

# ASC

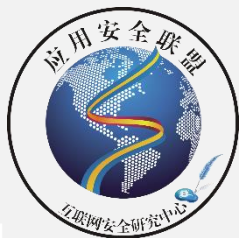
## 应用安全联盟

# 2016 移动物联网安全高峰论坛

# 云与虚拟化安全的新挑战与防御

铱迅CEO 杨谦

Copyright © by SecZone All rights reserved.





# 目录

**1 云与虚拟化现状**

**2 云与虚拟化的安全挑战**

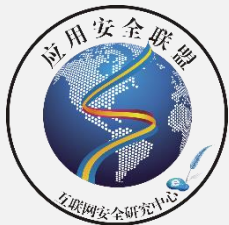
**3 云与虚拟化安全防护技术**

**4 云与虚拟化防护的典型实践**



# CLOUD AND VIRTUALIZATION

## 云与虚拟化的现状



# 云计算的发展风起云涌



## 云计算概念

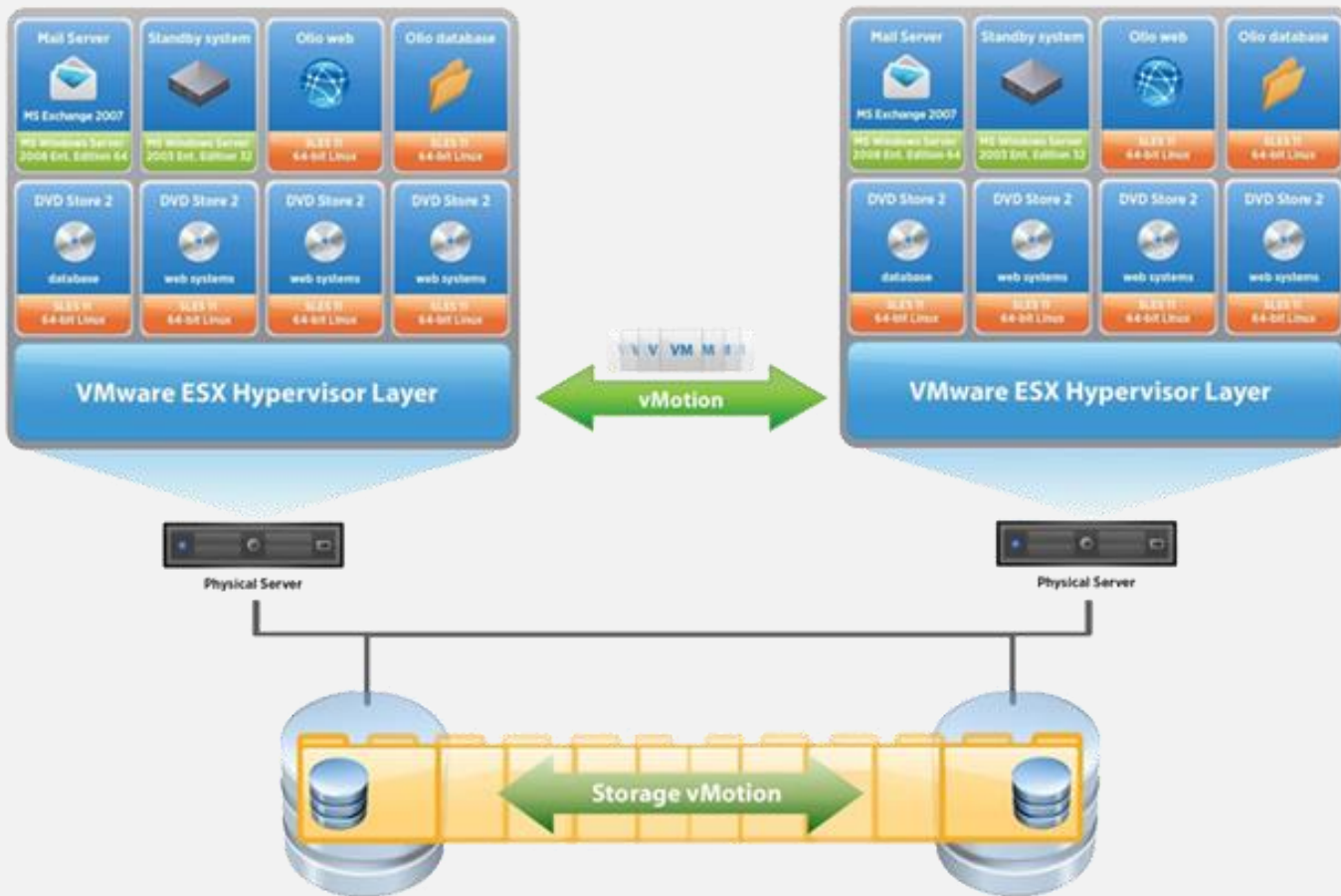
- 云计算是一种IT资源的交付和使用模式，指通过网络以按需、易扩展的方式获得所需的硬件、平台、软件等资源。

