2013年4月18日星期四

HUAWEI ENTERPRISE ICT SOLUTIONS A BETTER WAY

Huawei NIP 主打胶片

enterprise.huawei.com

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Content

1 现状与挑战

2 产品价值/特点

3 成功案例

HUAWEI

安全攻击层出不穷，企业损失严重

2012年安全攻击事件层出不穷

2012

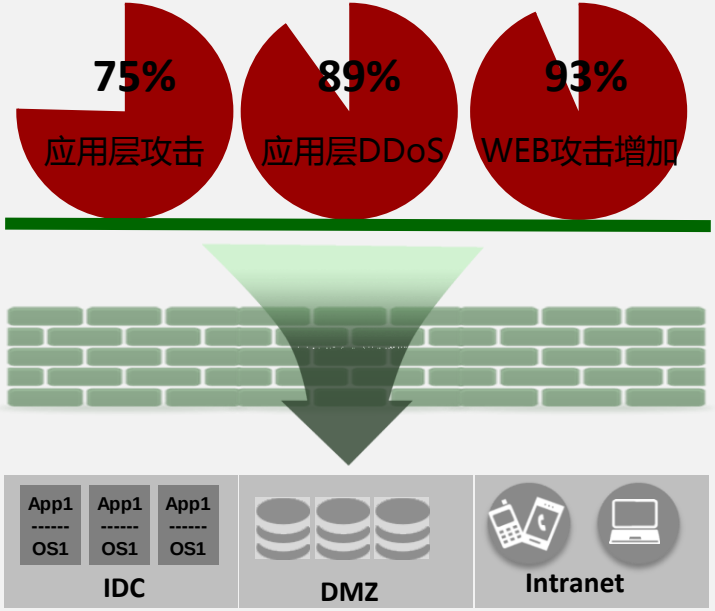
- SONY：索尼游戏受攻击，受影响用户约7800万，直接经济损失1.71亿美元。
- FOXCONN：代工客户姓名和密码被窃取，同时富士康所有邮件账户和密码被公开，其中包括CEO郭台铭。
- NEUSOFT 东软：CT机核心技术被窃取，涉案人员28人，案值6400多万元。
- vmware：VMware的ESX Hypervisor的源代码被黑客公布在互联网上，Vmware不得不建议用户马上升级到最新代号为ESXi的hypervisor。
- HY.BROTHERS 华谊兄弟传媒：华谊兄弟网络被黑客入侵，黑客获取了登录证书并在互联网上公布入侵情况。

企业因信息安全事件损失惨重

- 网络攻击给全球带来了**1110亿**美元的损失
- 2011年，全球共计登记信息泄露事件819起，总损失金额超过**200亿**美元
- 据国安部统计，我国63.6%的企业用户处于“高度风险”级别，每年因网络攻击导致的经济损失高达上**百亿**。

HUAWEI

网络攻击变化：应用层攻击



- 应用层攻击威胁巨大，尤其是针对Web应用的攻击
- 基于浏览器和应用漏洞对客户端的攻击成为主流
- APT攻击威力强大，多种攻击方式深度组合
- 攻击变种逃避技术日趋成熟

