Huawei Enterprise A Better Way

华为Secoway USG2000&5000系列统一安全网关售前培训

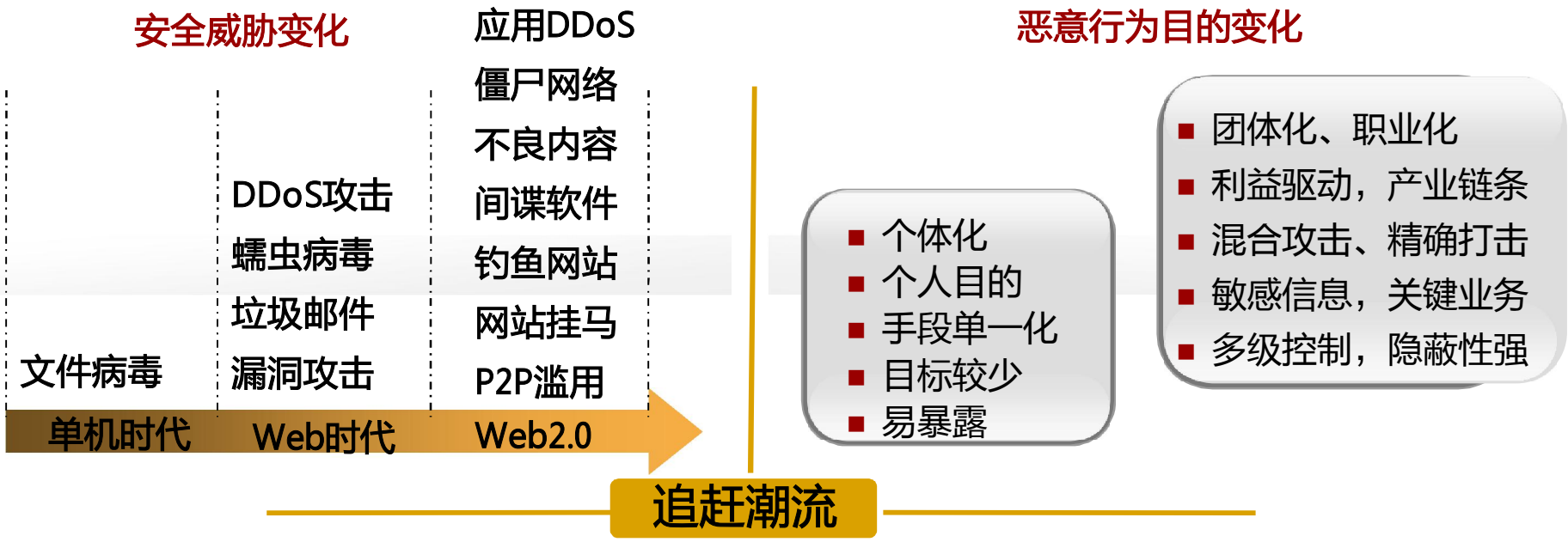
enterprise.huawei.com

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

目录

安全风险发展与变化

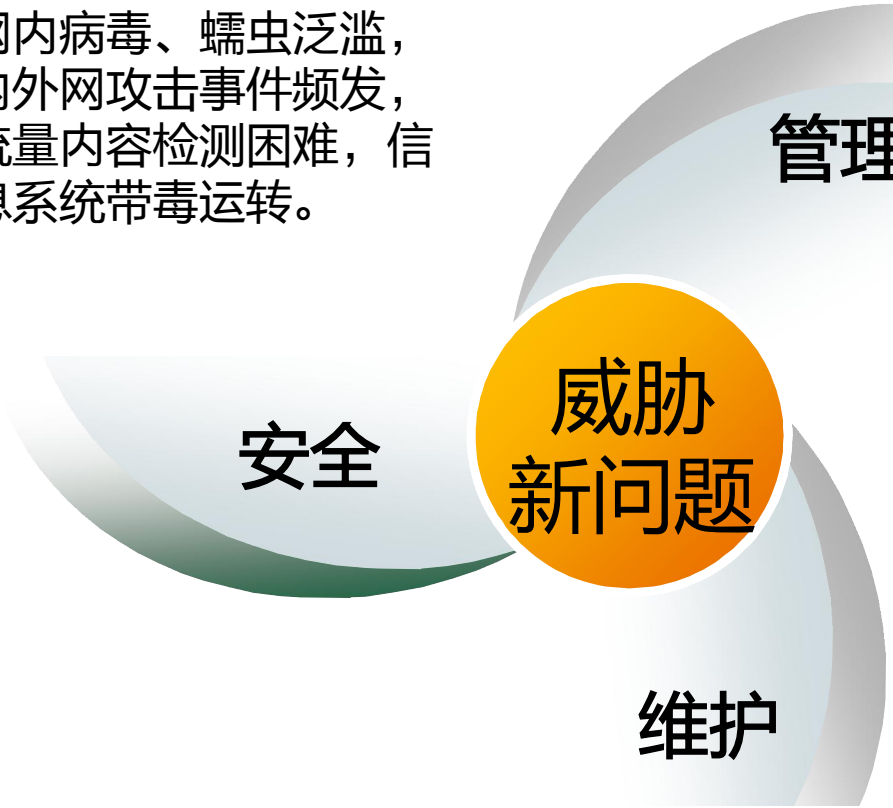


各类安全产品各自为战

边界防护	内网安全	运行维护
防火墙、IDS、IPS IPSec\SSL VPN WAF、SWG 垃圾邮件过滤 流量控制、应用加速 ……	CA系统、NAC 终端安全系统 文档安全系统 安全审计系统 漏洞扫描系统 ……	网络设备管理系统 安全设备管理系统 日志管理系统 操作系统维护工具 ……

传统安全威胁新问题

网内病毒、蠕虫泛滥，
内外网攻击事件频发，
流量内容检测困难，信息系统带毒运转。



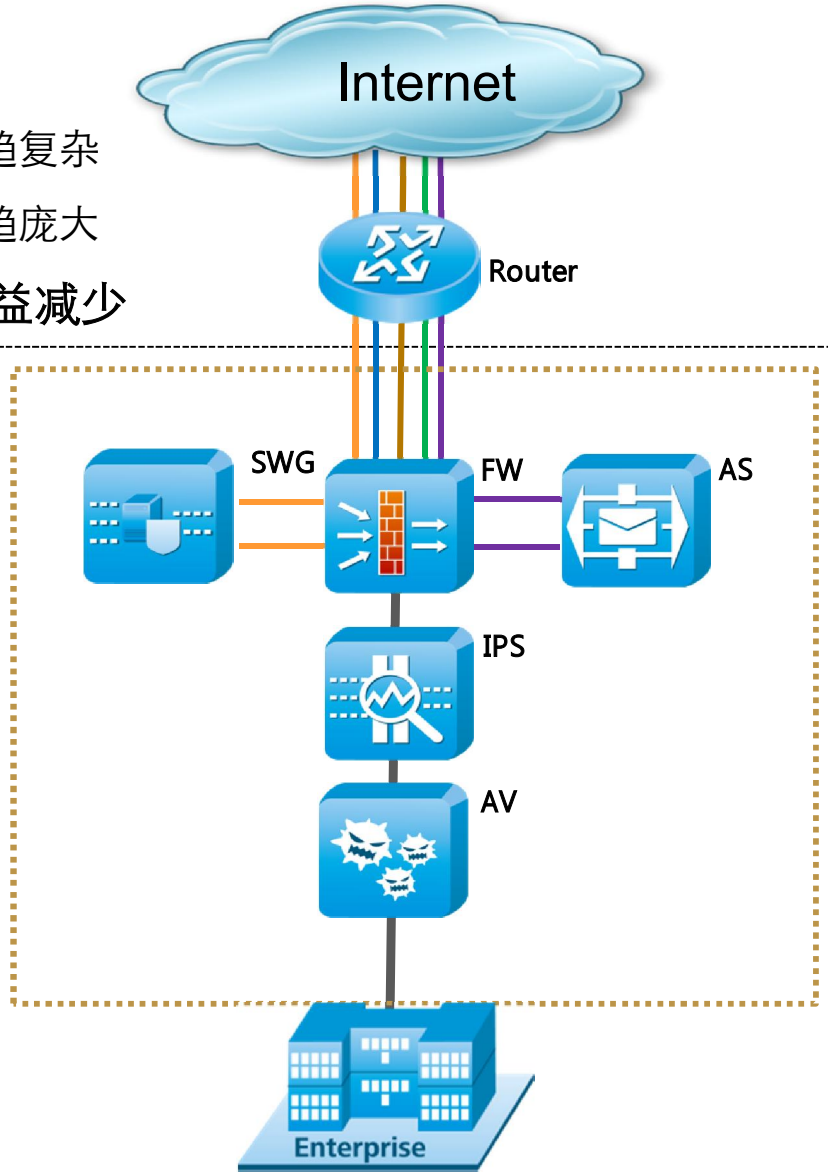
缺乏安全意识，随意浏览下载，极易中招；
滥用网络，关键业务无法保障，效率低下；
应用控制薄弱，难以准确管理网络应用；
用户难以识别，无法精确管理用户行为。