## 云计算发展

- 云计算被看作第三次IT浪潮，服务功能日益完善，种类日趋多样，云服务高速成长



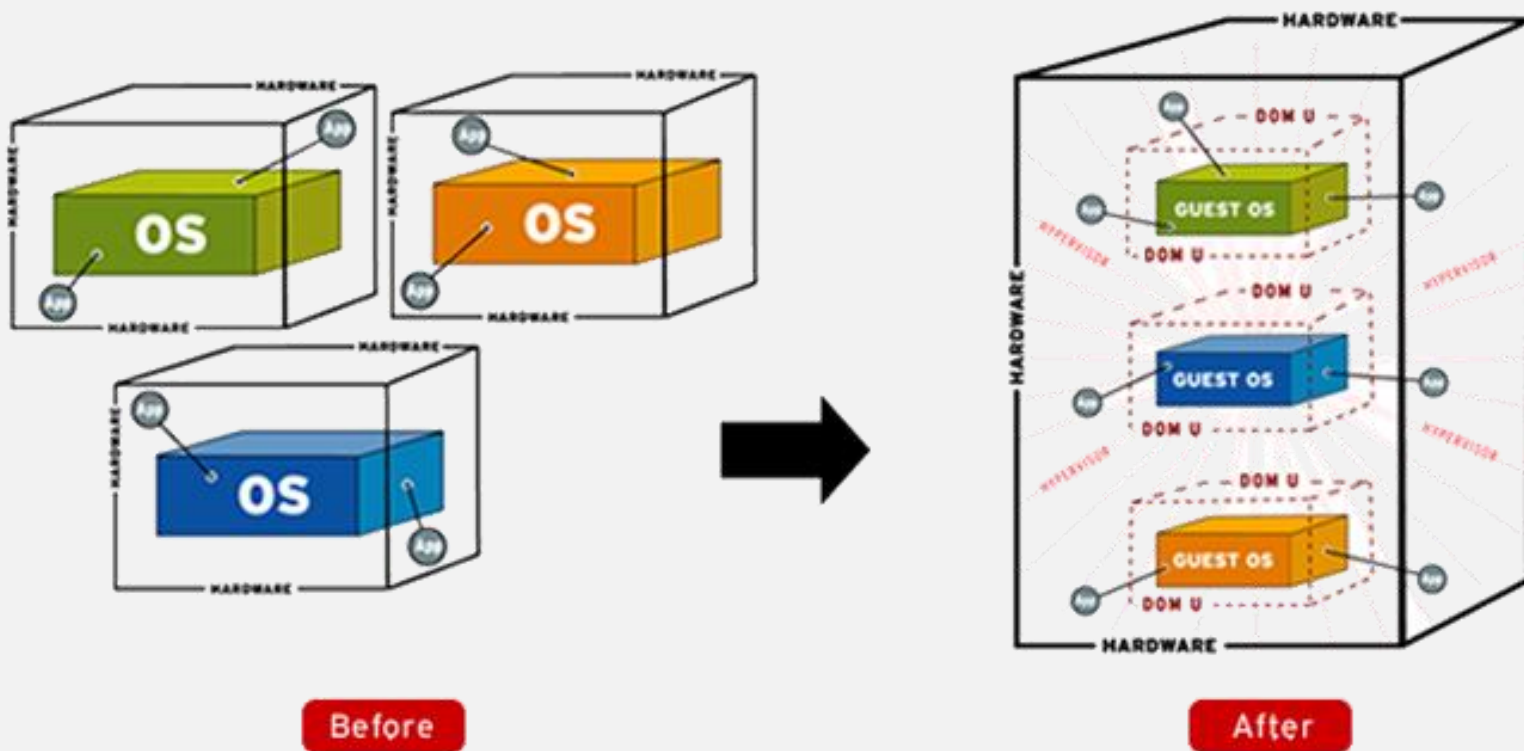
# 虚拟化技术典型结构



虚拟化平台结构



# 虚拟化技术介绍



**N台物理服务器并入一台虚拟化服务器**



# 虚拟化的优势



虚拟化整合使得IT基础架构从一般运行环境  
转换到战略性计算平台



# CHALLENGE

# 云与虚拟化的安全挑战





# 云与虚拟化安全问题依旧



云的传统安全威胁



# 挑战一

# DDOS



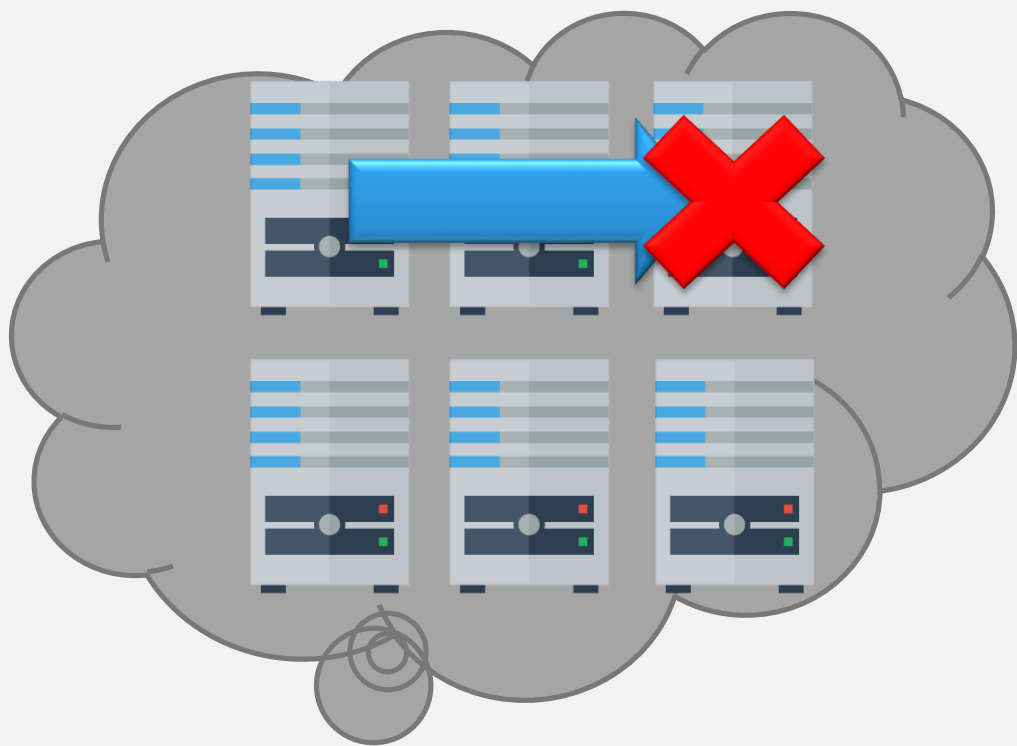
## 挑战一 外部巨量的DDoS攻击



外部网络出口带宽  
被DDoS堵塞



## 挑战一 内部DDOS攻击



内部DDoS绕过  
出口抗D设备



# 挑战二

# 网络入侵

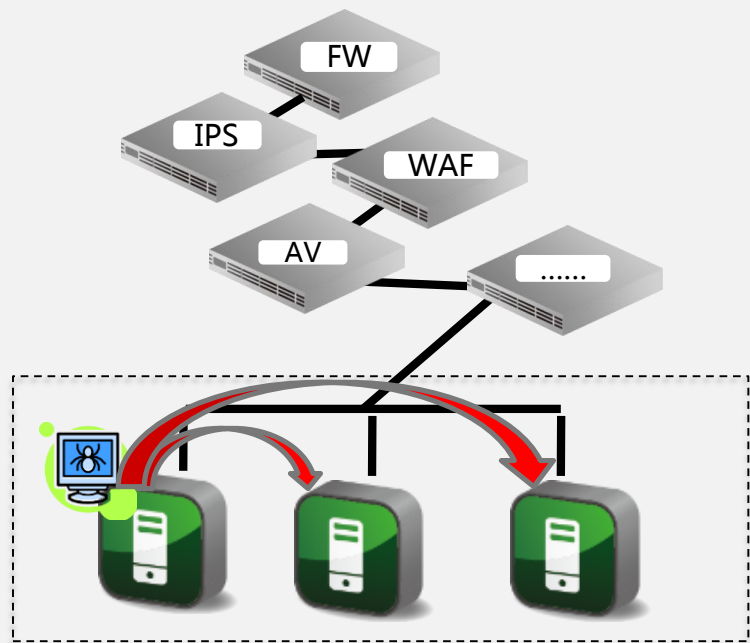


## 挑战二 入侵攻击



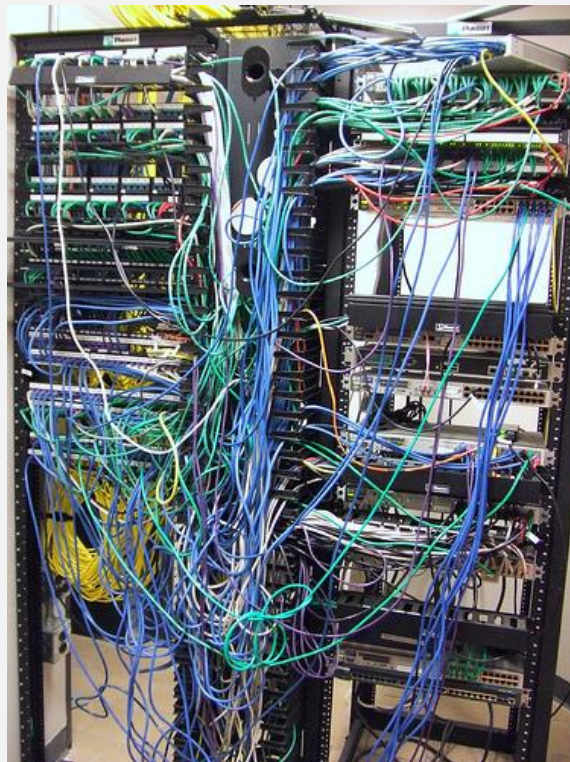


## 挑战二 传统串设备方案成瓶颈



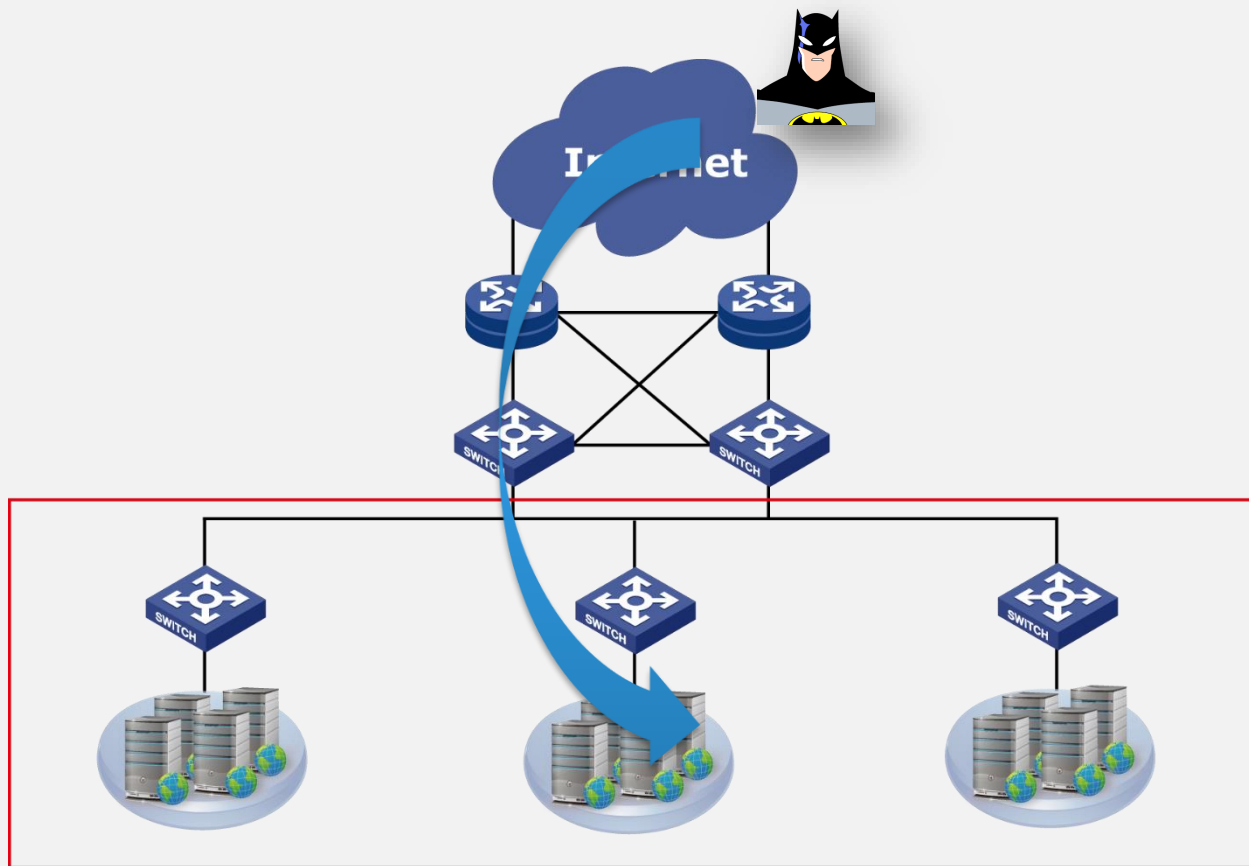