攻击行为越来越利益化，攻击组合和逃避技术越来越成熟

HUAWEI

安全攻击的防范

- 针对客户端的攻击
- 针对Web应用的攻击
- 针对应用的DDoS攻击
- P2P侵占网络带宽
- 蠕虫、木马感染
- 网络型DOS攻击
- 漏洞利用攻击

- 针对终端的攻击防护
- 针对服务器的攻击防护
- 针对网络基础设施的攻击防护
- 针对关键业务攻击防护

Content

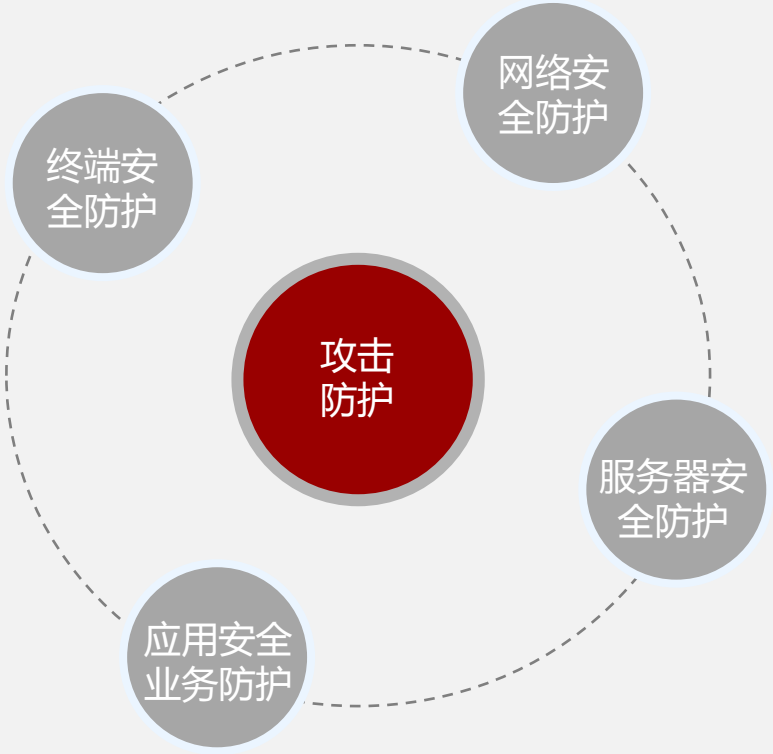
1 现状与挑战

2 产品价值/特点

3 成功案例

HUAWEI

NIP防攻击——深度检测，全面防护



攻击防护

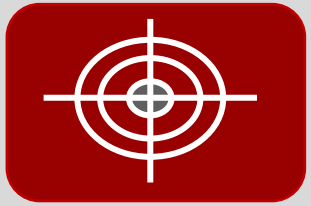
终端安全防护
- 终端准入控制、安全加固

网络安全防护
- 攻击入侵深层检测，全面防护
- 高性能、易管理

服务器防护
- 网络防护+攻击预警+主机保护+漏洞管理

应用安全防护
- WEB防攻击
- Email全面保护

NIP 产品亮点



□全面防护—场景全覆盖，降低用户安全投资

✓提供最高达12G的IPS防护性能，全面覆盖用户各带宽场景；

✓支持对互联网出口、分支互联、数据中心、服务器前等场景入侵防护；

✓提供针对服务器防护、客户端防护等六大类漏洞攻击防护

□准确检测——“零”误报，提高安全管理效率

✓基于漏洞签名库，检测精准，“零”误报，确保用户业务正常运行。

✓签名库85%默认开启率，确保系统上线即实时防护；

✓签名库80%的默认阻断率，自动阻截关键威胁，确保用户安全无忧。

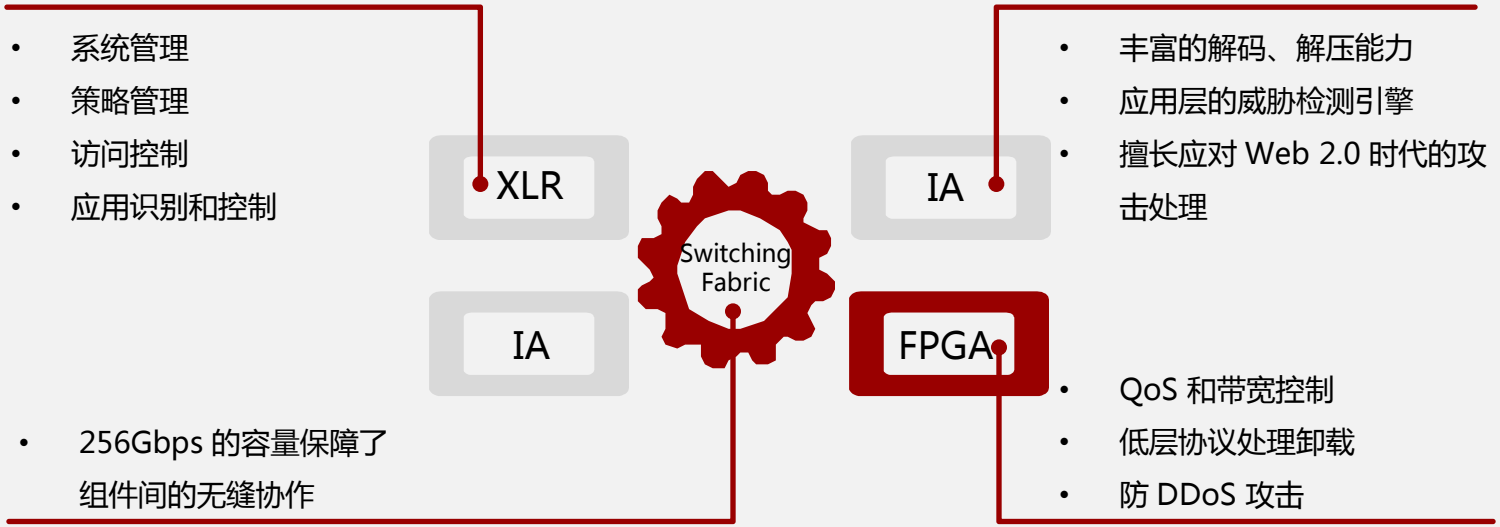
□易于使用——“零”配置上线，降低用户管理维护成本

✓不需要设置网络参数和变更网络结构，即插即用，实时防护

✓超过十种场景策略模板，实现零配置上线

✓数十种报表，全面呈现网络安全状况

万兆NIP，“真”性能，成就用户安全无忧



HTTP:12Gpbs | **小包:12Gpbs** | **大包:32Gpbs**

HUAWEI

全面防护- 场景全覆盖

NIP场景对应表

产品系列	互联网出口	DMZ区	部门隔离	分支互联	IDC
NIP2050/ NIP2050D	Y	Y	Y	Y	
NIP2100/ NIP2100D	Y	Y	Y	Y	
NIP2130/ NIP2130D	Y	Y	Y	Y	
NIP2150/ NIP2150D	Y	Y	Y	Y	
NIP 2200/ NIP2200D	Y	Y		Y	
NIP 5100/ NIP5100D	Y	Y			
NIP 5200/ NIP5200D	Y	Y			Y
NIP5500/ NIP5500D	Y				Y

