



SAVA应用 - 基于SAVA的DDoS检测与防御

胡延楠
ZGC实验室

大规模伪造源地址DDoS攻击仍面临挑战

- 伪造源地址一直是DDoS攻击的重要因素之一
 - 目标端检测和防御
 - 检测→引流→清洗→回注
 - 缺点：存在防御能力上限
 - 云端检测和防御
 - DNS/AnyCast引流
 - 缺点：流量绕路，增加额外时延
 - 中间网络检测与防御
 - 基于NetFlow采样分析
 - 缺点：准确性、及时性、非攻击时也不断采样
 - 之前的SAV技术：BCP38
 - uRPF：假阳性假阴性问题
 - ACL配置管理复杂
 - Ingress Filtering限出不限入
- 
- SAVA
 - 从准确性、性能及激励性上解决现有源地址验证技术的缺陷
 - 通过接入、域内、域间的体系化验证，使更准确快速的源地址验证成为可能
- 
- SAVNET标准化 -> 厂商实现
 - 参考IPv6的推广与部署过程
 - **SAVA设备的部署，也必然是一个漫长的过程**

SAVA少量部署对DDoS攻击的影响

接入网部署

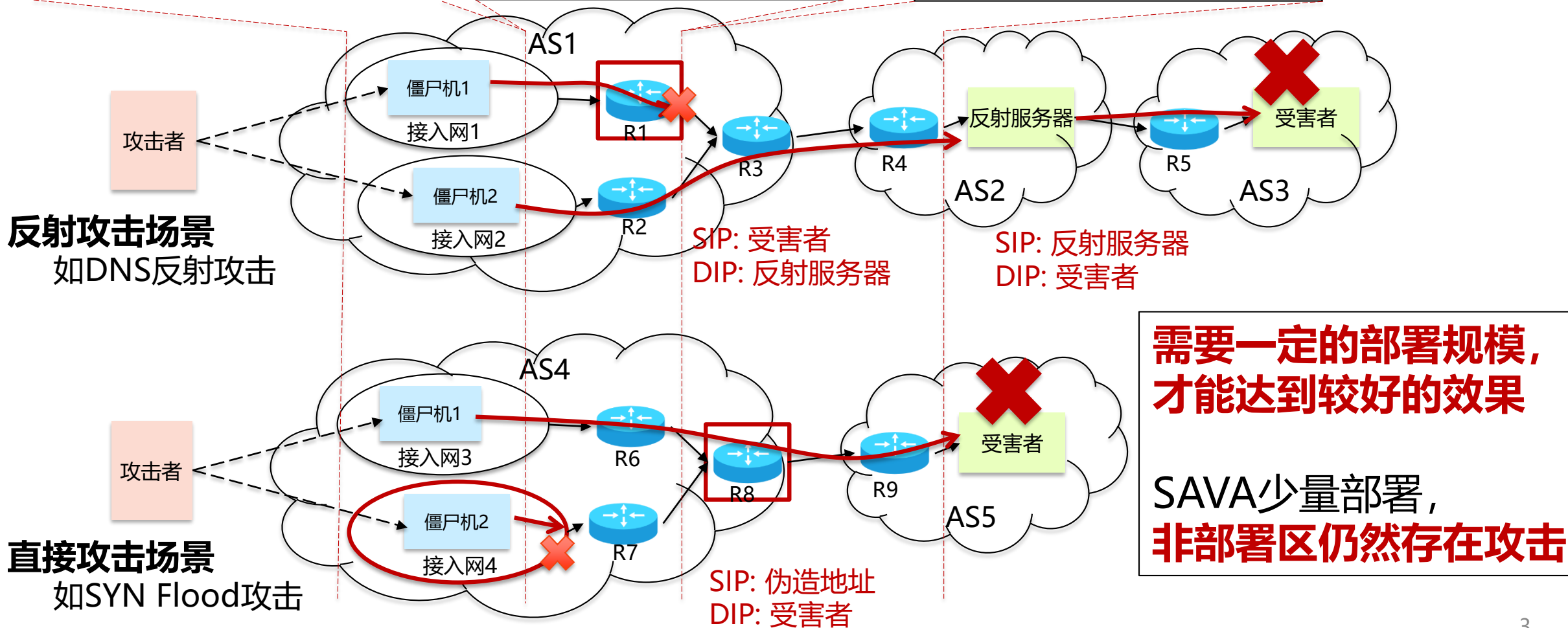
主机粒度防御效果好，很难要求所有接入网均部署SAVA

域内部署

前缀级别防御，难以防御同地址前缀内的源地址伪造

域间部署

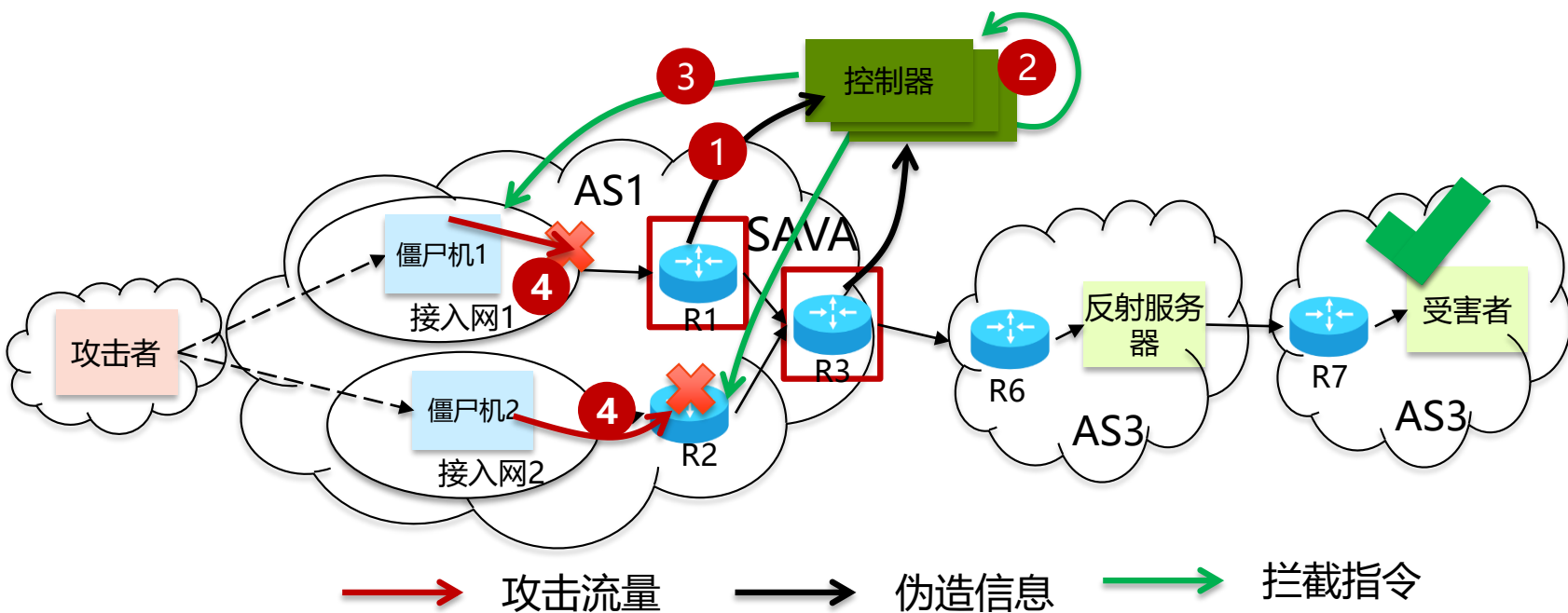
AS级别地址段防御，难以防御同AS内的源地址伪造



如何在少量部署的场景下更好发挥SAVA的优势？

- 现状：检测到伪造源地址后，**直接丢弃**
- 直接丢弃的缺点
 - 大规模攻击时，僵尸机广泛分布，少量部署效果有限
 - 持续直接丢弃，存在僵尸机向非SAVA部署区域迁移的可能
- SAVA的核心是绑定锚和IP的对应关系，检测到源地址伪造后，可以执行任意动作
- 在SAVA**增量部署过程中**，应优先进行**信息上报**而非直接丢弃
 - 通过伪造源地址报文信息(IP、端口号、TCP标识、地理位置等)，可以**检测各种反射攻击和直接攻击**
 - 能够**更准、更早的**发现潜在威胁，在形成大规模攻击之前做出响应