设备繁多，
技术更新快，
多套管理系统各自为政，
维护管理人员缺乏。

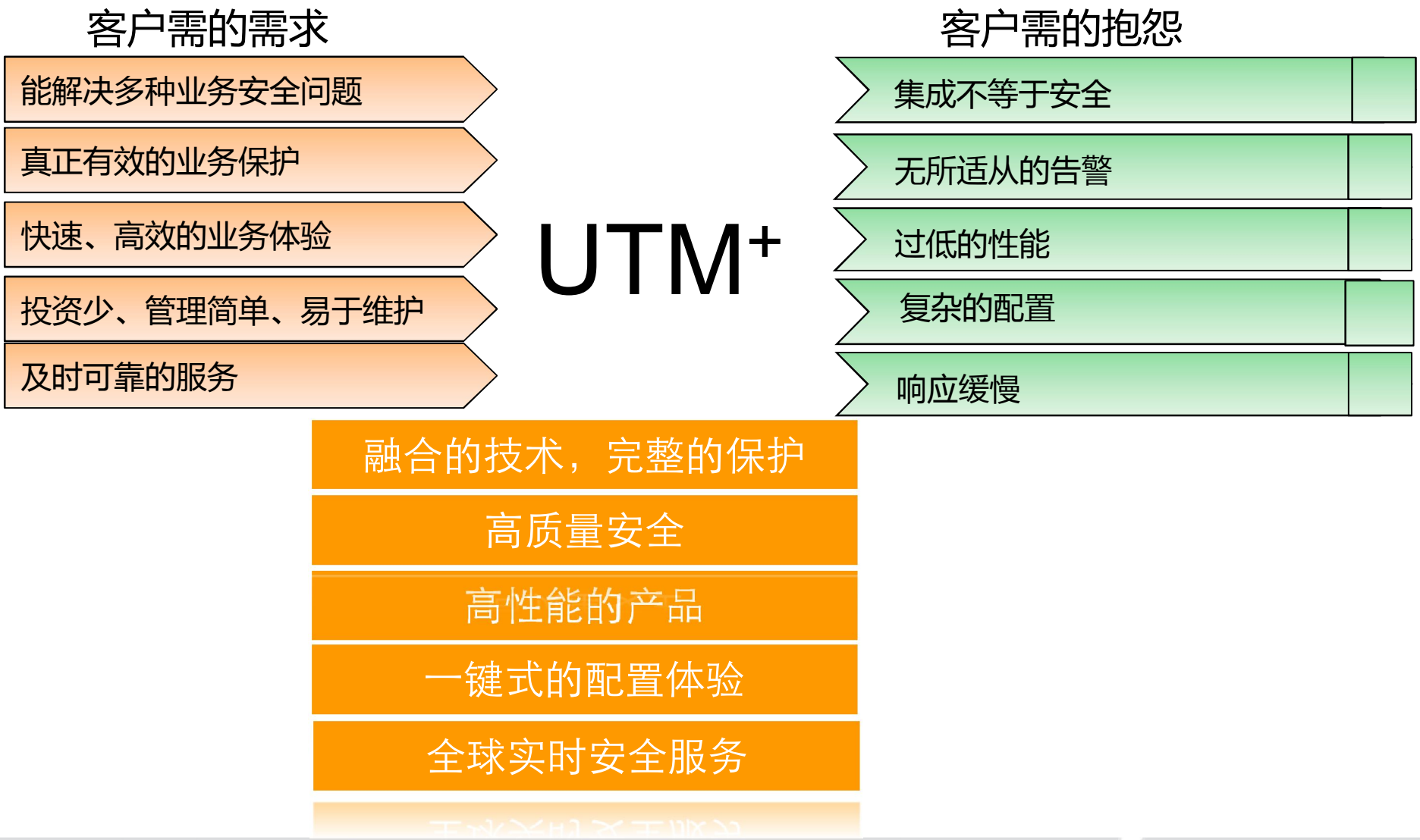
传统网络安全方案的问题

- 安全方案日趋复杂
- 运维成本日趋庞大

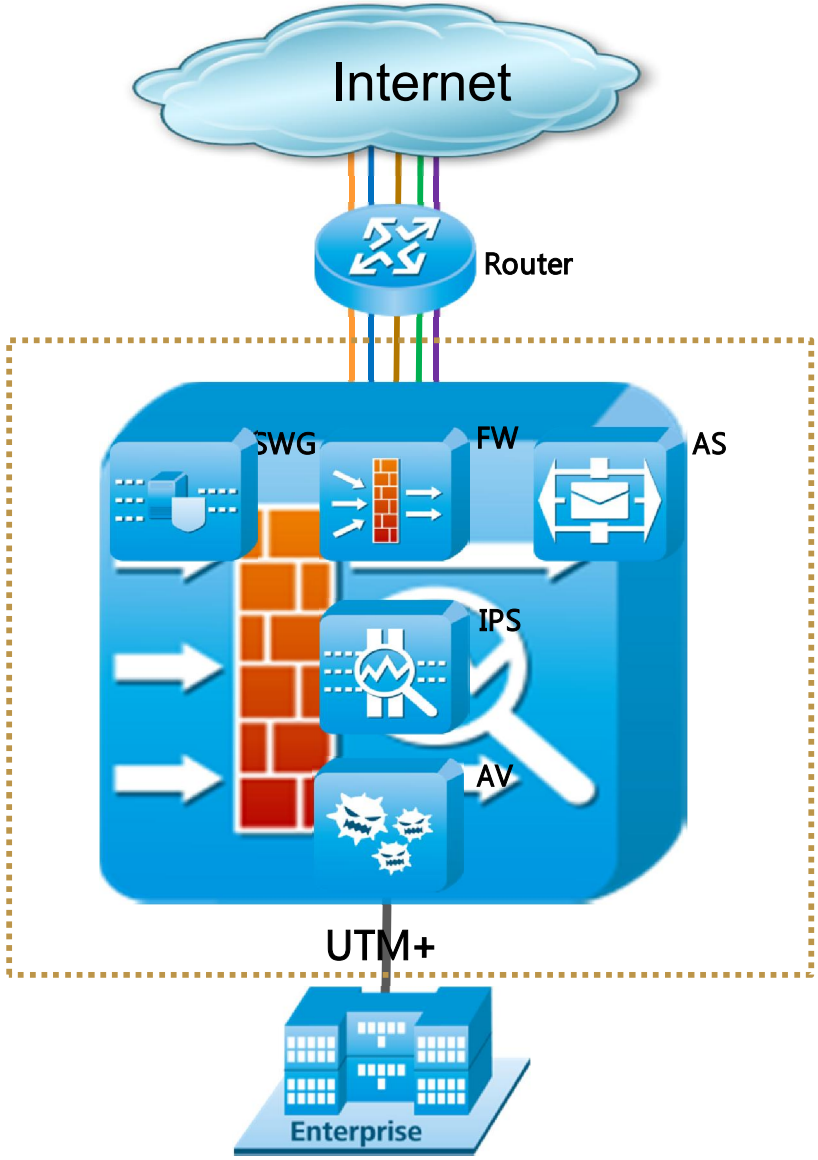
投入增加，收益减少



客户的期望


客户需的需求
能解决多种业务安全问题
真正有效的业务保护
快速、高效的业务体验
投资少、管理简单、易于维护
及时可靠的服务
UTM+
客户需的抱怨
集成不等于安全
无所适从的告警
过低的性能
复杂的配置
响应缓慢
融合的技术，完整的保护
高质量安全
高性能的产品
一键式的配置体验
全球实时安全服务

