2013年4月18日星期四

HUAWEI ENTERPRISE ICT SOLUTIONS A BETTER WAY

即插即用，实时防御

— NIP入侵防御产品

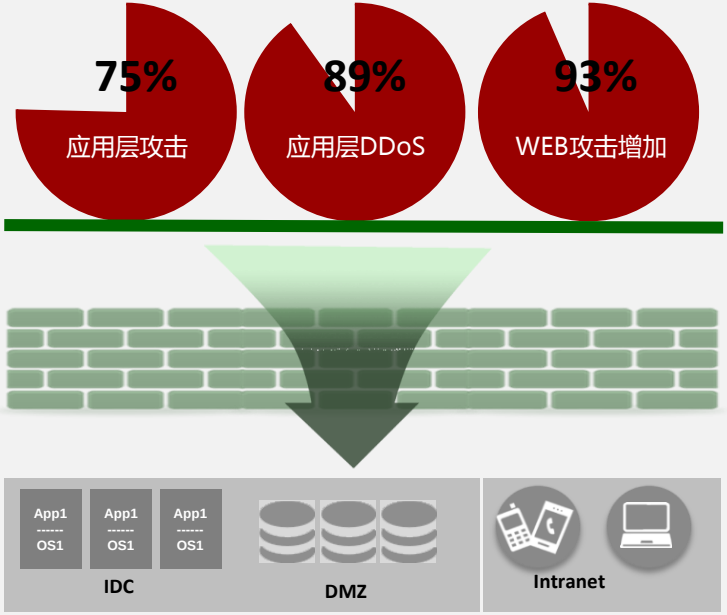
enterprise.huawei.com

HUAWEI TECHNOLOGIES CO., LTD.

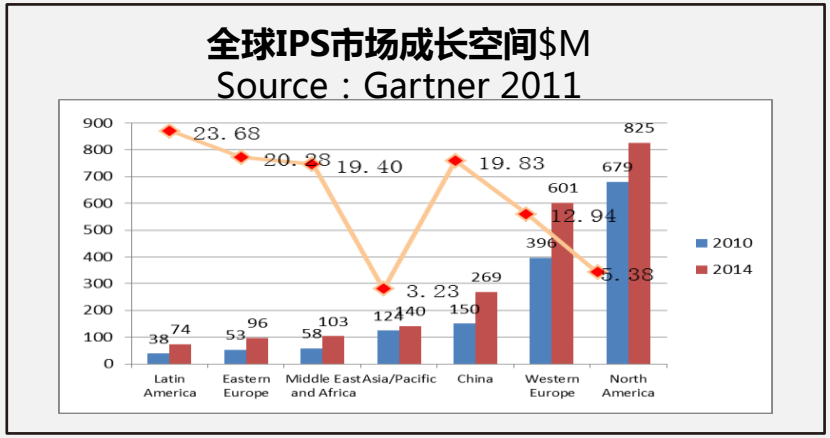
HUAWEI

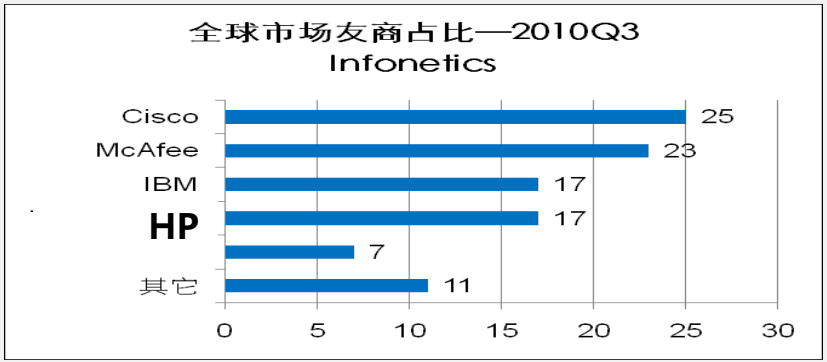
Content

IPS市场驱动以及基本情况



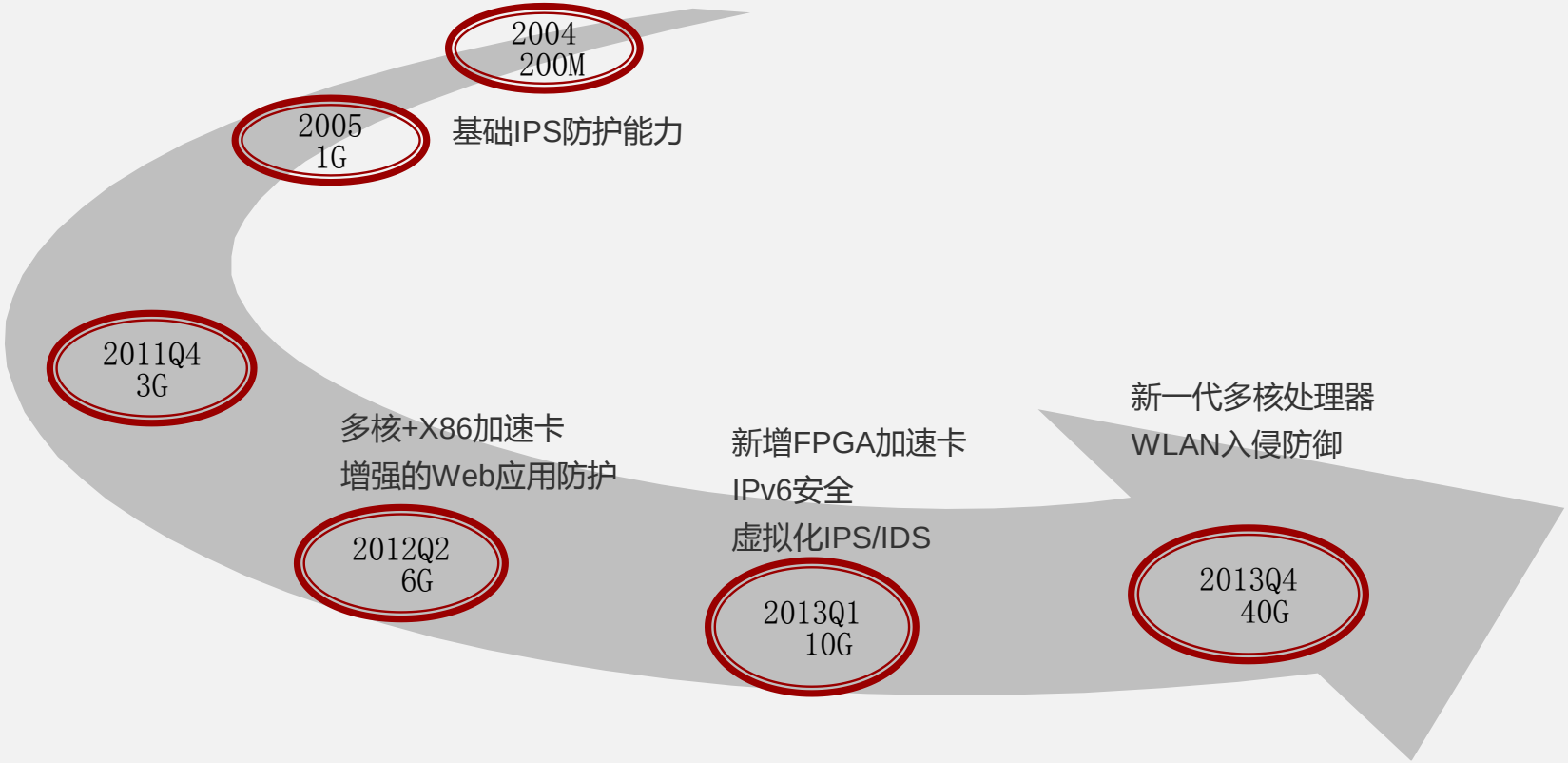
- 应用层攻击威胁巨大，尤其是针对Web应用的攻击
- 基于浏览器和应用漏洞对客户端的攻击成为主流
- APT攻击威力强大，多种攻击方式深度组合
- 攻击变种逃避技术日趋成熟





HUAWEI

华为NIP研发进展



HUAWEI

NIP 销售场景

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

产品概述

华为入侵防御系统NIP性能分布从800M到10G，可实现网络访问控制、针对应用识别和控制、针对应用漏洞的威胁防护、以及针对流量型和应用层的DDoS攻击的防护，主要应用于企业、园区、IDC（Internet Data Center）和校园网等，为客户提供应用和流量安全保障。

