智能安全引领高校网络安全建设

李云龙

国家政策提倡自主可控并鼓励安全技术创新

---资料来源：IDC2014年度安全市场分析报告

- 国家信息安全战略文件发布
  - **大力发展智能检测技术**
  - 实现可信计算环境
  - 提倡自主可控，提高国家网络安全实力
- 2014年初，中央网络安全与信息化领导小组成立
- 十八届三中全会决定设立国家安全委员会
- 发改委：组织实施国家信息安全专项， 2013年8月，提出了三类重点课题
- 国务院关于《大力推进信息化发展和切实保障信息安全的若干意见》，2012年6月
  - 提高风险隐患发现、监测预警和突发事件处置能力
- 信息安全产业“十二五发展规划”， 2011年12月
- 信息安全等级保护 2007年6月
  - 积极防御、综合防范
  - 信息系统分等级实施保护
  - 技术管理综合治理

“智能”是业界公认应对挑战的“利器”

---令人担忧的网络安全，推动了安全技术的快速发展

66%

66%的数据泄露在30天内没有被发觉

4

系统受攻击后平均在4个月恢复

243

有些攻击在243天后才被发现

42%

过去三年针对性攻击增长了42%

网络安全建设的追求：提前预知风险、防范未知威胁

智能安全

- ✓ 主动的学习与异常预警
- ✓ 运用大数据技术对海量日志的关联分析及威胁定位
- ✓ 基于“信誉”评估的策略联动及主动防御
- ✓ 着眼于历史趋势的“健康”状态跟踪与响应

智能为什么能够引领网络安全技术的发展

应用层

会话层

网络层

第一阶段 – 包过滤

- 简单的ACL

第二阶段 – 状态检测

- 基于IP连接状态
- 使用ALG跟踪协议栈，无法应付加密或基于HTTP的应用

Juniper NETWORKS

CISCO

FORTINET

天融信 TOPSEC

第三阶段 –基于用户与应用的下一代防火墙

- 通过应用特征和应用的表现来识别应用
- 可以对加密过的应用阻断或限速
- 基于角色的用户识别

开心网 迅雷5 Baidu百度 SAP YOUKU优酷.com 土豆网 WORLD WARCRAFT skype msn ORACLE BitTorrent Messenger Google Docs webex YouTube Broadcast Yourself

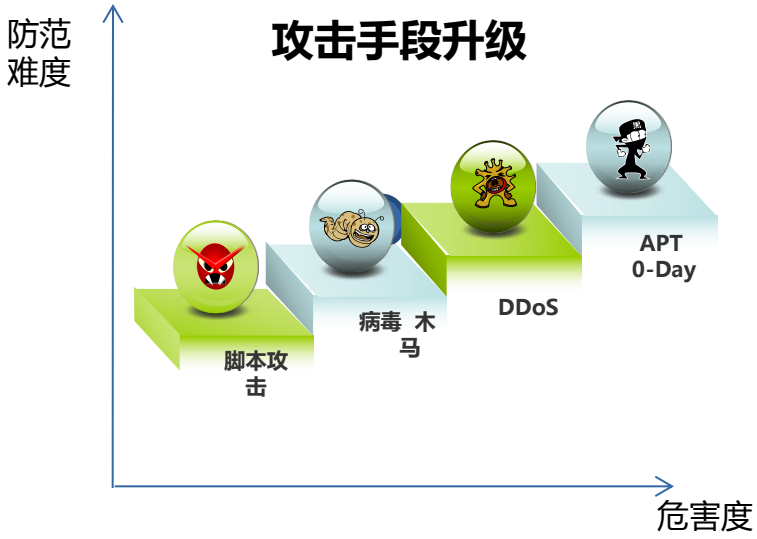
第四阶段 - 智能安全

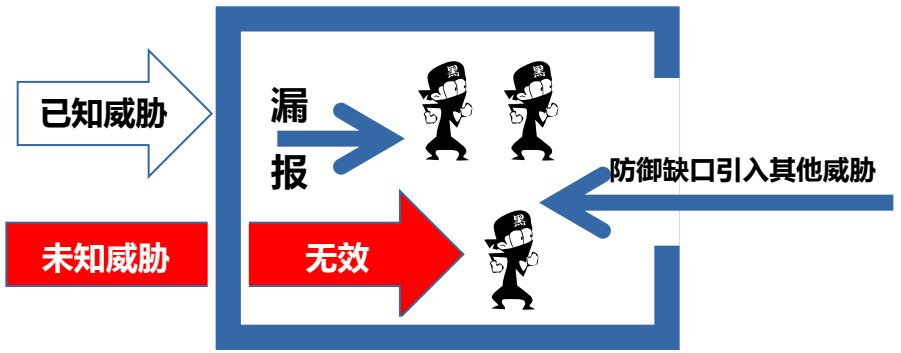
- 智能分析业务连续性状态
- 智能检测业务行为异常
- 安全策略智能联动

Hillstone NETWORKS

1995年以前	1996-2007	2008-2012	2012-

老办法解决不了企业面临的新安全威胁





技术瓶颈

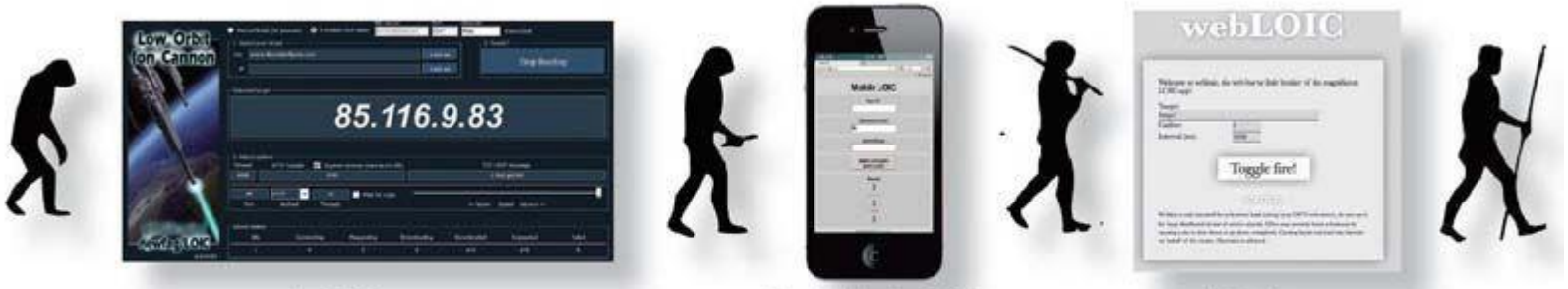
- 已知威胁：特征覆盖不可能达到100%，总有漏掉的攻击行为；
- 未知威胁：传统基于模式匹配的监测方式对其无效；