串糖葫芦、性能瓶颈、延迟高、  
无法精细控制、无法自主控制

企业内网





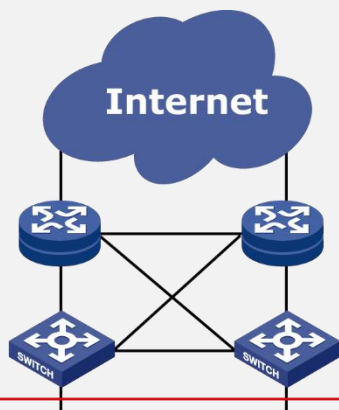
## 挑战二 入侵攻击之南北向







## 挑战二 入侵攻击之东西向



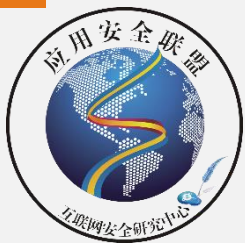
东西向流量  
虚拟机之间攻击不设防

虚拟交换机





# 挑战三 10风暴

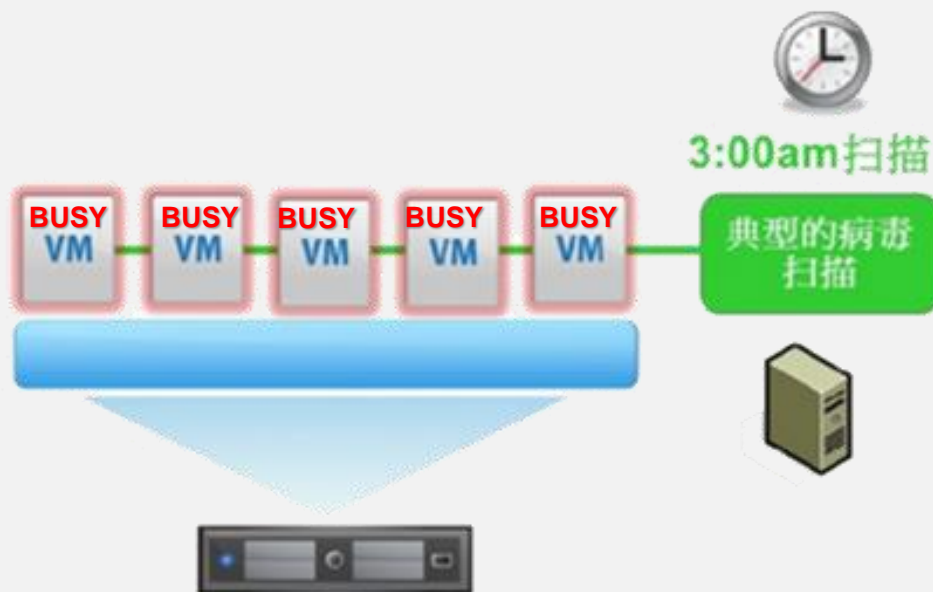


## 挑战三 IO风暴

单台VM被攻击，在短时间内频繁请求磁盘上的随机文件，造成超过物理磁盘的IO极限。

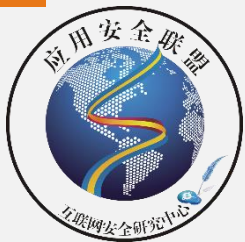


典型的如“防病毒风暴”  
(AV - Storming)





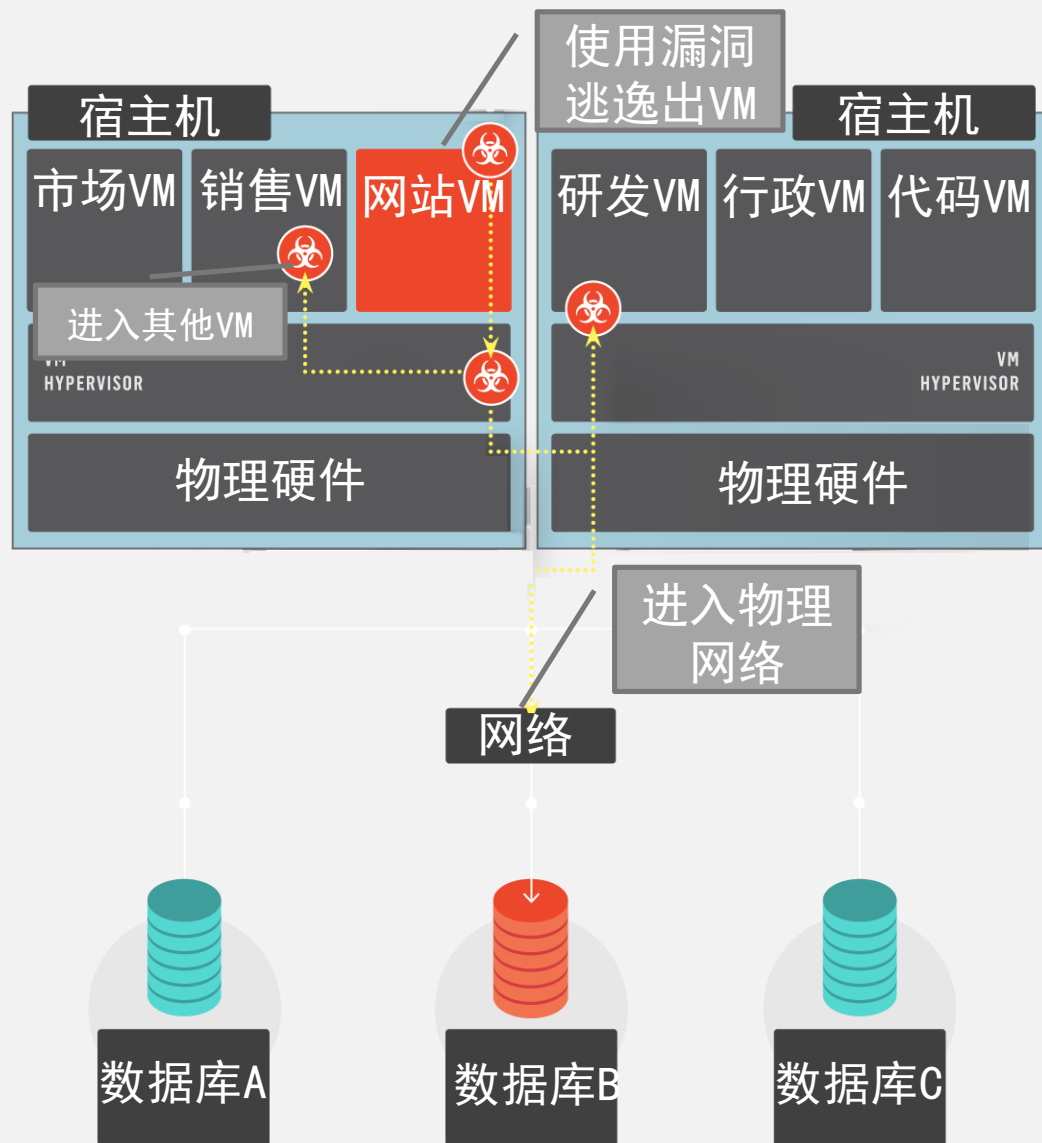
# 挑战四 虚拟机逃逸



## 挑战四 虚拟机逃逸

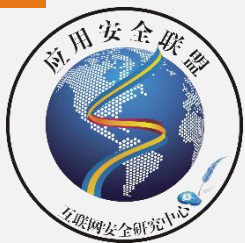
虚拟机逃逸 (Virtual Machine Escape) 是一种应用，其中攻击者在允许操作系统与管理程序直接互动的虚拟机 (VM) 上运行代码。