销售场景：

互联网出口：部署在外网Internet边界，放在防火墙前面

DMZ 区防护：部署在Internet边界，放在防火墙DMZ区

部门隔离：部署在内部局域网段之间

分支互联：部署在广域网边界

IDC：部署在数据中心

卖点：

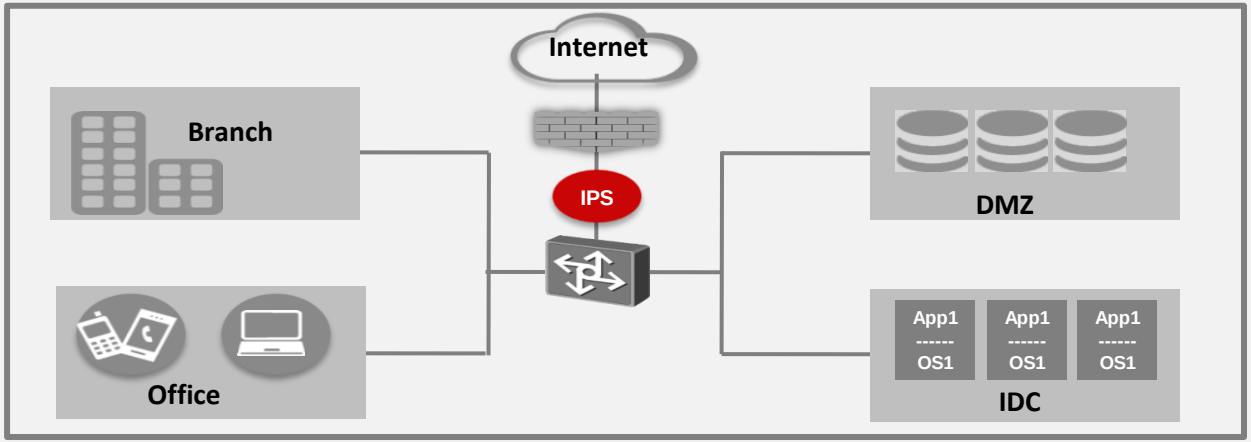
85%：签名库默认开启率达到85%，做到即插即用

80%：签名库默认阻断开启率达到80%，实时防护

0：采用多重检测技术，“0”误报率

L7：对应用层DDoS深度分析，实现对应用的DDoS防护

NIP 销售场景1-互联网出口



客户痛点：

•缺失对应用层威胁的有效防护及监控

•无法精确控制各种应用，如P2P，网络游戏等

•面对DDoS攻击，特别是应用层的攻击几乎毫无防护能力

场景卖点

应用识别-----能识别的应用达到1200+，实现精细化的应用防护，节省了出口带宽，保证了关键业务的业务体验；

L3-L7层DDoS防御：深度识别三到七层的DDOS攻击，实现“0”误报，有效保护了基础网络设备；

推荐产品：

可以依据出口带宽大小，部署不同的NIP产品

目标客户：

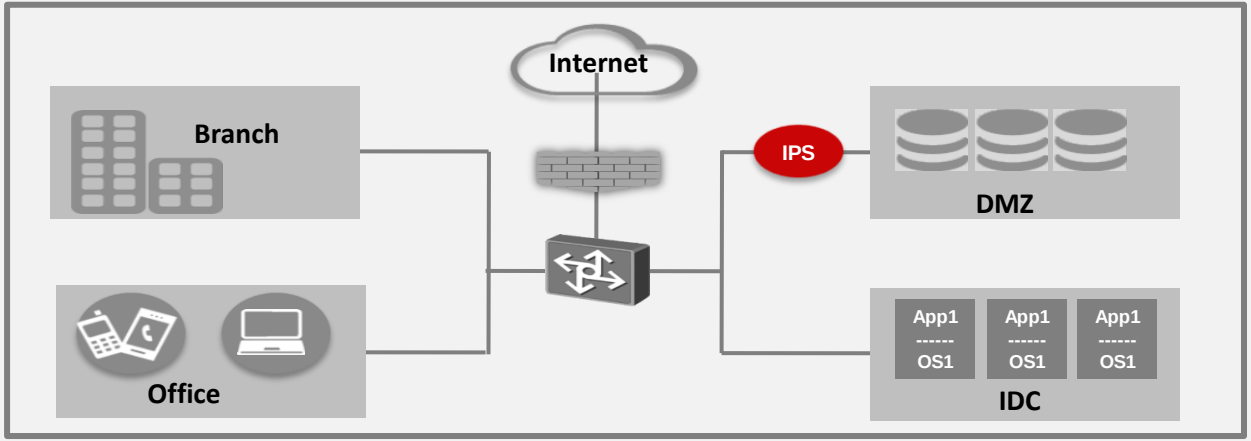
SMB小型企业 、大中型各类企业；

政府；学校；

运营商、IDC、ISP

HUAWEI

NIP 销售场景2-DMZ区



客户痛点：

•大量针对WEB应用的DDOS攻击无法防范

•大量针对WEB的恶意攻击，如SQL注入、跨站攻击等

• 针对DMZ区的服务器系统攻击无法防护

• 网页无法防篡改

场景卖点

L7层DDoS防御：深度识别七层的DDOS攻击，实现0误报，低漏报，有效保护了基于应用的DDoS攻击；

基于漏洞的签名-----基于漏洞签名有效防护了各种攻击的变种、逃避等，有效实现了虚拟补丁的功能；

SQL注入、跨站等基于Web的安全防护

推荐产品：

可以依据出口带宽大小，部署不同的NIP产品

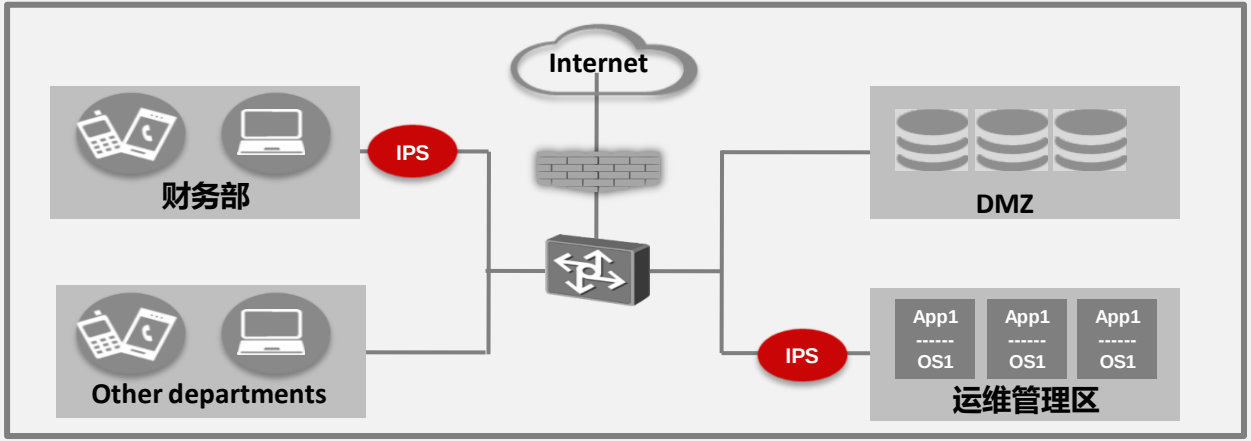
目标客户：

SMB小型企业 、大中型各类企业；

政府；学校；

运营商、IDC、ISP

NIP 销售场景3-部门隔离



客户痛点：

- 已被入侵主机可能把威胁扩散至全网
- 关键用户区缺少有效监控
- 面对可能的内部主动攻击缺少监控、防护
- 内部恶意攻击无法追溯

场景卖点

基于漏洞的签名-----基于漏洞签名有效防护了各种攻击的变种、逃避等，有效实现了对僵尸蠕虫木马病毒等内部攻击的防护；

“零”误报-----综合多种检测技术，实现零误报，保证业务正常

推荐产品：

可以依据出口带宽大小，部署不同的NIP产品

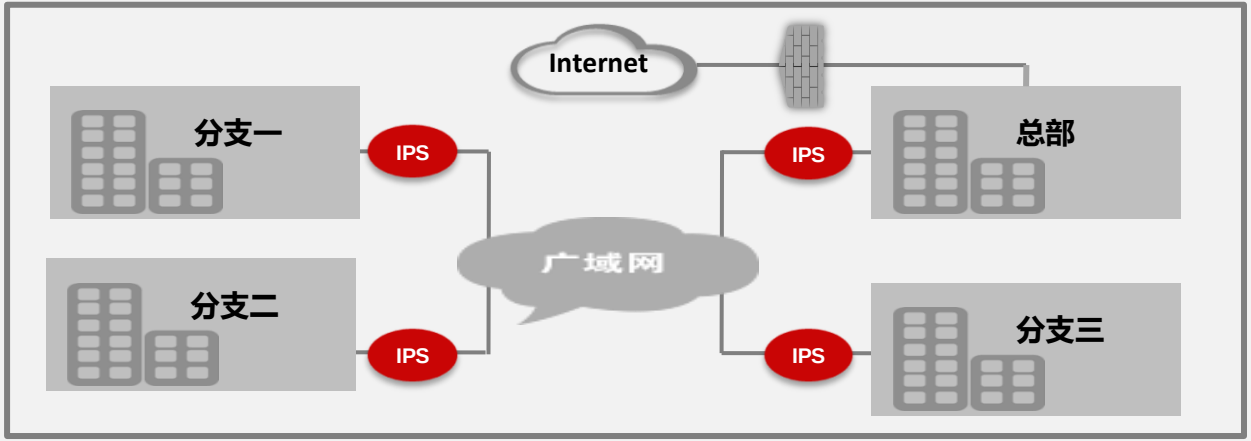
目标客户：

SMB小型企业 、大中型各类企业；

政府；学校；

运营商、IDC、ISP

NIP 销售场景4-分支互联



客户痛点：