管理问题

- BYOD引入静态策略无法防护的问题；
- 被动防护难以对抗持续攻击；
- 防护时机：只关注了威胁进入瞬间；
- 防护位置：只关注了边界点安全

边界防护技术容易被攻击绕过

网络中大量存在的U盘、移动设备等带入威胁，如何在数据被大量窃取前更早发现？



攻击工具的“平民化”，来自内部的攻击更容易绕过边界防护手段而对企业网带来更大的威胁

动静结合，全方位防护

iNGFW

智能 i

行为分析

发现内网潜在风险

\+

下一代防火墙
NGFW

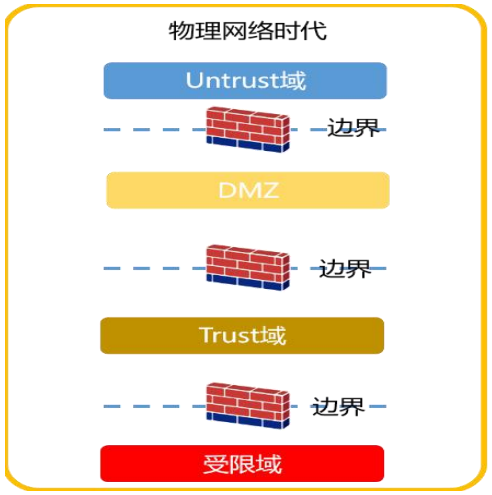
特征过滤

过滤已知网络威胁

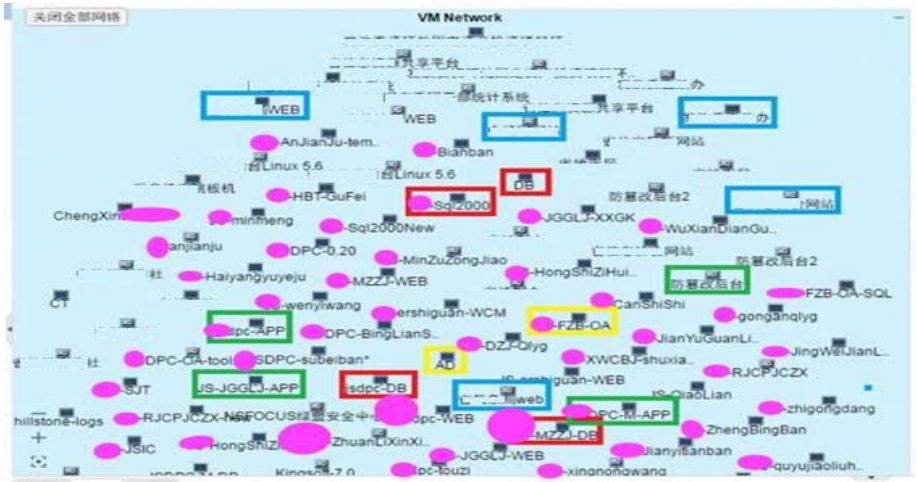
网络攻击链揭示攻击者意图，掌握受损程度

云计算内网络安全边界消失

- **理想的内部结构**

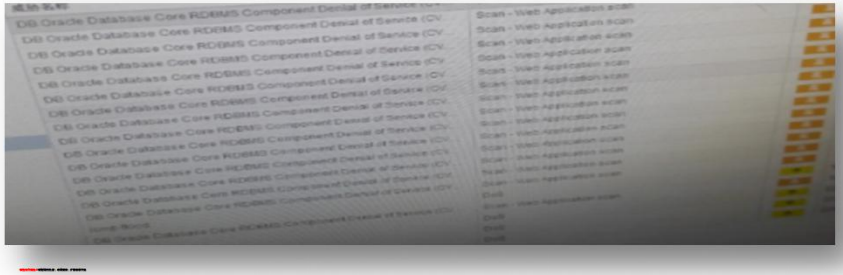


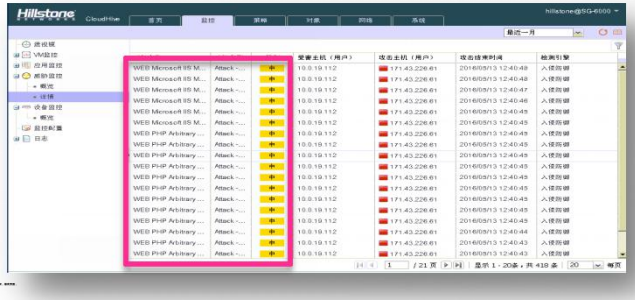
现实云计算内部

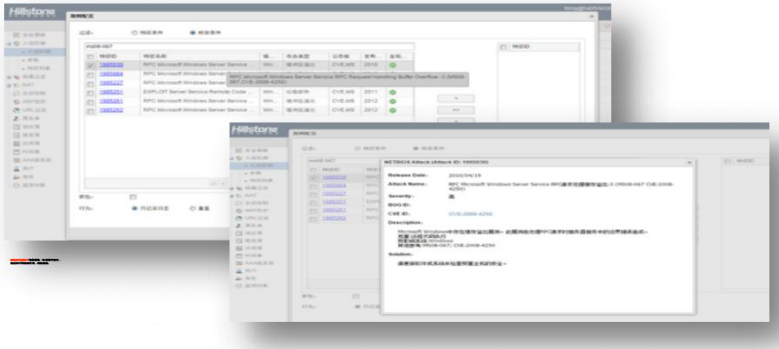


9

云计算内部网络安全事件频发







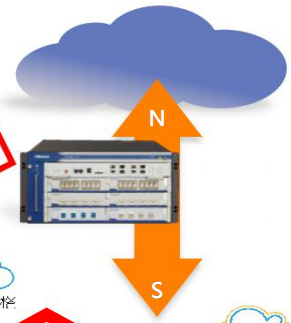
在山石网科的山石云格和山石云界客户试用活动中，共发现应用层、网络侧攻击二十余类，遍及所有客户……