互联出口防护：

•对应用层威胁进行有效防护及监控
•精确控制各种应用，如P2P，网络游戏等
•对DDoS攻击包括应用层DDOS攻击防护

DMZ区防护：

•实现对WEB应用的各种攻击防范，如恶意攻击，如SQL注入等
• 针对DMZ区的服务器系统攻击防护，实现虚拟补丁功能
• 实现网页防防篡改

部门隔离：

•防止入侵主机可能把威胁扩散至全网，对关键部门进行有效监控
•对内部主动攻击监控、防护， 追溯

分支互联防护：

•有效防护蠕虫和无关流量在广域网传播，降低网络传输效率
•防止低安全级别和安全状况差的分支上的病毒、木马等通过广域网向其他分支或总部扩散

数据中心防护：

•实现对系统漏洞防护，以及对数据库、web服务器攻击防护
•防范攻击者对数据中心敏感信息窃取、非法篡改等攻击

全面检测-威胁全覆盖

服务器攻击检测

防止对HTTP、FTP、DNS、Mail等服务器的各种攻击：缓冲去溢出、系统或服务漏洞攻击、暴力破解等。

客户端攻击检测

针对客户日常应用，如：Office文档、PDF ,多媒体以及浏览器提供检测，避免客户端免成为Botnet或网马的受害者。

Web攻击检测

检测Web应用相关攻击，包括Web2.0及后台数据库； 对注入攻击、跨站脚本、目录穿越等提供重点防护。

网络滥用检测

- 检测P2P、视频应用，保障业务带宽；
- IM、在线存储、web邮箱、网络隧道证券及游戏的访问，影响员工效率。

恶意软件检测

- 蠕虫
- 木马
- 间谍软件
- 广告软件