•蠕虫造成的垃圾流量防护，消耗广域网有限的带宽

•大量与工作无关的上网流量在广域网上传播，降低广域网的传输效率

•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

场景卖点

应用识别-----能识别的应用达到1200+，实现精细化的应用防护，保证了关键业务的业务体验；

“零”误报-----综合多种检测技术，精确识别病毒、木马等，实现零误报，保证业务正常

推荐产品：

可以依据出口带宽大小，部署不同的NIP产品

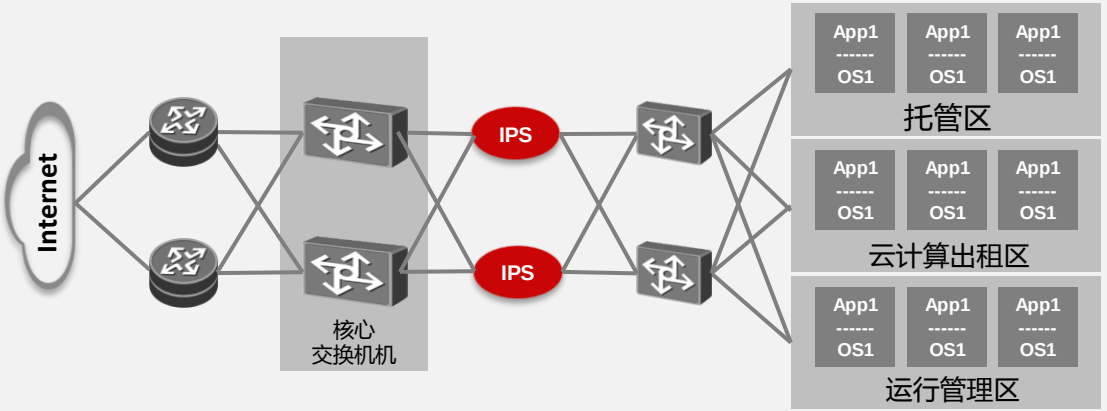
目标客户：

大中型各类企业；

政府；

运营商、IDC

NIP 销售场景5-IDC防护



客户痛点：

•IDC中大量的系统漏洞无系统防护

•SQL注入等攻击影响数据库系统安全

•无法防范恶意攻击者对数据中心的敏感信息窃取、拒绝服务、非法篡改等

场景卖点

85%默认开启率：高开启率有效的防护了系统漏洞防护，提供虚拟软件补丁服务，保证服务器正常运行

基于漏洞的签名库：有效防范恶意攻击者对数据中心的敏感信息窃取、拒绝服务、非法篡改等

“真”性能：高流量环境下有效保护业务安全

推荐产品：

NIP5500

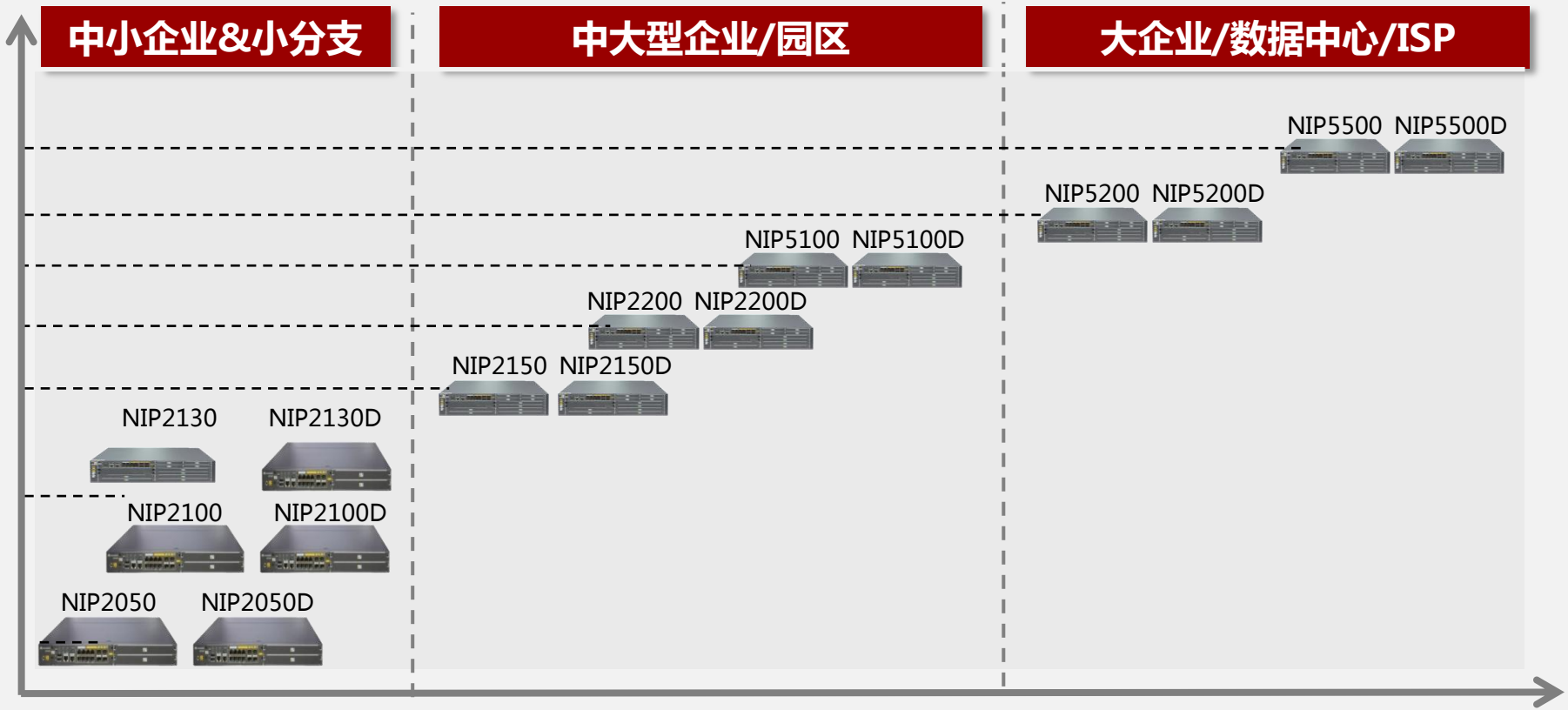
目标客户：

IDC

HUAWEI

Content

产品型号


中小企业&小分支
中大型企业/园区
大企业/数据中心/ISP
NIP5500
NIP5500D
NIP5200
NIP5200D
NIP5100
NIP5100D
NIP2200
NIP2200D
NIP2150
NIP2150D
NIP2130
NIP2130D
NIP2100
NIP2100D
NIP2050
NIP2050D

HUAWEI

NIP产品价值

保护客户端

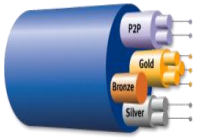
- 客户端应用防护
- 恶意软件防护

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



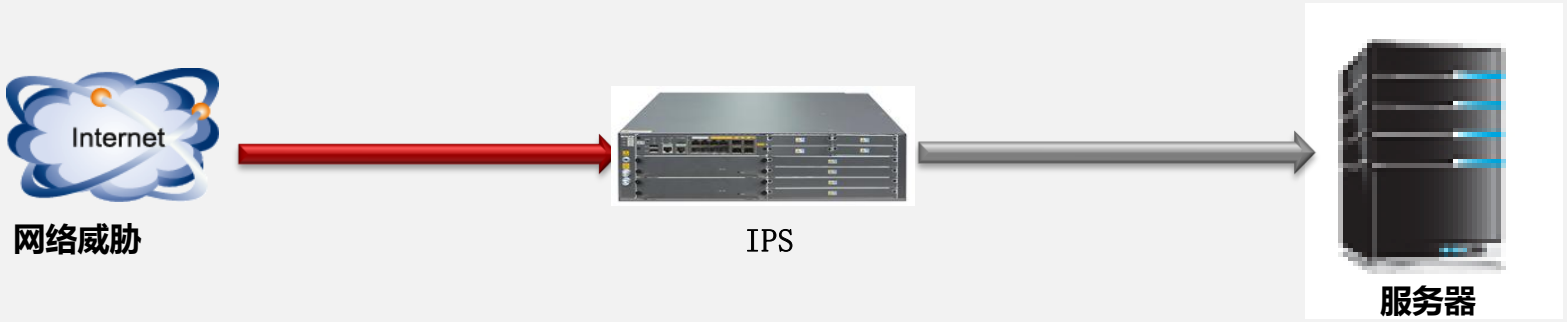
- 应用带宽管理

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

保护服务器



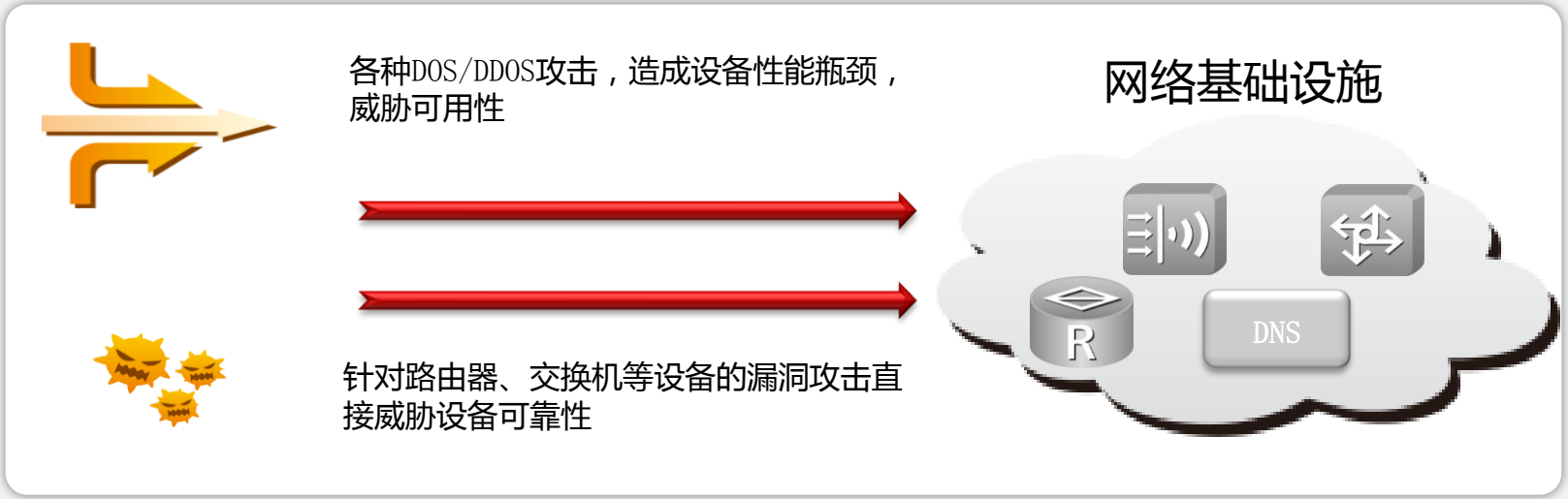
攻击前期	• 网络扫描 • 漏洞扫描	→	• 基于网络异常发现网络扫描 • 基于行为特征发现漏扫工具	
攻击中期	• 漏洞攻击 • Web应用攻击 • DOS攻击 • 暴力破解	→	• 虚拟补丁技术检测漏洞攻击 • Web应用防护 • 完整的DOS防御 • 基于行为检测发现暴力破解	
攻击后期	• 种植恶意软件 • 操控被攻击设备	→	• 检测恶意软件并阻断 • 检测控制、外传流量	← • 外传数据信息 • 成为傀儡主机