10

层层防护，从微入手: 虚拟化全方位保护

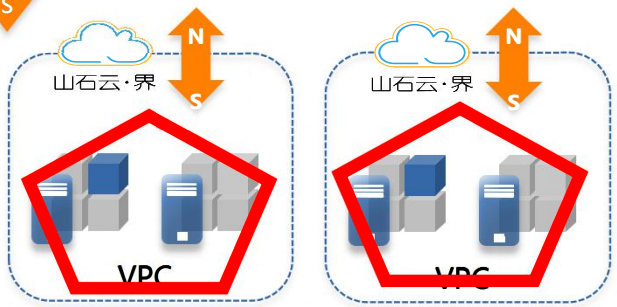
山石网科全系列硬件安全产品
- 提供整个云数据中心的基础架构的南北向网络安全监控

大边界

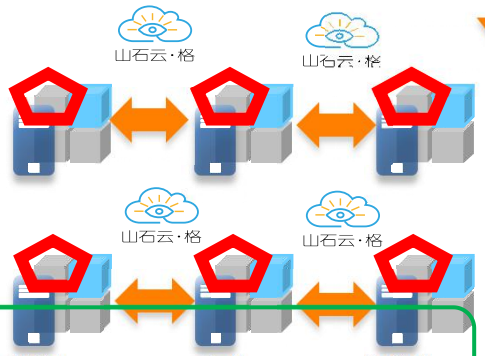


山石云·界
- 提供租户级、业务系统间的隔离与南北向网络安全防控
- 提供NFV框架下的安全服务链能力

小边界

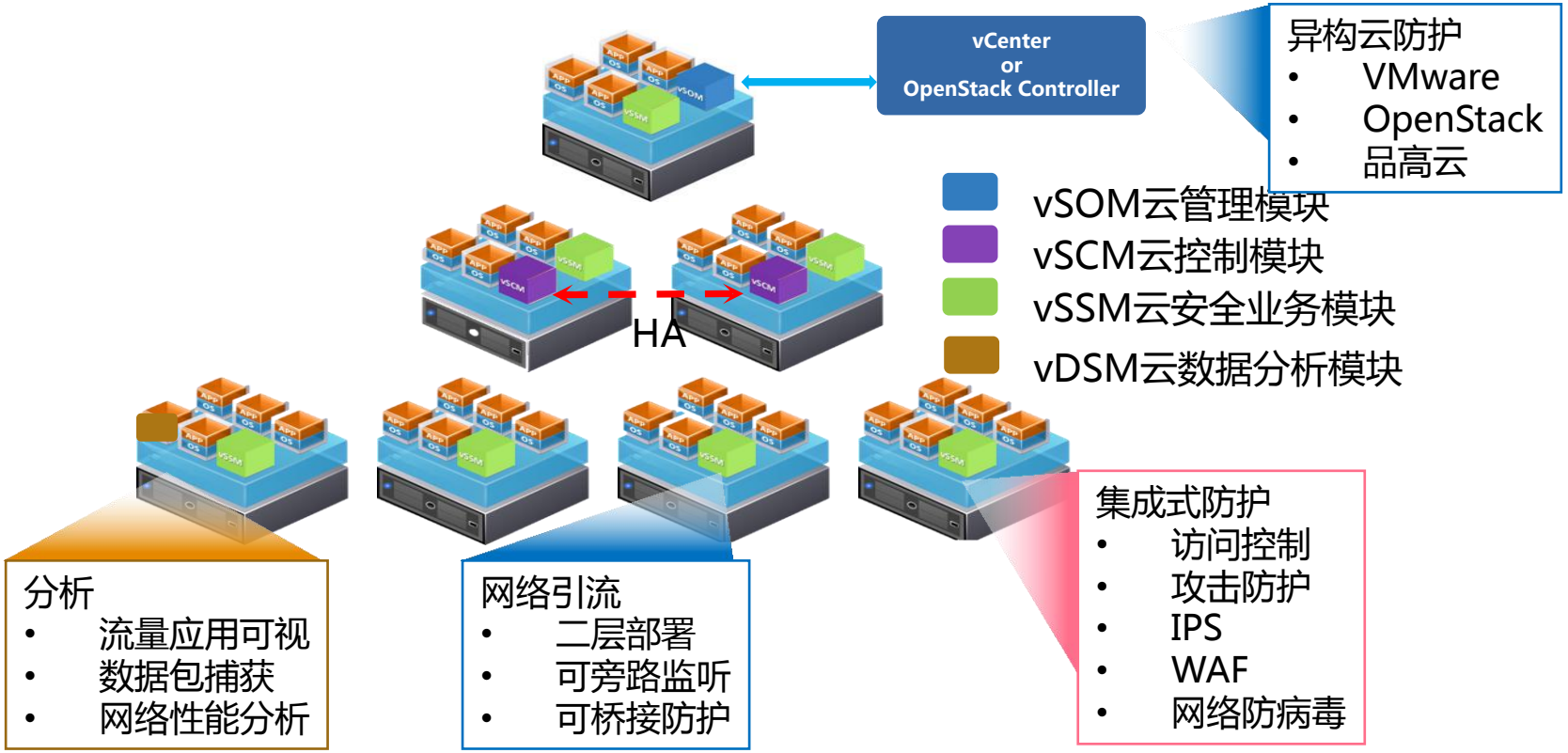


微边界



山石云·格
- 提供虚机级别的东西、南北向网络安全监控
- 面向私有云，行业云场景

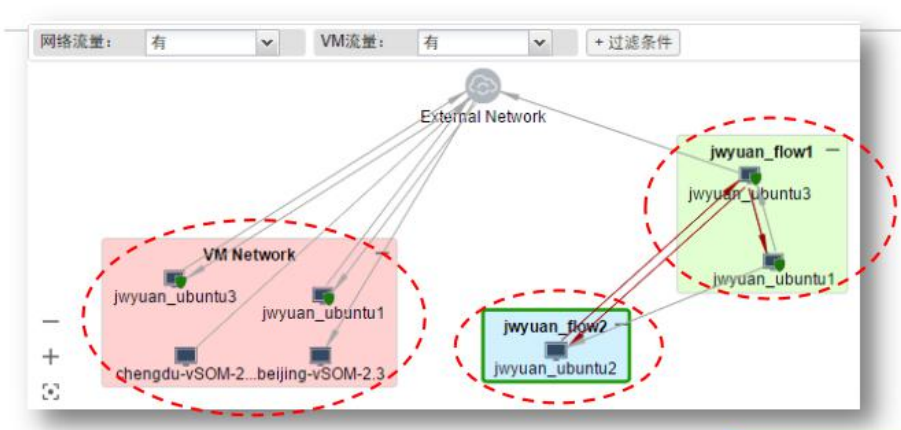
“山石云·格”全分布式微隔离产品

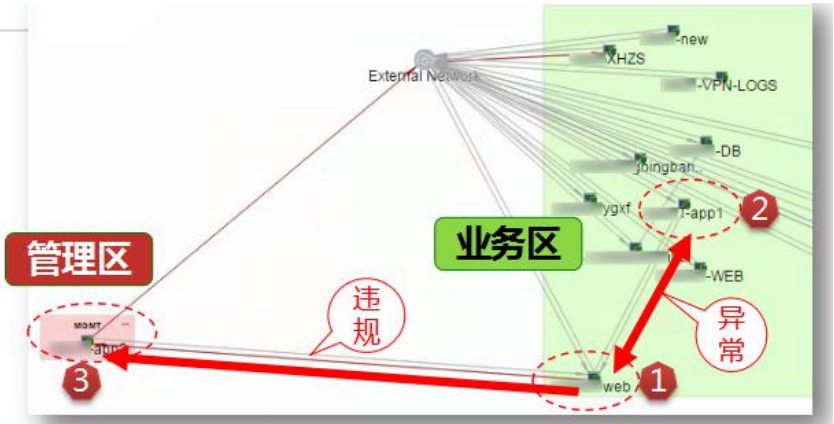


资产可视化


云内监控范围统计
系统状态
最近一天
物理主机
88%
7 已部署
8 总共
CPU许可证数
100%
14 已使用
14 总共
虚拟机
35%
9 被保护
26 总共
网络
0%
0 被保护
4 总共
各组件运行状况监测
安全服务状态
最近一天
vCenter
vSOM
vSCM
vSSM/vDSM
总共：8
在线：8
VM Top 10
流量
最近一月
上行流量
下行流量
38.15M
28.61M
19.07M
9.54M
0M
流量(Bytes)
10.0.0.11
邮件服务@CloudHive
应用 Top 10
流量
最近一天
3T
2.5T
2T
1.5T
1T
512G
0G
流量(Bytes)
TLS1
HTTP
HTTP视频
哔哩哔哩
迅雷
UDP下载及视频
HTTP文件下载
BT
爱奇艺
RTMFP
总流量
最近一天
6G
4G
2G
0G
流量(bps)
04/20 18:00
04/21
04/21 06:00
04/21 12:00
网络概况统计