华为UTM+解决方案



华为UTM+解决方案：

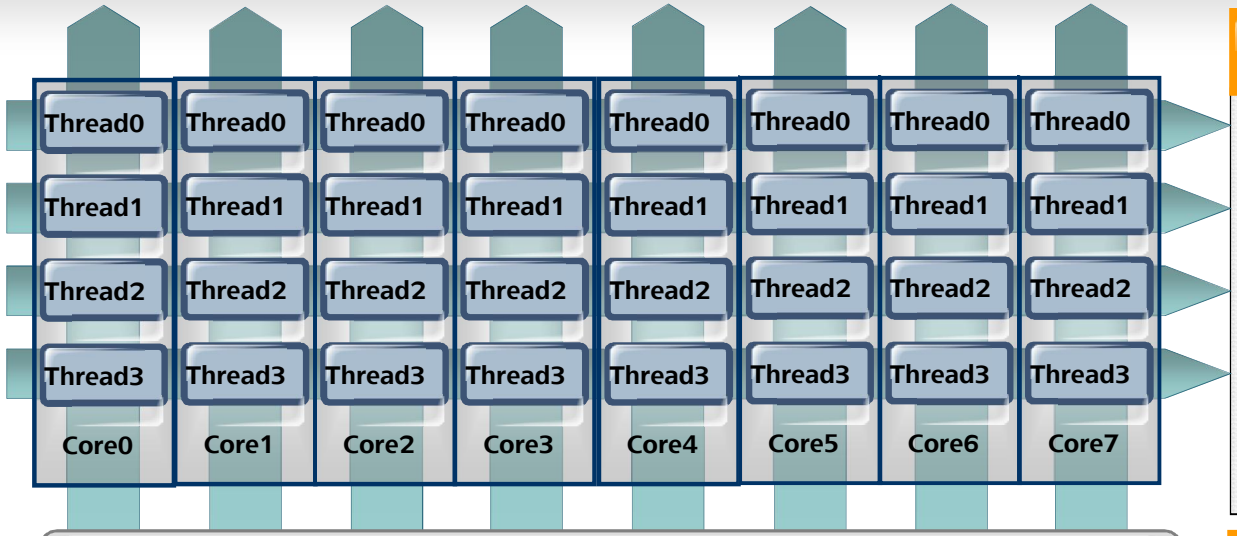
- Firewall
- UTM
- 内容过滤
- 流量控制
- 上网行为管理

华为UTM+特点：

- 多种业务集成
- 简单有效的统一管理
- 更低的TCO
- 更好的支持和响应

架构-高性能多核硬件

领先架构 | 丰富功能



最大支持8核32个虚CPU并行处理，配合加速芯片实现性能业界领先。

领先的架构平台

软硬件有机结合

先进多核硬件架构，多线程并行处理与实时多任务安全操作系统VSP完美融合。

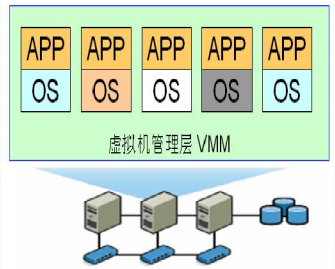
流程优化

对安全处理流程进行优化，特别是针对首包的处理，使得USG具备业界第一的每秒新建数；

将数据解封装和深度检测进行分离，实现多种深度检测并行处理，大幅提升系统在深度检测状态下的性能。

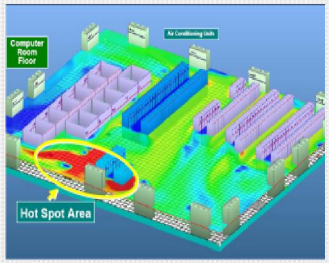
多核的优势

软件灵活性高

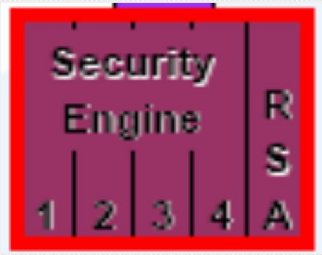


处理性能高

单位功耗低



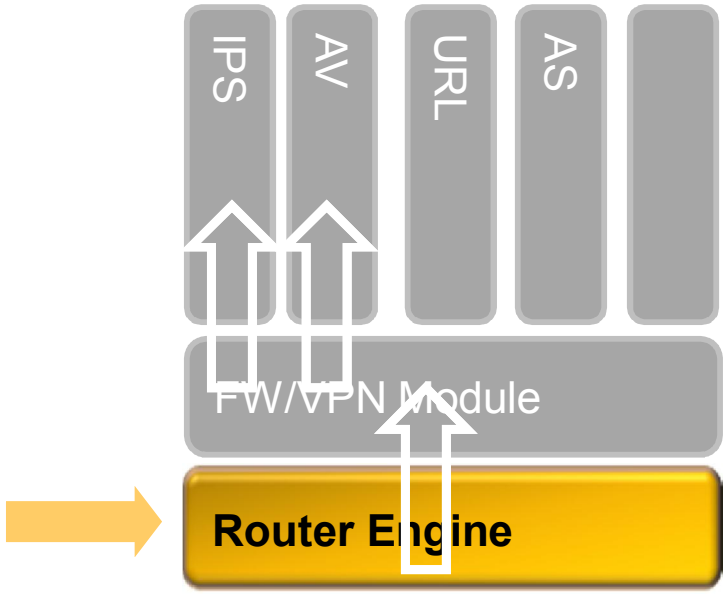
硬件加速引擎



架构-高效软件

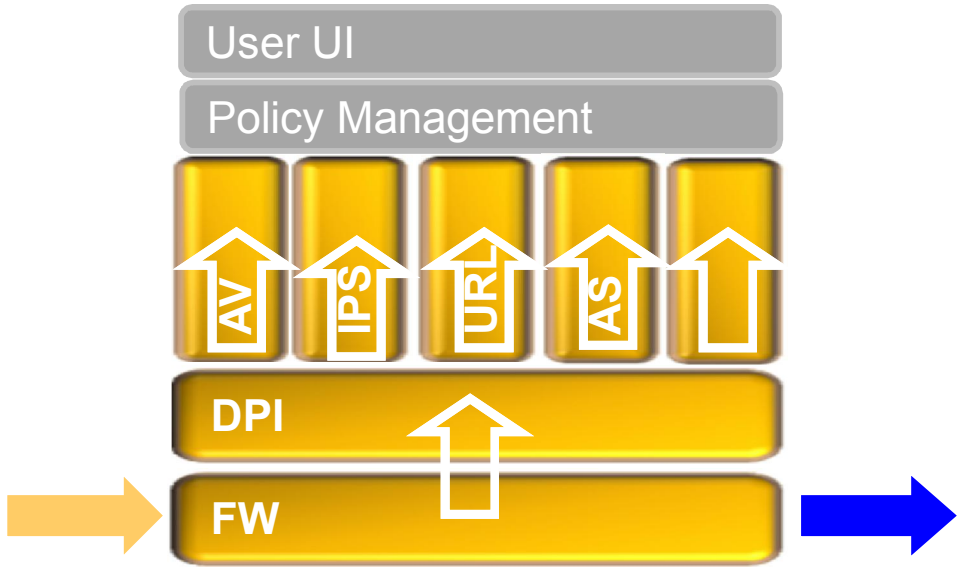
领先架构 | 丰富功能

传统UTM的内核-插装式



- 内核只完成传统的路由转发，安全模块插在路由引擎之上
- 数据流需通过路由引擎的干涉才能被动进入安全模块
- 架构安全性低，数据处理效率差

UTM+安全内核-全融合



- 安全能力融合入系统内核，主动完成安全检测
- 数据流在整个转发过程，通过安全内核
- 各模块并行工作，效率高，安全性高

架构-基于用户的安全策略

领先架构 | 丰富功能

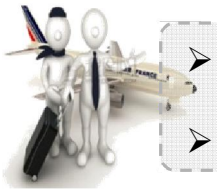
用户认证	安全策略	用户管理
➢ 本地/第三方认证 ➢ 事前/会话认证 ➢ Web/AD/Radius/LADP多认证方式	➢ 基于用户的策略 ➢ 基于用户的审计	➢ 本地/第三方用户管理 ➢ 组织架构管理&同步 ➢ 用户状态管理