HUAWEI

保护客户端

- 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、蠕虫及对操作系统的攻击防护；

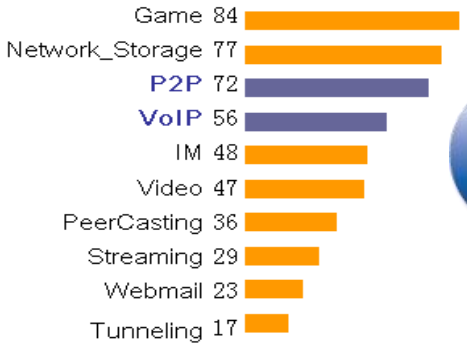
保护基础设施



- 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

- 支持协议1200+
- 定制化需求的快速响应能力



主流应用协议的识别控制，可以有效的保障业务带宽，并提高企业IT治理水平：

- 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、在线存储以及隧道传输等控制，防止机构内部文件非法外传；

全面检测：威胁覆盖全面

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深度检测，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

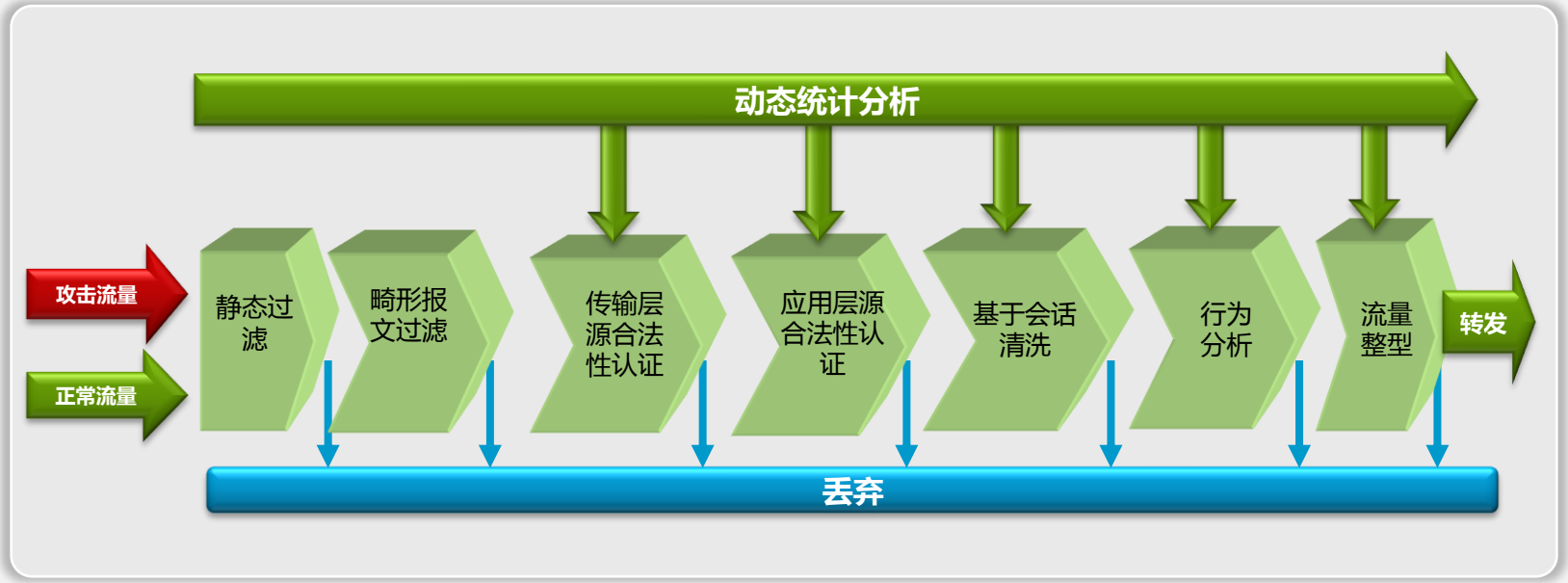
DDOS检测

- 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

检测技术全面

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
文件类型识别	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

全方位抵御L2-L7层DDOS



- 流量自学习能力；
- 抵御应用层DDOS：Web、DNS、VoIP等；

精准检测—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

全面防护—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，每秒监控流量18000G+

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

NIP 产品亮点

□精确防护：“零”误报，高效阻断业务威胁

✓精准的漏洞特征库，高达80%的默认签名开启率

✓2~7层DDoS防护，自动配置阈值，精准防护DDoS攻击

✓1200+ 应用识别

□业界真实的IPS 性能，最高10Gpbs防御能力

✓系统采用XLR多核+IA通用处理器+FPGA架构

✓在流量峰值的情况下，依然保持稳定的检测防御性能

□零配置上线，安全全景报表，轻松掌握，易于使用

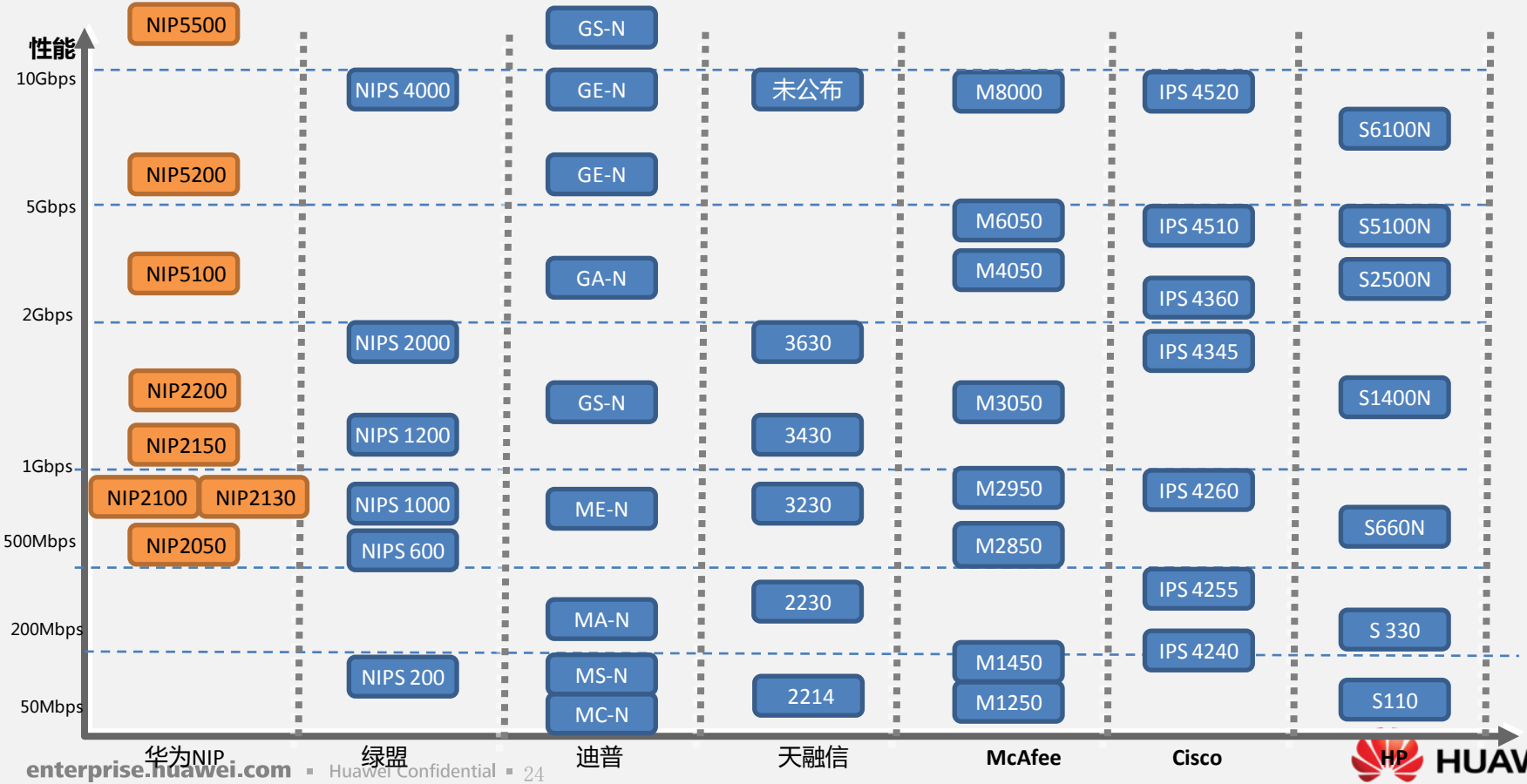
✓不需要设置网络参数和变更网络结构，即插即用，实时防护

✓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

Content

友商性能型号映射


性能
10Gbps
5Gbps
2Gbps
1Gbps
500Mbps
200Mbps
50Mbps
NIP5500
NIP5200
NIP5100
NIP2200
NIP2150
NIP2100
NIP2130
NIP2050
NIPS 4000
NIPS 2000
NIPS 1200
NIPS 1000
NIPS 600
NIPS 200
GS-N
GE-N
GE-N
GA-N
GS-N
ME-N
MA-N
MS-N
MC-N
未公布
3630
3430
3230
2230
2214
M8000
M6050
M4050
M3050
M2950
M2850
M1450
M1250
IPS 4520
IPS 4510
IPS 4360
IPS 4345
IPS 4260
IPS 4255
IPS 4240
S6100N
S5100N
S2500N
S1400N
S660N
S 330
S110
华为NIP
绿盟
迪普
天融信
McAfee
Cisco
HP