资源分布，交互关系





粗看

网络构架

虚机密度

虚机间的交互关系复杂度

细看

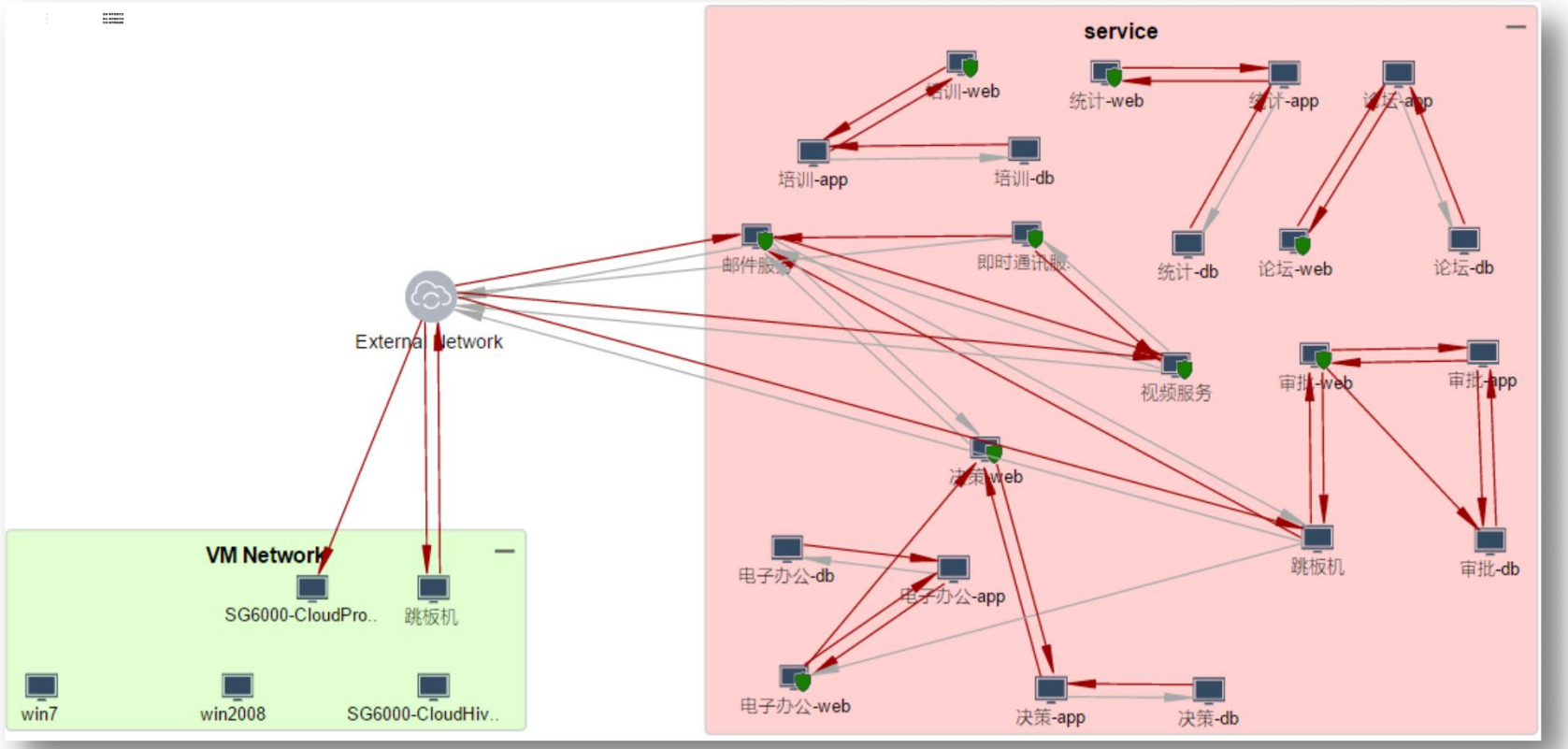
网络和虚机的从属关系

网络间的流量交互关系

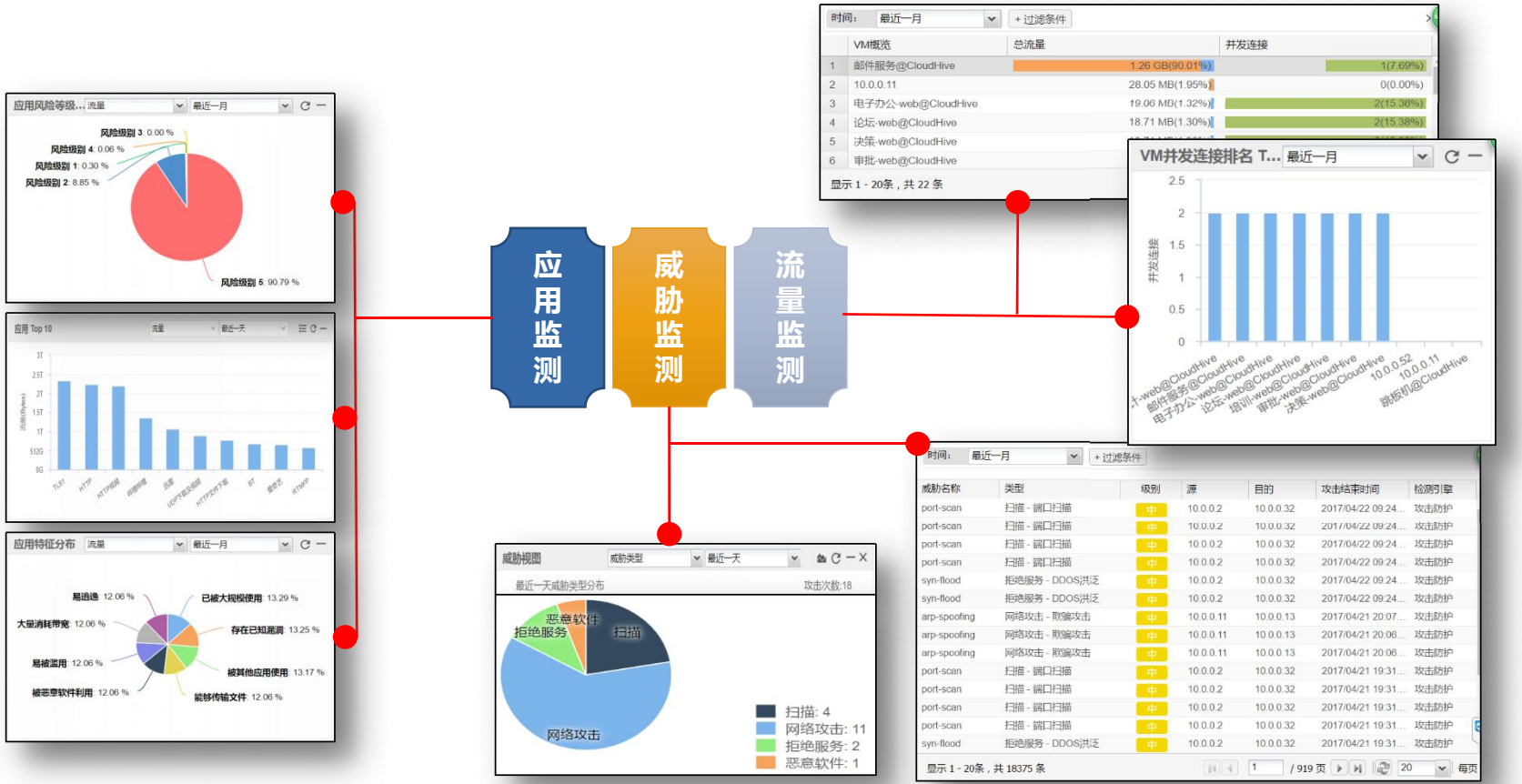
虚机间的流量交互关系

异常和违规行为

复杂交互关系呈现


service
培训-web
统计-web
统计-app
论坛-app
培训-app
培训-db
邮件服务
即时通讯服务
统计-db
论坛-web
论坛-db
External Network
视频服务
审批-web
审批-app