- 僵尸网络

DDOS检测

- 针对网络流量的DoS
- 针对应用服务的DoS
- 针对操作系统的DoS
- 扫描探测

全面防护- 多种业务保护

保护客户端

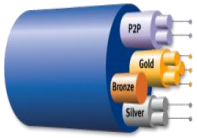
- 客户端应用安全防护
- 客户病毒防护
- 恶意软件防护

保护服务器

- 服务器漏洞防护
- Web应用防护
- 恶意软件防护
- DDOS防护

IPS 核心价值

保护带宽性能



- 应用带宽管理
- 基于时间的应用访问策略

保护基础架构

- DNS、交换路由设备漏洞防护：
- DDOS防护

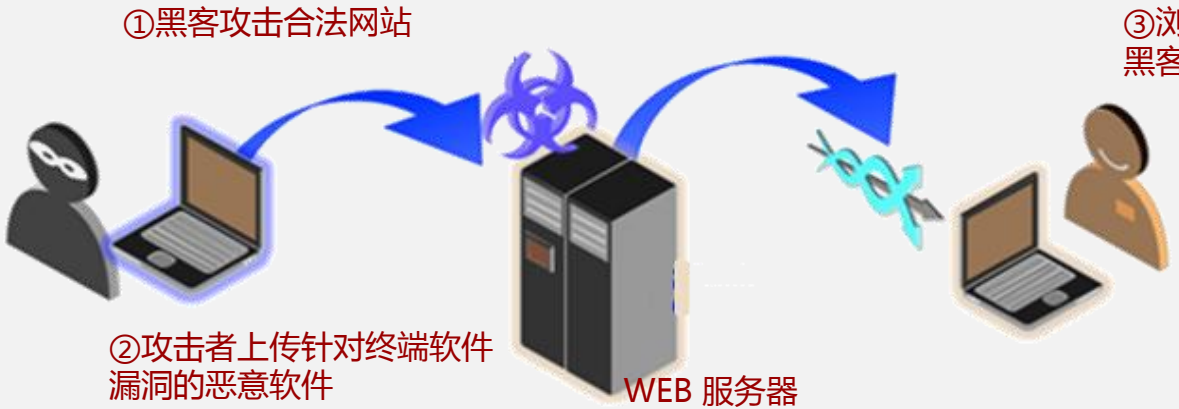
服务器漏洞防护	客户端应用防护	WEB应用防护	应用带宽管理	恶意软件防护	DDOS防护

HUAWEI

保护服务器，确保业务永续和数据安全

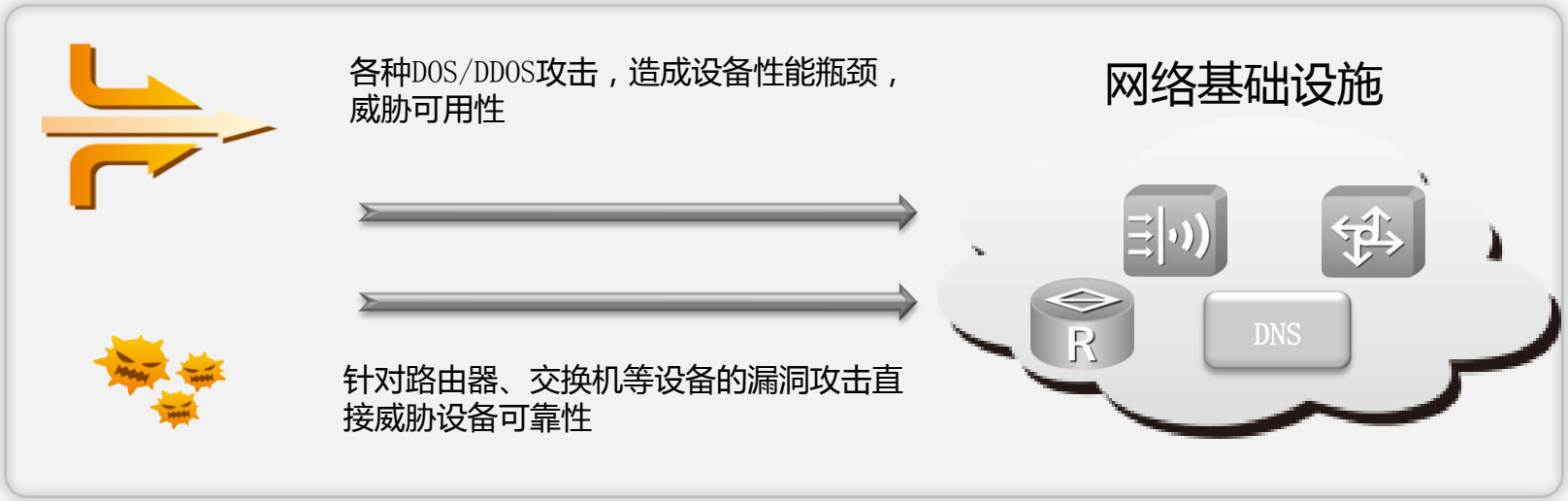
攻击前期	• 网络扫描 • 漏洞扫描	→	• 基于网络异常发现网络扫描 • 基于行为特征发现漏扫工具	
攻击中期	• 漏洞攻击 • Web应用攻击 • DOS攻击 • 暴力破解	→	• 虚拟补丁技术检测漏洞攻击 • Web应用防护 • 完整的DOS防御 • 基于行为检测发现暴力破解	
攻击后期	• 种植恶意软件 • 操控被攻击设备	→	• 检测恶意软件并阻断 • 检测控制、外传流量	← • 外传数据信息 • 成为傀儡主机