利用SAVA信息进行全网防御

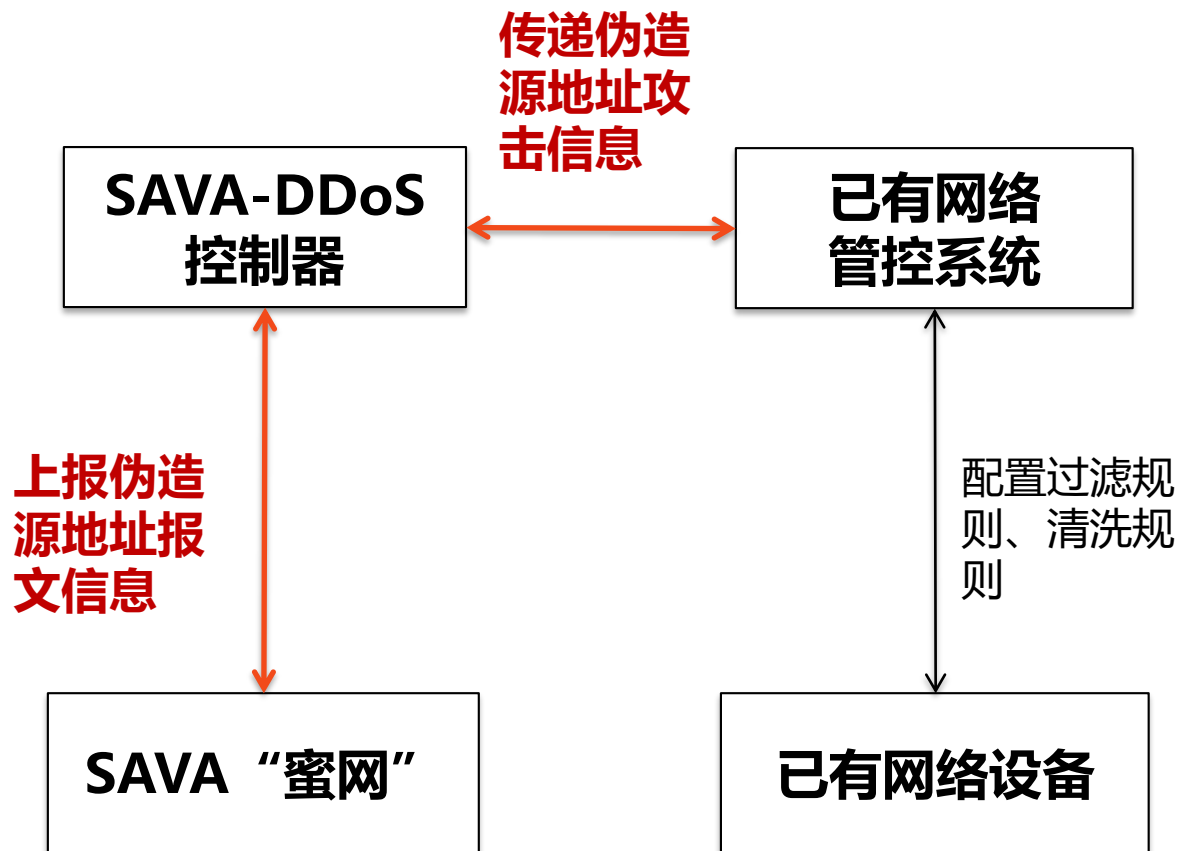


1. 攻击提前检测
2. 攻击行为分析
3. 协同拦截策略
4. 大规模攻击体系化防御

- 构建攻击行为分析系统，实现攻击识别及溯源
- SAVA部署越多，系统越大，数据越多，分析越全面
- 非必要不拦截，关键时刻发挥作用，攻击威慑作用

基于SAVA的DDoS检测与防御架构

SAVA-based Anti-DDoS Architecture[*draft-cui-savnet-anti-ddos*]



- **SAVA设备**
 - 识别并上报伪造信息
- **SAVA-DDoS控制器**
 - 可扩展：分布式部署，逻辑集中
 - 层次化：接入、AS域内、AS域间，逐层汇聚，域间按需共享
- **重点**
 - SAVA设备上报伪造报文信息
 - 攻击信息传递

伪造源地址信息上报及攻击信息的传递

- 功能
 - 发现伪造源地址之后，上报五元组、源MAC、TCP标识、位置等信息
- 现状
 - 基于SNMP trap/syslog，不同厂商实现不一致，且信息缺失
 - 接入网（有线/无线）、域内网络、域间网络 SAVA可检测到的伪造源地址信息存在差异性
- 定义统一的伪造信息上报方式/数据模型
 - 可能的路线
 - YANG + NETCONF Event Notification
 - IPFIX
- 功能
 - 攻击信息传递、发现、心跳、路由信息等
- 需求
 - 对丢包有鲁棒性、支持双向通信、支持安全机制等
- IETF DOTS (DDoS Open Threat Signaling) 是一个很好的基础
 - 定义了攻击信息的传递机制及协议
 - 受攻击方可以向攻击缓解方请求防护
 - 可以支持正反向通知，支持ACL配置，支持管理配置及状态查询等
- 利用并扩展DOTS

总结

- 少量部署场景，利用源地址伪造信息上报来发挥SAVA的优势
- 通过攻击行为检测和分析，结合全网资源进行防御
- 准确性
 - 非抽样检测，准确性高
 - SAVA检测伪造源地址无假阴性和假阳性问题
 - 随着SAVA的部署，攻击识别准确率升高
- 安全性
 - 流量无需经过第三方，无隐私问题
 - 不影响正常流量访问
- 实时性/经济性
 - 在原有数据面线速清洗流量，避免处理和转发时延
 - 及时检测，无需采样检测的导出等待
 - 无攻击时无上报，无需持续检测，更经济
- 可扩展
 - 分布式拦截，防御能力理论无上限
 - 可接入其他信息联合检测
 - 可接入其他清洗设备联合防御

谢谢