决策-web
VM Network
跳板机
审批-db
电子办公-db
电子办公-app
SG6000-CloudPro..
跳板机
电子办公-web
决策-app
决策-db
win7
win2008
SG6000-CloudHiv..

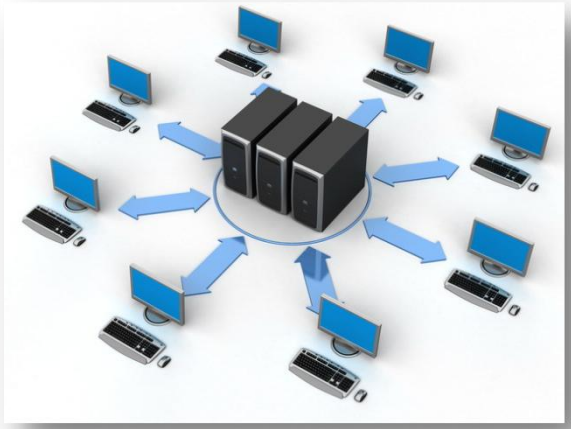
应用、威胁、流量看得见



16

解决方案及案例

众多高校用户选择Hillstone



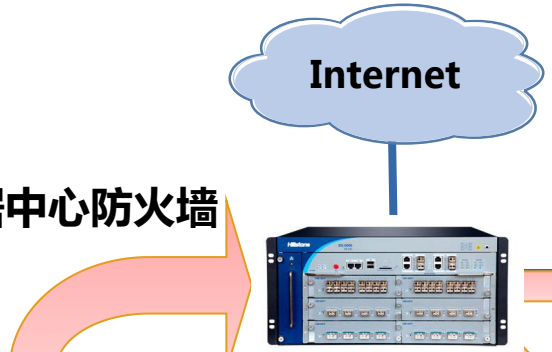
CERNET地区主节点高校中的7+所高校、省级节点高校中的14所高校选Hillstone