保护客户端，确保终端安全



- 浏览器及其插件（Java、ActiveX等）的安全防护；
- PDF、Word、Flash、AVI等文件层的攻击防护；
- 木马、蠕虫、病毒等及对操作系统的攻击防护；

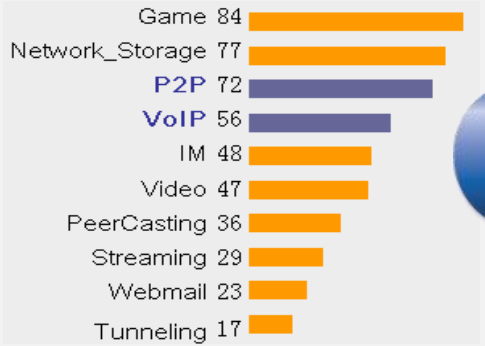
保护基础设施，确保网络



- 基于虚拟补丁技术，对基础网络设备的漏洞进行防护；
- 综合7种流量检测技术，对各种网络DOS、应用DOS（针对DNS、HTTP、SIP的基础服务）提供整体防护；
- 提供流量自学习功能，保障对各种异常流量攻击的准确检测；

保护带宽性能，提高带宽利用率

- 支持协议1200+
- 支持热门加密P2P协议
- 定制化需求的快速响应能力



- 对P2P、流媒体等应用带宽控制，保障网络资源有效使用；
- 限制使用IM、游戏、股票等应用，保障工作效率；
- Web Mail、在线存储等控制，防止机构内部文件非法外传；

准确检测-“零”误报，成就用户业务永续

- 基于漏洞的高质量威胁签名
  服务器攻击检测、客户端攻击检测、Web攻击检测、网络滥用检测、恶意软件检测、DDOS检测
- 零误报，全规则默认开启
  签名库默认开启率85%，默认阻断率80%
- 2~7层DDoS防护，自动学习流量模型并设置阈值，精准防护DDoS攻击
  七层流量DDoS攻击过滤，深度防御各种应用层DDOS攻击
- 八大攻击检测技术
  协议智能识别、数据包及流重组检测、高级逃避检测、应用协议还原及文件还原、攻击特征检测、基于漏洞的检测、基于攻击原理的启发式检测、网络行为/应用协议异常检测
- 1200+应用识别