QEMU官方公开了两个由LingLiu独立发现并报告的缓冲区溢出漏洞，通用漏洞编号分别为CVE-2015-7504和CVE-2015-7512，两个漏洞均存在于QEMU所虚拟实现的AMD PC-Net II网卡组件。



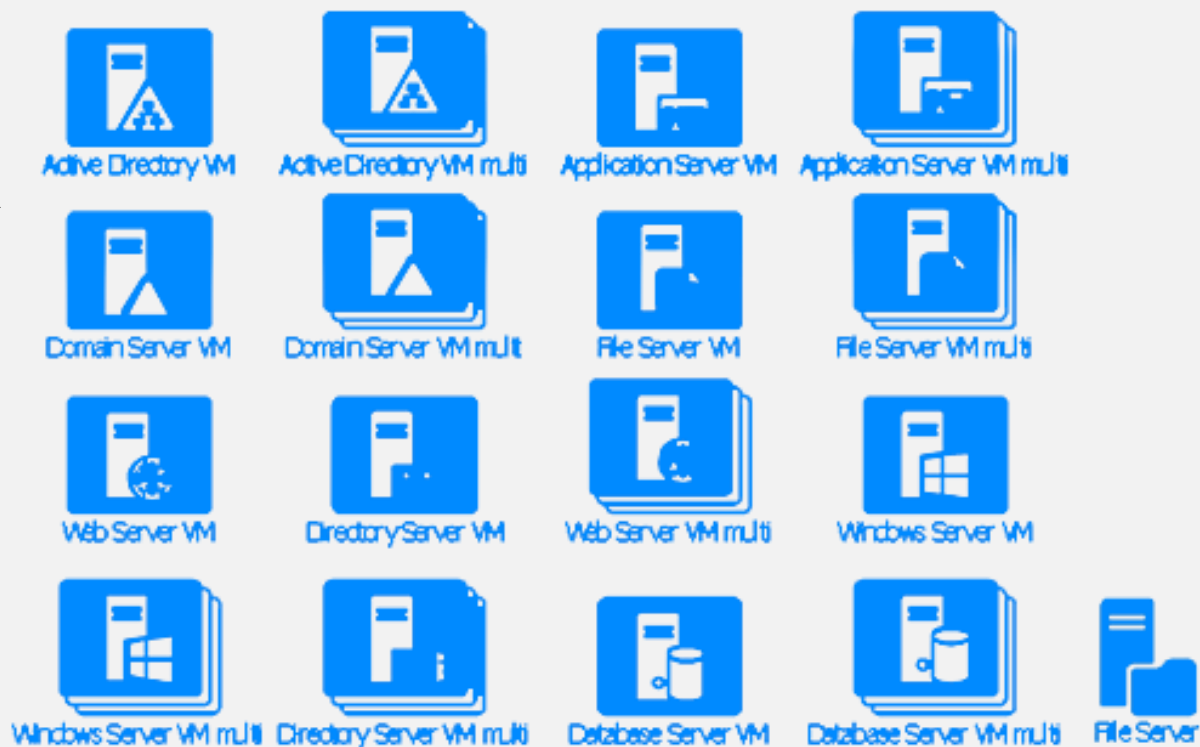


# 挑战五 安全管理



## 挑战五 安全管理

不同管理人员  
不同权限  
不同配置  
不同……





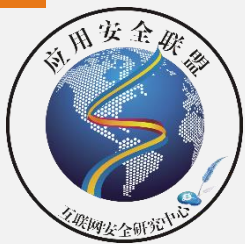
SOLUTION

# 云与虚拟化安全防护技术





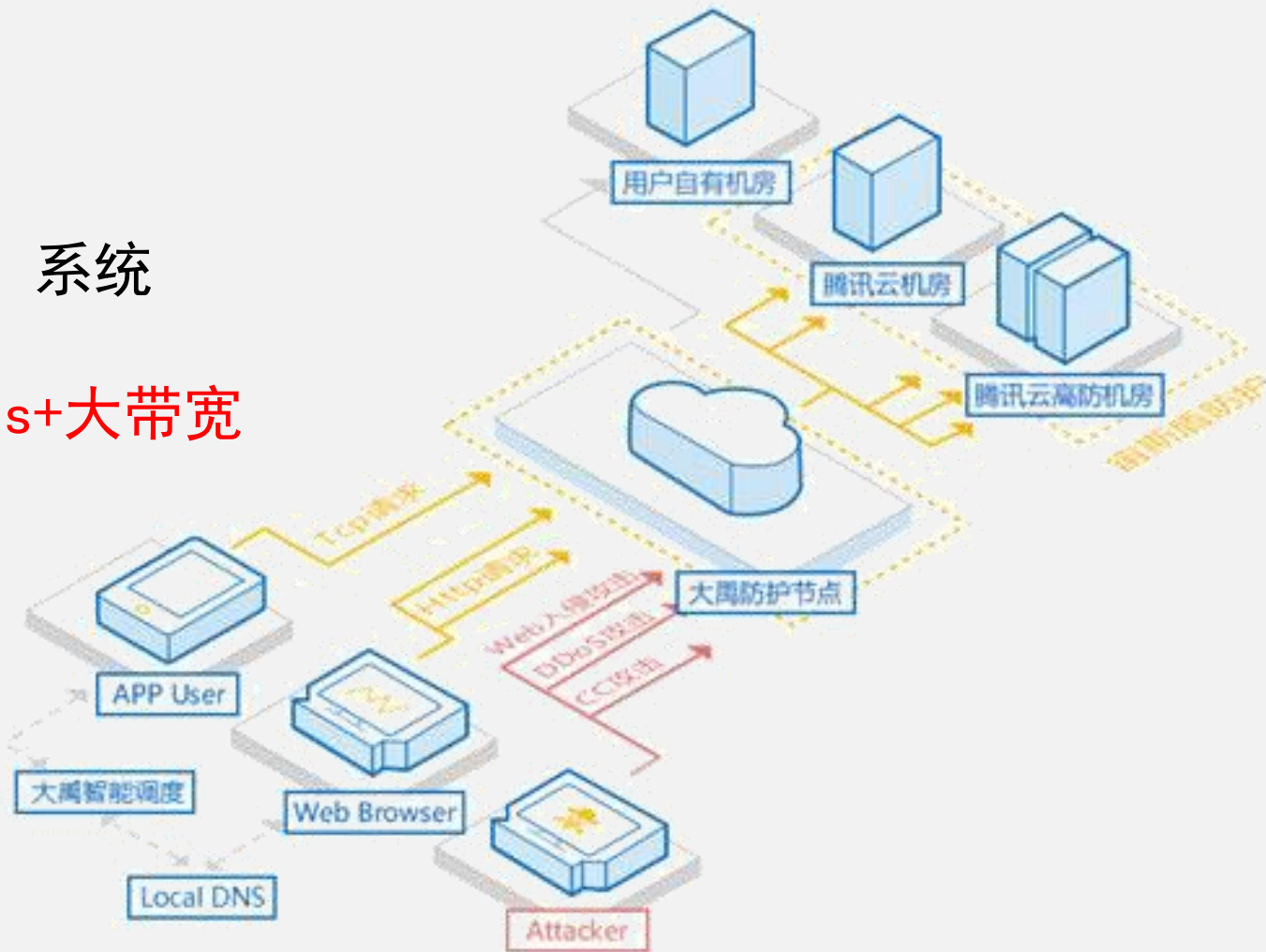
# DDOS怎么办？



# 解决一 公有云DDoS防御

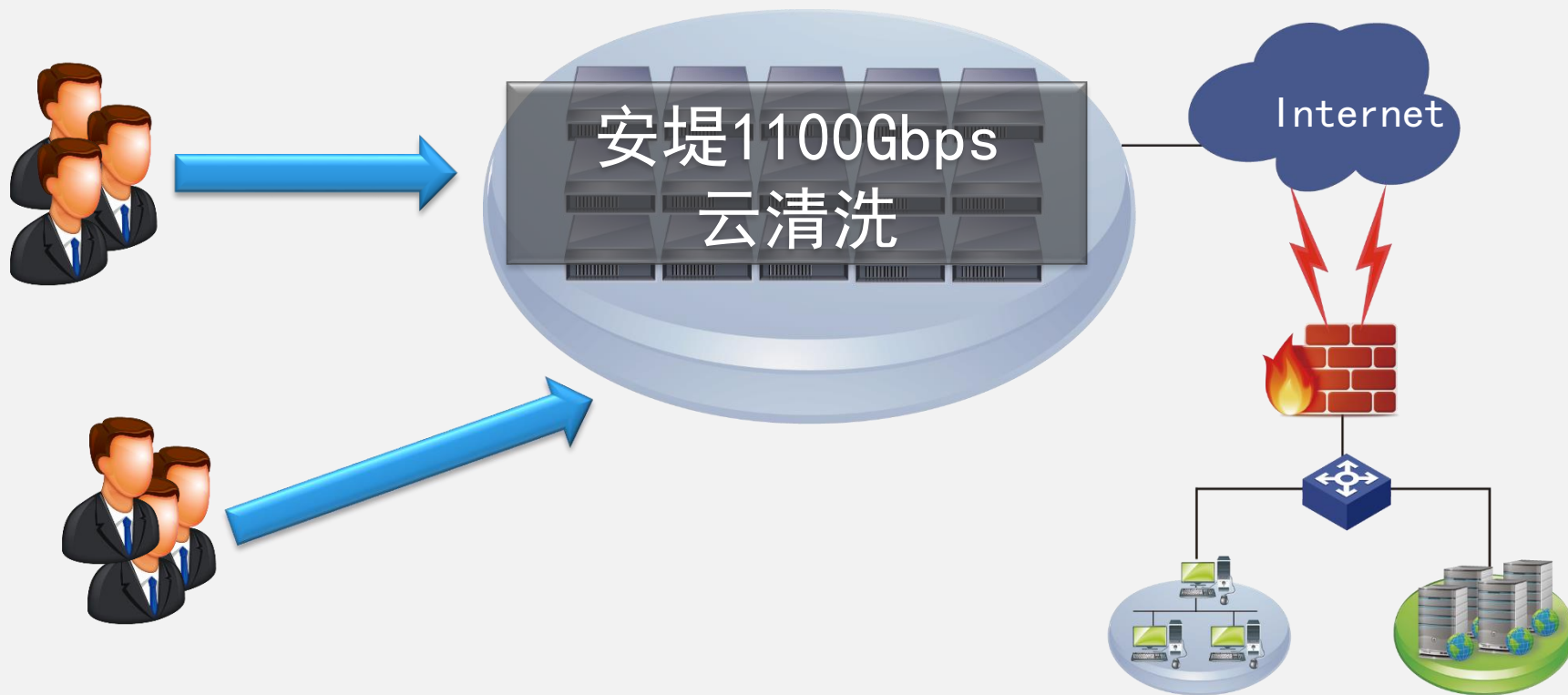
腾讯“大禹”系统

专有1000Gbps+大带宽



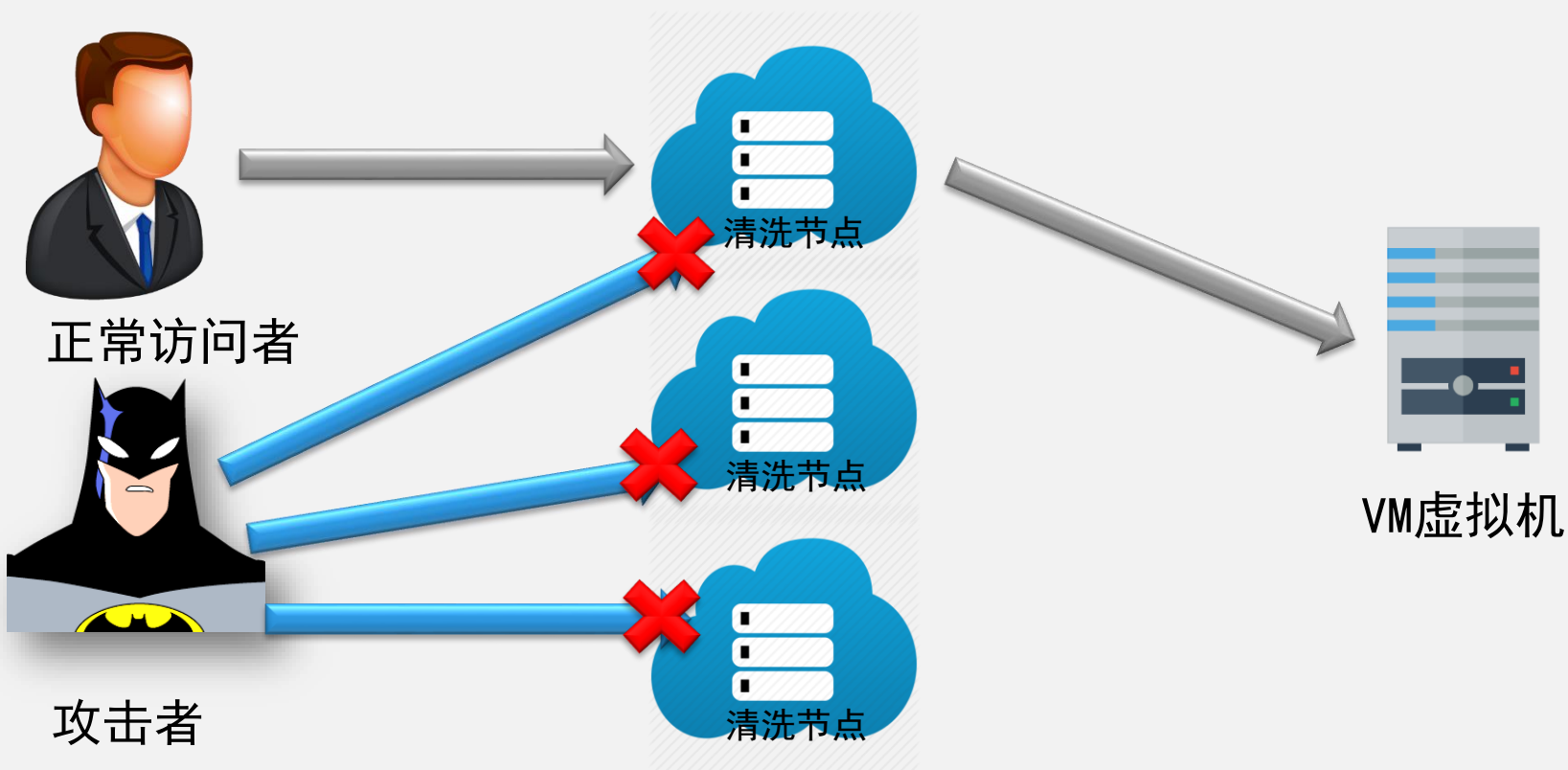


