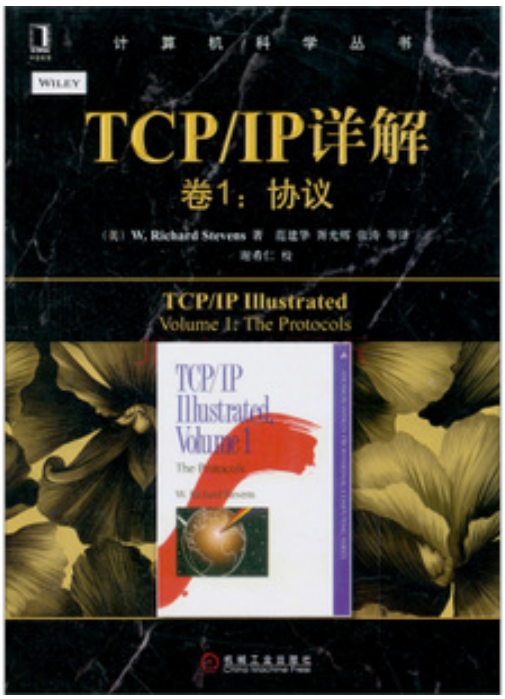
存储格式：采用prototbuf进行压缩，存储分为流量数据，会话元数据，告警数据，原始报文数据等，在运营时候进行关联生成宽表。

数据分布：每个机房单独上报数据，做整个机房数据的汇总。

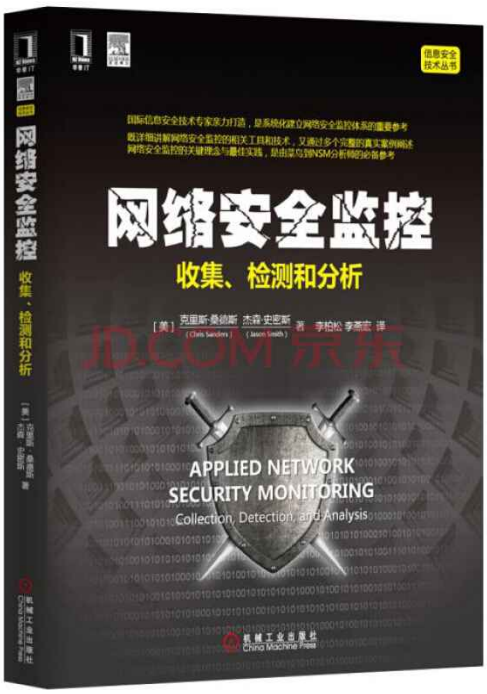
四、推荐信息

书籍：

1、《TCP/IP详解 卷1：协议》



2、《网络安全监控：收集、检测和分析》



网站：

- http://www.modsecurity.cn/
- https://www.hyperscan.io/
- http://dpdk.org

五、后纪：

上面简要叙述了安全系统架构设计的一些基础，下面我想用以前给架构师做培训时候总结出来的职责、能力和问题来结束本期的课程。

- 架构师职责：

  1.架构师需要根据业务需求所定制的合理且可落地的技术规范，

  2.指导落地软技能管理&&制定规范硬技能技术。

- 架构师的7种必备基础能力：

  1.开发能力

  2.架构能力

3.运维能力

4.沟通能力

5.行业业务理解深度

6.管理能力

7.学习能力

- 是否适合做架构师6问?

  1.喜爱技术有技术情怀吗?

  2.精通设计模式吗?

  3.对公司业务感兴趣吗?

  4.能带领技术团队吗?

  5.文档写的漂亮吗?

  6.自信吗?