



网络与系统安全

第七章 网络与系统防御

第四节 蜜罐

黄 玮

中国传媒大学



- 信息安全的本质——持续对抗
 - 网络渗透与系统入侵
 - VS.
 - 防火墙
 - 入侵检测
 - 应用程序安全加固
- 持续对抗的双方是**非对称**的对抗



- 工作量不对称

- 攻击方：夜深人静，节假日，攻其不备

- 防守方：24*7, 全面防护，木桶原理

- 信息不对称

- 攻击方：通过信息收集、网络扫描、探测、踩点对攻击目标全面了解

- 防守方：对攻击方一无所知

- 后果不对称

- 攻击方：任务失败，极少受到损失

- 防守方：安全机制被突破，资产损失，其他影响



- 使用蜜罐和蜜网来扭转对抗不对称局面
 - 扭转工作量不对称
 - 增加攻击成本—假目标
 - 扭转信息不对称—了解你的敌人!
 - 他们是谁?
 - 他们使用什么工具? 如何操作?
 - 为什么攻击你?
 - 扭转后果不对称
 - 防守方避免资产损失和其他影响
 - 计算机取证—对攻击方的威慑



本章内容提要

- 蜜罐发展史
- 蜜罐关键技术
- 蜜网技术
- 蜜罐与蜜网技术的应用



本章内容提要

- 蜜罐发展史
- 蜜罐关键技术
- 蜜网技术
- 蜜罐与蜜网技术的应用

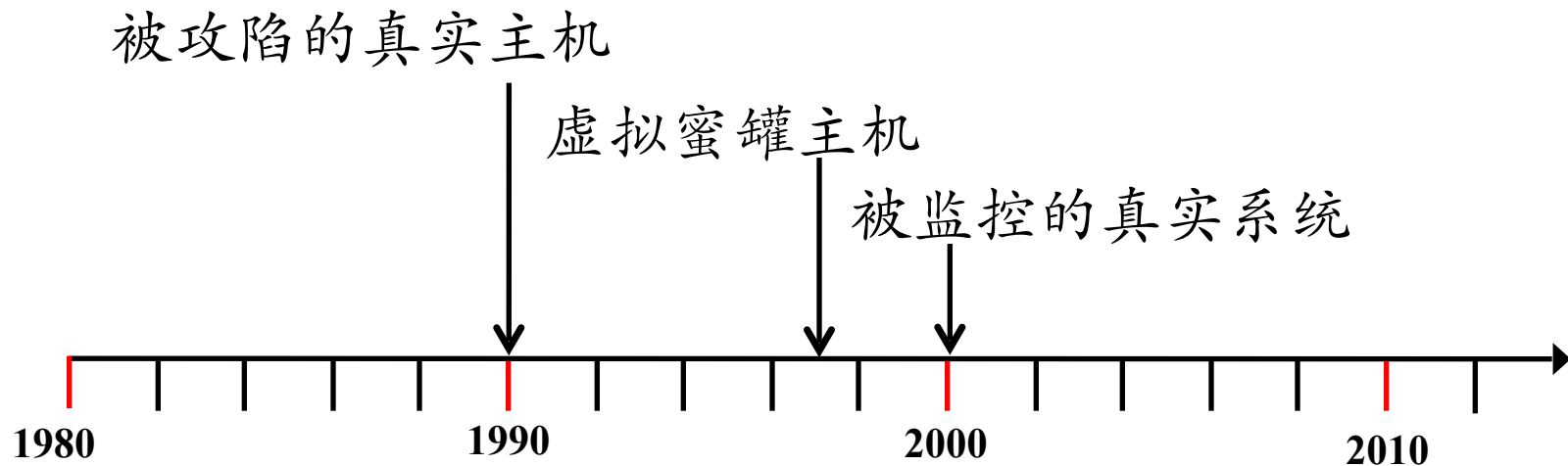


蜜罐的概念

- Honeypot
 - 首次出现在Cliff Stoll的小说“The Cuckoo’s Egg”(1990)
- 蜜网项目组给出如下定义（价值/意义）：
 - “A security resource who’s value lies in being probed, attacked or compromised”
 - 没有业务上的用途
 - 所有流入/流出蜜罐的流量都预示着扫描、攻击及攻陷
 - 用以监视、检测和分析攻击



蜜罐技术的发展历史



- 1990: << The Cuckoo's Egg >>
- 1997: Fred Cohen: DTK
—模拟网络服务，虚拟系统
- 2000: 蜜网项目组: Gen II蜜网



蜜罐的分类(1/2)

- 部署目标
 - 产品型
 - 研究型
- 交互性：攻击者在蜜罐中活动的交互性级别
 - 低交互型
 - 高交互型
 - 混合型



蜜罐的分类(2/2)

- 新型蜜罐
 - 主动式蜜罐
 - honeyfarm
 - honeytoken
 - honeyapp
 - honeyclient



产品型蜜罐

- 部署目标: 保护单位网络
 - 防御
 - 检测
 - 帮助对攻击的响应
- 需要网管尽可能少的工作
- 商业产品
 - KFSensor, Specter, ManTrap



- 部署目标：对黑客攻击进行捕获和分析
 - 这些“坏家伙”在干什么
 - 了解攻击方法
 - 捕获他们的击键记录
 - 捕获他们的攻击工具
 - 监控他们的会话
- 需要大量时间和精力投入！！
- 实例：Gen II蜜网, Honeyd



低交互型蜜罐

- 模拟服务和操作系统
 - 只能捕获少量信息
 - 容易部署，减少风险
-
- 实例：Specter, KFSensor, Dionaea, and Honeyd.



高交互型蜜罐

- 提供真实的操作系统和服务，而不是模拟
 - 可以捕获更丰富的信息
 - 部署复杂，高安全风险
-
- 实例：ManTrap, Gen II 蜜网

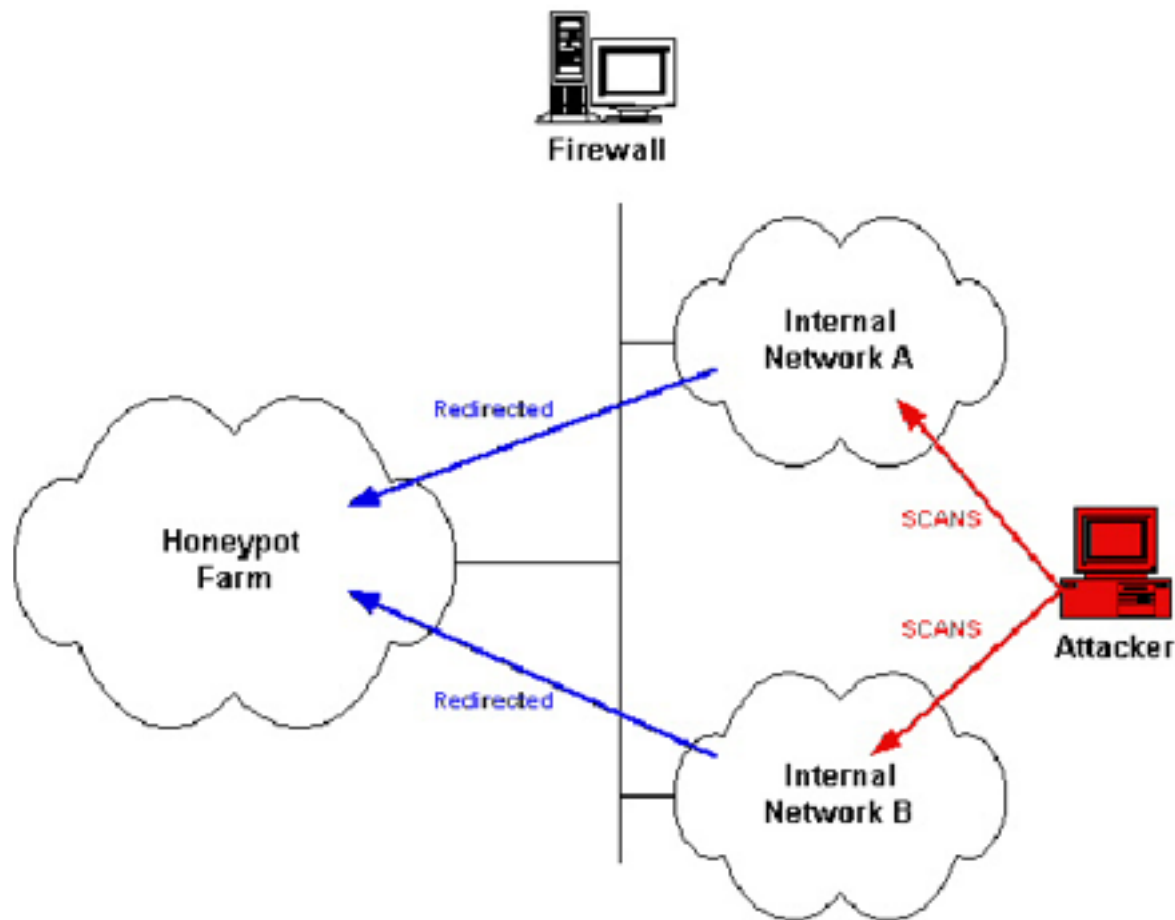


主动式蜜罐技术

- 动态蜜罐
 - 即插即用的解决方案
 - 自动调整
- 被动指纹识别技术
 - 了解所处的网络环境
- 动态配置
 - 虚拟蜜罐



Honeyfarm基本思想





- 对高价值目标映射蜜罐系统
——动态蜜罐技术
- 不需创建新的目标，而使用已存在的目标
- 将恶意的、未经授权的活动重定向到蜜罐
- 监视和捕获攻击者在蜜罐中的活动
- 计算机取证技术

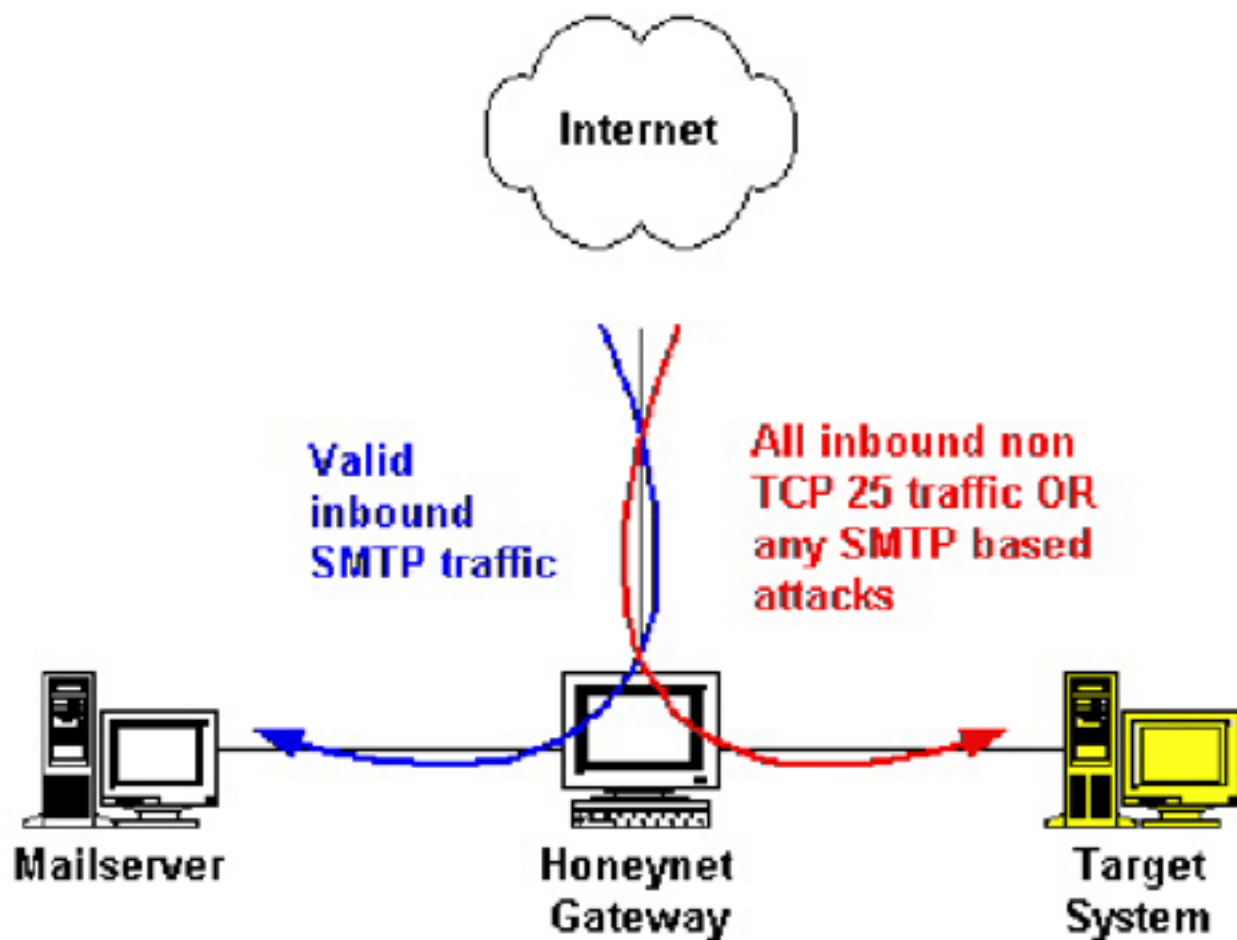


什么时候重定向?

- 非预期的流量 – Hot Zoning
 - 非业务(Non-production)目标端口
 - 非业务源端口
 - Time of day
- 已知攻击 – Bait-n-Switch
 - Snort的修改版本, 内联网关
 - 将检测到的活动重定向到蜜罐中
- 基于主机的监控
 - 监控主机上的未授权活动、或恶意活动, 然后重定向: PaX, Systrace



重定向示例





蜜罐的欺骗性

- 真实的系统环境
 - 系统标识
 - IP、traceroute 路径
 - 主机名、操作系统内核版本…
 - 系统配置和应用程序
 - 开放的网络服务…
 - 安装的应用程序
 - 数据内容
 - Proxy and cache?
- 优势：在一个高度可控的环境中愚弄/观察攻击者的所有行动



- 概念出发点：威胁不仅仅是针对信息系统，也针对信息本身。
- Honeytoken: 正常情况下不会使用的一些诱饵信息
 - 数据库诱饵记录
 - 伪造的弱用户名/口令对
- 如果Honeytoken一旦被访问, 预示着攻击发生, 对它进行监视跟踪



- Honeyapp: 应用层的蜜罐
 - 模拟应用层的服务对非自动化的攻击更具吸引力
 - 在应用层能够更有效地对攻击进行分析
- 实例
 - Web application honeypot



Honeyclient

- 越来越多的攻击针对客户端软件
 - Web浏览器
 - Email客户端
- Honeyclient的设计要考虑：
 - 应用协议本身
 - 需要捕获的攻击
- 基于完整性测试判断是否遭受攻击
 - 程序本身
 - 配置文件、注册表等
- 分类
 - Active honeyclient: 同步交互, 如web-based honeyclient
 - Passive honeyclient: 异步交互, 如email honeyclient



Web-based honeyclient

- 目标—找到危害浏览器的网站及攻击方式
 - 找到恶意站点: Google Search
 - 捕捉并分析攻击方法
 - 安装IRC bot, 成为傀儡主机
 - 安装代理服务
 - 安装spyware/adware, 或其他恶意代码
 - 获取敏感信息, 如信用卡号码、身份信息
 - Phishing website



异步交互honeyclient

- 基于IRC的honeyclient, 加入特定的IRC channel, 获取信息
 - Germany Honeynet Project – Drone
- 基于IM软件的honeyclient
- 基于Email的honeyclient
 - Phishing mail
- p2p based honeyclient
 - 从p2p网络中下载软件并执行



蜜罐实例

- DTK
- Honeyd
- Nepenthes(猪笼草)
 - Dionaea (捕蝇草)
 - Nepenthes PHARM



- Deception Toolkit

- Fred Cohen 等人于1997年首次对外公开发布
- 提供一些欺骗的手段（工具）来阻止攻击
- 低交互蜜罐的雏形
 - 支持简单的脚本编程自定义交互行为



- 搭建虚拟蜜罐与蜜罐网络的轻量级守护进程
- 模拟几乎任何类型的应用层服务与任何发行版的操作系统
 - IIS / ftp / telnet 等
- 低交互蜜罐
 - 支持脚本定制和配置
- 建议运行在沙盒环境中
 - systrace



Nepenthes (猪笼草) ——概述

- 项目历史

- Georg Wicherski独立开发mwcollect

- Paul Baecher 和Markus Koetter开发Nepenthes

- 2006 年2月mwcollect整合进Nepenthes

- mwcollect v4 的开发 得到了Kaspersky 实验室资助 (2009.2-2010.1)

- 运行在Linux上的低交互虚拟蜜罐

- 模拟多种Windows服务

- 自动下载恶意代码并发送到预定义服务器进行集中检测和分析



Nepenthes (猪笼草) ——关键技术

- 漏洞模块
 - 模拟包含已知漏洞的Windows服务(lsass, dcom, veritas, dameware等)
- Shellcode处理器和模拟器
 - 加载shellcode并模拟执行
- 下载模块
 - 执行恶意代码中的下载指令(http, ftp, curl等)
- 上传模块
 - 提交Norman, CWSandbox, postgres等供深入分析