150+高校，47所211工程院校、17所985高校选择Hillstone

17+高校选择Hillstone数据中心防火墙，支持大流量大并发互联网访问

14所Cernet地区及省高校节点选择Hillstone

山石防火墙与计费认证系统整合解决方案

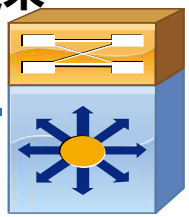


山石数据中心防火墙

山石安全审计平台

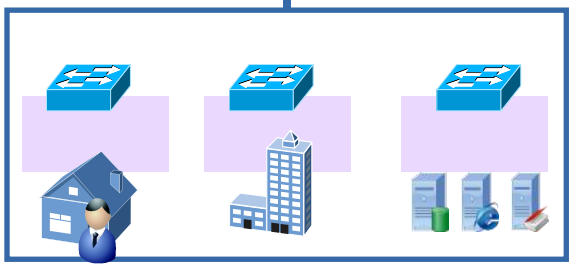
基于实名制的NAT、URL、IM日志审计和日志查询

将IP与用户身份信息关联起来



城市热点计费认证系统

账户授权、登录验证、账户管理、费用计算、认证的管理

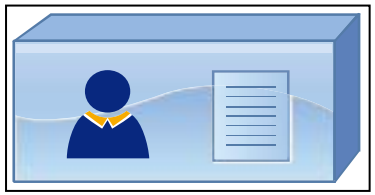


基于实名制用户的校园网安全管控与审计方案可实现：

- 基于用户的认证管理
- 基于用户的费用管理
- 基于用户的日志审计
- 基于用户的流量管理
- 基于用户的URL上网控制
- 基于用户的访问策略控制

实名制审计方案的建设效果

第三方计费认证系统



整合

山石安全网关 山石安全审计平台

用户	IP	MAC

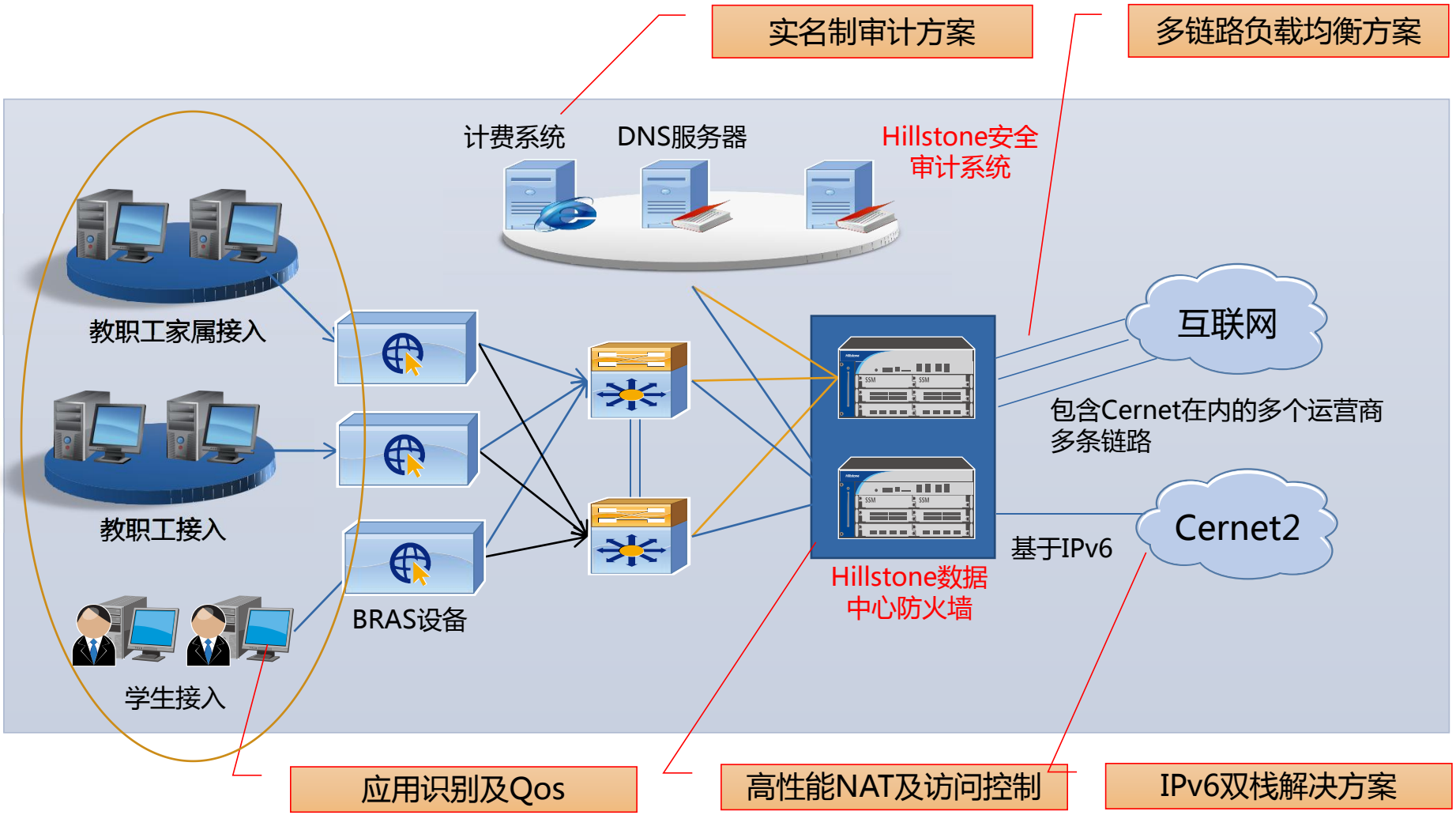
IP	NAT日志	URL日志	IM日志

通过整合实现：

- **基于“实名制”的访问控制**，包括应用控制、URL过滤；
- **基于“实名制”的带宽管理**，包括流量控制、带宽分配；
- **基于“实名制”的日志审计**，快速追溯到真实用户。