基于用户的架构

- IP缺乏组织架构含义，应对困难
- 复杂策略难以实施

易用性

- 管理层次自然对应企业组织架构
- 法规制度无缝融合管理策略



- 策略绑定IP，不能应对网络变化
- 策略固化，无法支撑人员流动办公

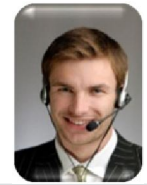
灵活性

- 安全策略与网络结构解耦
- 安全策略灵活支持移动办公

- IP等策略对象缺乏明确含义
- 多人共用一个终端无法区分策略

精确性

- 策略对象可以精确到具体的用户
- 可针对每一个终端用户制定策略



UTM+功能-基于漏洞的IPS引擎

领先架构 | 丰富功能

Identify → Parse → Scan

基于应用的识别

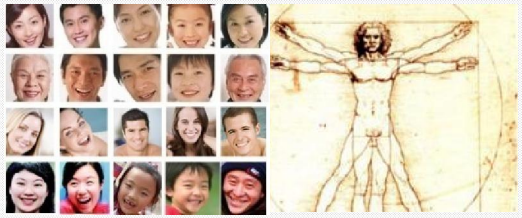
可识别超过240种协议

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

Symantec领先的IPS引擎

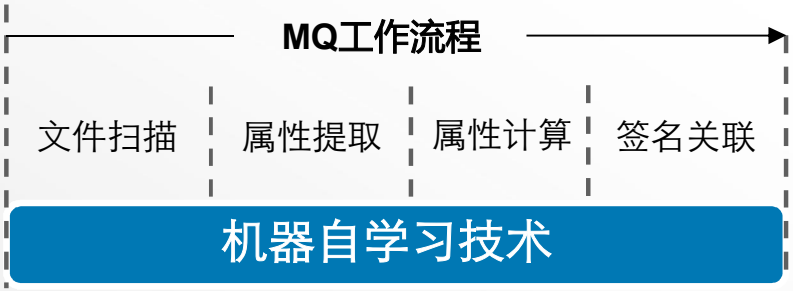
- 基于漏洞的签名，有效防止攻击变种、所有签名都可开启，并具有极低误报率
- 独特的识别能力，无需低效率的盲扫
- 新增漏洞签名到2000+种

UTM+功能-全球领先的AV引擎

领先架构 | 丰富功能

全球领先的反病毒引擎

静态启发式引擎



- 文件属性指文件的各类性状如：
  内嵌资源、段结构、数字签名等
  目前定义的文件属性已经超过125种

赛门铁克反病毒引擎主要优点

技术领先

文件级引擎，保证病毒检测的完整性；**增加FTP协议扫描。**
仿真检测技术，让病毒暴露其不良活动企图或者现出原形。
海量病毒检测能力，**可检测700多万种病毒。**