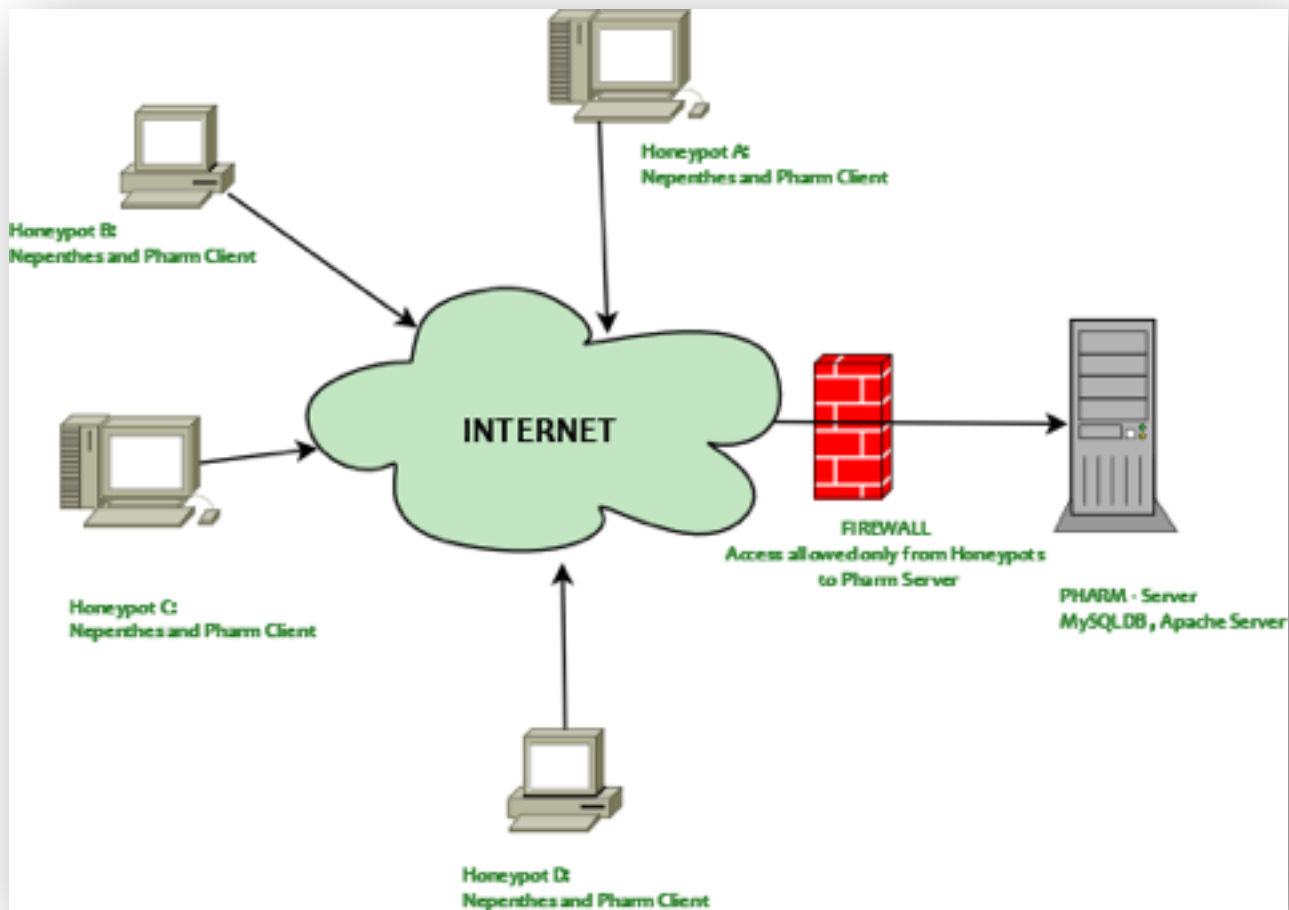
支持Nepenthes的在线恶意代码分析工具

- Norman sandbox - http://www.norman.com/security_center/security_tools/
- CWSandbox - <http://luigi.informatik.uni-mannheim.de/>
- Virus total - <http://www.virustotal.com/>



Nepenthes PHARM

- 客户端
 - 分布式部署 nepenthes 客户端
- 服务器端
 - 可控的数据汇总收集
 - 数据分析
- 信息门户
 - 分析结果展示





- Honeynet Project的开源项目

- 起始于2009年

- Nepenthes项目的后继

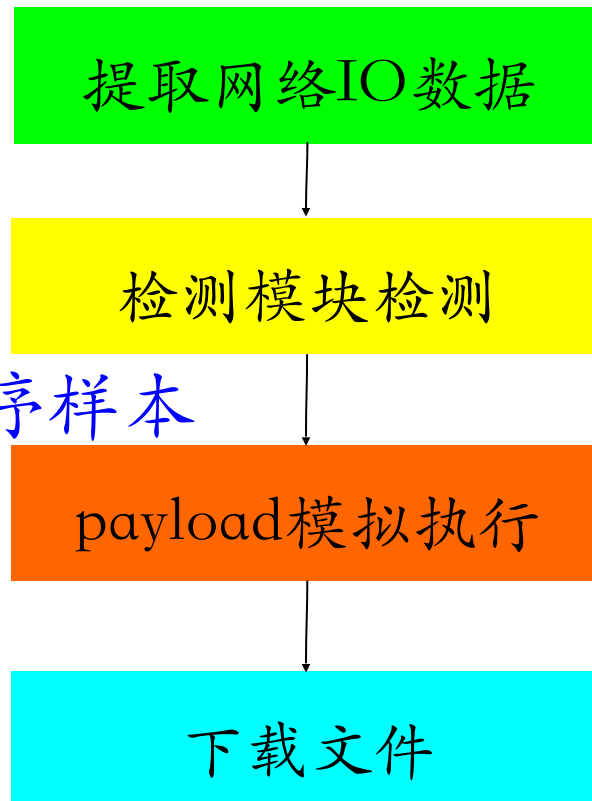
- 目的

- 诱捕恶意攻击，得到恶意程序样本

- 低交互式蜜罐

- 支持分布式诱捕

- 支持其他模块协同，如p0f





蜜罐技术优势

- 高保真—高质量的小数据集
 - 很低的误报率
 - 很低的漏报率
- 捕获新的攻击及战术
- 并不是资源密集型
- 简单



蜜罐技术弱势

- 劳力/技术密集型
- 局限的视图
- 不能直接防护信息系统
- 引入新的安全风险
——蜜罐被攻陷



- 发现蜜罐
 - 黑客知道要避免进入哪些系统
 - 向蜜罐反馈虚假、伪造的信息
 - 消除蜜罐的指纹
 - 蜜罐-反蜜罐技术：博弈/对抗问题
- 利用蜜罐攻击第三方
 - 期望黑客获得蜜罐的root权限
 - 黑客会将其用作危害第三方的跳板
 - 引入多层次的数据控制机制
 - 人为分析和干预



本章内容提要

- 蜜罐发展史
- 蜜罐关键技术
- 蜜网技术
- 蜜罐与蜜网技术的应用



本章内容提要

- 蜜罐发展史
- 蜜罐关键技术
- 蜜网技术
- 蜜罐与蜜网技术的应用



蜜罐的设计目标

- 捕获数据
- 避免被识别
- 防止被攻陷
- 提供有价值的分析报告
 - 攻击来源
 - 攻击意图
 - 攻击过程
 - 攻击结果

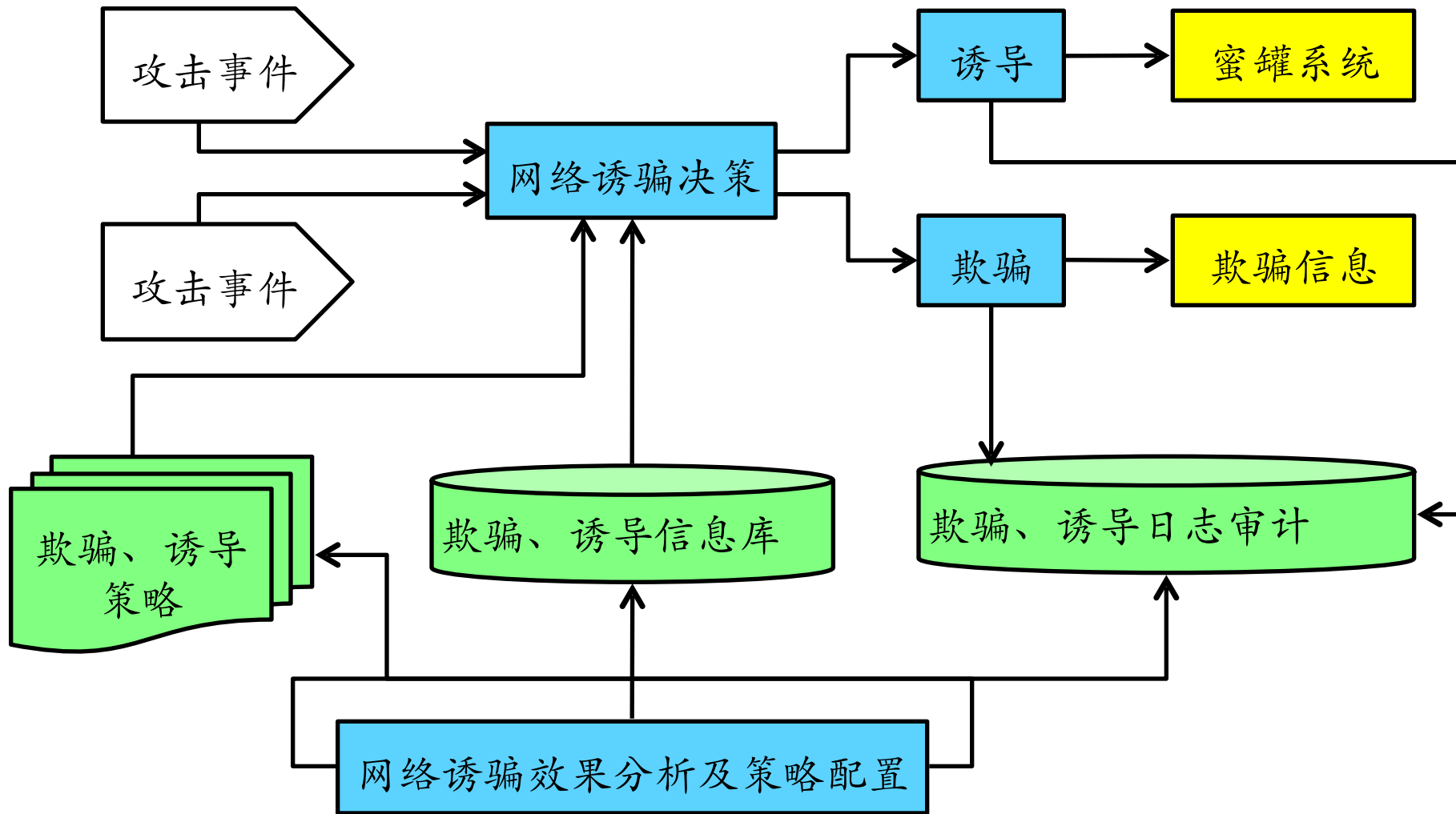


蜜罐的基本功能

- 伪装和模拟
 - 服务/应用/系统/网络/主机
- 数据捕获
 - 网络流量
 - 系统操作记录
 - 日志
- 数据控制
- 数据分析



蜜罐的基本体系架构





蜜罐的基本体系架构

- 决策

- 监听收集事件，根据策略与欺骗、诱导信息库中的记录进行比较后决定诱导或欺骗

- 诱导

- 将攻击者的连接转向蜜罐系统

- 欺骗（误导）

- 分析

- 系统所作的欺骗和诱导事件都记录到日志中，由分析模块进行分析，调整欺骗诱导策略



蜜罐实现的关键技术

- 网络欺骗技术
- 端口重定向技术
- 攻击（入侵）报警
- 数据控制
- 数据捕获
- 数据分析



网络欺骗技术(1/4)

- 设计目标
 - 让网络攻击者产生攻击/入侵蜜罐的兴趣
- 典型技术
 - 蜜罐主机
 - 陷阱网络
 - 诱导
 - 欺骗信息设计



网络欺骗技术(2/4)

- 蜜罐主机

- 空系统

- 无业务模拟的真实完整操作系统及应用程序

- 镜像系统

- 对生产业务进行镜像模拟

- 虚拟系统

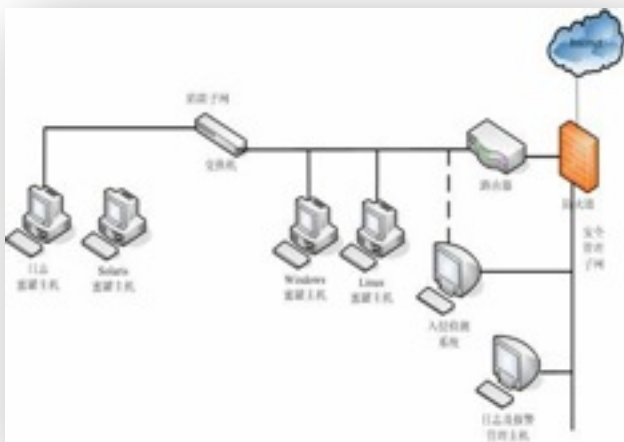
- 基于虚拟机软件的镜像系统



网络欺骗技术(3/4)

- 陷阱网络

—由多个蜜罐主机、路由器、防火墙、IDS、审计系统等组成的供攻击者入侵的网络



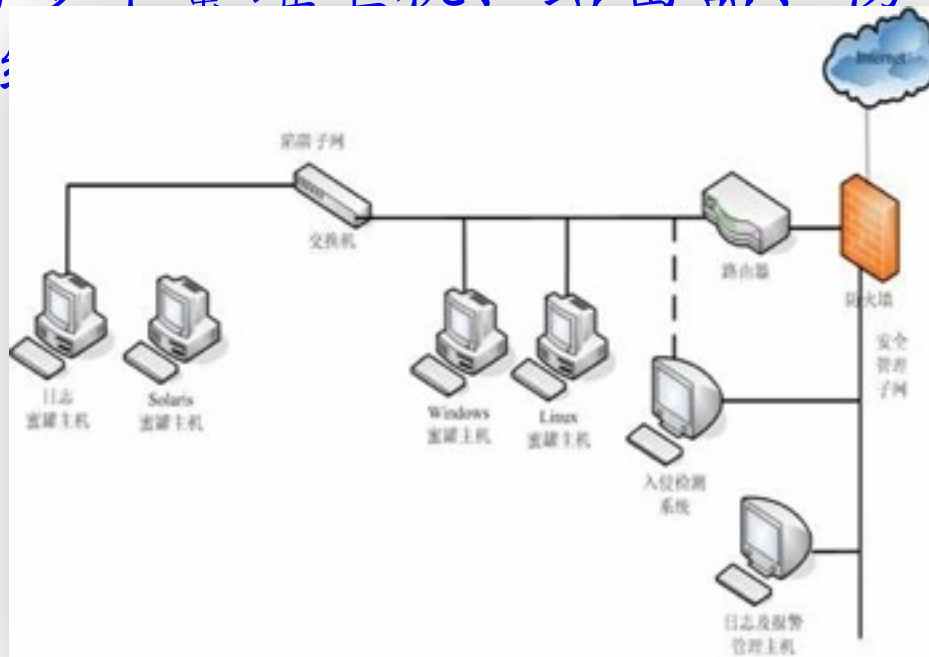
第一代陷阱网络



网络欺骗技术(3/4)

- 陷阱网络

—由多个蜜罐主机、路由器、防火墙、IDS、审计系统组成



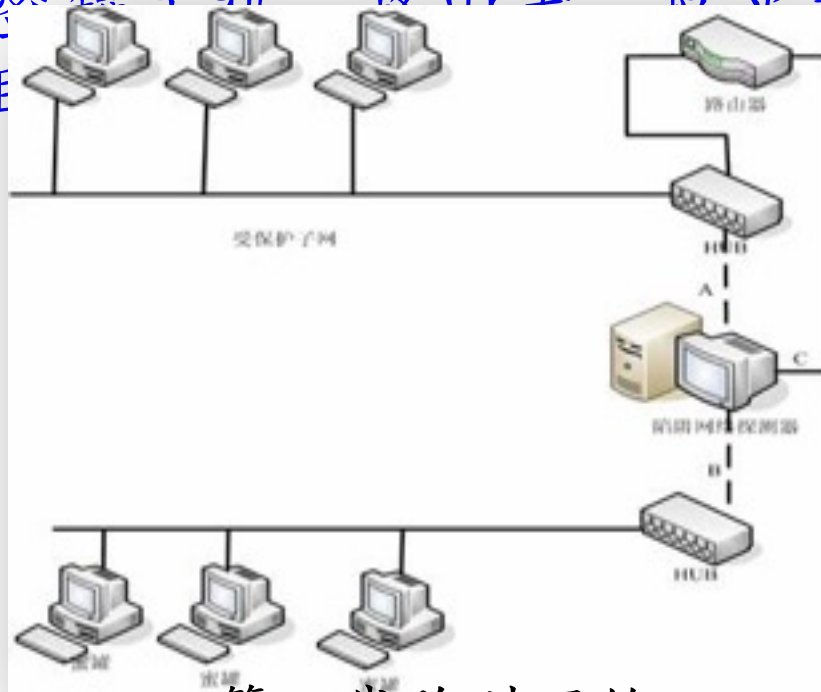
第一代陷阱网络



网络欺骗技术(3/4)

- 陷阱网络

—由多个蜜罐主机和路由器、防火墙、IDS、审计系统等组成



第二代陷阱网络



网络欺骗技术(3/4)

- 陷阱网络

—由多个蜜罐、防火墙、IDS、审计系统等组成



第三代陷阱网络



- 诱导
 - 基于地址转换技术的诱导
 - 基于代理技术的诱导
- 欺骗信息设计
 - 端口扫描欺骗设计
 - 主机操作系统信息欺骗设计
 - 后门欺骗信息设计
 - Web扫描欺骗信息设计
 - 口令欺骗信息设计



端口重定向技术

- 客户端重定向
- 服务器端重定向
 - 代理模式
 - 直接响应模式



攻击（入侵）报警

- 蜜罐设计的目的是为了被入侵
- 第一时间发现入侵
 - 参考《7.2 节 入侵检测》的入侵检测原理
 - 网络层面报警
 - 系统层面报警
 - 数据层面报警
- 限制入侵
 - 数据控制



- 需求

- 自动响应 or 手工干预?

- 至少设计两层的数据控制

- 纵深防御

- 充分考虑数据控制失败的情况

- 自动发现并阻止提权/破坏性强的攻击（入侵）行为

- 伪装

- 尽可能避免被攻击者察觉



- 《7.2 节 入侵检测》介绍过入侵检测的数据捕获来源
- 数据捕获来源（特别之处）
 - 系统层面：键盘捕获、屏幕记录、进程访问历史
 - 网络层面：支持攻击图（路径）构建
 - 数据层面：支持传播路径重构
- 数据捕获存储
 - 远程安全存储：不能在蜜罐本地存储



- 《7.2 节 入侵检测》介绍过入侵检测的数据分析算法

—基于异常的算法

- 基于特征选择异常检测
- 基于贝叶斯推理异常检测
- 基于模式预测异常检测
- 基于神经网络异常检测



数据分析——蜜罐和入侵检测的关系

	蜜罐	入侵检测
目的	<p>还原入侵</p> <ul style="list-style-type: none">• Where• What• How: 攻击图• Why: 攻击意图?• Who: 幕后推手?• Assessment: 风险影响评估	<p>发现入侵</p> <ul style="list-style-type: none">• Where: 入侵来源• What: 识别入侵类型
手段	<ul style="list-style-type: none">• 异常检测	<ul style="list-style-type: none">• 误用检测• 异常检测



本章内容提要

- 蜜罐发展史
- 蜜罐关键技术
- 蜜网技术
- 蜜罐与蜜网技术的应用



本章内容提要

- 蜜罐发展史
- 蜜罐关键技术
- 蜜网技术
- 蜜罐与蜜网技术的应用



什么是蜜网?