满足82号令和网络安全法要求日志存储不少于6个月

山石高校互联网安全接入方案



案例1：北方工业大学

校园网智能安全防护

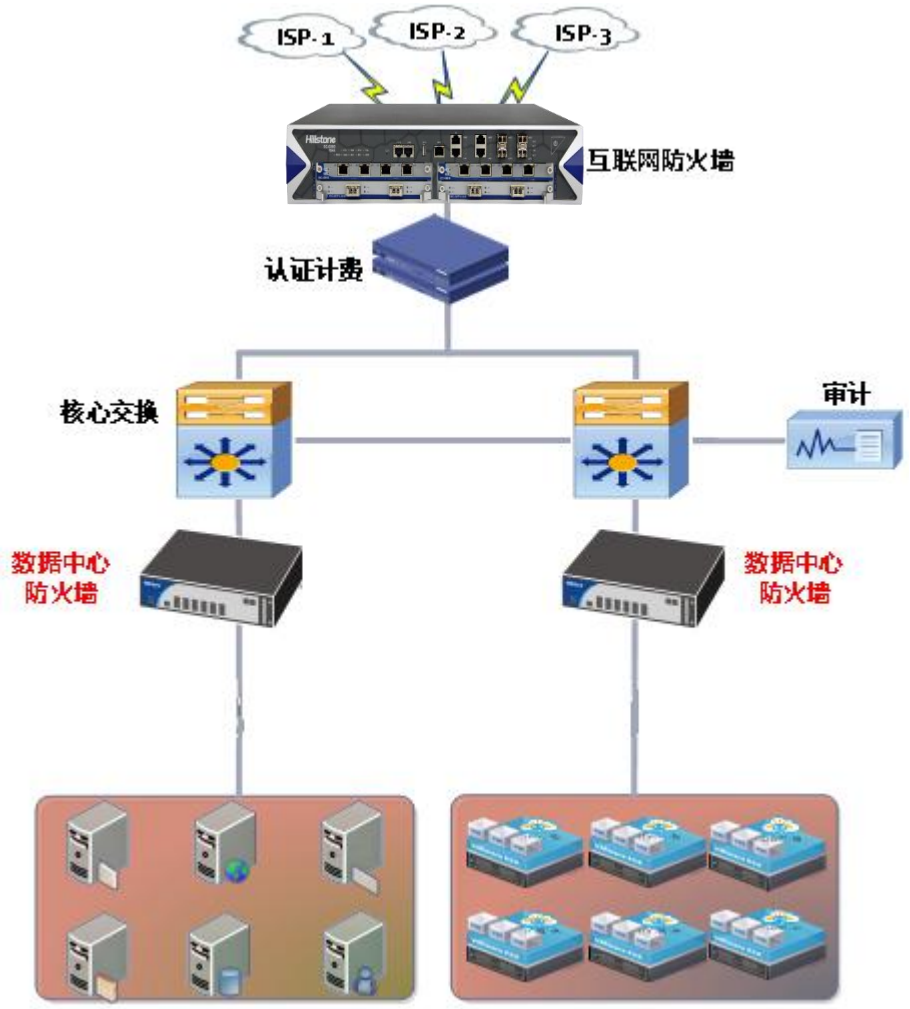
- 防火墙防护DOS和越权访问
- 入侵防御阻挡引用层攻击
- WAF防护网站安全
- 异常行为和未知威胁检测与防护