高检测率

病毒测试检出率高达**99%**
自动化学习引擎，**超125种特征扫描能力**，快速检测病毒变种。

快速响应

刀片式引擎，可以特征库一样不断升级
新的脚本引擎可以快速发布到工作中的反病毒引擎上

UTM+功能-全面的流量控制

领先架构 | 丰富功能

智能流量控制：

- 应用可控制
- 用户可识别
- 内容可检测
- 时间可分段
- 管理可视化

UTM+功能-智能上网行为管理

领先架构 | 丰富功能

准 准确率：96%

支持语言：10种 广

恶意URL库： 42K
钓鱼URL库： 13K
本地热点库： 100K
URL特征库： 65M
全

URL过滤

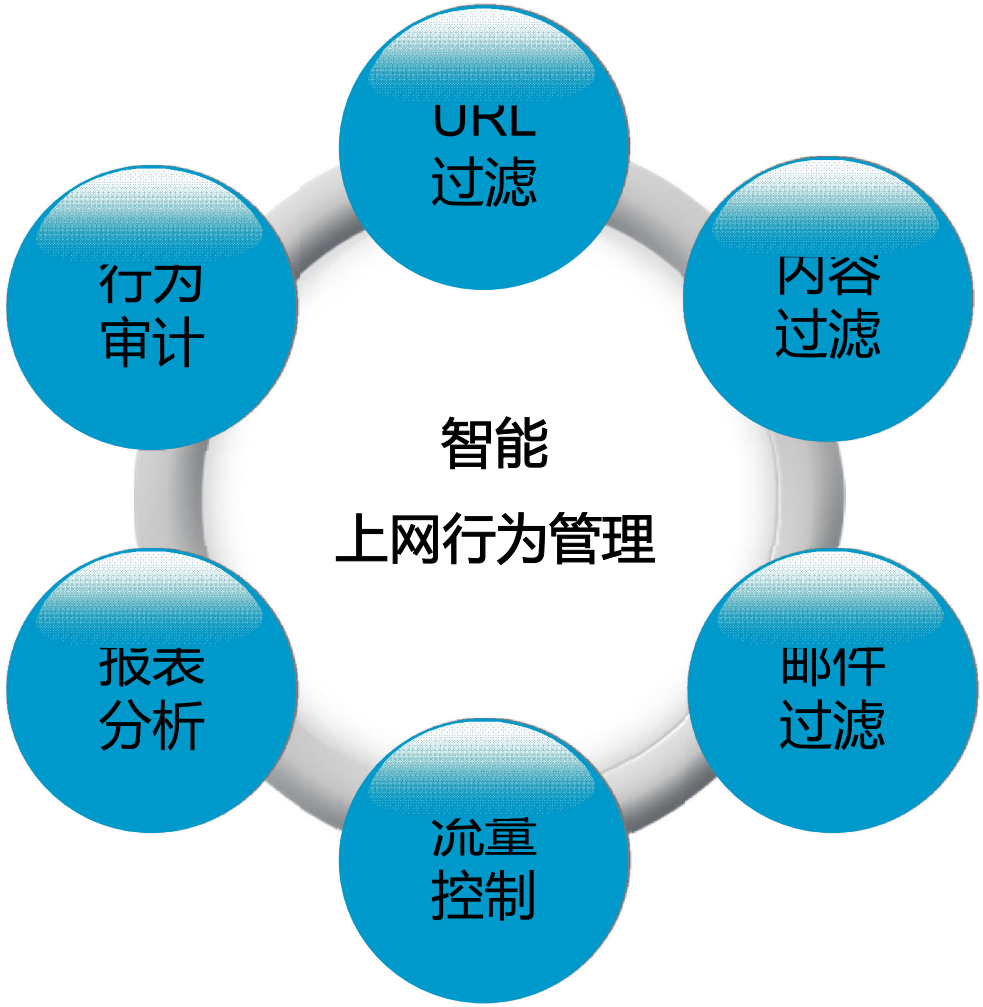
精细预分类：130种
支持用户自定义分类
细

内容过滤

- Web内容过滤
- 搜索关键字过滤
- FTP过滤

邮件过滤

- RBL名单过滤
- 收发件人、标题正文、附件过滤
- 附件内容过滤



UTM+功能- UTM虚拟化

领先架构 | 丰富功能

应用场景

- 数据中心安全服务，云计算安全服务，多用户安全业务隔离

主要功能

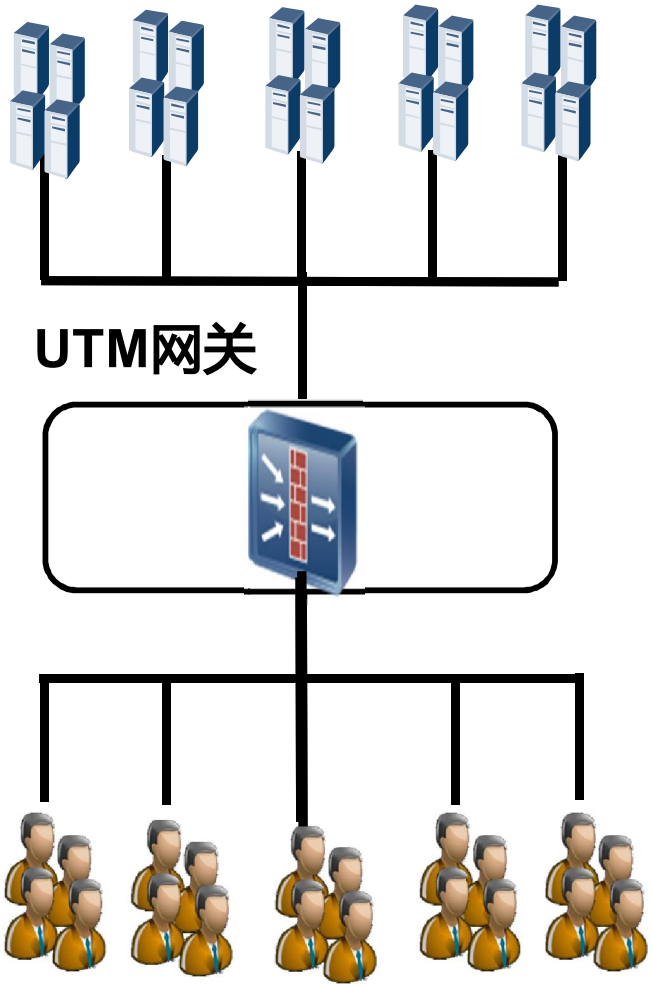
- FW、NAT、VPN、IPS、AV、URL、DPI、AS、Content Filter