- 实质上是一种研究型、高交互型的蜜罐技术
 - 对攻击者活动进行收集
- 一个体系框架
 - 包括一个或多个蜜罐
 - 高可控的蜜罐网络



- 在一台机器上部署蜜网的解决方案
 - Vmware / Virtualbox
 - Xen / KVM / QEMU
- 优势
 - 减少部署成本
 - 更容易管理
- 风险
 - 攻击虚拟系统软件，获得整个蜜网的控制权
 - 指纹



蜜网的需求

- 数据控制
 - 降低风险—使得蜜网不会被用以危害第三方
- 数据捕获
 - 检测并捕获所有攻击者的活动
- 数据收集
 - 分布式处理的基础
- 数据分析
 - 分析攻击者做了什么



蜜网项目组——The HoneyNet Project

- 非赢利性研究机构
- 使命
 - To learn the tools, tactics, and motives of the blackhat community and share these lessons learned
- 历史
 - 1999 – 非正式的邮件列表
 - June 2000 – 演变为蜜网项目组
 - Jan. 2002 – 发起蜜网研究联盟
 - Dec. 2002 – 10个活跃的联盟成员



蜜网项目组——目标

- Awareness
——意识到威胁的存在性
- Information
——通告威胁并进行相关教育
- Research
——提供研究机构展开独立安全研究的能力



蜜网项目组

- 蜜网项目组成员
 - 限制最多30人
 - 每个公司或组织同时最多2人
- 创始人及主席
 - Lance Spitzner (Sun Microsystems)



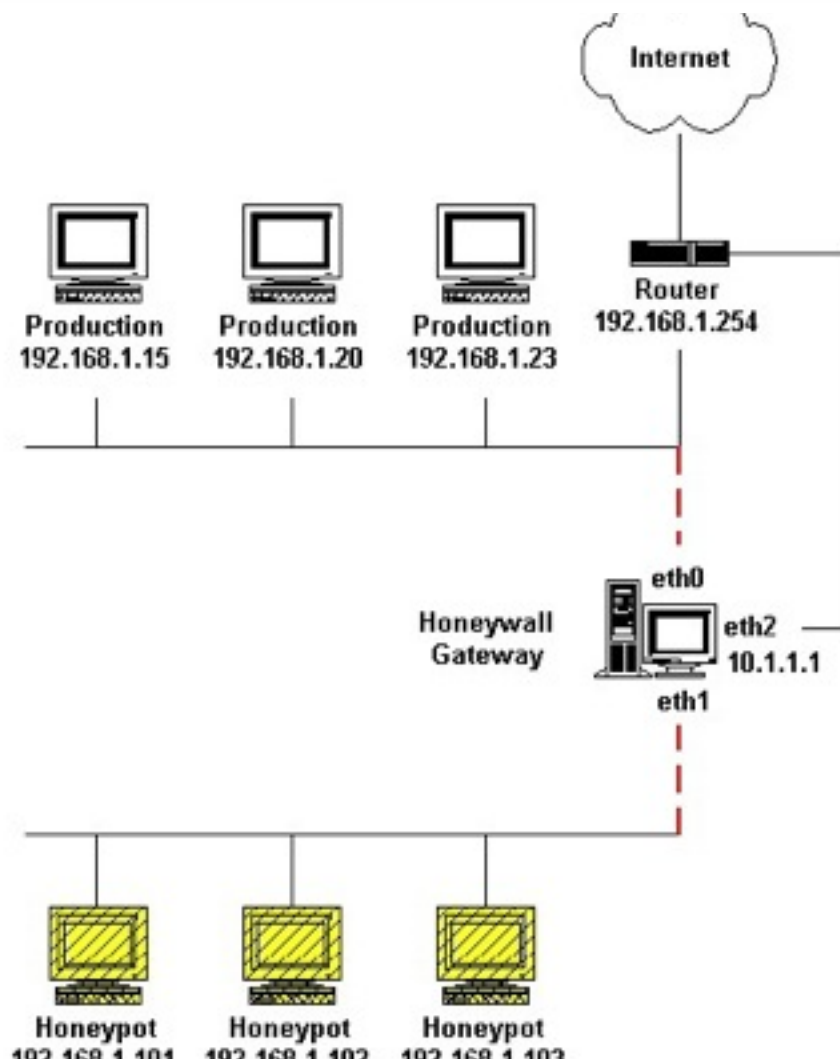
蜜网项目组规划

- Phase I: 1999-2001
 - Gen I蜜网技术: 概念验证
- Phase II: 2001-2003
 - Gen II蜜网技术: 成熟的蜜网技术方案
- Phase III: 2003-2004
 - HoneyWall — Eeyore: 可引导的CDROM, 集成数据控制和数据捕获工具
- Phase IV: 2004-2005
 - 对分布式的蜜网捕获的数据进行收集和关联的集中式系统 —kanga
- Phase V: 2005-
 - Data Analysis Framework — Walleye
 - New HoneyWall CDROM — Roo (2005年5月1日发布)



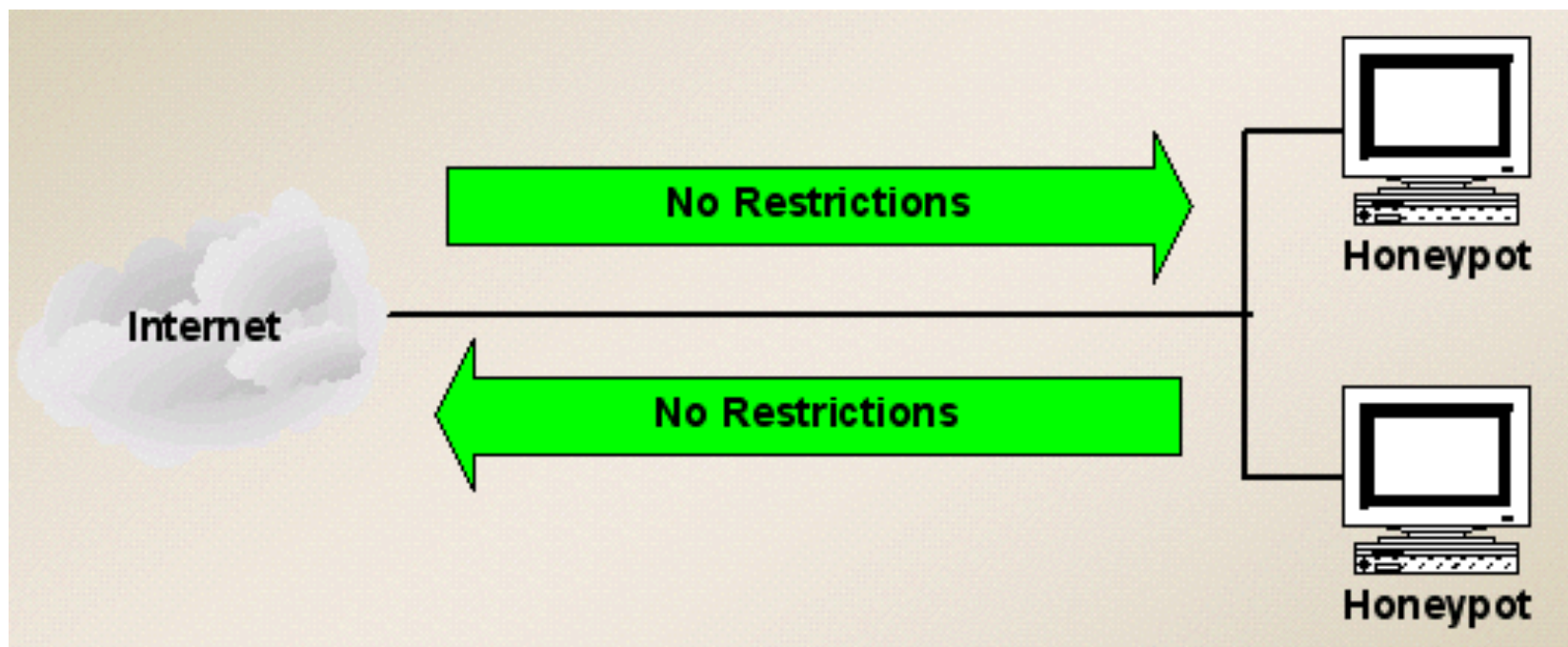
Gen II 蜜网技术

- Gen II 蜜网框架



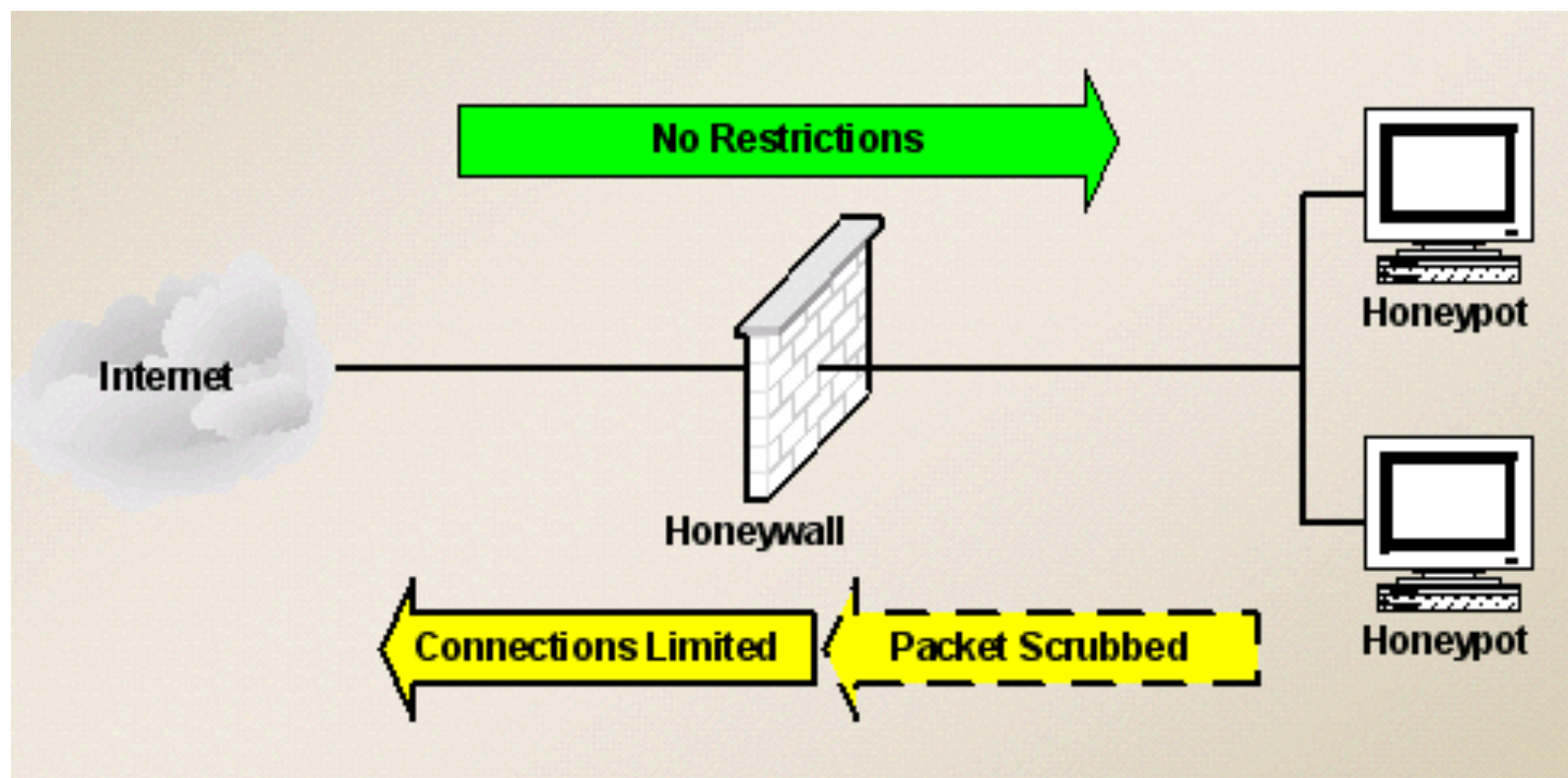


没有数据控制



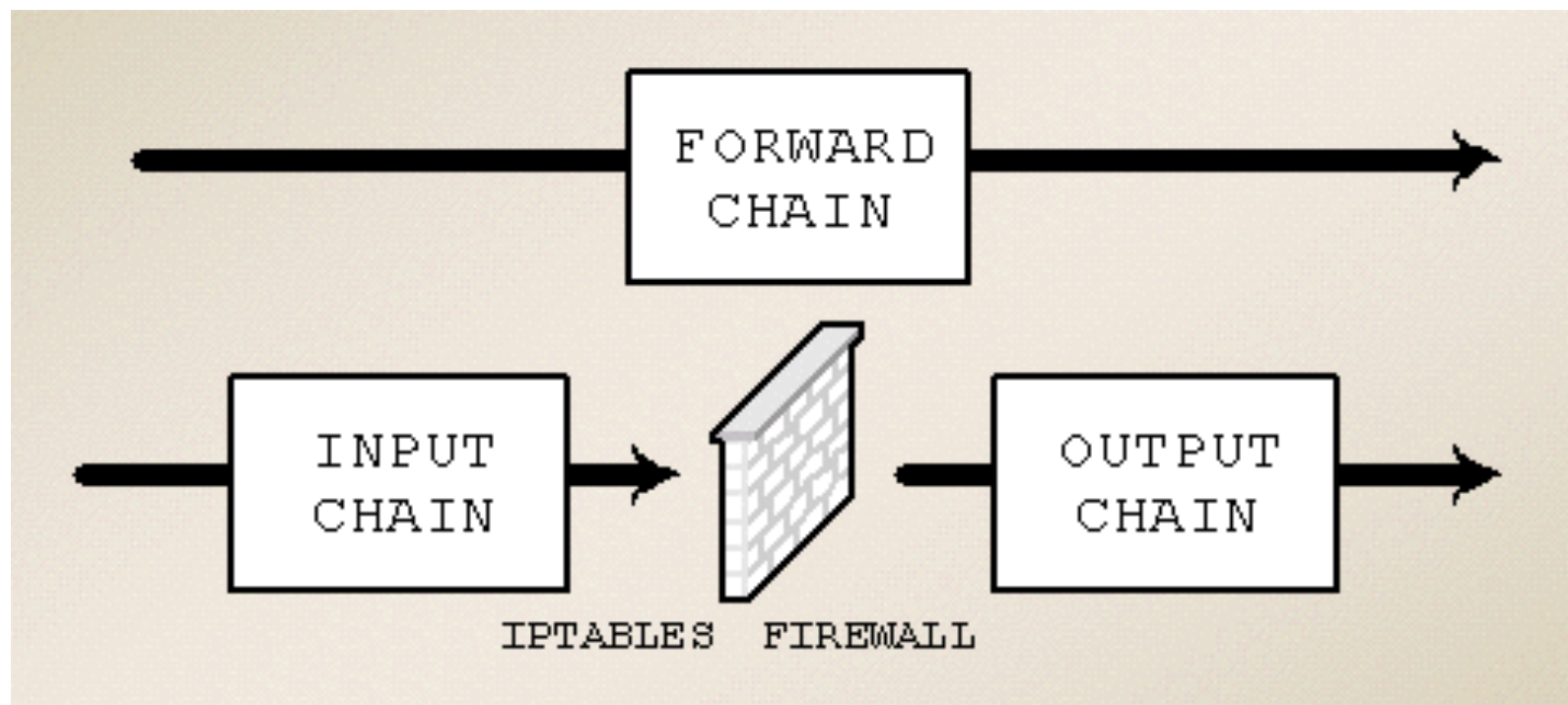


数据控制



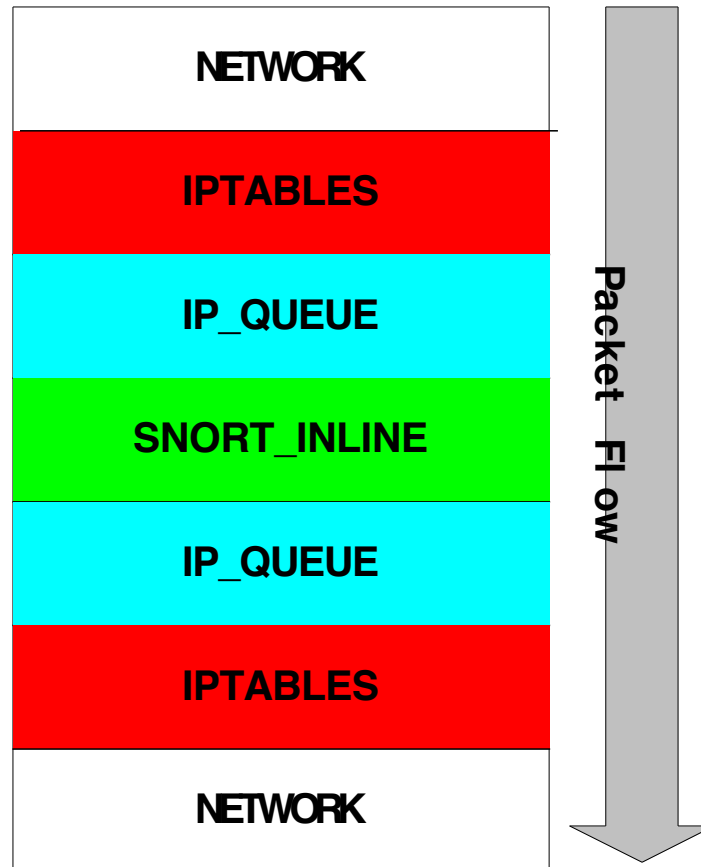


iptables 处理流程





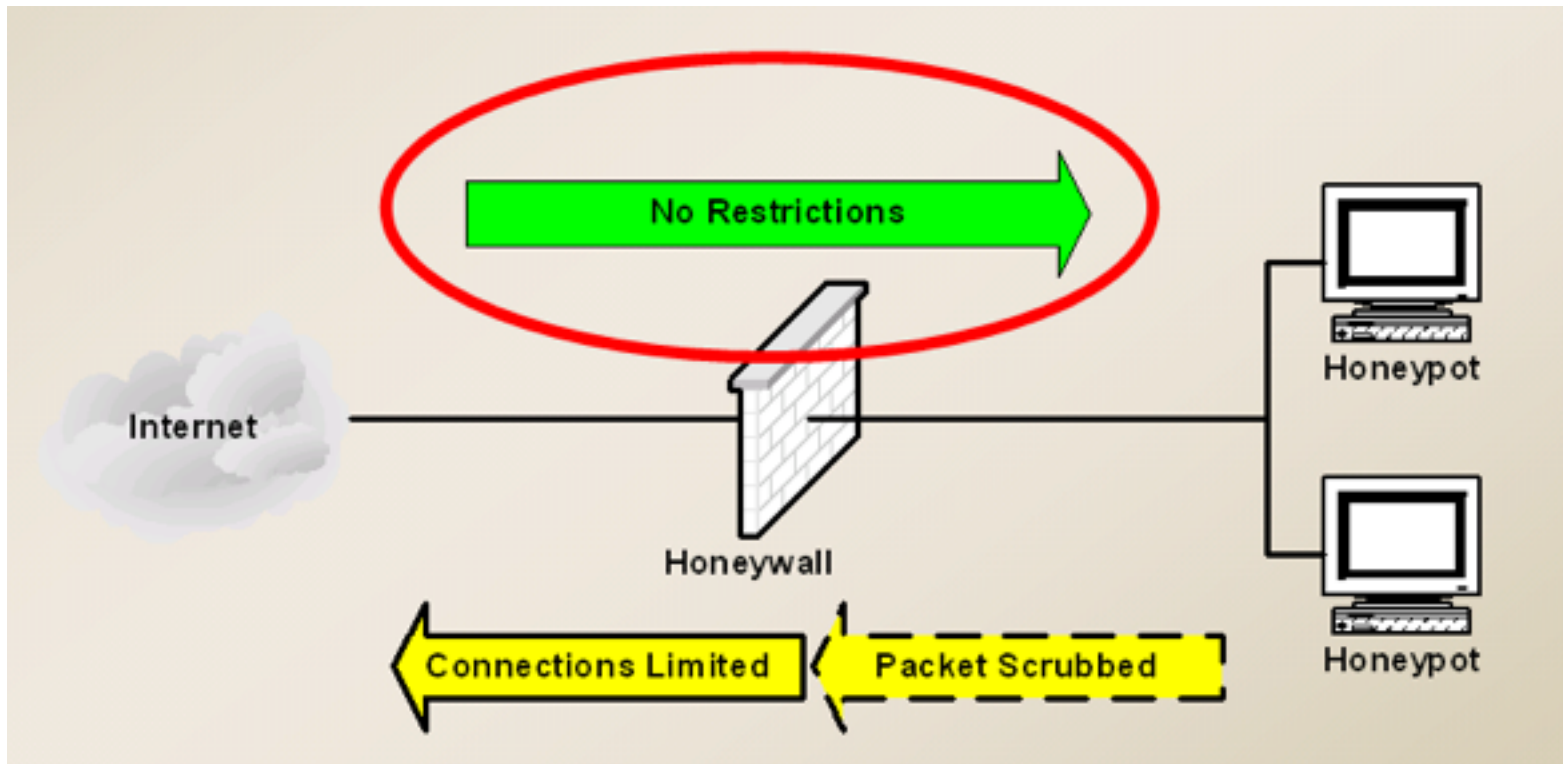
```
iptables -A FORWARD -i $LAN_IFACE -m state  
--state RELATED,ESTABLISHED -j QUEUE
```