准确检测– 基于漏洞检测技术

基于应用的识别

可识别超过240种协议

可识别多种伪装的数据

高效的内容解析

基于规范的解析，无需盲扫

深入的检测能力，缓存关键信息，忽略无关内容。

基于漏洞的扫描

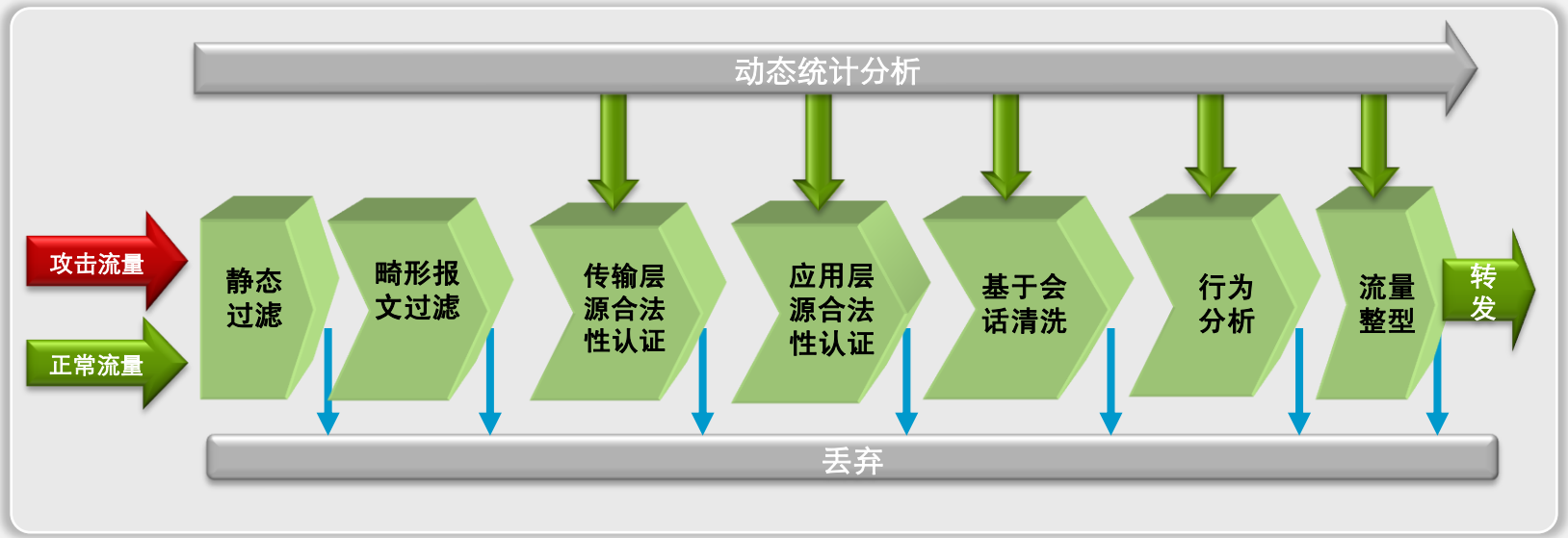
基于漏洞的签名，最小的签名关联，极低的误报

- 基于漏洞的签名，基于漏洞的签名：1条可检测识别成百上千的攻击，有效防止攻击变种；
- 独特的识别能力，基于精确识别内容的威胁检测，避免盲目的扫描大量信息导致低效率；
- 当前版本支持约3000+条签名规则，签名库每周升级，特殊情况及时发布最新签名，支持用户自定义签名规则

准确检测-多重检测技术

检测技术	用户价值
协议智能识别	保障对非标准端口应用的检测
数据包及流重组、高级逃避检测	防止逃避技术造成的漏报
应用协议识别	覆盖到文件级别的恶意威胁
攻击特征检测	对已知攻击方式或软件的检测
基于漏洞的检测	对已知漏洞及对应不同工具的检测
基于攻击原理的启发式检测	对未知漏洞和攻击的检测
网络行为/应用协议异常检测	对DoS、未知漏洞、滥用的检测

准确检测– 全方位抵御DDOS



- 现网千兆的DOS防护性能；
- 流量自学习能力；
- 抵御应用层DDOS：Web、DNS、VoIP等；

准确检测—全球攻击发现能力

遍布全球的蜜罐及攻击跟踪系统，实时捕捉恶意代码，分析黑客攻击

Power Fortress Cloud
安全研究中心

300+高级安全研究，定期（每周）或紧急（当重大安全漏洞被发现）方式发布

独立的漏洞发掘能力，为全球漏洞数据组织提供支持，包括CVE、CNCVE

HUAWEI

易于使用 – “零” 配置上线，成就用户卓越体验

- 签名库85%默认开启，实时智能防护
- 超过十种场景策略模板，实现零配置上线，适应各种用户场景

  DMZ、WEB、Mail、file、IDS模式……
- 各种类型报表，全面呈现网络安全状况

  提供时间、设备、网元等多维度的攻击统计功能
- 透明模式接入网络，零设置网络参数，即插即用

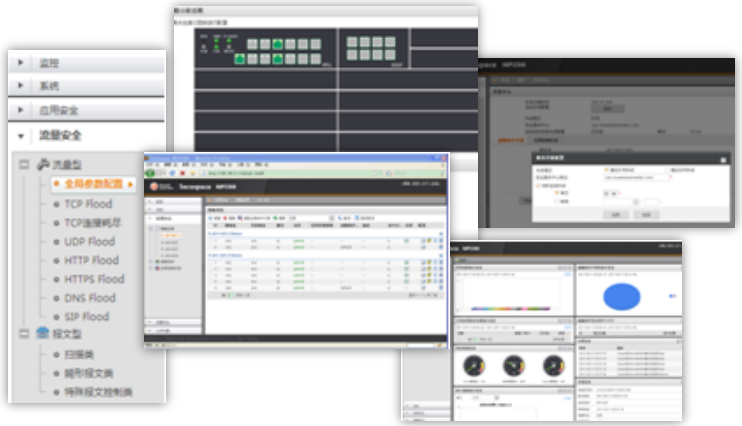
易于使用-网络流量自学习

通过网络流量基线学习，精确的得到正常业务的流量阈值，防止人工配置流量异常参数引起的错误

HUAWEI

易于使用-集中管理/报表分析

NIP Manager集中管理



实时报表 分析

- 基于Web的单机配置和NIP Manager集中管理方式；
- 智能化报表、日志功能，全面展示网络实时状况、历史信息及攻击排名、流量趋势走向；
- 定时网络健康状态报告，指导网络加固及 IT 活动实施；