重要指标

- 各虚拟UTM可弹性分配资源
  最大支持100个虚拟UTM

管理与维护

- 可独立配置各个虚拟UTM，
  虚拟UTM可拥有独立的管理系统



UTM+功能-丰富的路由特性

领先架构 | 丰富功能

先进的智能选路


基于用户的选路

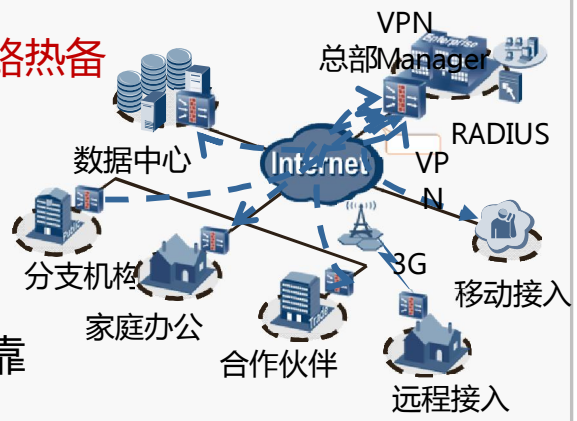

基于应用的选路


多链路权重选路

…

全面的VPN能力

- IPSec双机/双链路热备
- GRE/L2TP
- SSL/MPLS VPN
- 安全、灵活、可靠

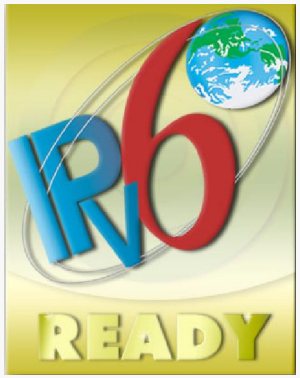


IPv6过渡技术

- 大容量的NAT能力
- 全面的IPv6过渡技术
- 丰富的IPv6升级路线
- 节约用户投资成本

IPv6丰富特性

- 丰富的IPv6路由协议
- 完备的IPv6链路层协议
- 系列支持IPv6 Ready金牌认证
- 全面的IPv6支持能力

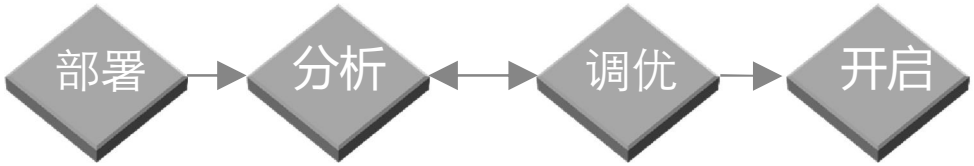


UTM+功能-一键配置

领先架构 | 丰富功能

- 传统UTM配置复杂，人为因素多，费时费力

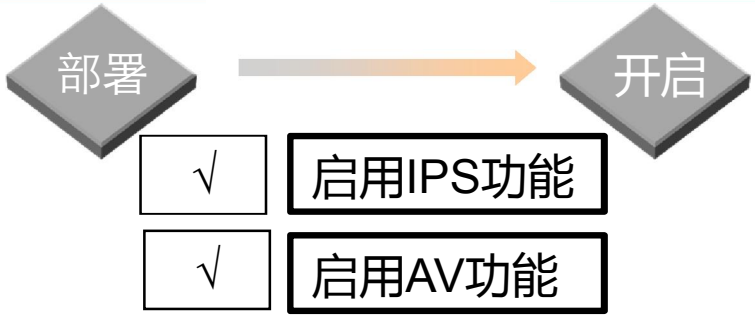
Step1 Step2 Step3 Step4



- 网络设计
- 部署调测
- 日志分析
- 数据挖掘
- 参数调整
- 策略关联
- 防护模式
- 策略应用

- UTM+无需复杂管理，一键配置

一键配置



一体化策略

- 一体化管理，一目了然
- 简化配置，提高效率
- 标配VSM和eLog，缺省管理3个网元

UTM+功能-直观易用的管理系统

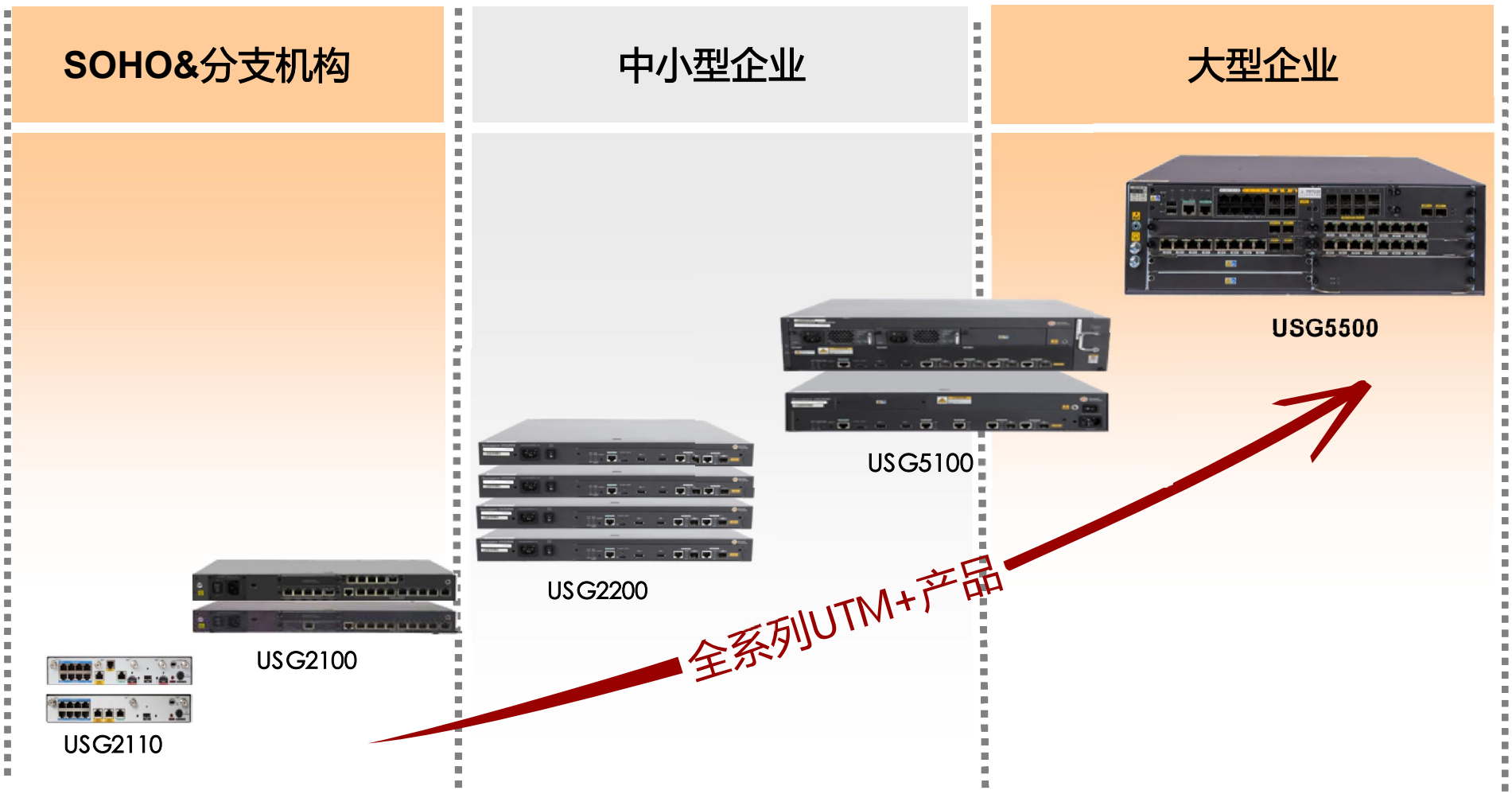
领先架构 | 丰富功能

用户关键字命中排行

表格数据按命中次数降序排列

序号	用户	主机IP	主要关键字	命中数(次)	主要应用	动作
1	张三	172.18.11.1	奖金(30次)	50	论坛发帖(10次)	被拦截(30次)、被记录(20次)
2	李四	172.18.11.2	报价(20次	40	邮件(40次)	被拦截(10次)、被记录(30次)
3	王五	172.18.11.3	策略(30次)	30	邮件(30次)	被拦截(20次)、被记录(10次)
4	赵六	172.18.11.4	绩效(20次)	20	邮件(20次)	被拦截(10次)、被记录(10次)
5	刘七	172.18.11.5	工资(10次)	10	论坛发帖(10次)	被拦截(5次)、被记录(5次)

华为UTM+产品全景图


SOHO&分支机构
中小型企业
大型企业
USG5500
USG5100
USG2200
USG2100
USG2110
全系列UTM+产品
高性价比
灵活接口
丰富接口、灵活插卡
高性能，高可靠

USG5500系列产品

型号规格

型号	高度	电源	固定接口	扩展槽位
USG5530S	1U	双交	4GE+4GE Combo	2*FIC
USG5530	3U	双交	4GE+4GE Combo	1*DMIC+4*FIC+2*DFIC
USG5550	3U	双交/直	4GE+4GE Combo	1*DMIC+4*FIC+1*DFIC
USG5560	3U	双交/直	4GE+4GE Combo+8GE SFP	1*DMIC+4*FIC+1*DFIC

USG5500

大型企业用户

- 定位： 高端千兆和低端万兆UTM
- 功能： 支持USG V3R1版本特性；

  最高32G FW性能，基于用户的安全策略，增强UTM功能，基于内容的安全过滤；

  强大的上网行为管理，支持IPv6，标配双电源(AC/DC可选)；

  USG5550和USG5560标配FPGA加速卡；
- 接口： 全系列新增USB-3G卡，高密度和低密度GE卡，10GE接口卡，光电Bypass卡，USG5500最大扩展接口可达56GE+14*10G

USG5100系列

型号规格

型号	高度	电源	最大接口
USG5120	2U	交/直	64GE+20FE
USG5150	3U	双交/直	84GE+28FE
USG5160	3U	双交/直	84GE+28FE

USG5100

中型企业用户（600-1000U）

- 定位： 高性能千兆UTM
- 功能： 支持USG V3R1版本特性；
  最高6G FW性能，基于用户的安全策略，增强UTM功能，基于内容的安全过滤；
  强大的上网行为管理，支持IPv6，提供直流机型，5150/5160提供双电源；
- 接口： 新增电口Bypass卡，高密度/低密度GE卡，多业务开放平台（X86卡），
  丰富的广域网接口卡FE / GE /Serial /E1 / ADSL2+/ G.SHDSL /3G/WIFI。

USG2200系列

型号规格

型号	高度	电源	最大接口
USG2210	1U	交流	22GE+20FE
USG2220	1U	交流	22GE+20FE
USG2230	1U	交流	22GE+20FE
USG2250	1U	交/直流	22GE+20FE
USG2250	1U	交/直流	22GE+20FE

USG2200

中小企业用户（100-600U）

- 定位：高性能百兆UTM
- 功能：支持USG V3R1版本特性；
  最高1G FW性能，基于用户的安全策略，增强UTM功能，基于内容的安全过滤；
  强大的上网行为管理，支持IPv6，提供直流机型；
- 接口：高密度/低密度GE卡，多业务开放平台（X86卡），
  丰富的广域网接口卡FE / GE /Serial /E1 / ADSL2+/ G.SHDSL /3G/WIFI。

USG2100系列

型号规格

型号	高度	电源	固定接口
USG2130/ USG2130W	1U	交流	1FE+8 FE
USG2160/ USG2160W	1U	交流	1FE+8 FE

USG2100

小企业用户 分支机构（30-100U）

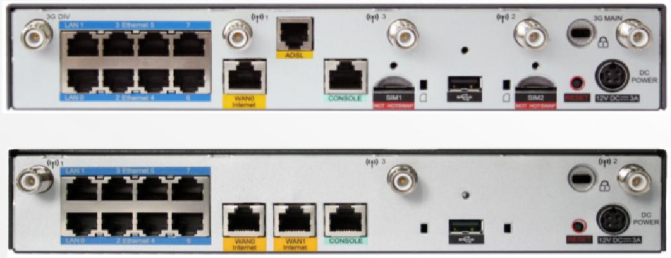
- 定位： 入门级百兆UTM
- 功能： 支持USG V3R1版本特性；
  最高200M FW性能，基于用户的安全策略，增强UTM功能，基于内容的安全过滤；
  强大的上网行为管理，支持IPv6 ，提供直流机型；
- 接口： 1FE+8 FE 固定，1 / 2 x 扩展插槽(2130/2160），
  丰富的广域网接口卡 Serial /E1 / ADSL2+ / FE / GE /3G / G.SHDSL，内置WIFI（-W机型）。

USG2110系列

型号规格

型号	固定接口
USG2110-F/ USG2110-F-W	2FE(WAN)+4FE(LAN)
USG2110-A-W	1ADSL+1FE(WAN)+8FE(LAN)
USG2110-A-GW-W	1ADSL+1FE(WAN)+8FE(LAN)+1*3G