Snort logging

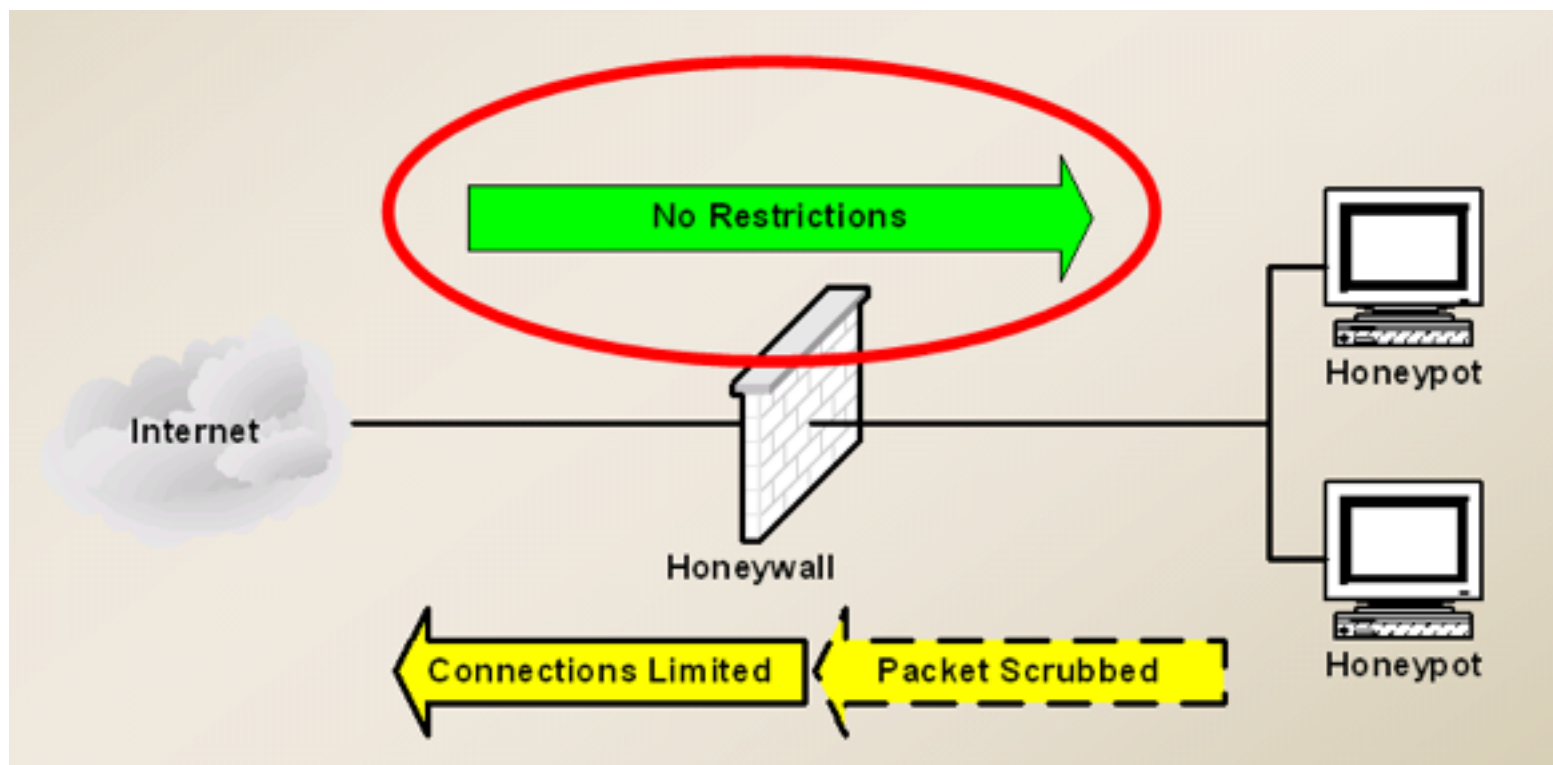
01/08-10:06:09.729583 [**] [111:10:1] (spp_stream4) STEALTH ACTIVITY
(XMAS scan) detection [**] {TCP} 10.10.10.3:46271 -> 10.10.10.10:1





iptables connection logging

Jan 8 09:52:43 honeywall user.warn klogd: INBOUND ICMP: IN=br0
OUT=br0 PHYSIN=eth0 PHYSOUT=eth1 SRC=10.10.10.3 DST=10.10.10.10 LEN=84
TOS=0x00 PREC=0x00 TTL=64





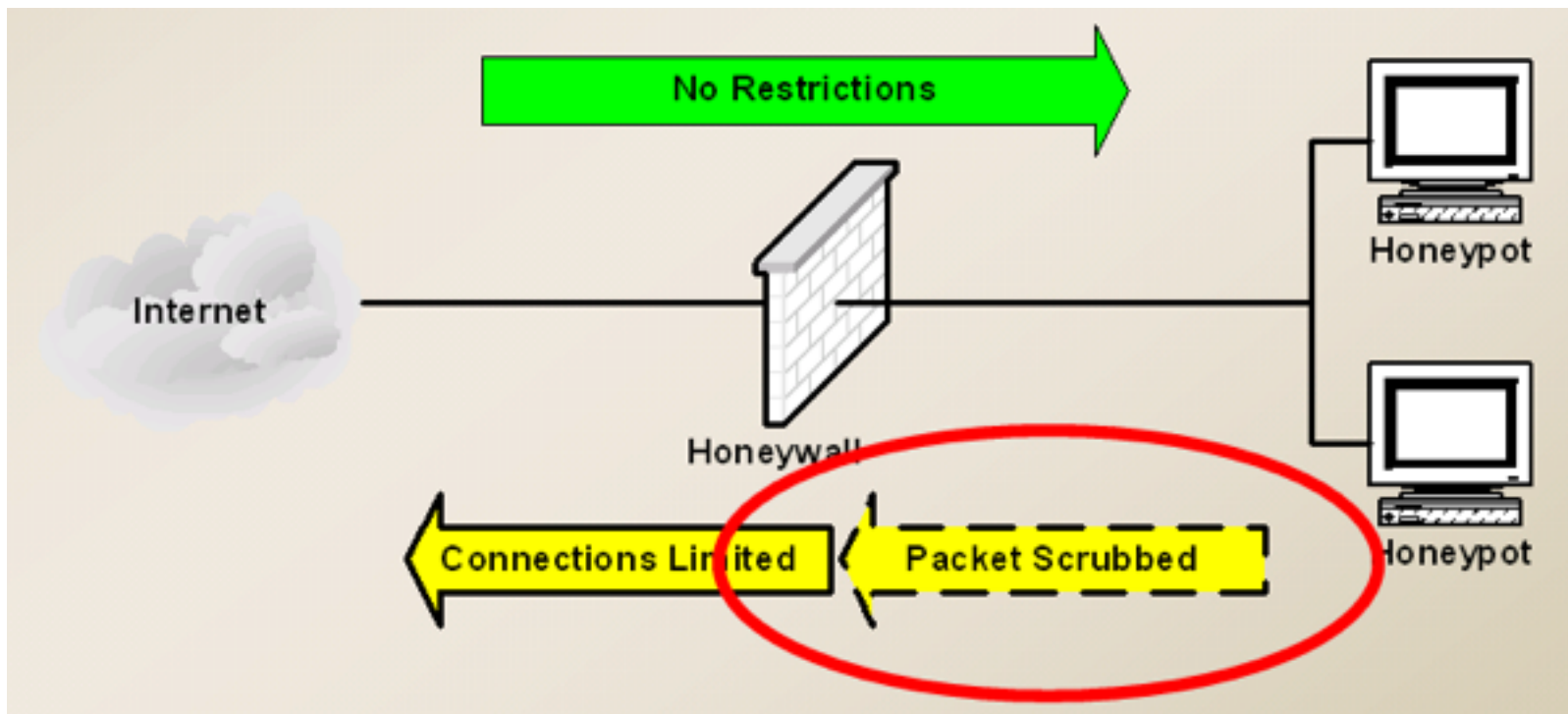
snort_inline logging

03/23-21:21:05.915340 [**] [1:0:0] Dropping Telnet connection [**]

[Priority: 0] {TCP} 10.10.10.10:39528 -> 192.168.1.20:23

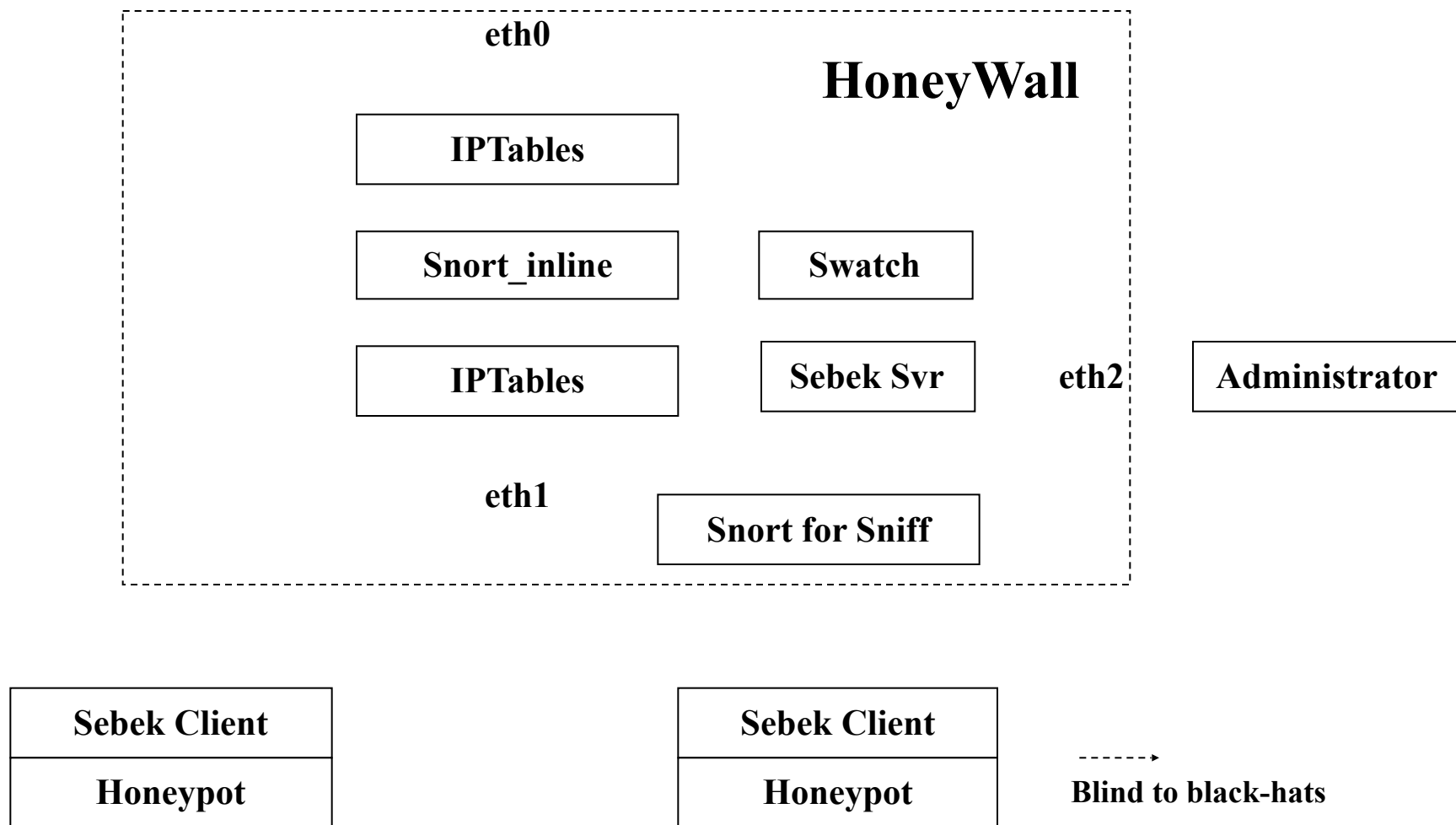
03/23-21:21:24.054533 [**] [1:0:0] Modifying HTTP GET command [**]