PK 绿盟：准、全

产品简介

- 国内最早的IPS厂商，品牌优；
- 工控机架构；
- 除基本功能外，Web安全（URL分类+信誉）、IM/P2P管理、防病毒模块均是收费项；
- 完成NSS测试。

打击点：

- 安全性：默认开启阻截签名不足40%，影响实际防御效果。
- 安全性：应用识别种类<500
- 安全性：DOS没有流量学习功能
- 安全性：NSS测试不佳：1200A实际性能500-720M，阻截率31.6-79%
- 性能：X86架构，大流量情况时延较大。1G以上建议客户比较时延变化。
- 硬件规格：无端口扩展能力，1U产品无冗余电源；
- 商务：默认只有1路IPS，Web防护、防病毒需要另外收费

优势点：

- 品牌影响力
- 功能丰富：防病毒、URL分类
- 易用性，特别是报警可读性强
- 报表系统相对完善

绿盟产品规格

		NIPS 200	NIPS 6000	NIPS 1000	NIPS1200	NIPS 2000
硬件规格	专用管理口	1	1	1	1	2
	网络接口	4GE	8GE	4GE+6SFP	4GE+4SFP	4GE+4SFP
	默认防护路数	1	1	1	1	1
	硬件Bypass	内置GE	内置GE	内置GE	内置GE	内置GE
	物理尺寸	1U	1U	2U	2U	2U
	电源	交流单电	交流单电	交流单电	交流冗余	交流冗余
软件扩展	Web安全模块	单独收费				
	IM/P2P管理模块	单独收费				
	防病毒模块	单独收费				
	授权增加防护路数	单独收费				

- 默认只有一路IPS防护，要求多路防护可提高商务成本；
- Web安全、防病毒模块需要单独收费
- 低端产品没有冗余电源

绿盟功能对比

类别		基本要素	绿盟	HW
管理部署	部署方式	在线、旁路、非对称路由、TAP	支持	支持
	特殊封装	MPLS、VLAN、IPv6、Q in Q、GRE	VLAN	MPLS、VLAN
	管理方式	基于设备的Web管理/集中管理	支持	支持
	策略应用	虚拟IPS/内置模板适应多种场景	可基于网段，10余种模板	可基于网段，10余种模板
	响应配置	block、TCPreset、隔离、抓包	支持	支持
	环境感知	信誉、漏洞、应用、用户等	仅支持应用	仅支持应用
威胁防护	应用服务防护	Web应用、邮件、FTP等	支持	支持
	客户端漏洞防护	浏览器、Office、多媒体等	支持	支持
	应用带宽控制	应用识别数量及限流功能	<500应用，支持限流	1000+应用，支持限流
	DoS防护	L3层DoS 以及 L7层DoS，流量学习	无流量学习功能	支持
	恶意软件防护	蠕虫、木马、间谍软件、Botnet	支持，可购买专门防病毒模块	支持
	高级威胁防护	协议异常、流量异常、行为异常	支持	支持
报表日志	知识库	中英文，完备的分类及解决方案信息	支持	支持
	报表生成	预定义报表，自定义报表、自动生成	支持	支持，自定义报表定制能力较弱
	报表导出	支持Word、PDF、HTML	支持	支持
	第三方联动	漏洞管理、HIPS、FW、SIEM	支持FW和SIEM	支持FW和SIEM

PK McAfee

产品简介




●全球最早的IPS厂商之一；

●专业的多核+FPGA+X86架构，产品线从100M-10G；

●Gartner象限中市场和技术全面领先

●NSS历次测试威胁覆盖率，默认阻断等各项指标领先

打击点：

1. 安全性：缺少应用层DoS防护能力，特别是针对HTTP、DNS、SIP等关键业务的DoS防护
2. 易用性：默认开启阻截签名较少（1000-），逐个确认开启需要大量策略调整工作
3. 易用性：对与知名应用运行在非标准端口的情况，需要手工配置端口才能检测；
4. 易用性：不具备设备自身的Web管理能力，单机管理也需要专门服务器安装管理软件；

回避点：

●SA业务感知>1100,涵盖主要Web2.0应用

●支持net flow检测，具备环境感知能力（漏洞、威胁趋势）和信誉检测能力

●可选NAC模块

McAfee产品规格

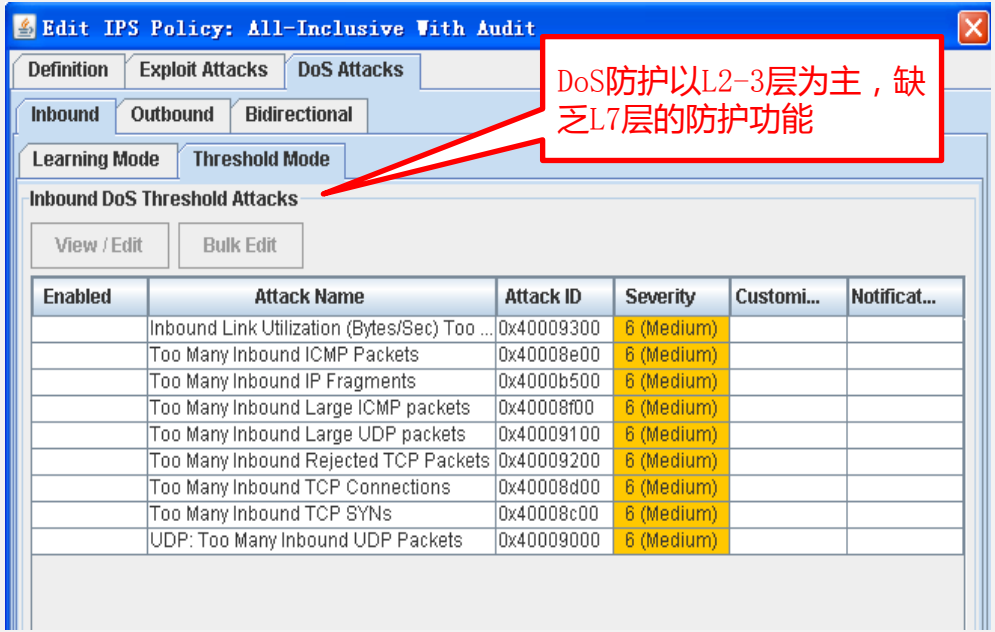
		M-8000	M-6050	M-4050	M-3050	M-2950	M-2850	M-1450	M-1250
性能	Real world	10Gbps	5Gbps	3Gbps	1.5Gbps	1.0Gbps	600Mbps	200Mbps	100Mbps
	Max throughput	20Gbps	10Gbps	4Gbps	2.5Gbps	1.5Gbps	1Gbps	300Mbps	150Mbps
	Total Sessions	4,000,000	2,000,000	1,500,000	750,000	750,000	750,000	80,000	40,000
	Connections Per Second	120,000	60,000	36,000	18,000	15,000	10,000	4,000	2,000
	虚拟IPS数量	5,000	5,000	5,000	5,000	100	100	32	16
	ACL rules	1,000	1,000	1,000	1,000	1,000	400	100	50
物理规格	尺寸	4U	2U	2U	2U	2U	2U	1U	1U
	GE接口	16	8	8	8	20	20	8	8
	10GE接口	12	8	4	4	N/A	N/A	N/A	N/A
	内置bypass	N/A	N/A	N/A	N/A	8	8	8	8
	专用管理口	1	1	1	1	1	1	1	1

McAfee功能对比

类别		基本要素	McAfee	HW
管理部署	部署方式	在线、旁路、非对称路由、TAP	支持	支持
	特殊封装	MPLS、VLAN、IPv6、Q in Q、GRE	支持	支持
	管理方式	基于设备的Web管理/集中管理	设备自身没有web管理	支持
	策略应用	虚拟IPS/内置模板适应多种场景	可基于子接口，20余种模板	可基于网段，10余种模板
	环境感知	信誉、漏洞、应用、用户等	支持	仅支持应用
威胁防护	应用服务防护	Web应用、邮件、FTP等	支持	支持
	客户端漏洞防护	浏览器、Office、多媒体等	支持	支持
	应用带宽控制	应用识别数量及限流功能	1000+应用，支持限流	1000+应用，支持限流
	DoS防护	L3层DoS 以及 L7层DoS，流量学习	L7层DoS防护能力不足	支持
	恶意软件防护	蠕虫、木马、间谍软件、Botnet	支持	支持
	高级威胁防护	协议异常、流量异常、行为异常	支持，并通过NetfFow全网检测	支持协议异常、流量异常检测
报表日志	知识库	中英文，完备的分类及解决方案信息	支持	支持
	报表导出	支持Word、PDF、HTML	支持	支持
	第三方联动	漏洞管理、HIPS、FW、SIEM	支持	仅支持FW和SIEM

McAfee打击点：应用层DoS缺失

- 现今最具威胁的DDoS均是针对具体应用的，如Web、DNS、SIP等，一个页面生成需要的资源远大于TCP连接，也可以很容易瘫痪系统
- McAfee 现有版本缺少足够的应用层DOS防护能力；
- HW NIP产品有丰富的针对应用层DDOS攻击的检测与防范技术