HUAWEI

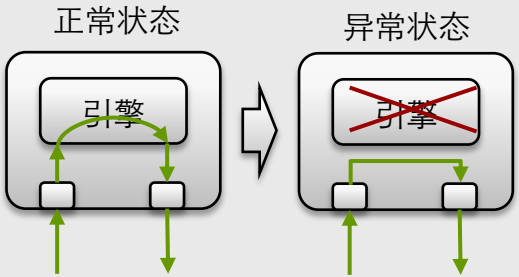
易于使用 - 电信级可靠性

电信级硬件设计

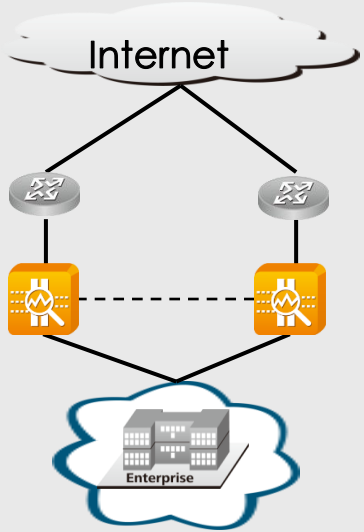
- 支持温度监控、风扇热插拔，可适应恶劣环境应用
- 双电源互相热备份，并且支持热插拔
- 按照电信产品要求设计

设备自身失效保护

- 基于软件的Bypass
- 基于硬件的Bypass
  - 电口Bypass
  - 多模光口Bypass
  - 单模光口Bypass



HA高可靠部署



HUAWEI

Content

1 现状与挑战

2 产品价值/特点

3 成功案例

4

杭州某大学校园网

客户需求

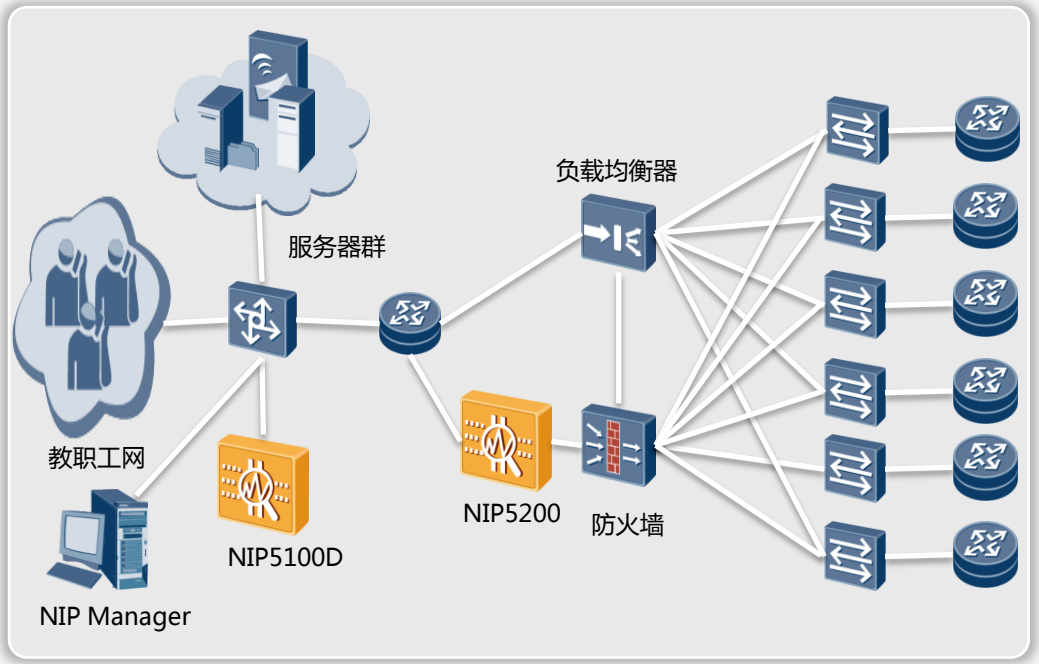
- 服务器前缺乏细粒度安全防护，存在遭受应用层攻击风险
- 教职工网络缺乏安全监控
- 入侵防御、入侵检测产品需要进行统一管理，减轻网络管理员负担