[Priority: 0] {TCP} 10.10.10.10:38533 -> 192.168.1.20:80



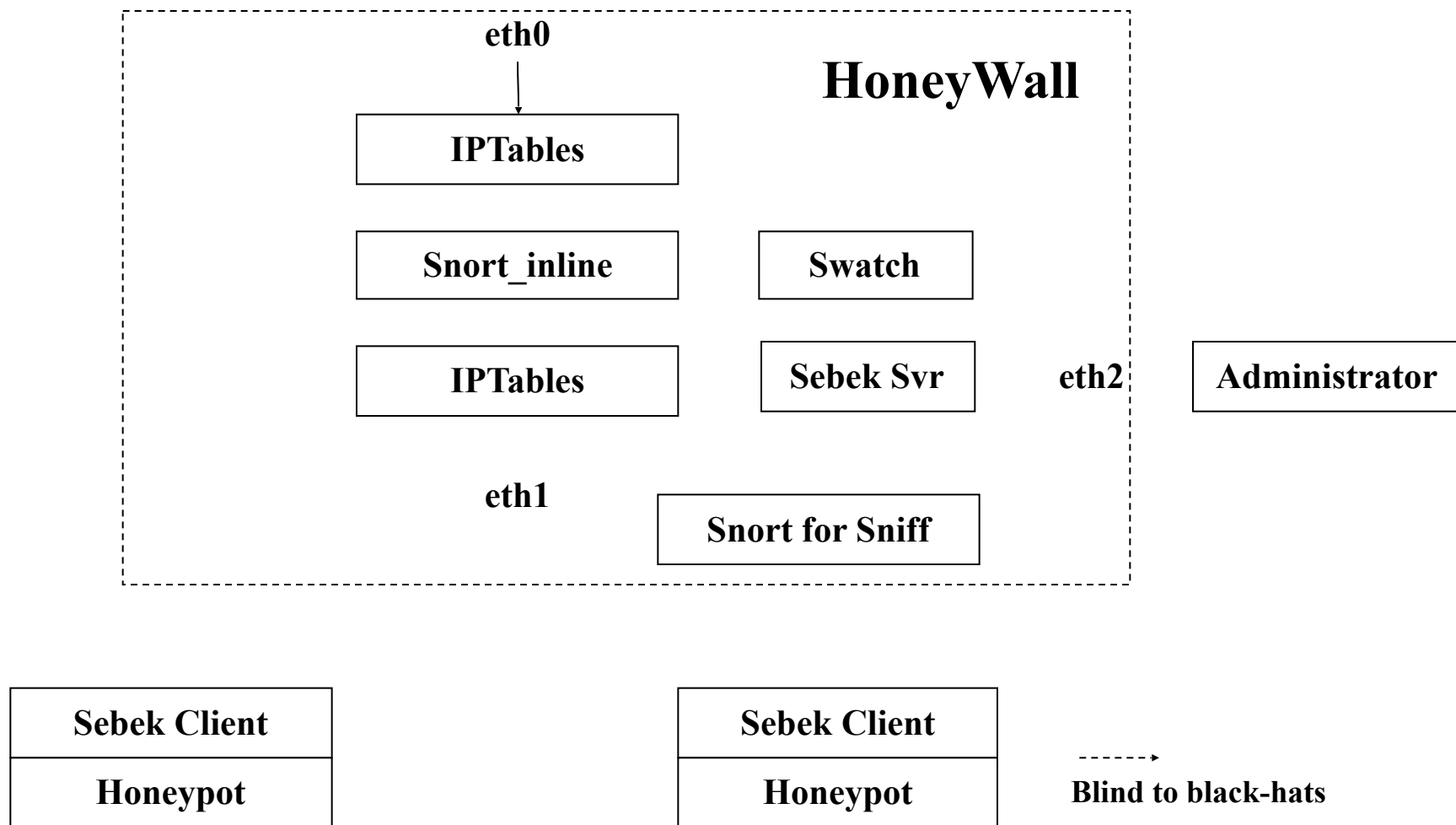


Gen II 蜜网技术 - 数据捕获



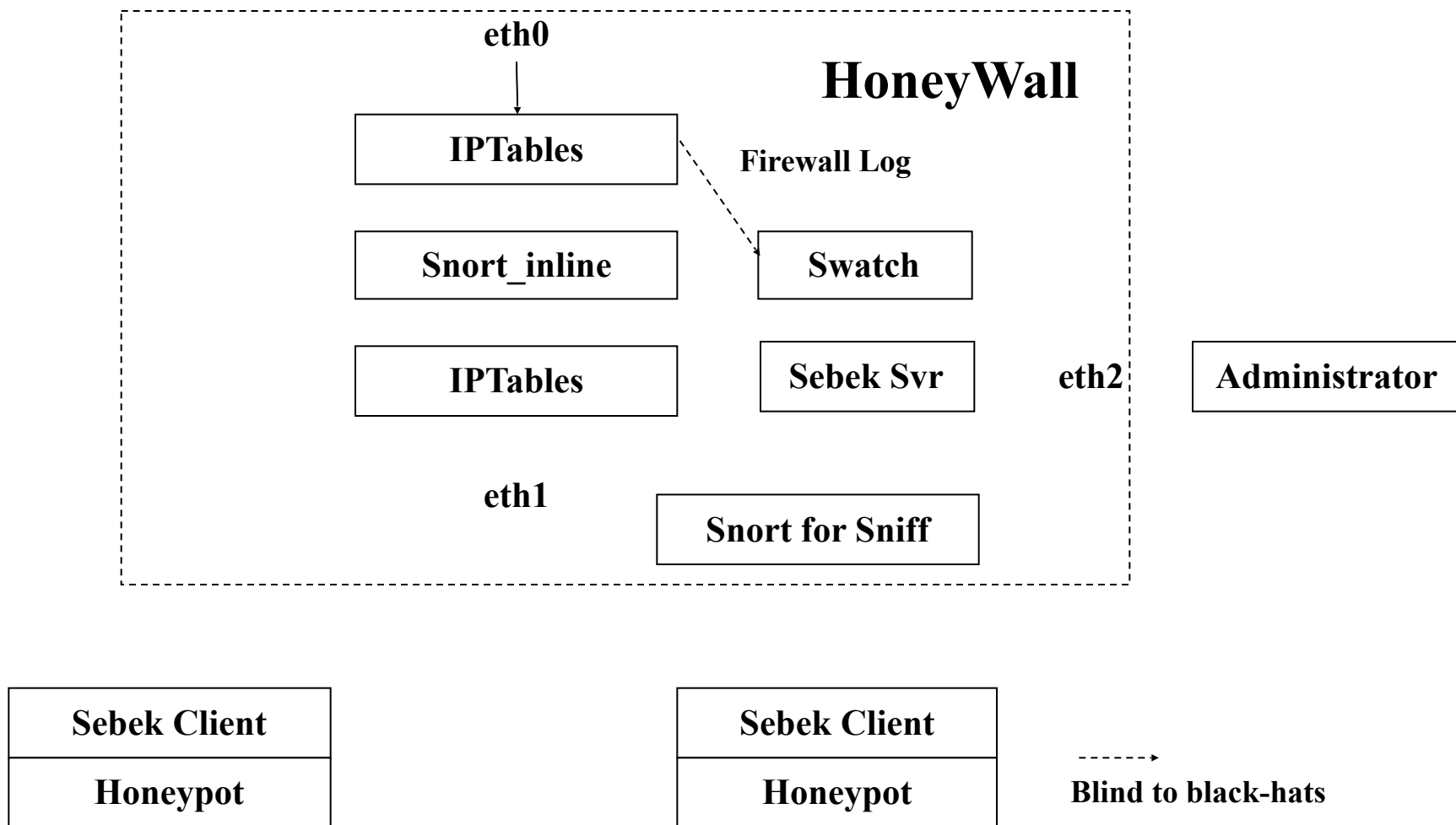


Gen II 蜜网技术 - 数据捕获



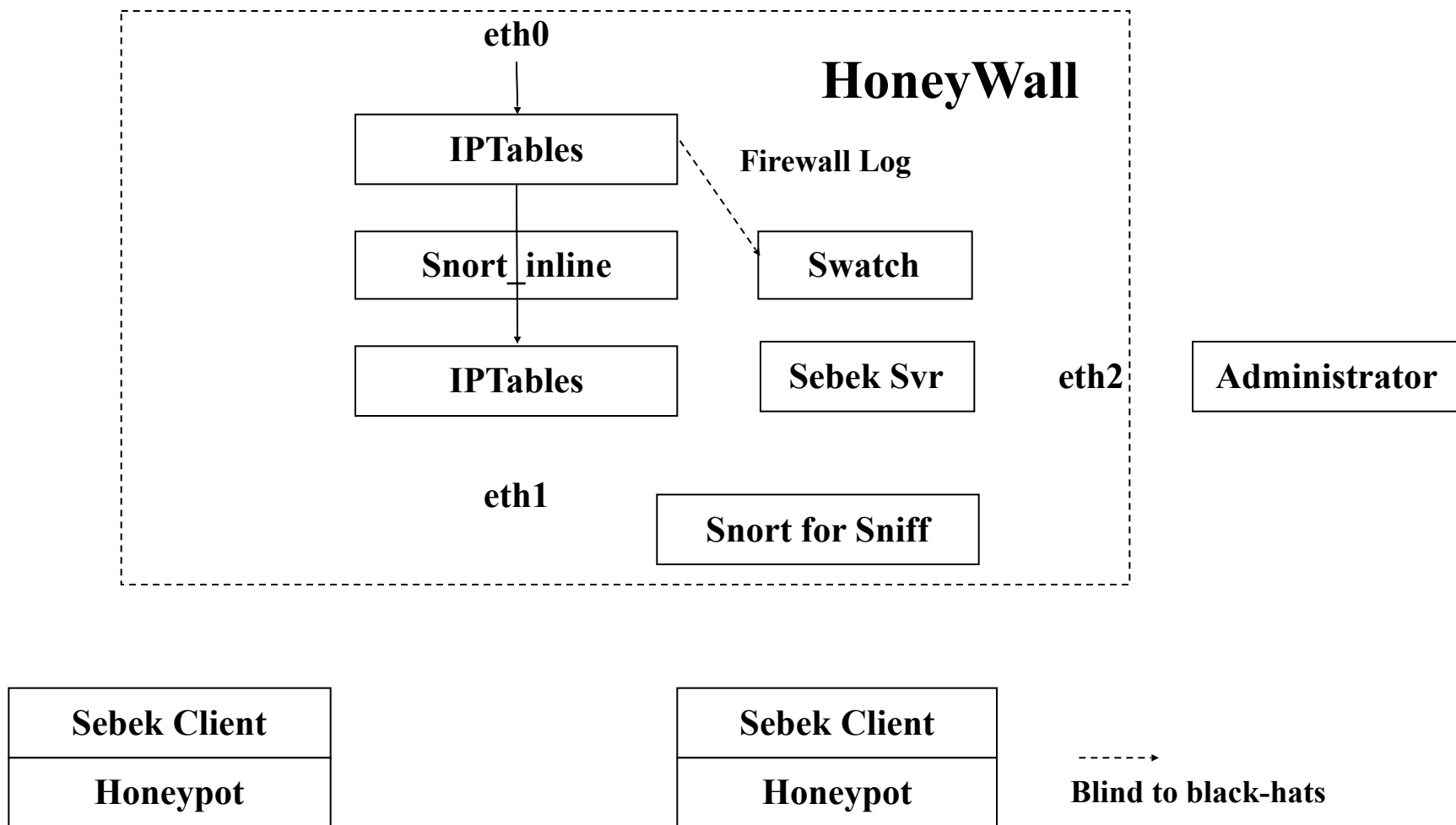


Gen II 蜜网技术 - 数据捕获



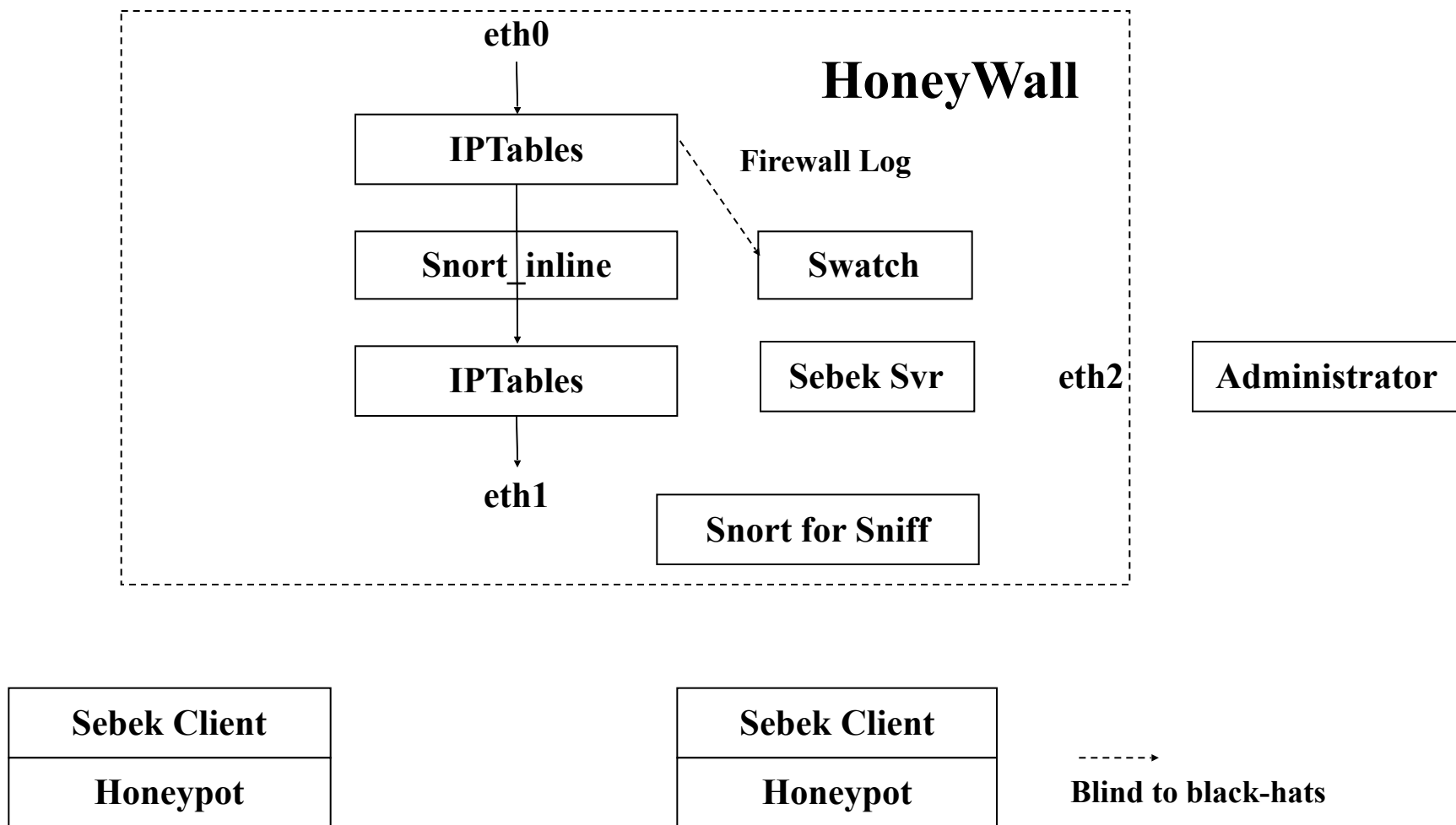


Gen II 蜜网技术 - 数据捕获



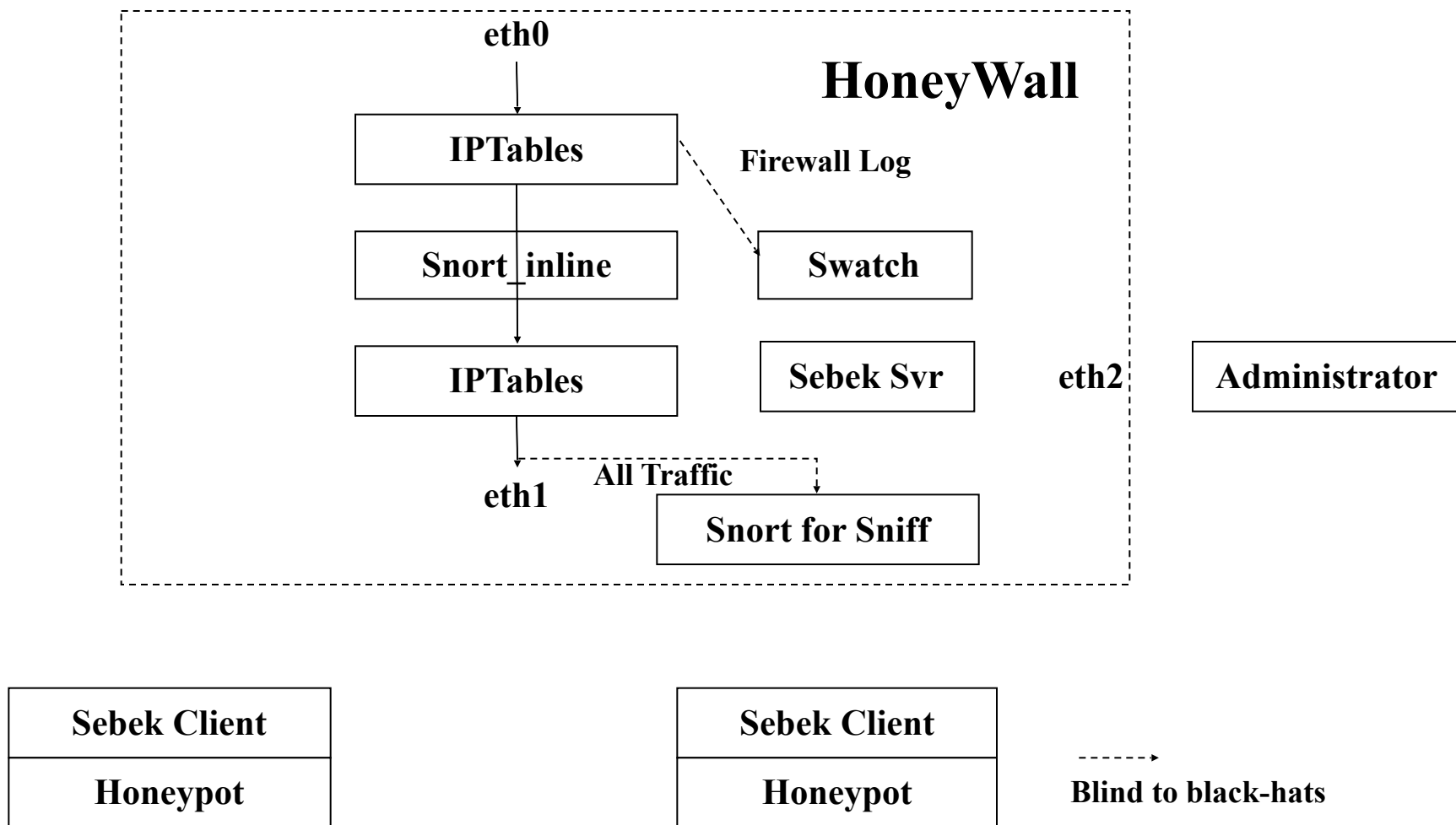


Gen II 蜜网技术 - 数据捕获



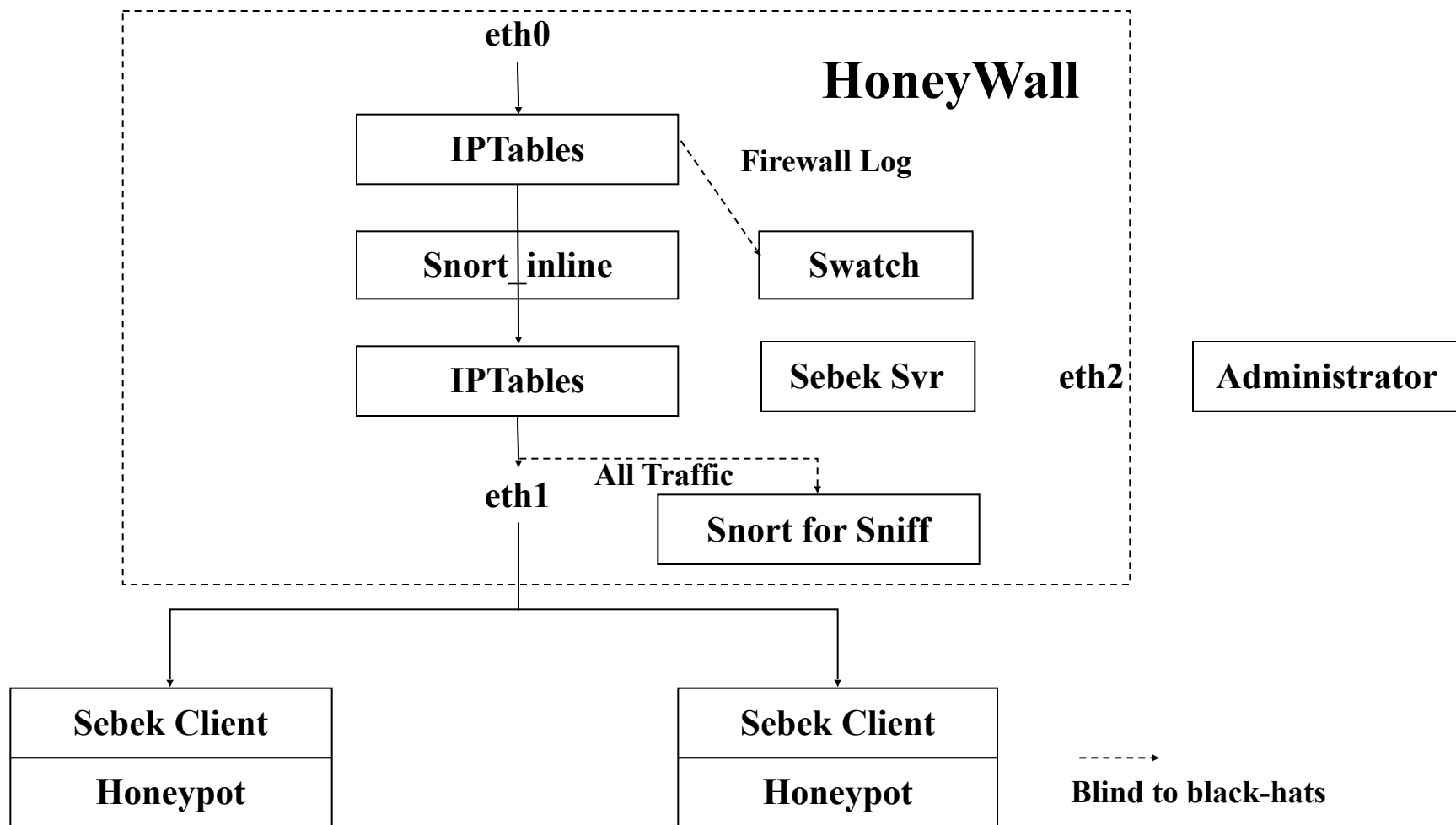


Gen II 蜜网技术 - 数据捕获



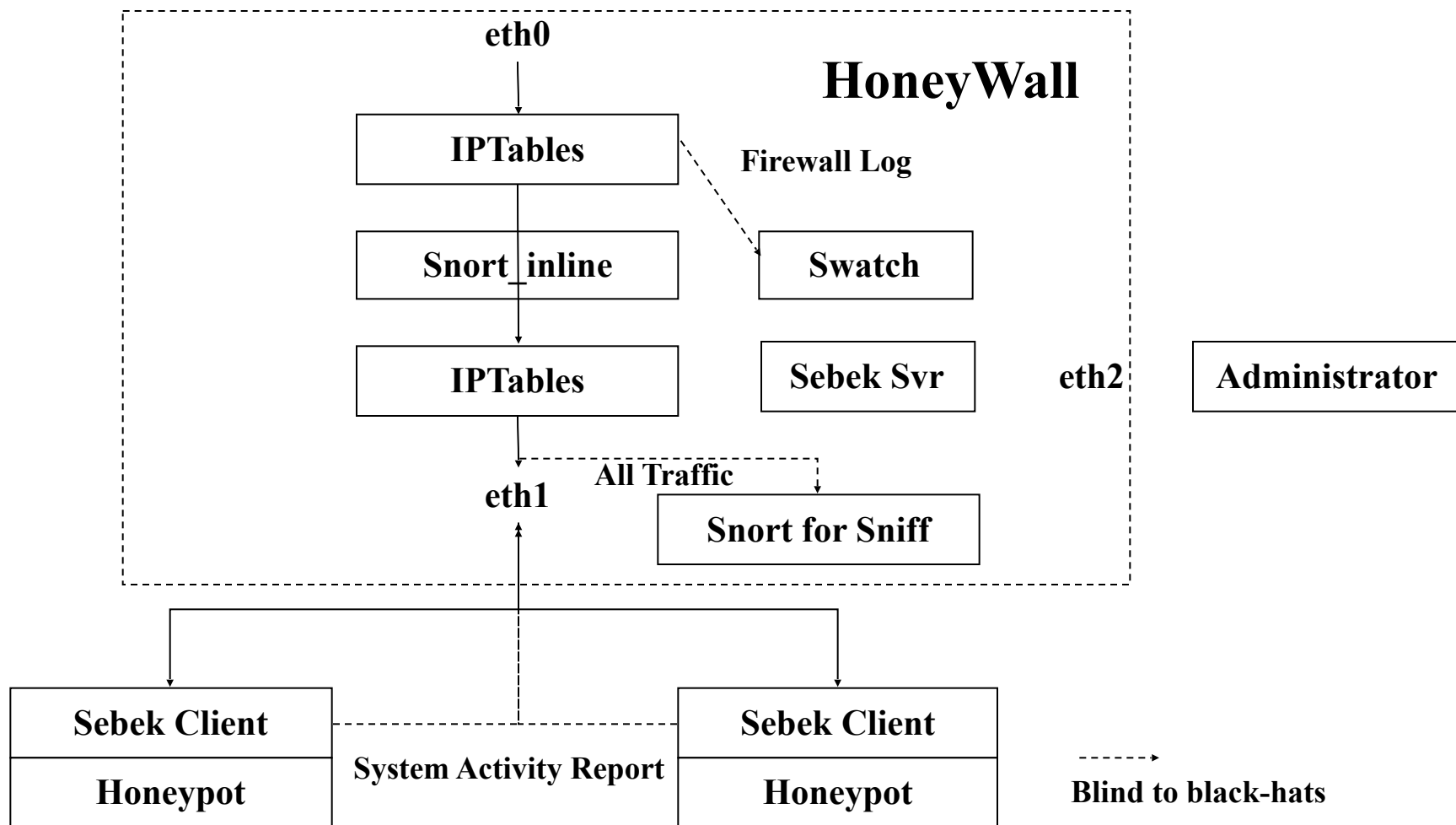


Gen II 蜜网技术 - 数据捕获



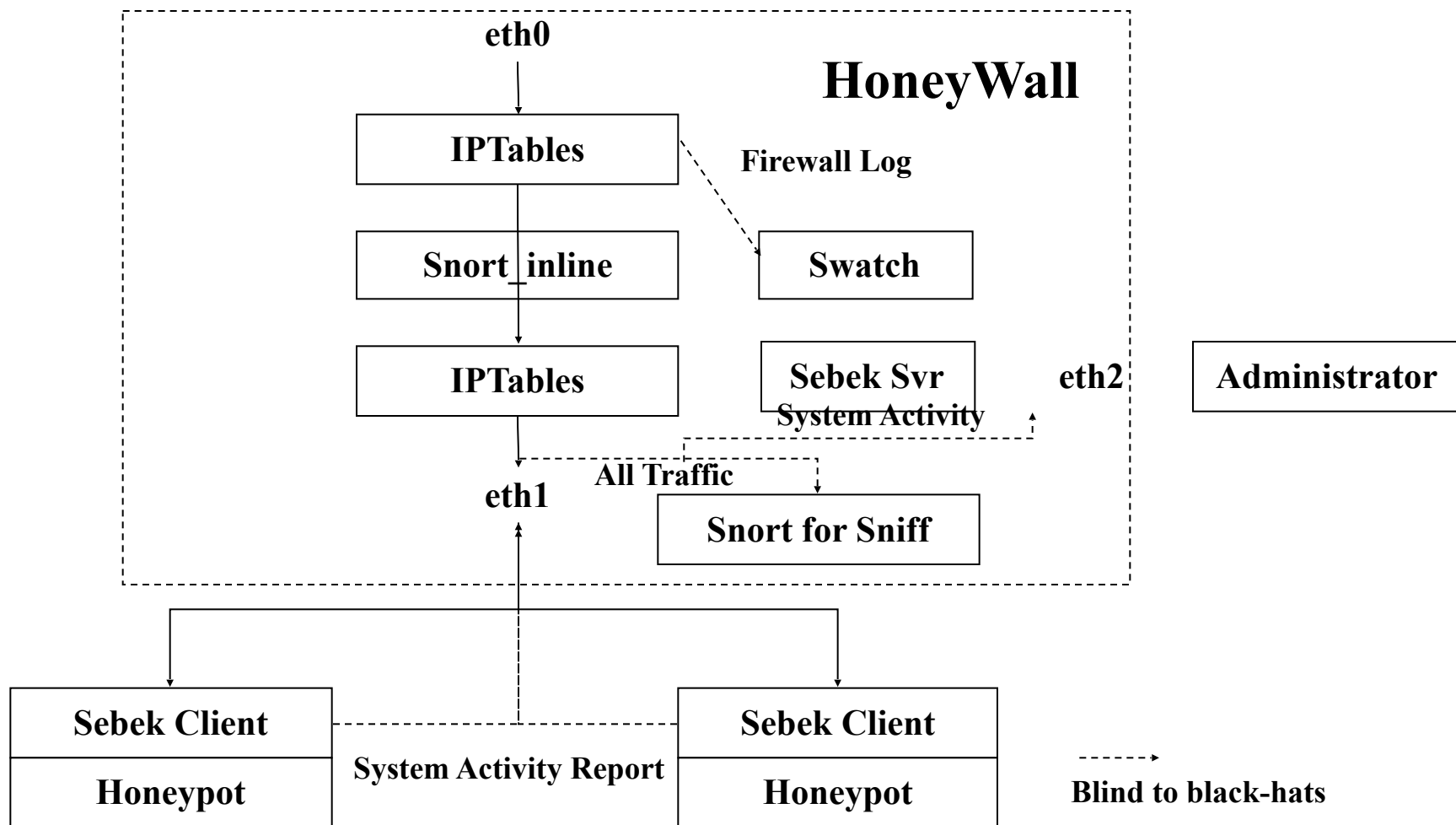