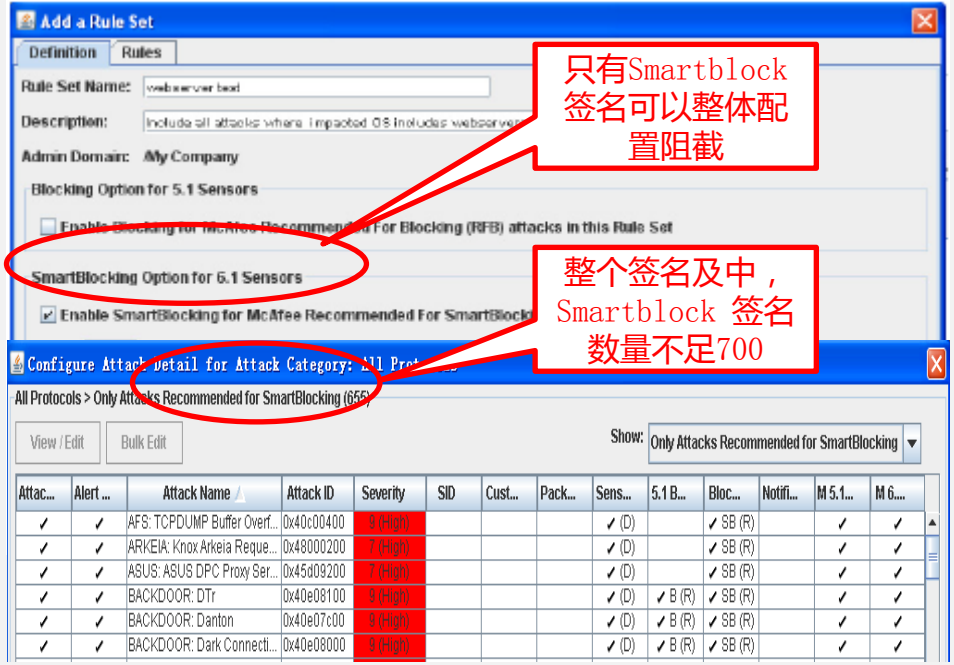
Enabled	Attack Name	Attack ID	Severity	Customi...	Notificat...
	Inbound Link Utilization (Bytes/Sec) Too ...	0x40009300	6 (Medium)		
	Too Many Inbound ICMP Packets	0x40008e00	6 (Medium)		
	Too Many Inbound IP Fragments	0x4000b500	6 (Medium)		
	Too Many Inbound Large ICMP packets	0x40008f00	6 (Medium)		
	Too Many Inbound Large UDP packets	0x40009100	6 (Medium)		
	Too Many Inbound Rejected TCP Packets	0x40009200	6 (Medium)		
	Too Many Inbound TCP Connections	0x40008d00	6 (Medium)		
	Too Many Inbound TCP SYNs	0x40008c00	6 (Medium)		
	UDP: Too Many Inbound UDP Packets	0x40009000	6 (Medium)		

重点优势场景：互联网出口防护、DMZ区防护

HUAWEI

打击点详解：推荐阻截签名少

- 只有Smartblock的签名可以基于签名集配置阻截，所有签名中Smartblock签名不足700，占总数<30%,
- 其它签名开启阻截需一个一个的到确认配置
- ***McAfee IPS要达到理想的防御效果需要大量的签名调整工作，易用性不佳***



重点优势客户：中小型企业、学校等

HUAWEI

打击点详解：非典型端口需手工配置

- 在企业员工上网场景以及运营商IDC场景，都不可能掌握应用协议的采用的端口全面信息；
- McAfee产品需要配置这些协议的端口，因此实际上对这些非标协议缺乏防护能力
- HW NIP产品根据流量自动判断应用协议，无需手工配置，提供周到的防护

重点优势场景和客户：中小型企业以及IDC安全防护

HUAWEI

PK Cisco

产品简介




●全球最早的IPS厂商之一；

●X86架构（IPS4300,IPS4500有模式匹配硬件加速模块）

●全球市场占有率排名第一，达到25%的市场份额，在Gartner象限中市场和技术全面领先

打击点：

1. 性能：C公司IPS产品检测吞吐量差，在大流量、富媒体流量情况下检测效果下降
2. 安全性：缺少应用层DOS防护能力，无法方法针对HTTP、DNS、SIP等定制的DOS攻击
3. 配置管理：C公司配置管理复杂，需接受培训才能完成配置
4. 应用识别：C公司应用识别数量为600+，识别能力远低于我司
5. 接口扩展能力：C公司的接口扩充能力有限，部分型号不支持扩充

回避点：

●防护能力：不比拼签名数量，强调我司只针对常见的和最新的威胁进行防护，目前C公司拥有近6K条漏洞签名，防护的范围比较广

●组网能力：强调接口对串接直路防护能覆盖大部分场景，且最有效，C公司在网络技术方面积累深厚，IPS产品在2层/3层网络部署中，均有较好方案

PK HP（TipPingPoint）

产品简介

●两条产品线：

N系列NP+FPGA，750M-8G，

IPS系列 X86，20M、100M、300M

●曾经最专业的IPS产品品牌，经3COM和HP两次收购后，影响力下滑

打击点：

●安全性：硬件架构限制解码能力（HTML等），致使客户端防护能力不足。

●安全性：缺少应用层DOS防护能力，无法方法针对HTTP、DNS、SIP等定制的DOS攻击

●安全性：SA业务感知数量少于500

●中国本土化：缺少中文版本，缺少网游、炒股类别应用识别

优势点：

●N系列专用硬件，时延指标领先；

●具备信誉和环境感知能力（漏洞、威胁趋势、应用）；

●漏洞跟踪团队DV-Lab知名度高

HP（TP）产品规格

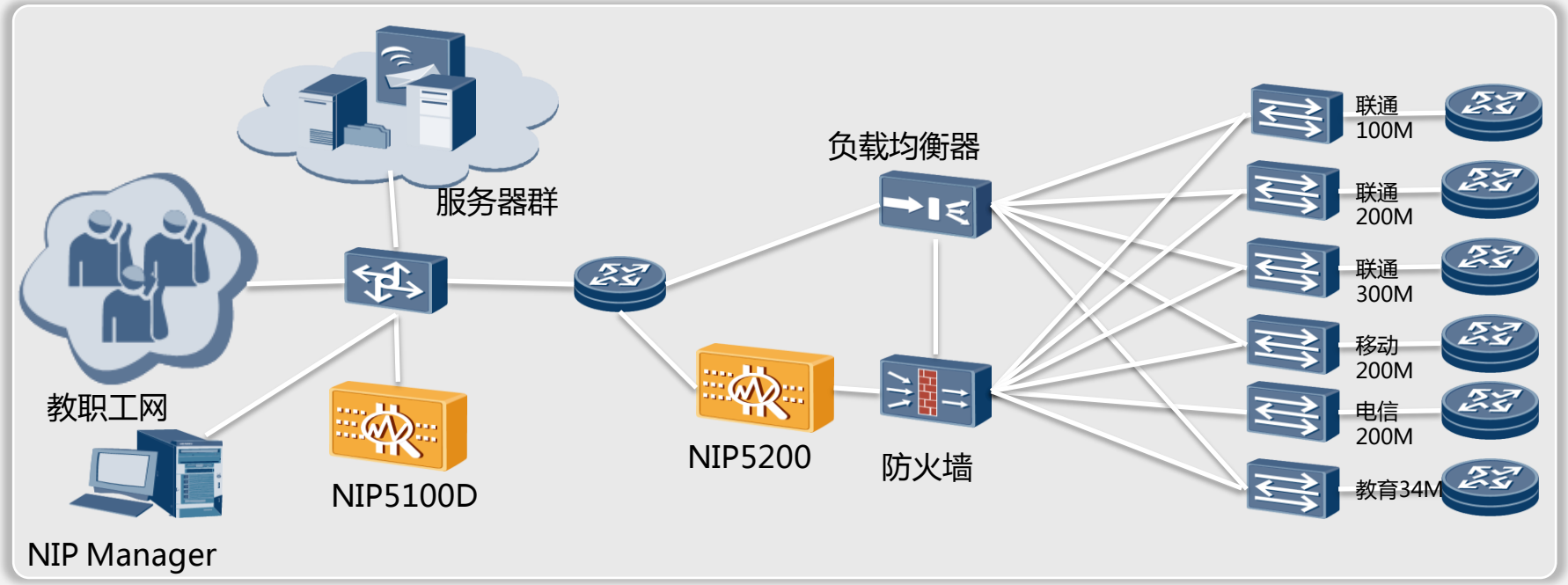
		S110	S330	S660N	S1400N	S2500N	S5100N	S6100N
性能	IPS/IDS吞吐	100M	300M	750M	1.5G	3G	5G	8G
	网络吞吐	100M	300M	750M	1.5G	15G	15G	15G
	典型时延	<600us	<600us	<80us	<80us	<80us	<80us	<80us
	最大网络会话	1,000,000	1,000,000	6,500,000	6,500,000	10,000,000	10,000,000	10,000,000
	最大安全会话	250,000	250,000	1,200,000	1,200,000	2,600,000	2,600,000	2,600,000
	新建会话速率	9,700	18,500	115,000	115,000	230,000	230,000	230,000
硬件规格	网络接口	8GE	8GE	10GE 10SFP	10GE 10SFP	2XFP 10GE 10SFP	2XFP 10GE 10SFP	2XFP 10GE 10SFP
	硬件Bypass	内置	内置	外置可选	外置可选	外置可选	外置可选	外置可选
	电源	AC	AC	AC	AC	AC&DC	AC&DC	AC&DC
	物理尺寸	1U	1U	2U	2U	2U	2U	2U

HP 功能对比

类别		基本要素	HP	HW
管理部署	**部署方式**	在线、旁路、非对称路由、TAP	支持	支持
	特殊封装	MPLS、VLAN、IPv6、Q in Q、GRE	支持	支持
	策略应用	虚拟IPS/内置模板适应多种场景	可基于网段	可基于网段，10余种模板
	响应配置	block、TCPreset、隔离、抓包	支持	支持
	环境感知	信誉、漏洞、应用、用户等	支持	仅支持应用
威胁防护	**应用服务防护**	Web应用、邮件、FTP等	支持	支持
	应用带宽控制	应用识别数量及限流功能	<500应用，支持限流	1000+应用，支持限流
	DoS防护	L3层DoS 以及 L7层DoS，流量学习	支持	支持
	恶意软件防护	蠕虫、木马、间谍软件、Botnet	支持	支持
	高级威胁防护	协议异常、流量异常、行为异常	支持	支持
报表日志	**知识库**	中英文，完备的分类及解决方案信息	不支持中文	支持
	报表生成	预定义报表，自定义报表、自动生成	支持	支持
	第三方联动	漏洞管理、HIPS、FW、SIEM	支持漏洞管理、FW、SIEM、NBAD	支持FW和SIEM