USG2110



小企业用户 分支机构（2-30U）

- 定位：SOHO桌面UTM
- 功能：　支持USG V3R1版本特性；

  最高120M FW性能，基于用户的安全策略，增强UTM功能，基于内容的安全过滤；

  强大的上网行为管理，支持IPv6 ，提供直流机型；
- 接口：1FE+8 FE 固定；

  内置WIFI（-W机型）

UTM+丰富板卡系列

低速接口


MIC-1SA


MIC-1E1\CE1


FIC-2E1\CE1


FIC-4E1\CE1


MIC-2SA


MIC-1ADSL2+


MIC-1/2/4G.SHDHL


FIC-8E1\CE1

无线接口


MIC-Wi-Fi

高速接口


MIC-1FE


MIC-5FE


FIC-1GE


FIC-4GE


FIC-2F2C


FIC-8GE电


FIC-8GE光


FIC-2*10G


FIC-2*10G+8GE


DMIC-8FE+2GE


DMIC-2*10G


4GE电口Bypass


2路光口Bypass

DFIC板卡


DFIC-ESP


DFIC-16GE+4SFP


DFIC-18FE+2SFP

目录

中低端USG产品与友商的竞争关系

USG	Juniper SRX	CISCO ASA	Fortinet FG	天融信 NGFW	启明星辰 USG	H3C Secpath	网御星云	网域神州
USG5530S	SRX1400	5585-S20	310B/300C	TG5230	3610D		5434	G60
				TG470C	4000D		5834	
							5A34	
USG5530			620B/600C	TG470C	4600D		K7000	
				TG5330				
				TG5628				
USG5550	SRX3400	5585-S40	1000C	TG5728	8000E		8000	X100
				TG5622	5200		9201	
					10000E			
USG5560	SRX3600		1240B			F5000		X300

中低端USG产品与友商的竞争关系

USG	Juniper SRX	CISCO ASA	Fortinet FG	天融信 NGFW	启明星辰 USG	H3C Secpath	联想网御 power	网域神州	东软 Neteye
USG2130	SSG5/ SSG20 (160M)	5505	100A	TG-1403		F100-S	V-160		FW4010
USG2160			200A	TG-1503		F100-A			
USG2210	SSG140(350 M)/ SSG320(450)	5510	300A	TG-1508	300B	F100-E	V-214	SecGate 3600-F3	FW4016
				TG-1608			V-318		
USG2220	SSG350(5 50M)/SSG 520(650M)	5520	100C	TG-4324			V-224	SecGate 3600-F4	FW4032
			400A				V-418		
USG2230	SRX210/ SSG550(1G+)	5540	500A	TG-4424	600C		V-324	SecGate 3 600-F5	FW4120
USG2250			800	TG-4430	800C		V-514	SecGate 3 600-F6	
							V-424		
USG5120	SRX240	5550	800	TG-4628	800C	F1000-C	Power V-3816	SecGate3 600-G4	FW4032
USG5150				TG-5030		F1000-S	Power V-4414		
USG5160						F1000-A			

优势特性

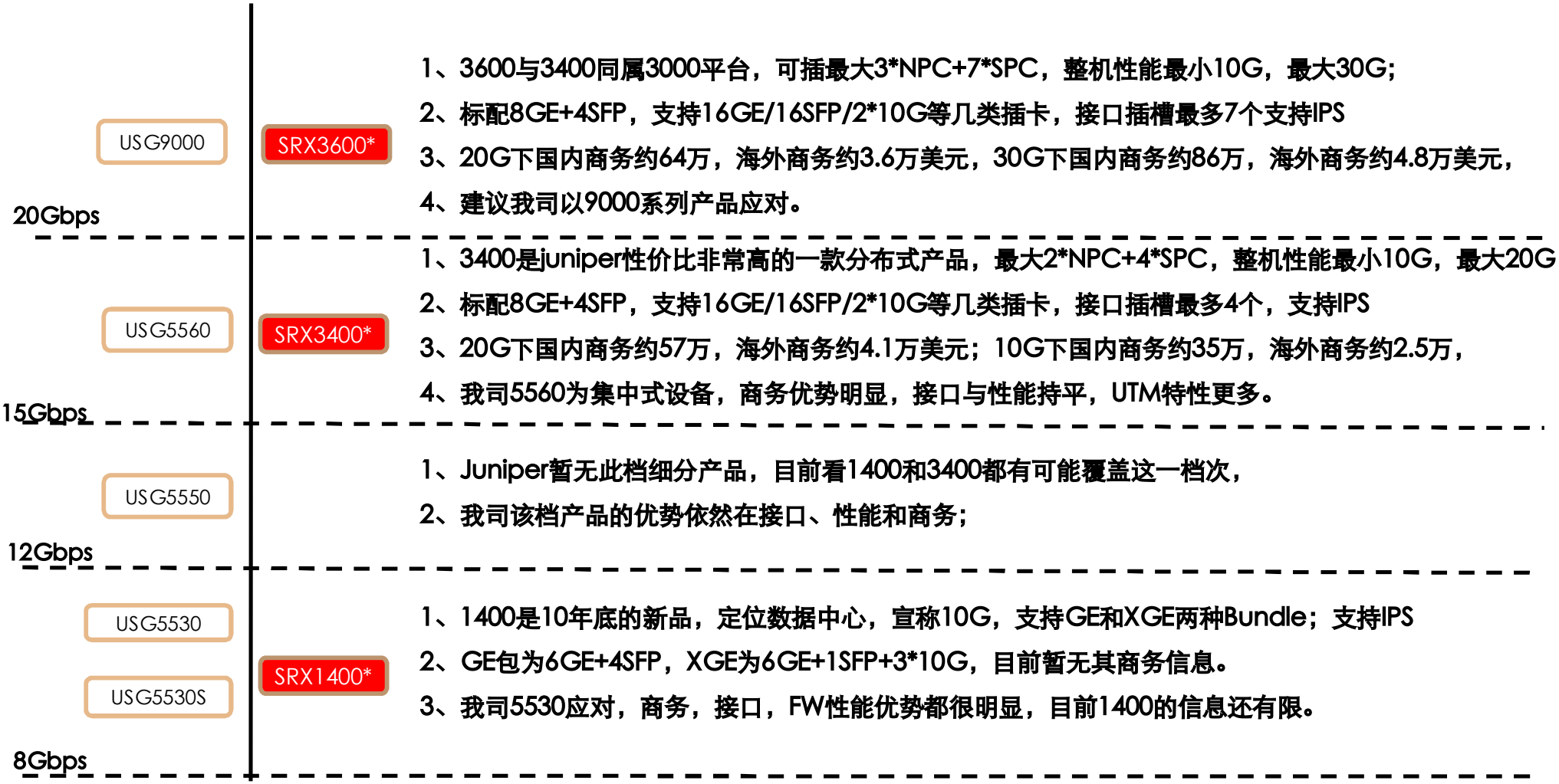
- 强劲、可靠的UTM
  - 赛门铁克先进的IPS、AV引擎，业界领先的检出率
  - 丰富的邮件过滤、URL过滤功能
  - UTM虚拟化，每个虚拟防火墙均可独立配置安全防护策略
- 全面的深度DPI
  - 1000+应用协议识别
- 海量安全策略或大数据量交换的数据中心
  - 多安全域之间的隔离
- 大容量NAT（大容量NAT会话、无限制NAT转换）
  - 校园网、大型园区网出口；广电网络城域网、互联网出口
- IPv6
  - 高等院校、大型科研机构、实验网、运营商。