# 解决一 私有云DDoS防御 大流量云清洗





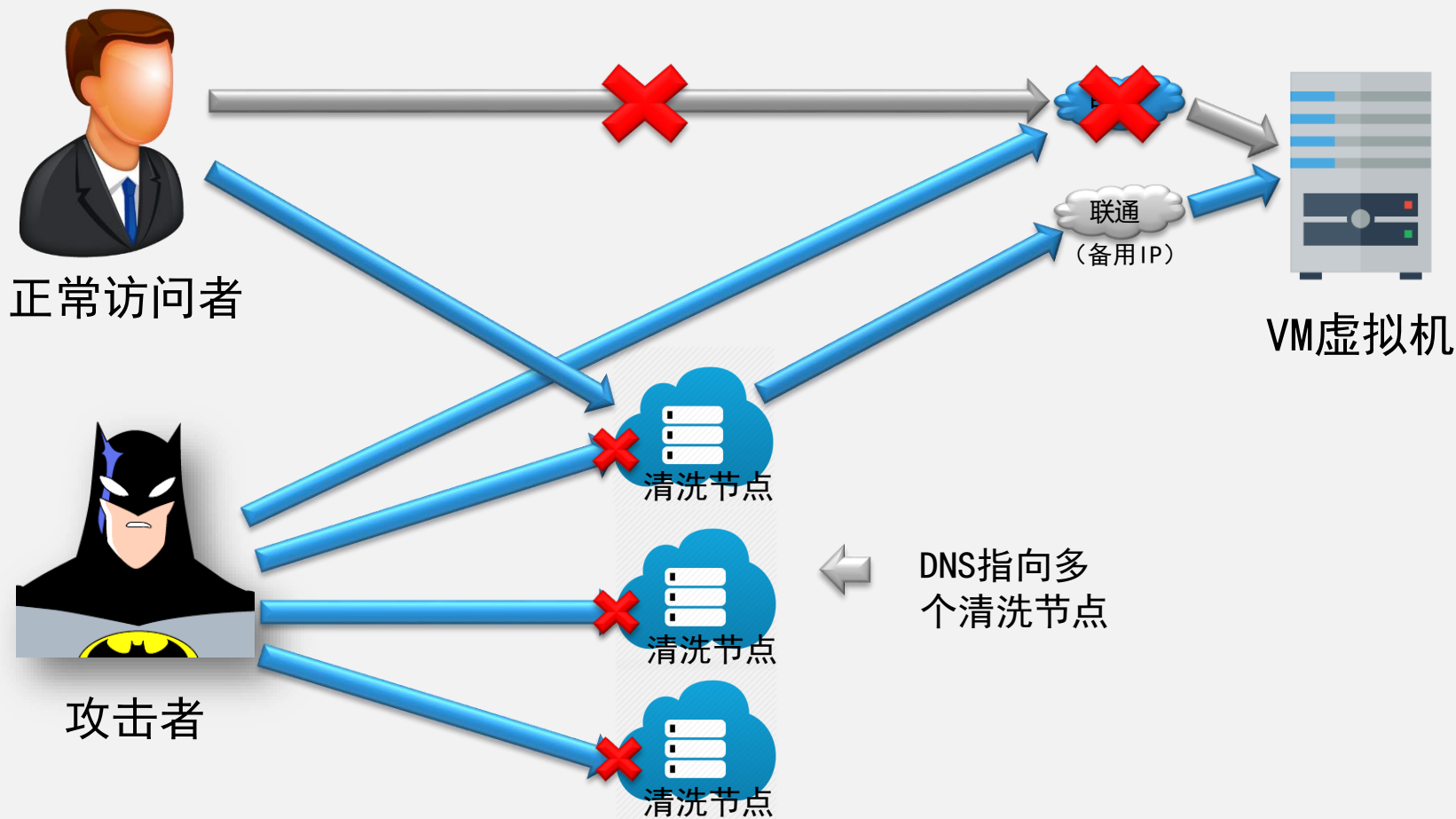
# 解决一 私有云DDoS防御 永久流量牵引



<http://anti.cc> 安堤的清洗集群



# 解决一 私有云DDoS防御 攻击时牵引



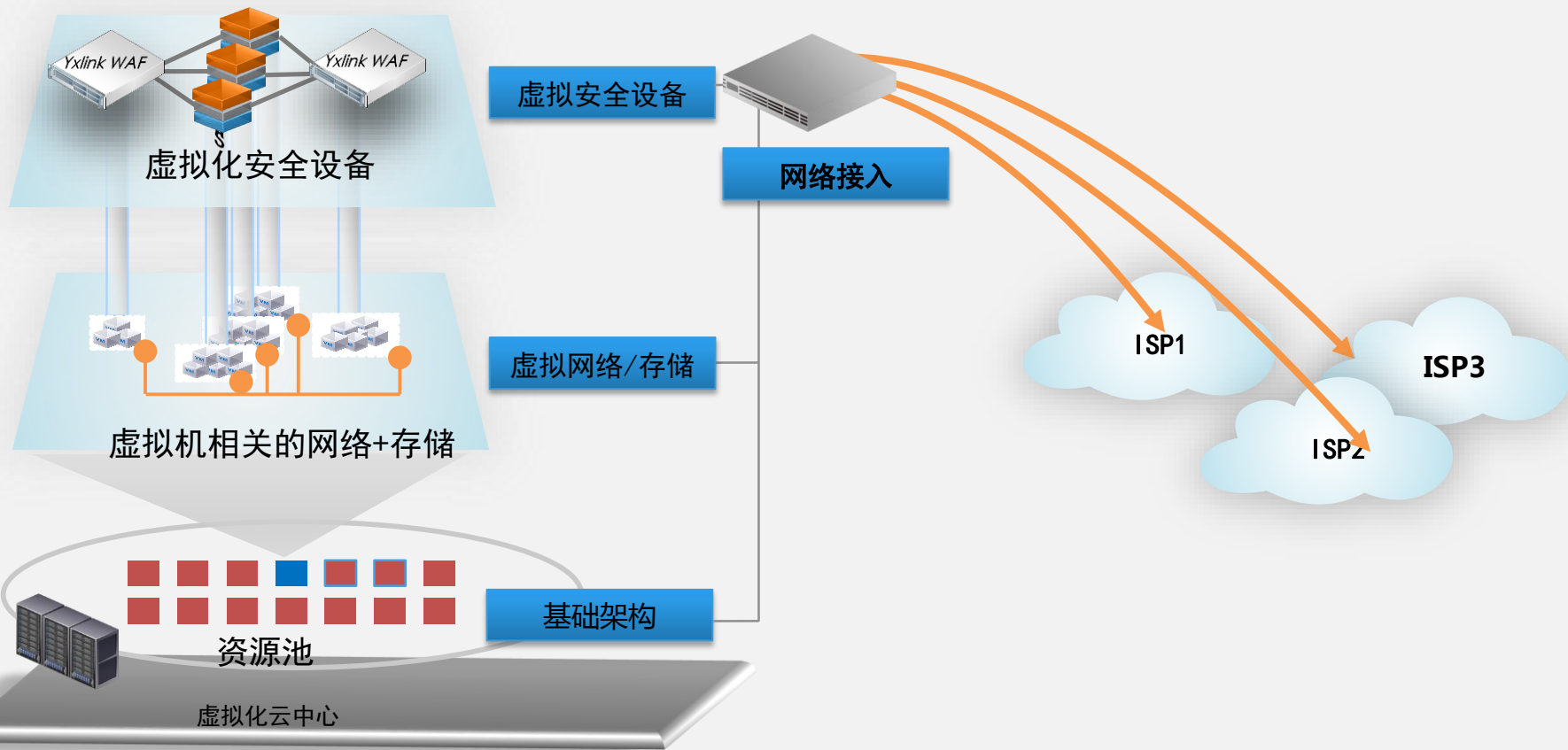
<http://anti.cc> 安堤的清洗集群



# 网络攻击 如何防？

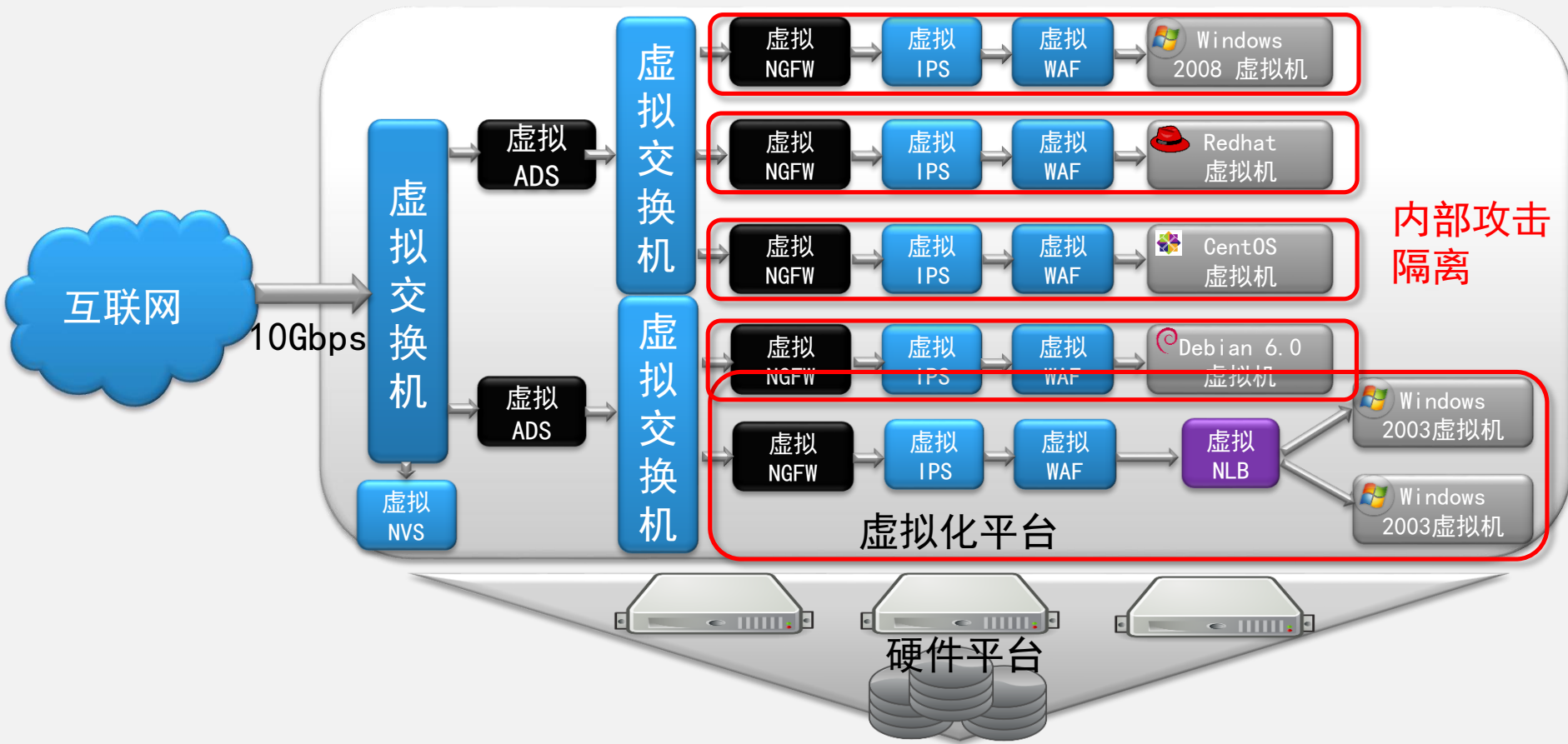


## 解决二 虚拟化安全设备防御攻击





## 解决二 虚拟化安全设备防御攻击







## 解决N 其他手段

无代理防病毒  
限制单个VM的IOPS  
配置基线核查  
漏洞扫描

应用服务

■■■■■



SAMPLE

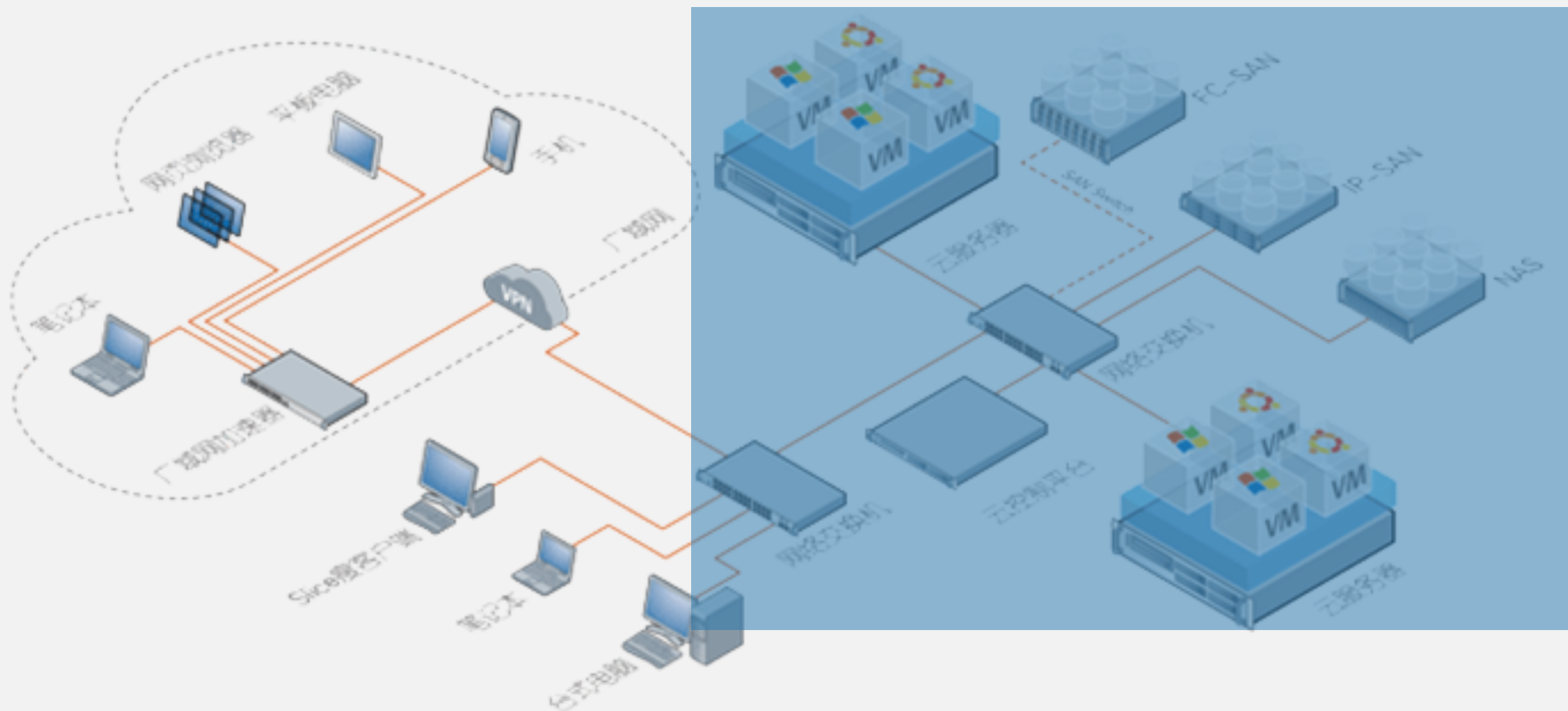
# 云与虚拟化防护的典型实践



## 虚拟化防护的典型实践

某市级政府，对各委办局服务器进行**虚拟化改造**，并进行防御。