Content

杭州某大学校园网



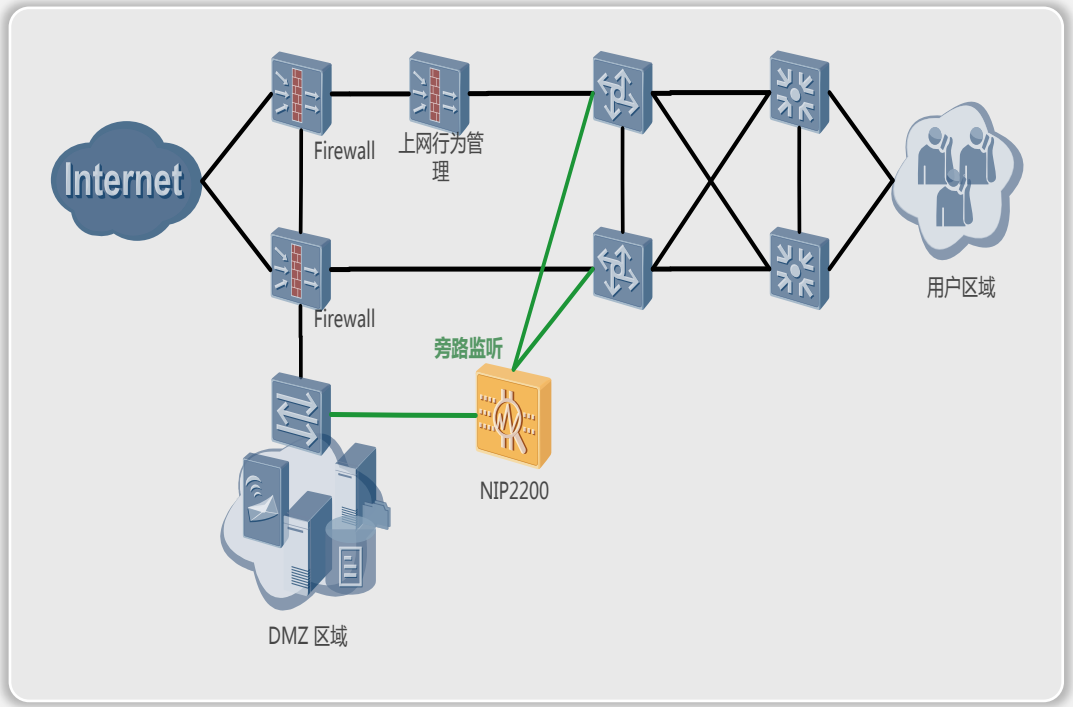
主要诉求

- 同时要求威胁监控和防护
- 服务器防护
- 集中管理

方案亮点：

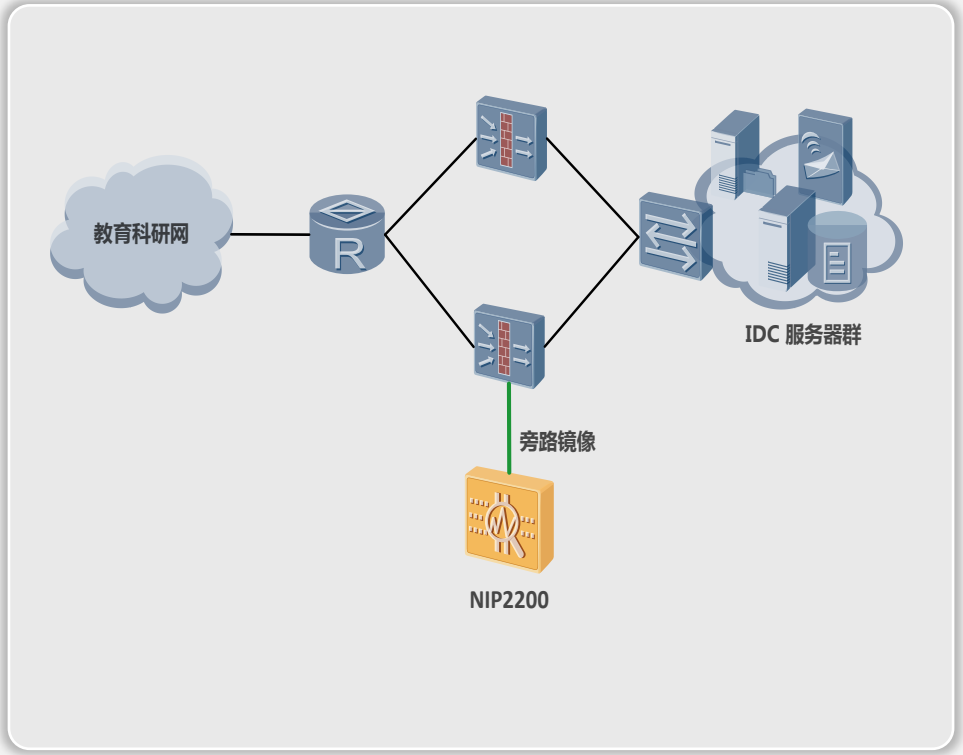
- 直路部署NIP5200，配合防火墙，零配置高性能防护服务器威胁
- 旁路部署NIP5100D，对全流量监控检测，实时展示网络状态
- NIP Manager集中管理设备

深圳宝安机场



客户面临挑战：
多路采样，不同安全策略需求
解决方案：
通过部署一台 NIP 设备，来实现多路网络的统一侦听和分析
方案亮点：
利用旁路部署方式，对多个不同网络同时进行监听；未来可升级到在线部署方式，保护客户投资

上海教科委（教育网）



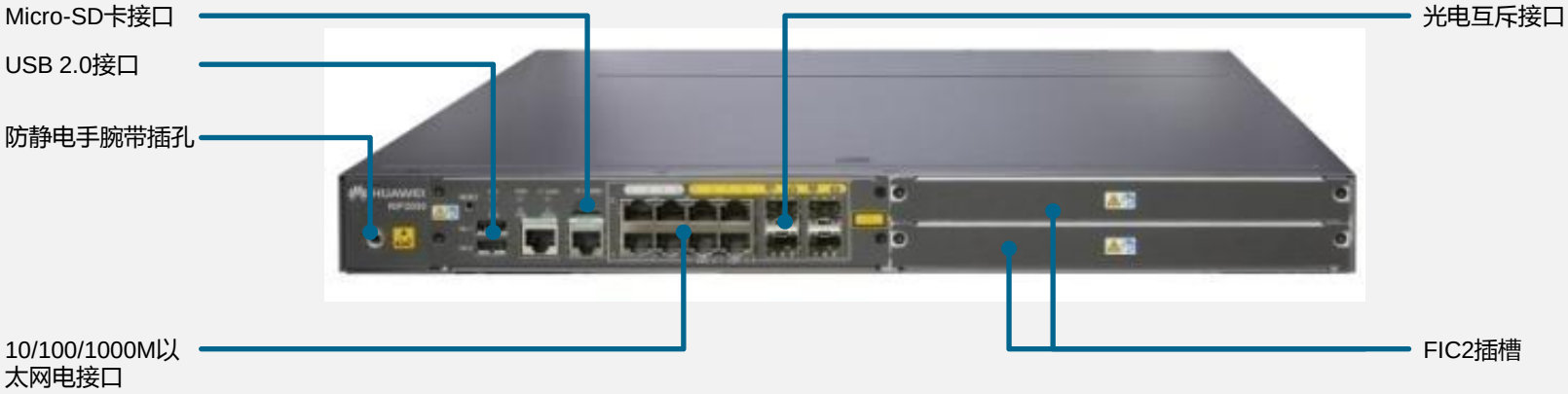
客户面临挑战：
服务器威胁繁多
缺少对威胁管理的可视化能力

解决方案：
NIP实现流量和威胁的分析管理，直观了解网络威胁现状

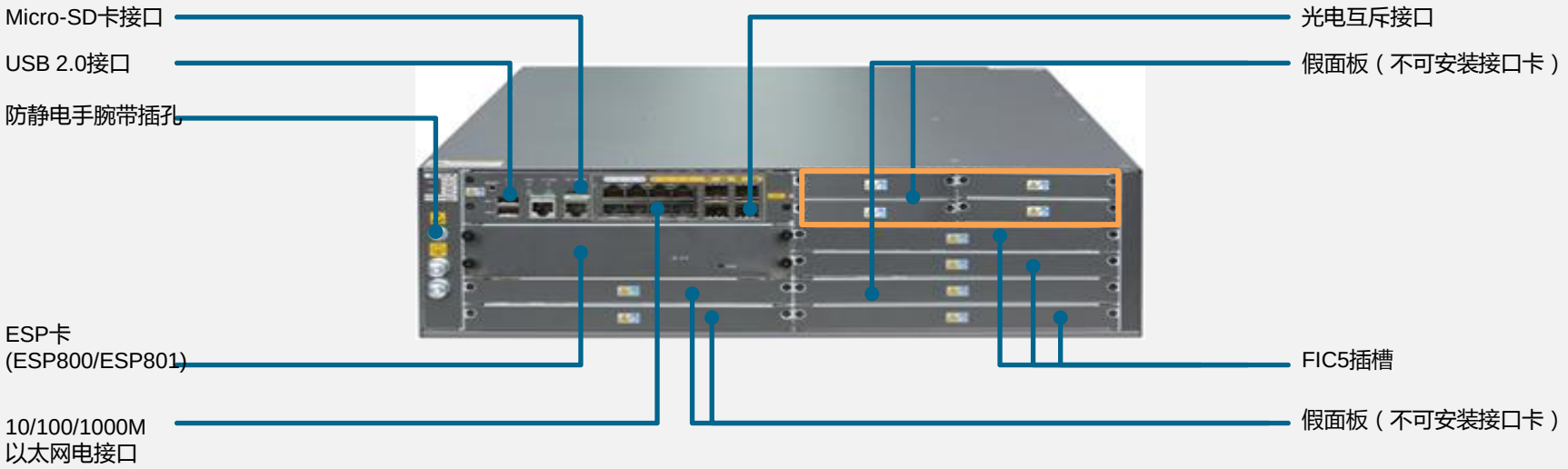
客户利益：
利用 NIP 的旁路部署方式，对于 L2-L7 各种流量和威胁信息进行统一可视化管理；
从网络流量应用组成到 DDoS、应用层漏洞攻击、Web 应用类攻击，都一目了然