数据中心防火墙双机防护

内网安全域和外网安全域同时开启攻击防护策略

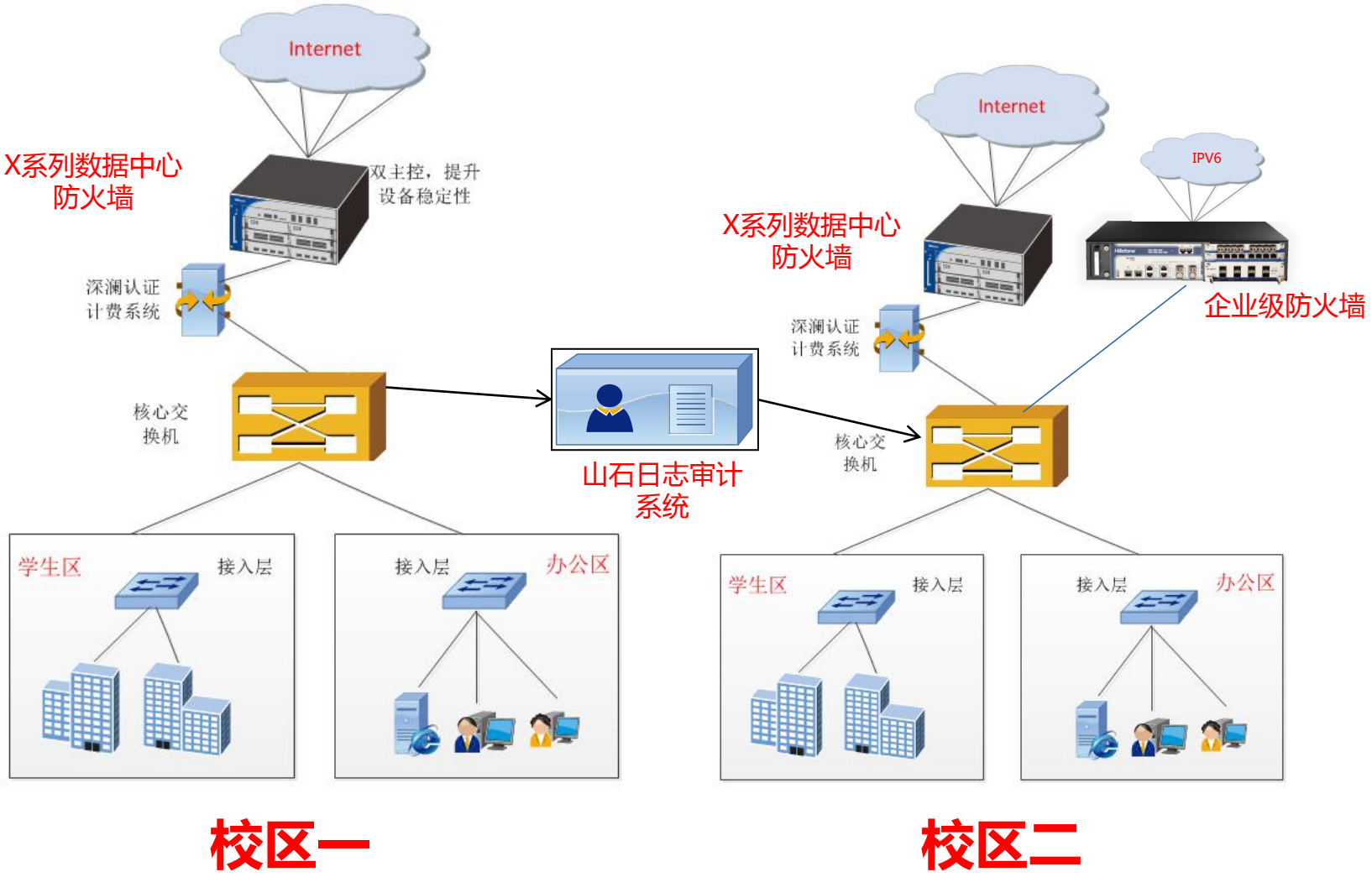
双机热备保障可靠性

✓ 服务器区防火墙双机热备部署

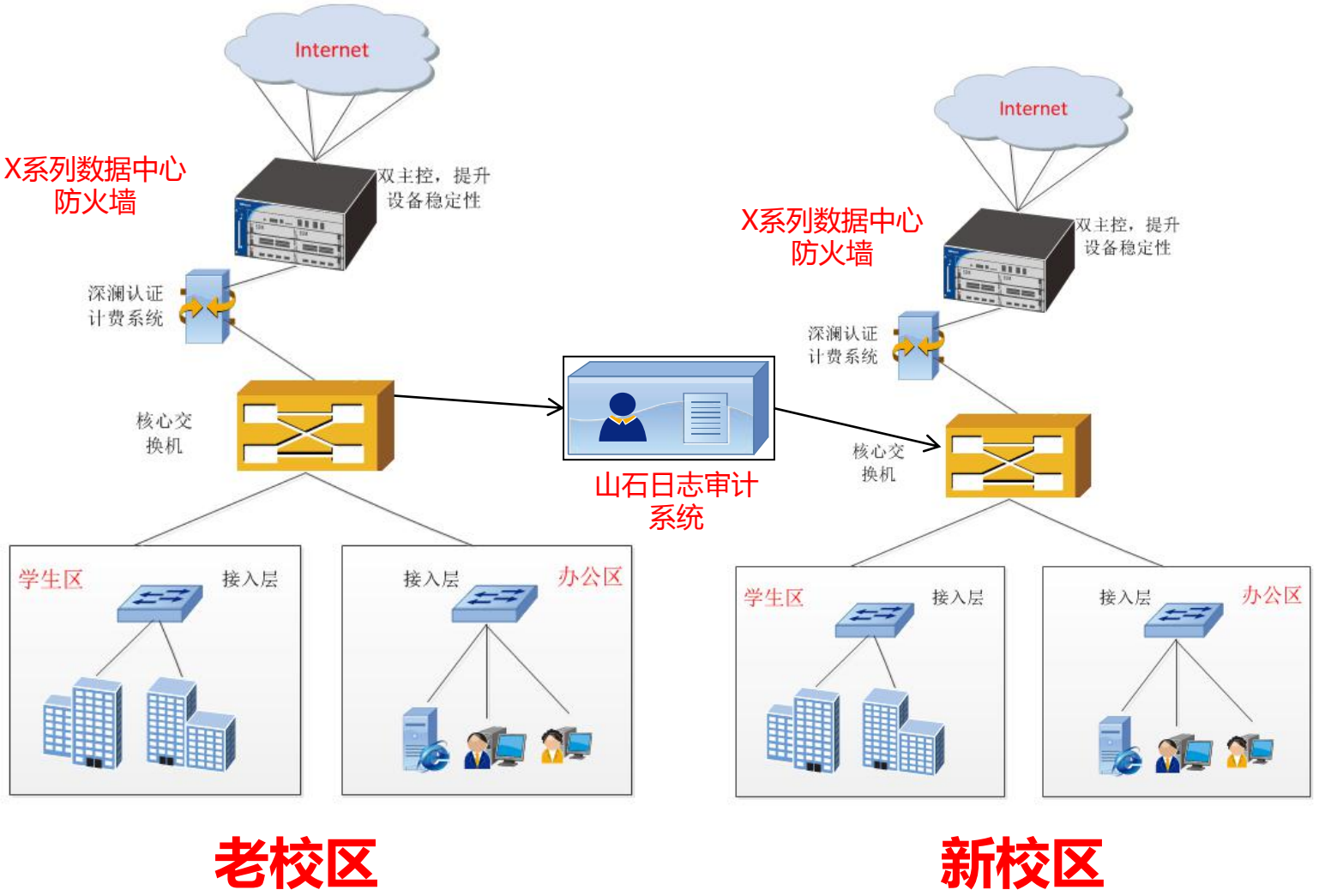


山石云格虚拟化安全防护

案例2：北京建筑大学


Internet
X系列数据中心
防火墙
双主控，提升
设备稳定性
深澜认证
计费系统
核心交
换机
学生区
接入层
接入层
办公区
山石日志审计
系统
Internet
IPV6
X系列数据中心
防火墙
企业级防火墙
深澜认证
计费系统
核心交
换机
学生区
接入层
接入层
办公区
校区一
校区二

案例3：天津大学


Internet
X系列数据中心
防火墙
双主控，提升
设备稳定性
深澜认证
计费系统
核心交
换机
山石日志审计
系统
Internet
X系列数据中心
防火墙
双主控，提升
设备稳定性
深澜认证
计费系统
核心交
换机
学生区
接入层
接入层
办公区
学生区
接入层
接入层
办公区
老校区
新校区

用户调查问卷

如有问题，请联系我们

服务热线： 400-828-6655

www.hillstonenet.com.cn