Gen II 蜜网技术 - 数据捕获



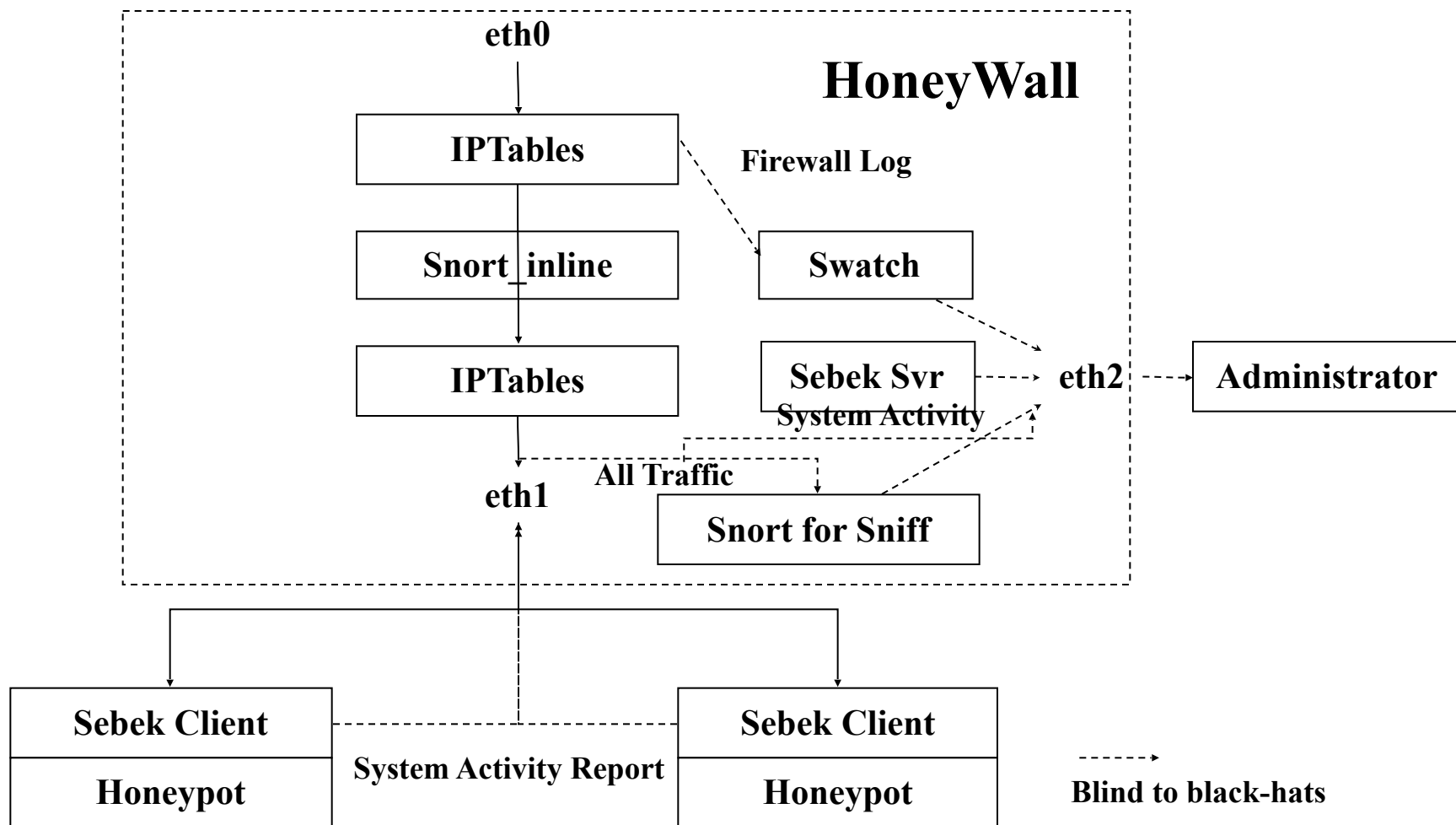


Gen II 蜜网技术 - 数据捕获



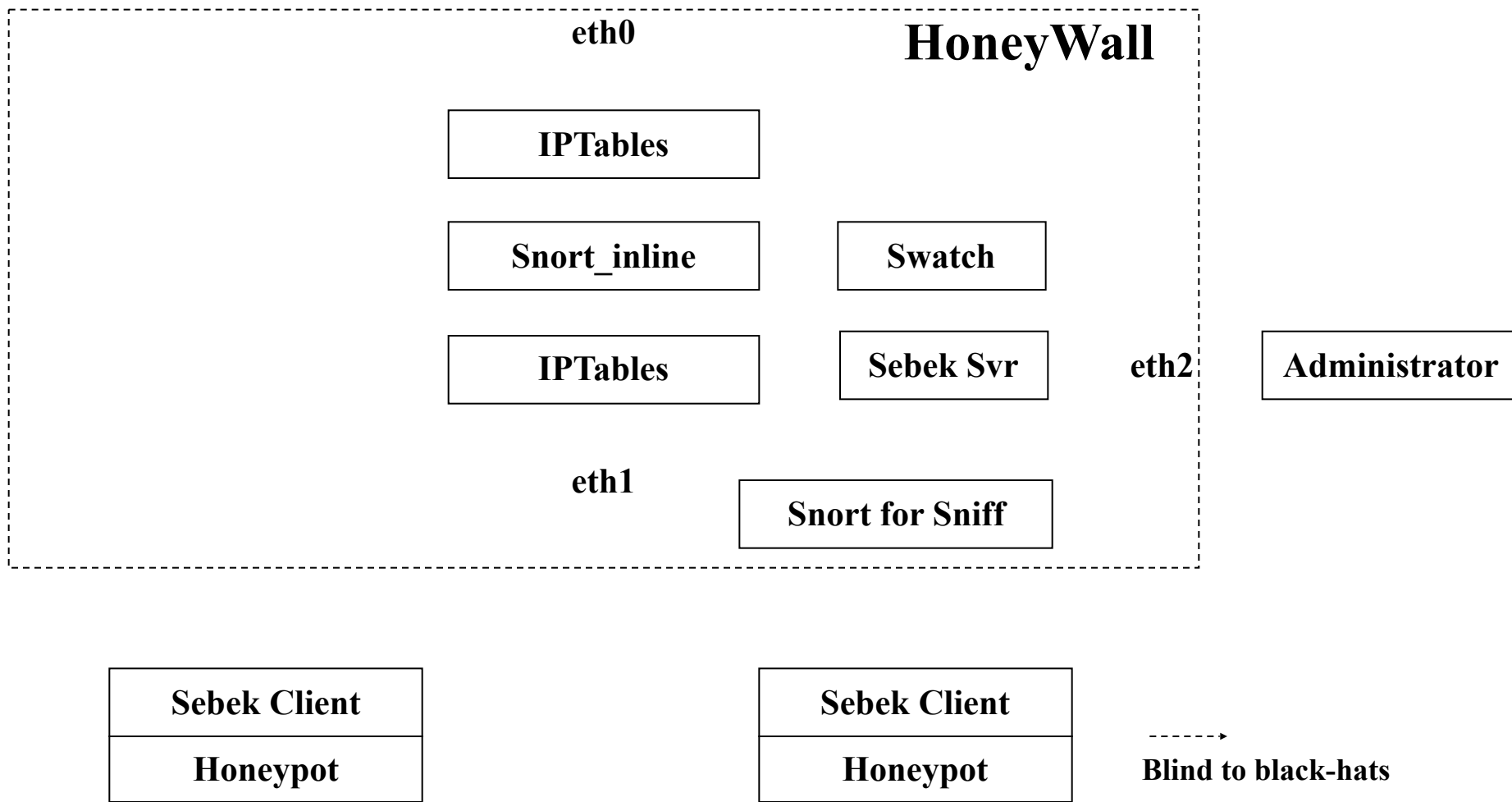


Gen II 蜜网技术 - 数据捕获



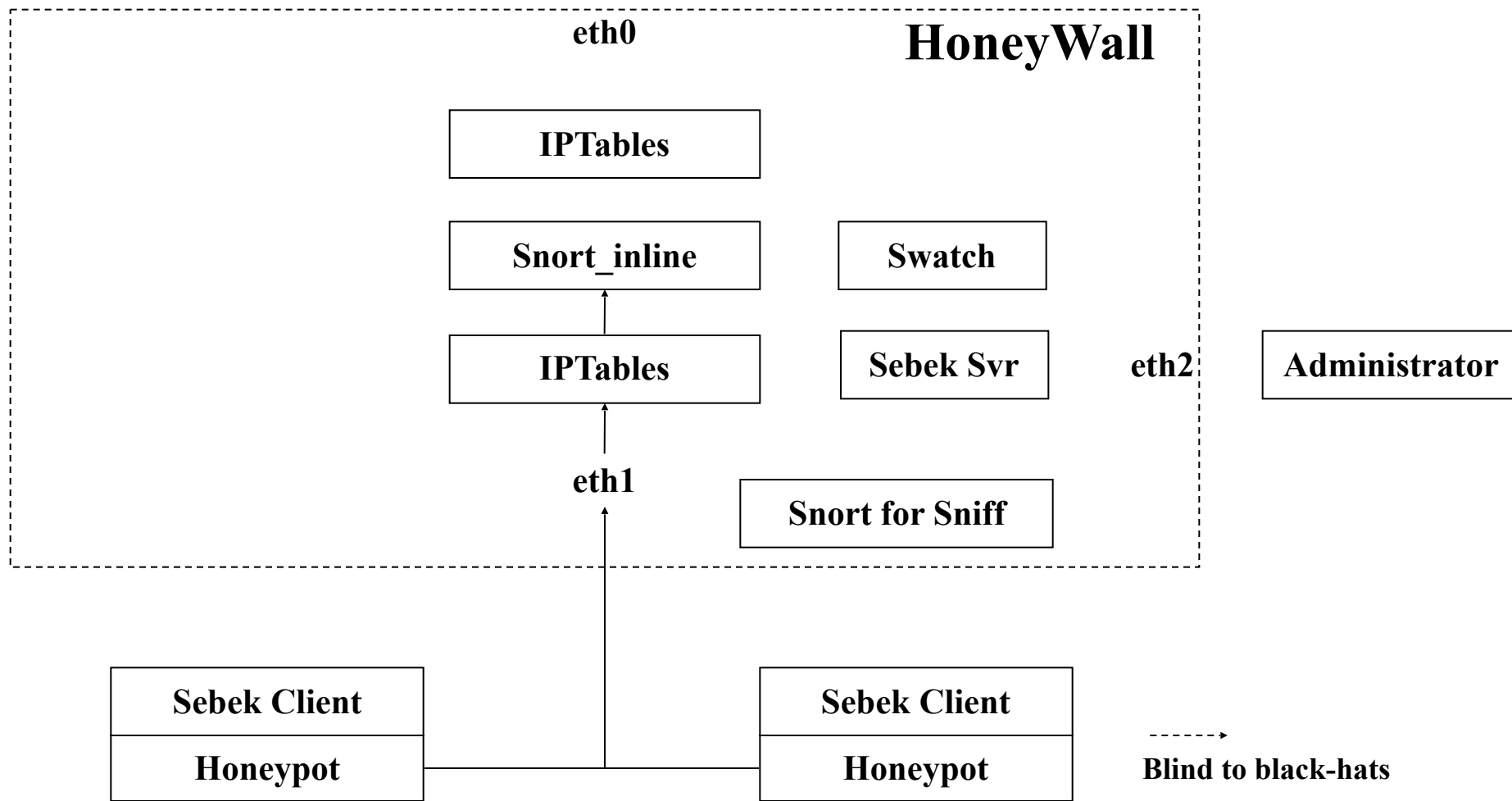


Gen II 蜜网技术 - 数据控制



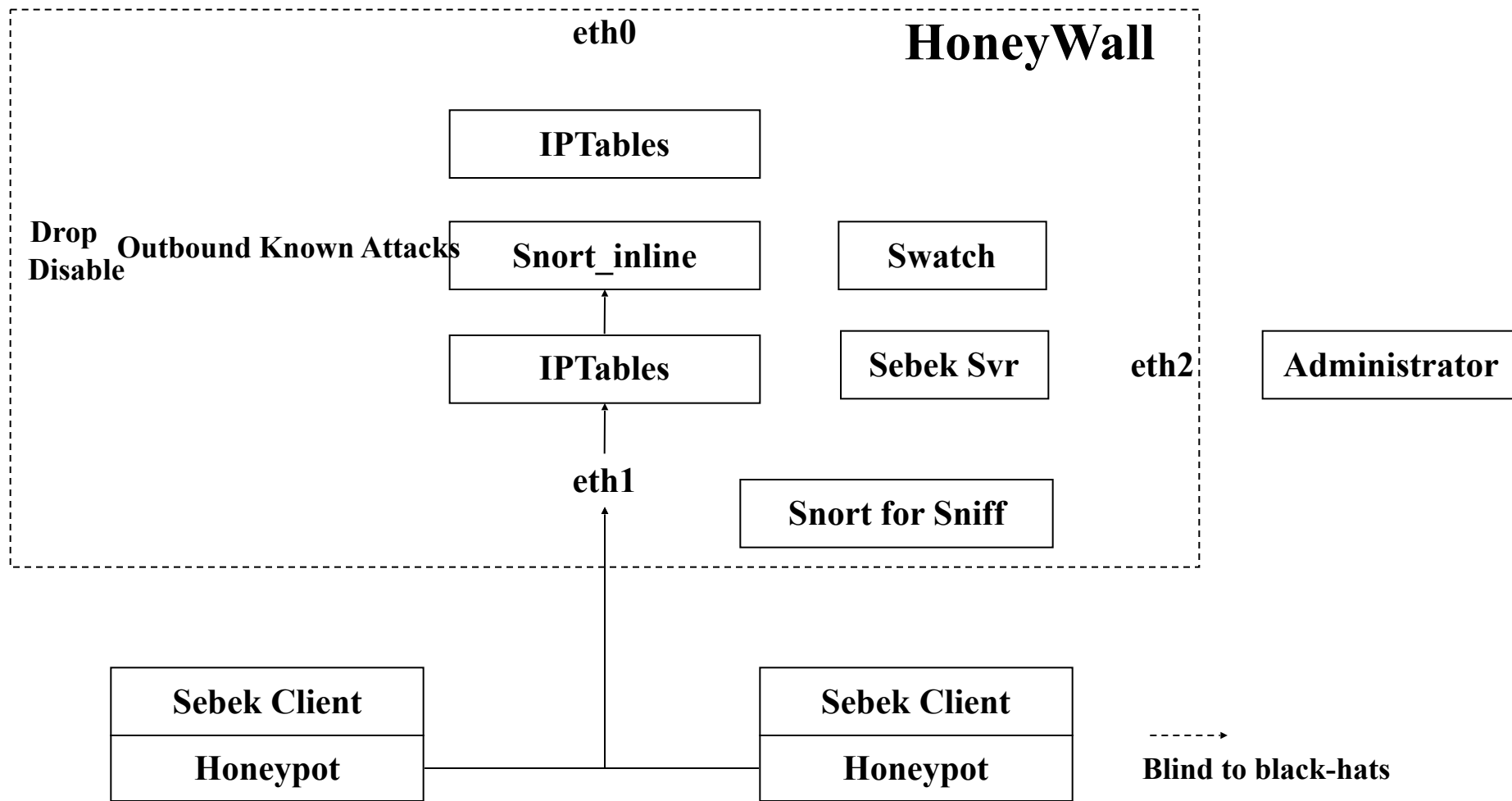


Gen II 蜜网技术 - 数据控制



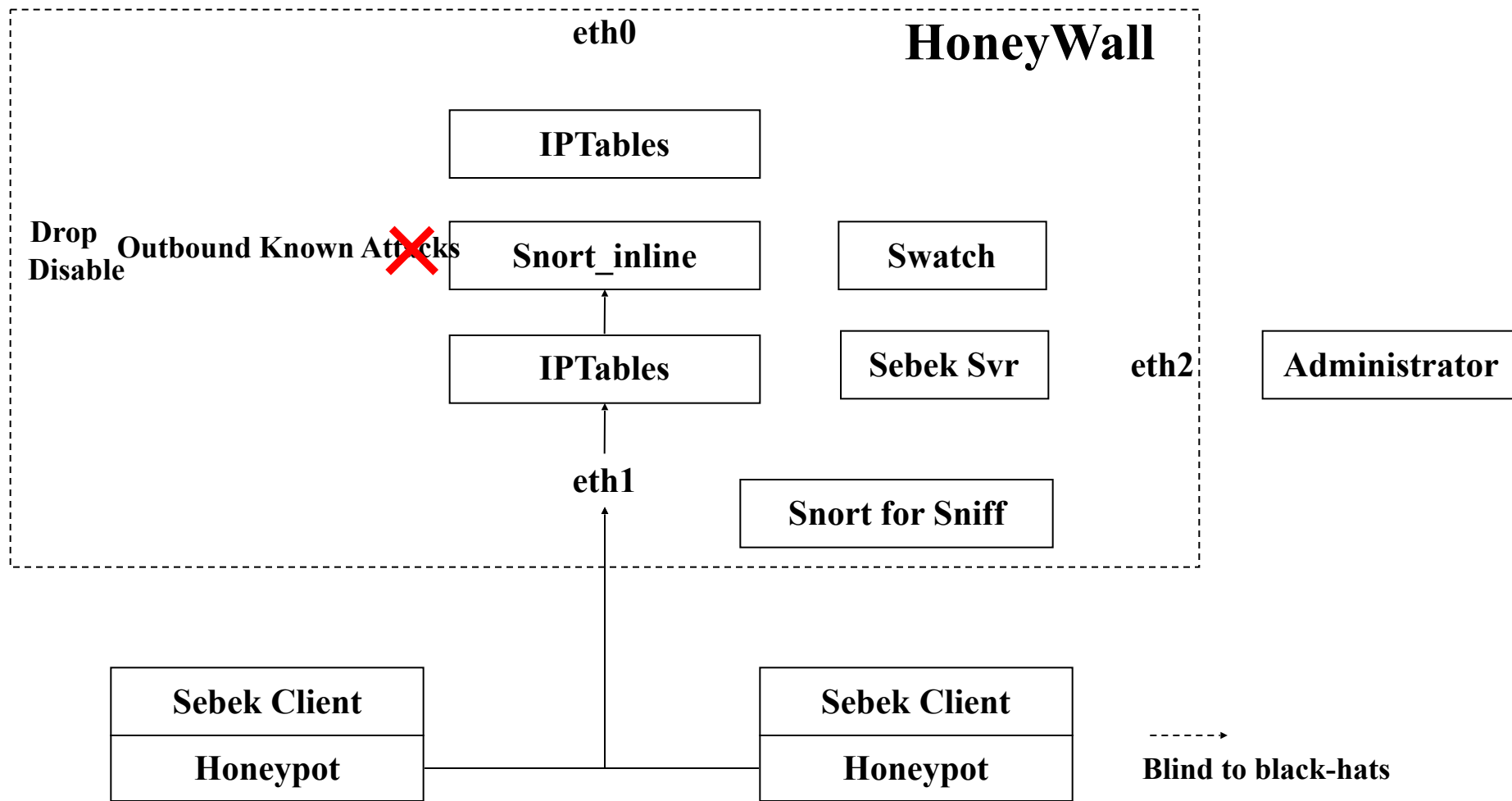


Gen II 蜜网技术 - 数据控制



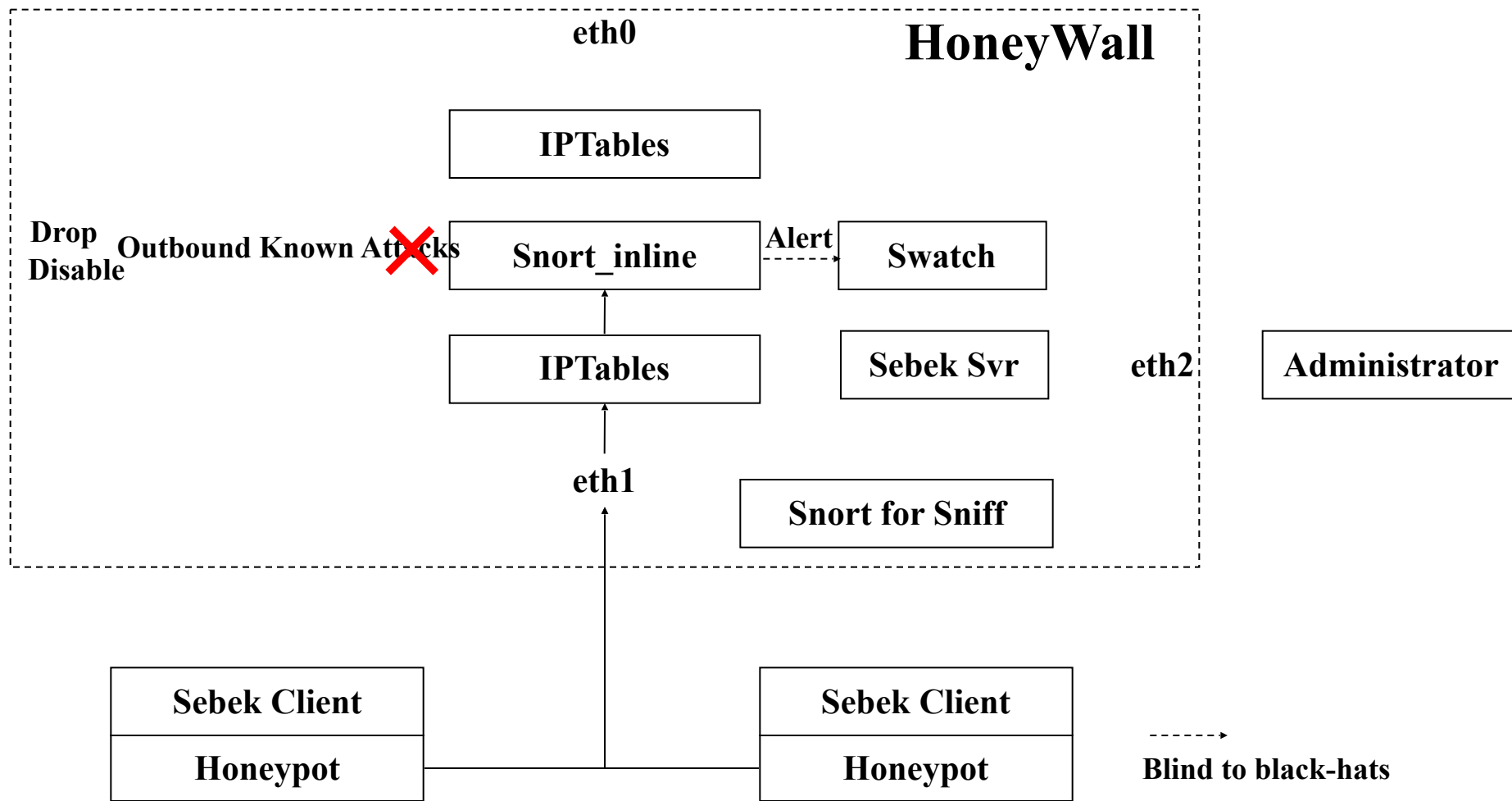


Gen II 蜜网技术 - 数据控制



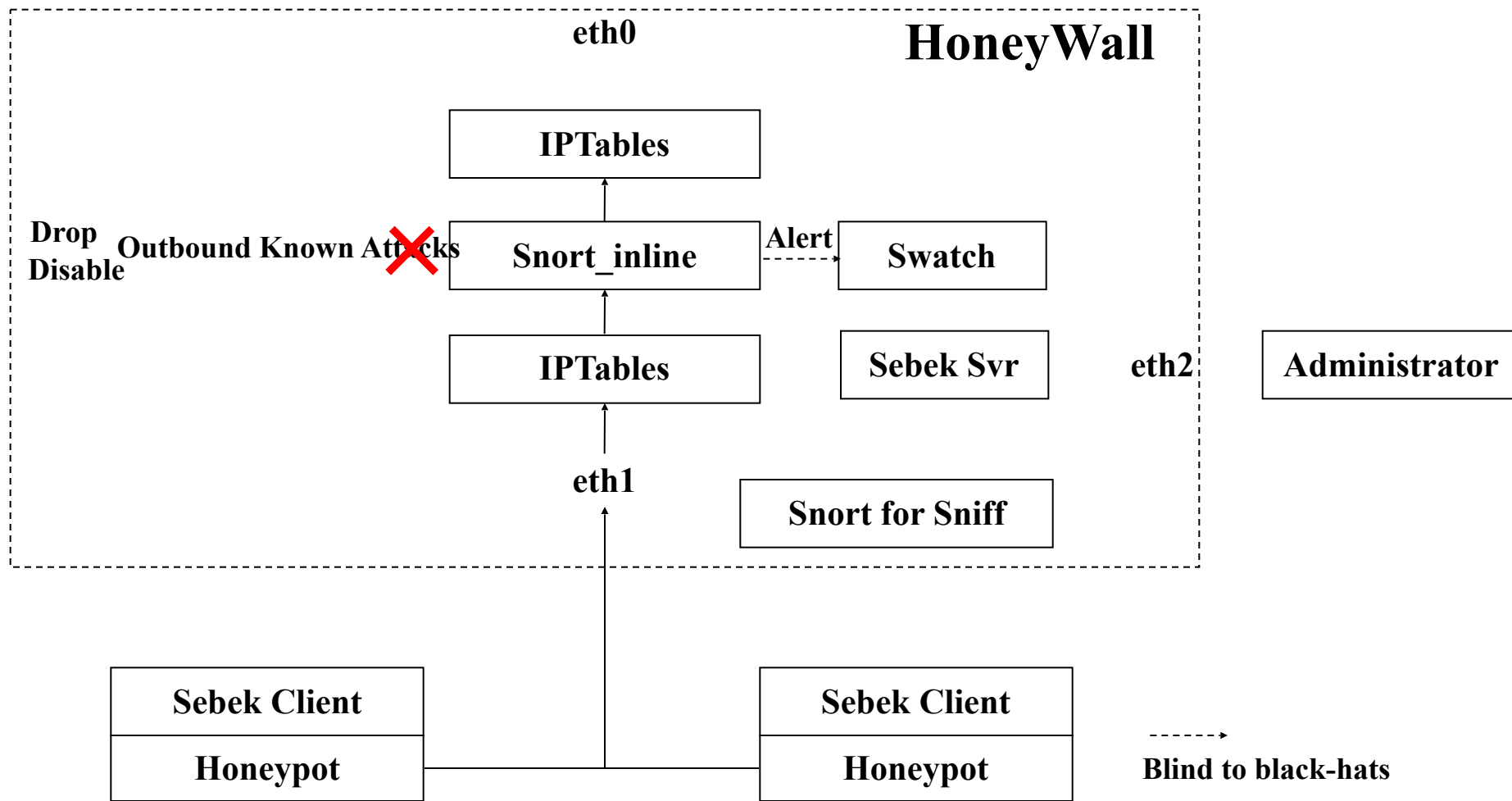


Gen II 蜜网技术 - 数据控制



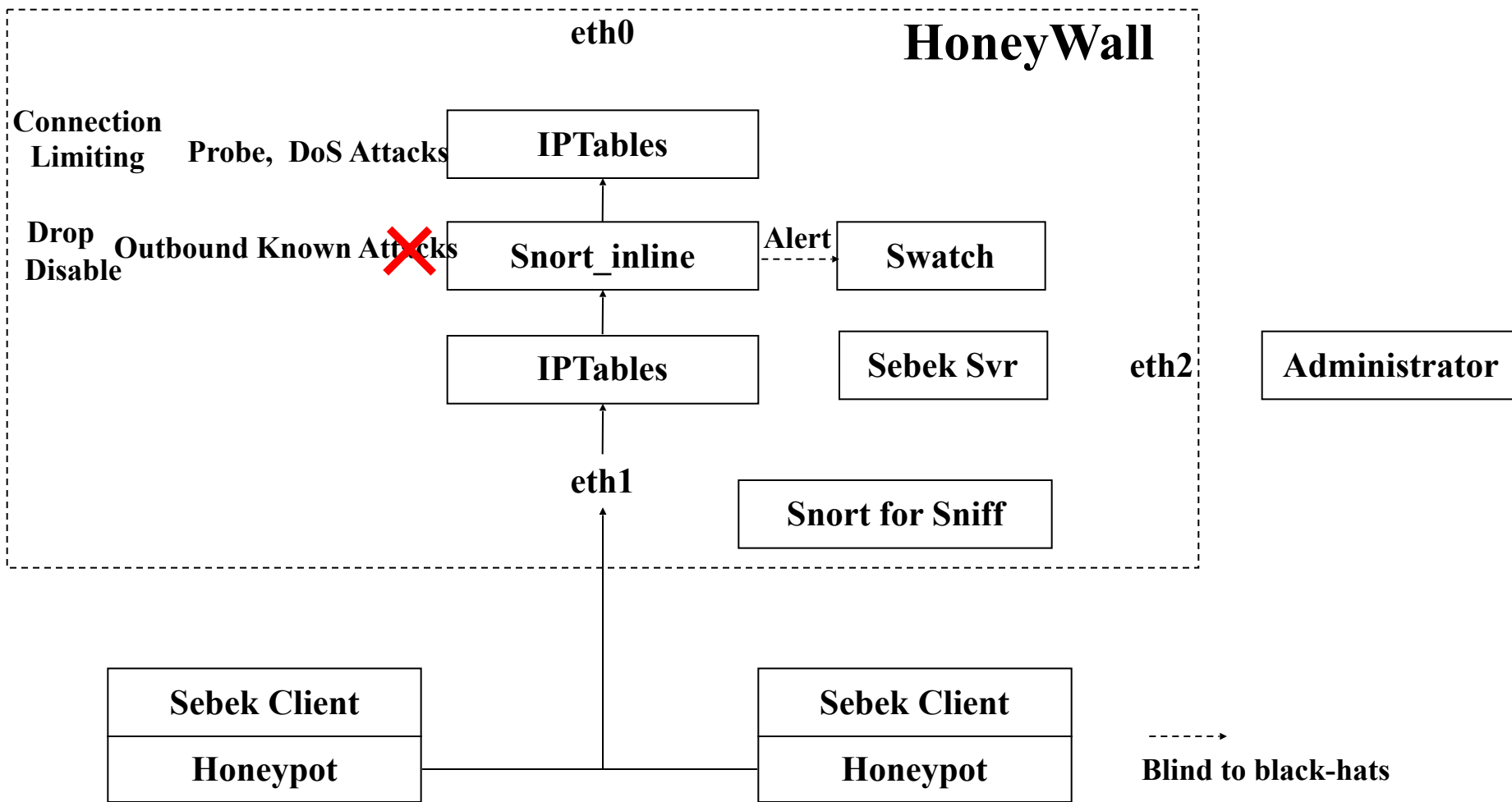


Gen II 蜜网技术 - 数据控制