每个政府单位有**独立**的虚拟服务器、安全设备的管理权限





# 虚拟化防护的典型实践

Yxlink Safety Virtualization Platform

帮助与文档 管理员

网络拓扑 network topology

选择 选框 放大 缩小 全屏 导出 搜索设备 编辑 刷新

虚拟机管理  
虚拟网络管理  
网络拓扑  
设备列表  
实体机管理  
系统配置

物理出口  
交换机  
路由器  
下一代防火墙  
虚拟机

虚拟网络



# 虚拟化防护的典型实践

Yxink Safety Virtualization Platform

帮助与文档 管理员

虚拟机 virtual machine

操作行为

- 创建虚拟机
- 开机
- 关机
- 挂起
- 重启电源
- 关闭电源
- 全选
- 删除
- 刷新

序号	虚拟机名称	状态	IP地址	CPU	内存	磁盘使用率	IO读写	网络流量
1	REHL6.5_x64	已关机	--	--	--	--	--	--
2	Easted-view	已关机	--	--	--	--	--	--
3	windows70007	运行中	192.168.1.32	2%	14%	15%	20.4KB/s	2KB/s
4	Debian_8.6	已关机	--	--	--	--	--	--
5	Debian_8_x86_64	已关机	--	--	--	--	--	--
6	Mysql DB1	已关机	--	--	--	--	--	--
7	Mysql DB2	已关机	--	--	--	--	--	--
8	WEB	已关机	--	--	--	--	--	--
9	FTP	已关机	--	--	--	--	--	--
10	Linux	已关机	--	--	--	--	--	--
11	Debian_8.6 克隆	已关机	--	--	--	--	--	--
12	Android	已关机	--	--	--	--	--	--
13	Sql Server	已关机	--	--	--	--	--	--
14	Solaris 2.4	已关机	--	--	--	--	--	--
15	Microsoft Wind...	已关机	--	--	--	--	--	--