华为解决方案

- 互联网出口直路部署华为NIP5200，配合防火墙，零配置高性能防护服务器威胁
- 核心交换机上旁路部署NIP5100D，对全流量监控检测，实时展示网络状态
- NIP Manager集中管理设备

客户价值

- 在互联网出口利用高性能防护产品解决了服务器群在应用层、木马、蠕虫病毒的困扰
- 对教职工网流量进行监控，同时旁挂部署避免单点故障带来的网络中断风险
- 统一设备管理降低了网络管理员的工作强度



HUAWEI

广西某厅数据中心建设

客户需求

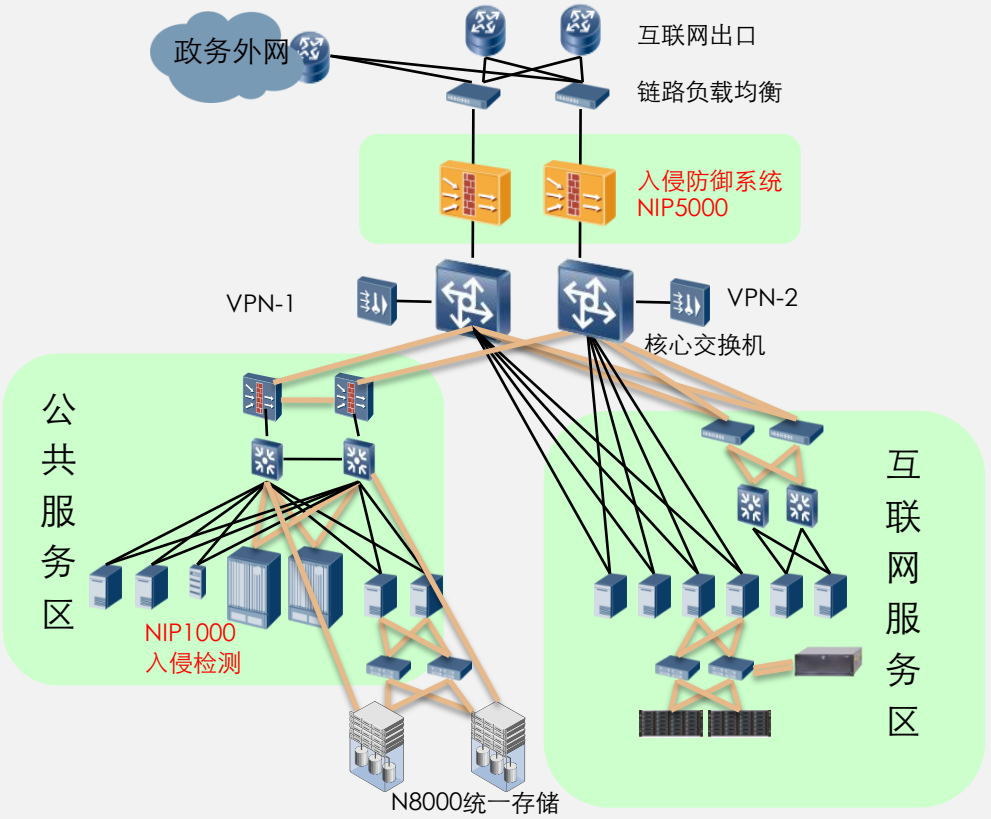
- 整合自治区、市、县三级建设行政主管部门局域网，最终达到建设行政主管部门互联互通、信息共享、结构合理、运转协调、安全稳定、功能完善的业务网络系统。
- 实现建设系统政务管理和决策支持的网络化，形成网上双向互动式的自治区住房城乡建设系统公众信息服务体系。

华为解决方案

- 在网络安全方面，利用IPS+IDS的方式有效防御应用层攻击;
- 在公用服务区边界串行部署两台千兆UTM，做3-7层的安全过滤和攻击防护;
- 在应用层安全方面，部署了TSM、VSM、eLog等软件。

客户价值

- 建成比较完善的自治区住房和城乡建设厅政务外网平台、政务信息共享交换系统和网络信任与安全体系
- 自治区住房和城乡建设厅60%的业务将实现网上办理
- 在一定程度上解决全区建设厅业务指导难、监管难、执行难的问题，全区住房和城乡建设监管能力明显提高。



HUAWEI

HUAWEI ENTERPRISE ICT SOLUTIONS A BETTER WAY