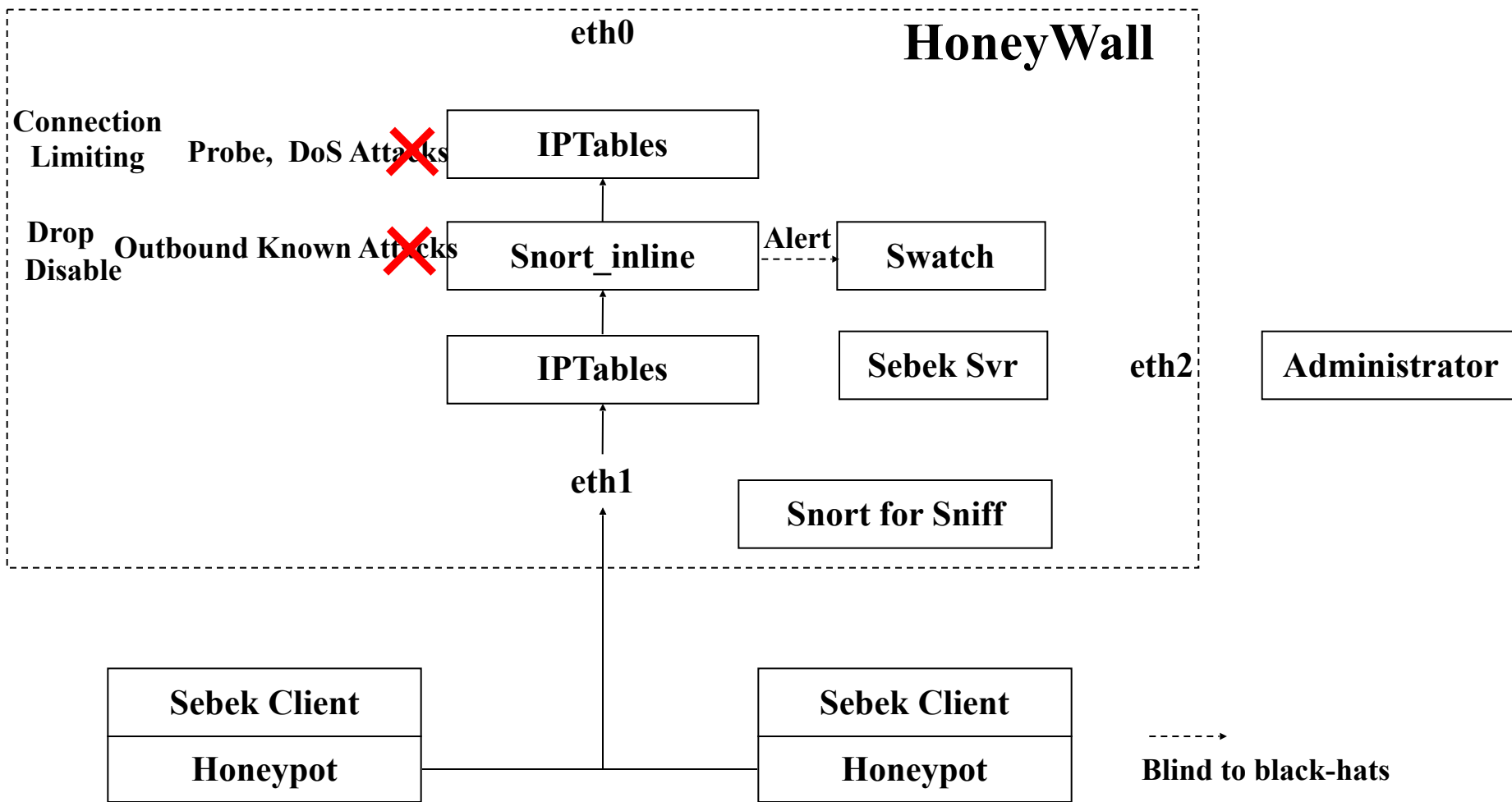


Gen II 蜜网技术 - 数据控制



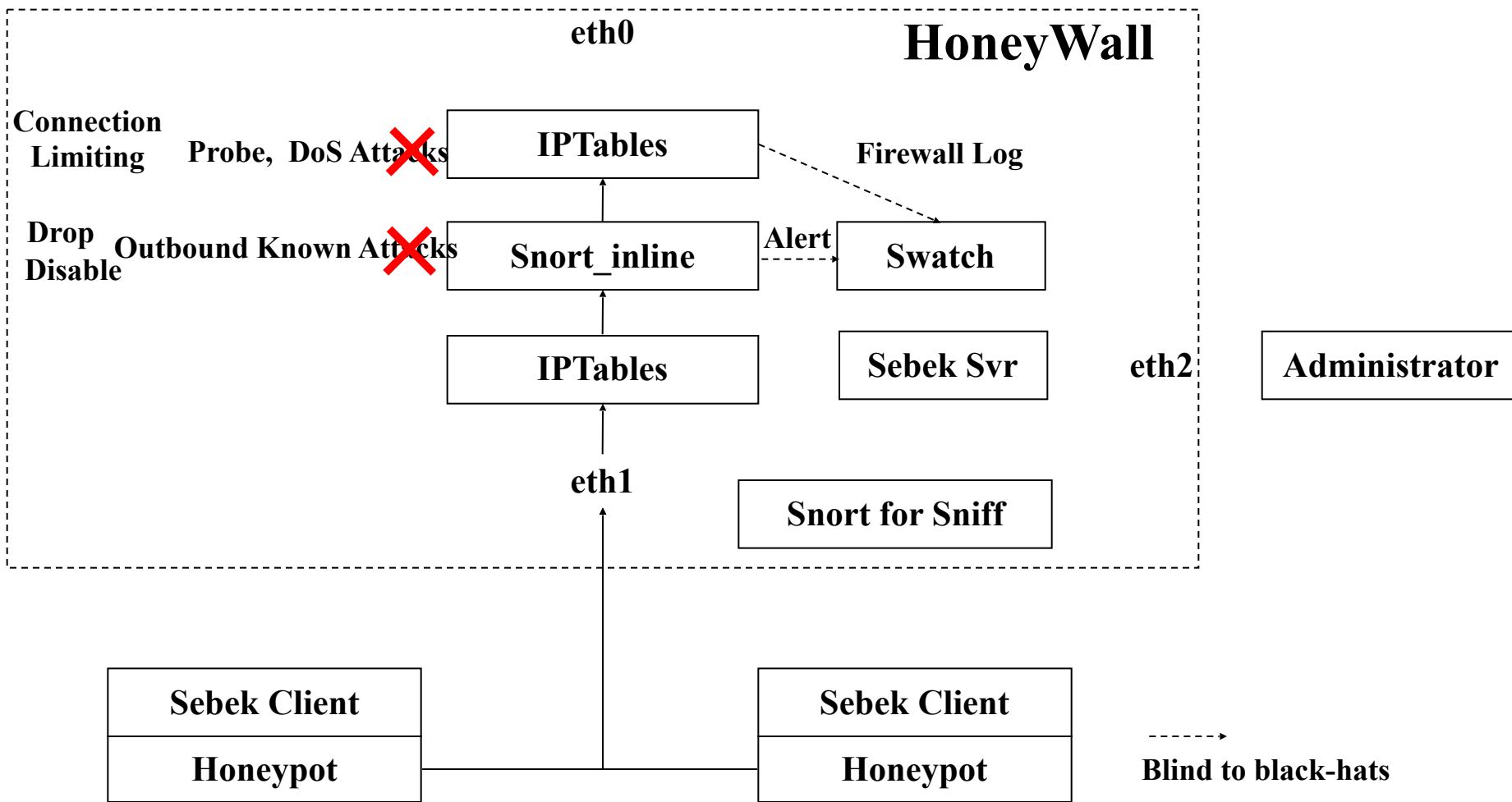


Gen II 蜜网技术 - 数据控制



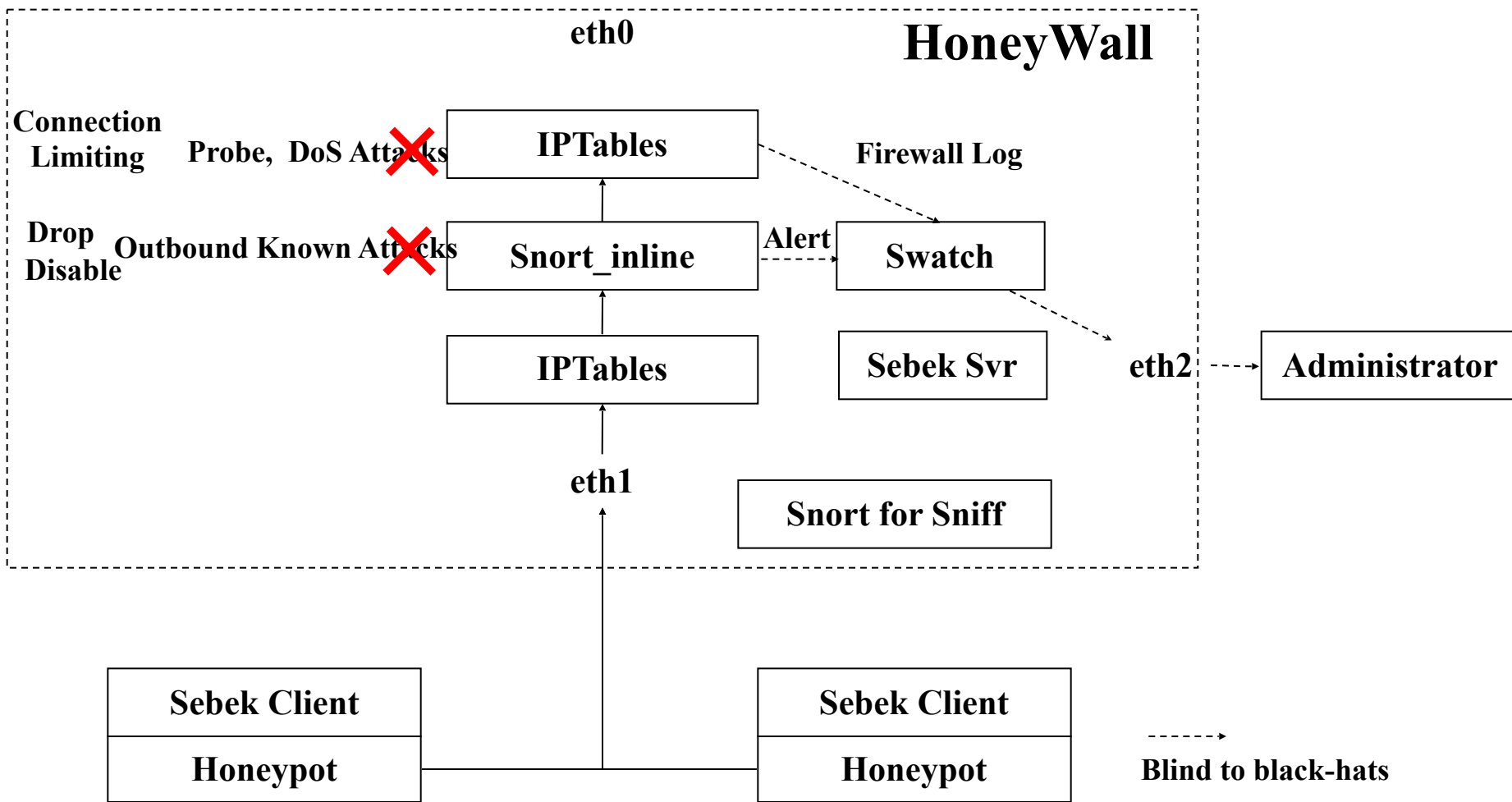


Gen II 蜜网技术 - 数据控制



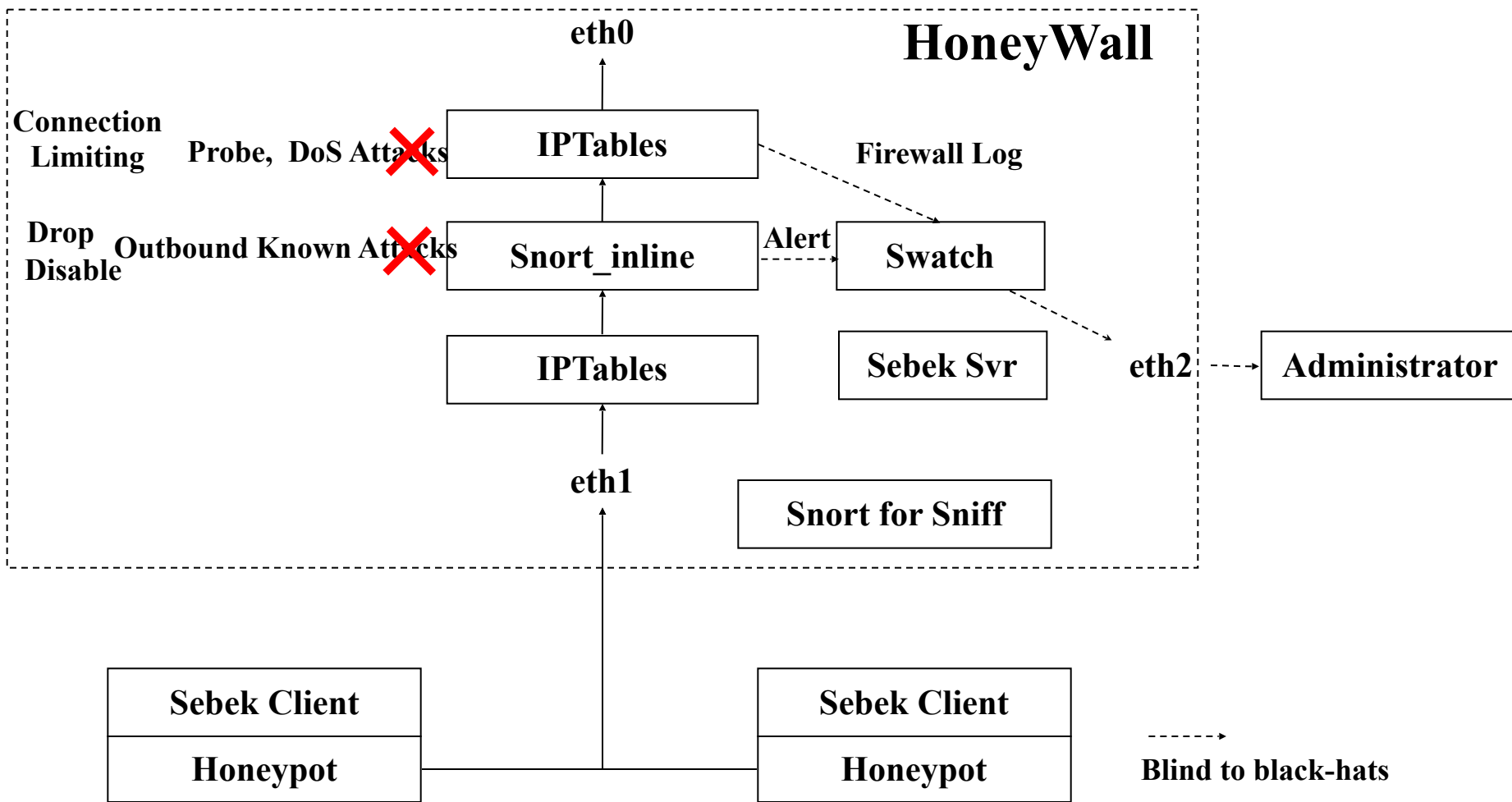


Gen II 蜜网技术 - 数据控制





Gen II 蜜网技术 - 数据控制





本章内容提要

- 蜜罐发展史
- 蜜罐关键技术
- 蜜网技术
- 蜜罐与蜜网技术的应用



本章内容提要

- 蜜罐发展史
- 蜜罐关键技术
- 蜜网技术
- 蜜罐与蜜网技术的应用



典型应用场景

- 恶意代码捕获
- 恶意代码分析
- 入侵取证
- 分流攻击流量



参考文献

1. The HoneyNet Project <http://www.honeynet.org/>
2. 中国蜜网项目组 <http://www.honeynet.org.cn/>
3. [http://en.wikipedia.org/wiki/Honeypot_\(computing\)](http://en.wikipedia.org/wiki/Honeypot_(computing))
4. <http://www.symantec.com/connect/articles/virtual-honeynets>
5. <http://www.projecthoneypot.org>
6. DTK <http://all.net/dtk/dtk.html>
7. SysTrace <http://www.citi.umich.edu/u/provos/systrace/>
8. Nepenthes <http://nepenthes.carnivore.it/>
9. PHARM <http://www.nepenthespharm.com/>
10. <http://www.blackhat.com/html/bh-usa-02/bh-usa-02-speakers.html#Honeynet>
11. 网络蜜罐与网络诱骗技术的研究与应用 <http://210.40.7.188/E%27yan/09/MGXP/000.asp>



课后思考题

- 举几个生活中的类比蜜罐实例
- 用自己的话去描述蜜罐的核心思想关键字：
诱、骗、捕