Content

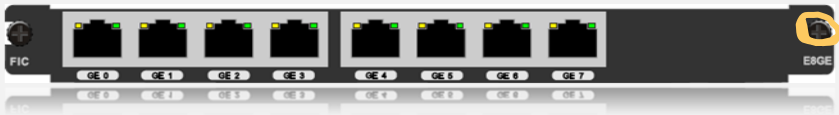
NIP 2100


Micro-SD卡接口
USB 2.0接口
防静电手腕带插孔
10/100/1000M以太网电接口
光电互斥接口
FIC2插槽

NIP 2200/5100/5200/5500



扩展接口板



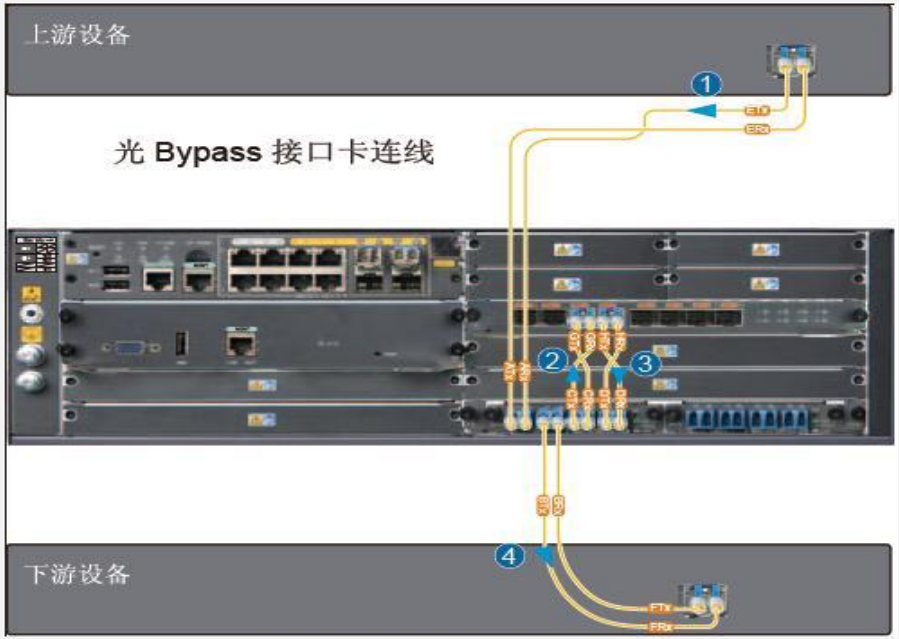
8GE电接口扩展卡

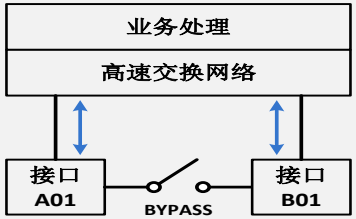
8GE光接口扩展卡

4GE电接口bypass接口卡

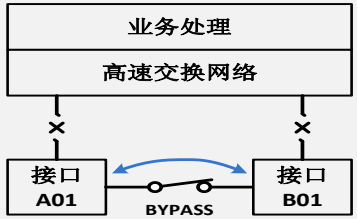
两路光接口bypass接口卡

光bypass卡的配置





正常工作中



系统异常触发 BYPASS

- 光bypass卡需另外配置
- 4 接口的光bypass卡保护一路数据
- 正常数据流向：1 - 2 - 3 - 4
- 数据bypass流向：1 - 4

异常情况包括：主机软件系统异常，系统硬件故障，设备掉电等

HUAWEI

NIP 配置

Step 1 – 选择主机（部分展现）

1.1	主机
NIP2100-AC-01	NIP2100交流主机(4GE电+4GE Combo,4G内存,2交流电源)-含HS NIP网络智能防护系统软件-含12月知识库升级服务
NIP2200-AC-01	NIP2200交流主机(4GE电+4GE Combo,4G内存,2交流电源)-含HS NIP网络智能防护系统软件-含12月知识库升级服务
NIP5100-AC-01	NIP5100交流主机(4GE电+4GE Combo,4G内存,2交流电源)-含HS NIP网络智能防护系统软件-含12月知识库升级服务
NIP5200-AC-01	NIP5200交流主机(4GE电+4GE Combo,4G内存,2交流电源)-含HS NIP网络智能防护系统软件-含12月知识库升级服务
NIP5200-DC-01	NIP5200直流主机(4GE电+4GE Combo,4G内存,2直流电源)-含HS NIP网络智能防护系统软件-含12月知识库升级服务

Step 2 – 选择模块

1.2	业务模块
FIC-4GE-BYPASS	4GE电口Bypass卡-含HS通用安全平台软件
FIC-8GE	8GE电口卡-含HS通用安全平台软件
FIC-8SFP	8GE光口FIC卡-含HS通用安全平台软件
FIC-2LINE-M-BYPASS	2链路LC/UPC多模光接口Bypass保护卡-含HS通用安全平台软件
FIC-2LINE-S-BYPASS	2链路LC/UPC单模光接口Bypass保护卡-含HS通用安全平台软件
FIC-2SFP+	2*10GE光口FIC卡-含HS通用安全平台软件
FIC-2SFP+&8GE	2*10GE光口+8GE电口卡-含HS通用安全平台软件

Step 3 – 选择知识库License

1.3	知识库升级特性
LIC-IPS-12-NIP2100	知识库升级服务时间12个月-含HS NIP网络智能防护系统软件
LIC-IPS-36-NIP2100	知识库升级服务时间36个月-含HS NIP网络智能防护系统软件
LIC-IPS-12-NIP2200	知识库升级服务时间12个月-含HS NIP网络智能防护系统软件
LIC-IPS-36-NIP2200	知识库升级服务时间36个月-含HS NIP网络智能防护系统软件
LIC-IPS-12-NIP5100	知识库升级服务时间12个月-含HS NIP网络智能防护系统软件
LIC-IPS-36-NIP5100	知识库升级服务时间36个月-含HS NIP网络智能防护系统软件
LIC-IPS-12-NIP5200	知识库升级服务时间12个月-含HS NIP网络智能防护系统软件
LIC-IPS-36-NIP5200	知识库升级服务时间36个月-含HS NIP网络智能防护系统软件

Content

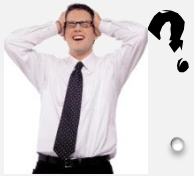
华为“渠道功夫”——怎样获取资料和帮助

武器一: 企业网网站

http://enterprise.huawei.com/cn/

- 渠道政策
  - 发布华为公司的渠道政策
- 渠道伙伴查询
  - 查找渠道伙伴
- 合作伙伴申请
  - 成为华为的渠道合作伙伴
- 合作伙伴专区
  - 随时随地获得华为的支持（资料和工具）

武器二: 资料问题反馈email

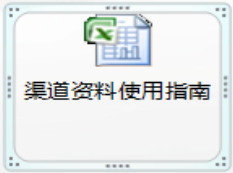


我有问题和建议怎么反馈？

enterprise_channel@huawei.com

武器三: 渠道资料用户使用指南

1. 华为企业网站渠道文档有哪些？
2. 怎样使用这些渠道资料
3. 怎样获得这些渠道资料
4. 我有疑问/意见，怎么反馈？



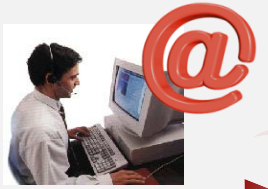
HUAWEI

渠道资料书架

- 品牌资源
  - 产品图片
  - 软文
  - 展会易拉宝
  - 渠道宣传期刊
  - 展厅参观指南
  - 样板点参观指南
- 案例
  - 案例集
- 主打胶片
  - Key message &宣传口径
  - 主打胶片（高层版）
  - 主打胶片（技术版）
- 彩页
  - 产品彩页（简版）
  - 产品彩页（详版）
  - 速查手册
  - 特性彩页
  - 板卡彩页
- 投标
  - 产品规格清单
  - 产品对比表
  - 订购指南
  - 产品生命周期公告
  - 产品概述
  - 产品硬件描述
  - 技术建议书
  - 入网证
  - 入网测试报告
  - 第三方报告
  - 用户报告
  - 其他测试报告
  - 获奖证书
- 销售指导
  - 销售一指禅
  - 销售策略指导
- 培训
  - 产品售前培训资料
  - 技术FAQ
- 白皮书
  - 技术白皮书

HUAWEI

怎样获得售前支撑



合作伙伴/客户

enterprise_channel@huawei.com

*Country		*Company Name	
*Product		Project Name	
*Contact Person		*Phone	
*Email Address			
*Question Description			

Call Center

华为渠道经理
华为总代接口人

合作伙伴/客户

400-822-9999

7*24小时开通 Email和电话售前支撑：

- 加入华为，成为合作伙伴
- 产品和解决方案咨询
- 售前相关问题
- …

HUAWEI

Open Discussion

Any Questions?

HUAWEI ENTERPRISE ICT SOLUTIONS A BETTER WAY