虚拟机管理

- 概览
- 虚拟机
- 分组
- 快照
- 镜像
- 日志
- 虚拟网络管理
- 实体机管理
- 系统配置

虚拟机分组

- 默认分组
- 数据库
- WEB服务器
- FTP服务器

集群管理



# 虚拟化防护的典型实践—虚拟NGFW

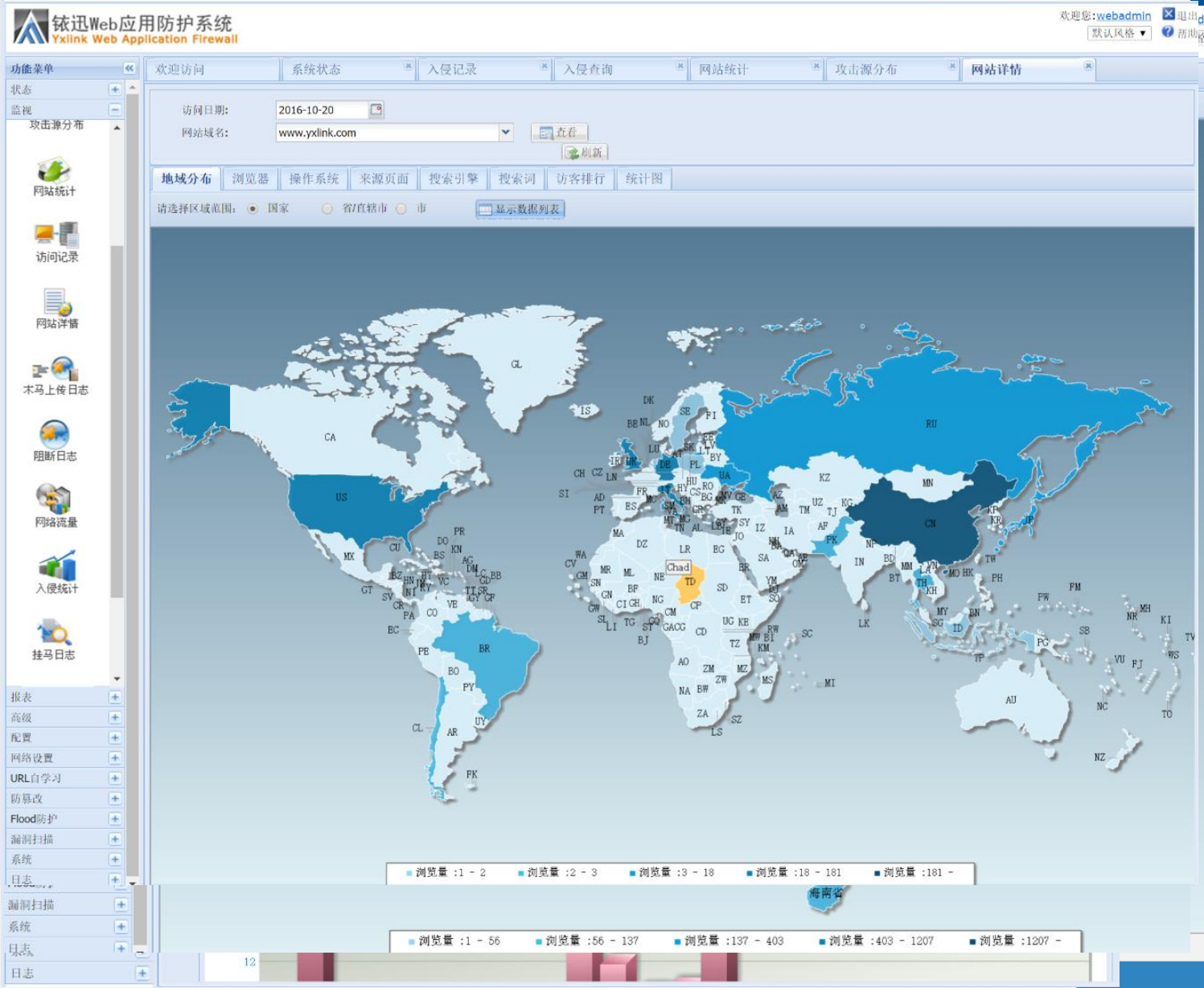
- 虚拟NGFW:
1. 防火墙过滤策略
  2. 入侵防御日志
  3. 综合信息





# 虚拟化防护的典型实践—虚拟WAF

虚拟WAF





# 虚拟化防护的典型实践—虚拟AD应用交付

## 虚拟AD应用交付： 负载均衡

欢迎管理员: webadmin ▾ ▶ 应用 ② 帮助

**驭迅应用交付系统**  
Yxlink Application Delivery System

🏠 首页 | 🧑‍🌾 链路负载 | 📦 服务器负载 | ⚙️ 全局负载 | 📊 数据分析 | 🌐 网络配置 | ⚙️ 系统管理

虚拟服务 | 服务 | 服务组 | 健康检查 | 访问控制

⚙️ 换肤

### 代理虚拟服务 - 编辑

名称

监听IP + ETH1 ✕

监听端口  ✔

状态  启用  停用

SSL卸载  开启  关闭 ?

导入证书 ➕ 导入授权证书

开启访问控制  开启  关闭

默认服务组  新建

说明

✔ 提交 取消

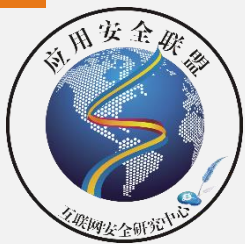




# 虚拟化防护的典型实践—虚拟抗DDoS

虚拟ADS：  
抗DDoS攻击





# 虚拟化防护的典型实践—虚拟IPS入侵防御

## 虚拟IPS入侵防御

Yalink 入侵防御系统  
Yalink Intrusion Prevention System

欢迎您: webadmin 退出  
默认风格 帮助

功能菜单: 状态, 监视, 入侵记录, 入侵查询, 入侵统计, 阻断状态, 网络流量

策略: 高级, 报表, 配置, 网络设置

欢迎访问 | 入侵记录 | 入侵统计 | 入侵查询

删除 | 筛选 | 刷新 | 正常视图

请选择查看日期: 2013-06-25 | 快速查询 | 导出日志

序号	攻击时间	拦...	规则名称	规则类别	拦...	优...	源...	地理位置	目...	协议	源...	目...	次...
1...	2013-06-25...	1...	PHP函数CRLF注入尝试	PHP漏洞	检测	高	61...	河南省周...	202...	TCP	6...	80	24
1...	2013-06-25...	2...	BitTorrent scrape请求	P2P通讯	拦截	高	220...	浙江省宁...	202...	TCP	2...	80	33
1...	2013-06-25...	2...	BitTorrent宣布请求	P2P通讯	拦截	高	124...	广西百色...	202...	TCP	1...	80	209
1...	2013-06-25...	2...	BitTorrent scrape请求	P2P通讯	拦截	高	119...	广东省中...	202...	TCP	5...	80	72
1...	2013-06-25...	1...	union select - 可能的SQL注...	通用SQL...	拦截	中	218...	北京市...	202...	TCP	5...	80	130
1...	2013-06-25...	1...	在select语句中试用concat函...	通用SQL...	拦截	高	218...	北京市...	202...	TCP	5...	80	68
1...	2013-06-25...	2...	BitTorrent宣布请求	P2P通讯	拦截	高	202...	上海交通...	183...	TCP	80	3...	123
1...	2013-06-25...	1...	PHP函数CRLF注入尝试	PHP漏洞	检测	高	183...	广东省深...	202...	TCP	5...	80	24
1...	2013-06-25...	2...	BitTorrent scrape请求	P2P通讯	拦截	高	183...	广东省深...	202...	TCP	5...	80	12
1...	2013-06-25...	2...	BitTorrent宣布请求	P2P通讯	拦截	高	115...	陕西省西...	202...	TCP	4...	80	3...
1...	2013-06-25...	1...	PHP函数CRLF注入尝试	PHP漏洞	检测	高	216...	美国	202...	TCP	4...	80	77
1...	2013-06-25...	1...	PHP函数CRLF注入尝试	PHP漏洞	检测	高	202...	中山大学	202...	TCP	6...	80	3...
1...	2013-06-25...	2...	BitTorrent scrape请求	P2P通讯	拦截	高	220...	福建省南...	202...	TCP	5...	80	22
1...	2013-06-25...	2...	BitTorrent scrape请求	P2P通讯	拦截	高	42...	香港电...	202...	TCP	4...	80	24
1...	2013-06-25...	2...	BitTorrent scrape请求	P2P通讯	拦截	高	98...	美国新...	202...	TCP	6...	80	81
1...	2013-06-25...	2...	BitTorrent scrape请求	P2P通讯	拦截	高	113...	广东省东...	202...	TCP	2...	80	318

第 1 页, 共 95 页 | 显示第 1 条到 30 条记录, 一共 2823 条



## 虚拟化防护的典型实践—虚拟IPS入侵防御

下一代防火墙NGFW  
Web应用防火墙WAF  
交换机SWITCH  
路由ROUTER  
入侵防御系统IPS  
抗拒绝服务系统ANTIDDOS  
应用交付系统ADC  
漏洞扫描系统NVS  
虚拟专用网络系统VPN  
日志审计系统SAS  
.....

虚拟化  
安全设备



谢谢!

杨谦 18021500396  
qianyang@yxlink.com