How to beat Juniper-厂商维度

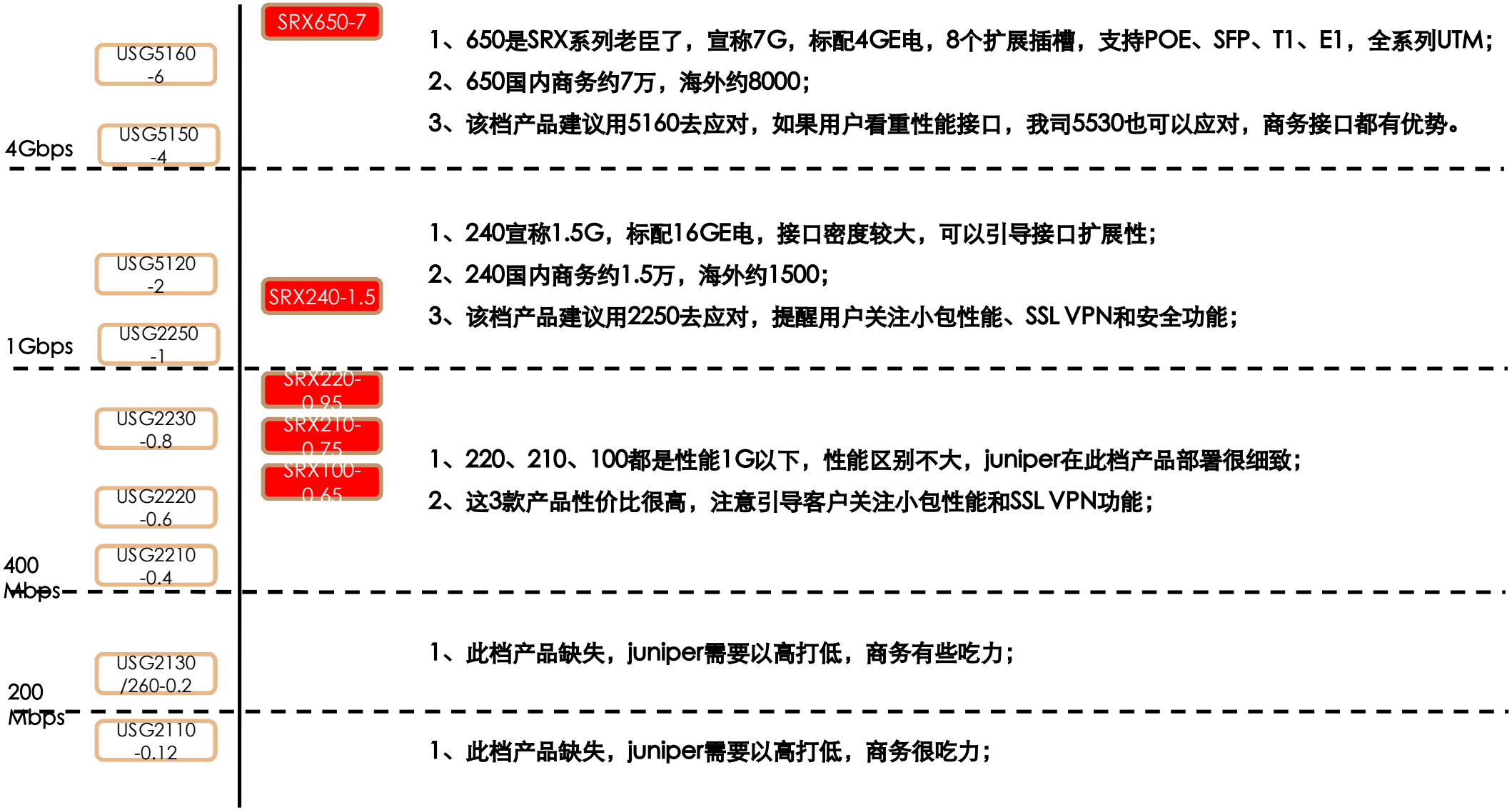
通用打击方式	基于行业的打击点					
	政府	金融	能源	教育	公共事业	企业
基于产品选择要素的打击点						
•**打击点-性能低**：Juniper SRX系列在FW小包/新建连接/VPN隧道数都较差。 •**打击点-功耗大**：Juniper SRX系列电源功耗都偏大（SRX650为650W）。 •**打击点-系列化差**：Juniper SRX系列的系列化较差，千兆只有2款产品。 •**打击点-用户松耦合**：Juniper SRX系列的安全策略都是基于IP地址的，跟用户关联不紧密，不支持基于用户的Qos、路由、FW策略等。 •**打击点-只有1400以上机型才支持基于app的管理控制**：SRX支持700+种app，HW支持1000+； •**打击点-不支持SSL VPN**：SRX全系列不支持SSLVPN功能，必须通过专业VPN设备才能部署； •**打击点-1400以上机型功能缺失**：不支持AV、AS、URL filtering； •**打击点-URL filtering地址少**：仅支持26million地址库，HW支持65million；	•**通用打击点。** •**特性打击点-合规性**：国外品牌，国内政府行业不能进入	•**通用打击点。** •**特性打击点-易用性**：差，英文的界面。 •**特性打击点-售后服务能力**：Juniper在中国的服务主要是依赖代理商完成的，相比厂商的直接服务，服务质量上不足。		•**通用打击点。** •**特性打击点-价格**：价格高。 •**特性打击点-易用性**：英文的界面，易用性差。 •**特性打击点-售后服务能力**：Juniper在中国的服务主要是依赖代理商完成的，相比厂商的直接服务，服务质量上不足。	

通用规避方式	基于行业的规避点				
	金融	能源	教育	公共事业	企业
基于产品选择要素的规避点					
•**规避点-二层链路、QoS、虚拟化、路由**：Juniper SRX继承了Netscreen和MX路由器的软件优势，在二层链路、QoS、虚拟化、路由等方面技术优势明显，要注意引导用户简单化的安全部署。 •**规避点-领先技术**：Juniper公司在数通方面的积累和Netscreen在安全方面的积累造就了Juniper是一个网络技术和安全技术领先的公司，要注意强调其安全产品线（SRX）为主流产品线，以太交换机（EX）和路由器才是Juniper的主要产品线。。	•**通用规避点。** •**特性规避点-数通特性强大**：数通功能强大，注意引导用户关注安全特性。		•**通用规避点。** •**特性规避点-已应用该品牌产品**：Juniper在企业网的交换路由应用案例较多，要注意引导客户将注意力放在安全产品上。		

How to beat Juniper-产品维度



How to beat Juniper-产品维度



How to Beat Cisco-厂商维度

通用打击方式	基于行业的打击点					
	政府	金融	能源	教育	公共事业	企业
基于产品选择要素/厂商选择要素的打击点						
•**打击点-性能低**：Cisco ASA系列在FW吞吐量/VPN性能/新建/并发等各方面表现都较差。 •**打击点-UTM特性不全面**：UTM功能仅支持IPS，而且需要通过扩展板卡支持。 •**打击点-扩展性差**：插槽数较少，仅有两个，后续扩展能力有限，且扩展板卡固定为防火墙板和IPS板； •**打击点-价格高**：Cisco ASA的价格很高，低端千兆产品都在5万以上。	•**通用打击点。** •**特性打击点-合规性**：国外品牌，国内政府行业不能进入。	•**通用打击点。**	•**通用打击点。** •**特性打击点-易用性**：差，英文的界面。 •**特性打击点-售后服务能力**：Cisco在中国的服务和Juniper一样，服务质量不足，是客户抱怨的重点。	•**通用打击点。** •**特性打击点-价格**：价格高。 •**特性打击点-易用性**：英文的界面，易用性差。 •**特性打击点-售后服务能力**：Cisco在中国的服务和Juniper一样，服务质量不足，是客户抱怨的重点。		

通用规避方式	基于行业的规避点				
	公共事业	能源	教育	金融	企业
基于产品选择要素/厂商选择要素的规避点					
•**规避点-稳定性高**：Cisco的产品以稳定性著称，注意引导用户关注性能值。 •**规避点-数通能力强**：Cisco的ASA继承了IOS的数通特性，注意引导用户关注安全特性。 •**规避点-IPS性能高**；Cisco通过板卡支持IPS功能，能够提高较高的性能，注意引导用户关注检出率。 •**规避点-国外领先品牌**：Cisco公司在交换路由方面是业界一流品牌，品牌效应好。	•**通用规避点**	•**通用规避点** •**特性规避点-已应用该品牌产品**：Cisco在企业网的交换路由应用案例较多，要注意引导客户将注意力放在安全产品上。			

How to Beat Cisco-产品维度

20Gbps

ASA5585-60*

1、5585-60宣称35G，并发200万，FW模式下6GE+4*10G，IPS模式下接口翻倍
2、裸机商务国内约50万，海外约11.3万美元，我司可用9300应对。
3、如果以5560应对，则商务，接口，UTM等方面均有明显优势

USG5560

ASA5585-40*

1、5585-40宣称20G，并发200万，FW模式下6GE+4*10G，IPS模式下接口翻倍
2、裸机商务国内约30.8万，海外约7万美元
3、该档可用5560应对，我司商务优势非常明显，可重点打击其UTM特性和接口扩展性。

15Gbps

USG5550

1、思科未细分该档产品，极可能以5585-20或5580-20覆盖，我司5550商务优势依然明显。

12Gbps

USG5530

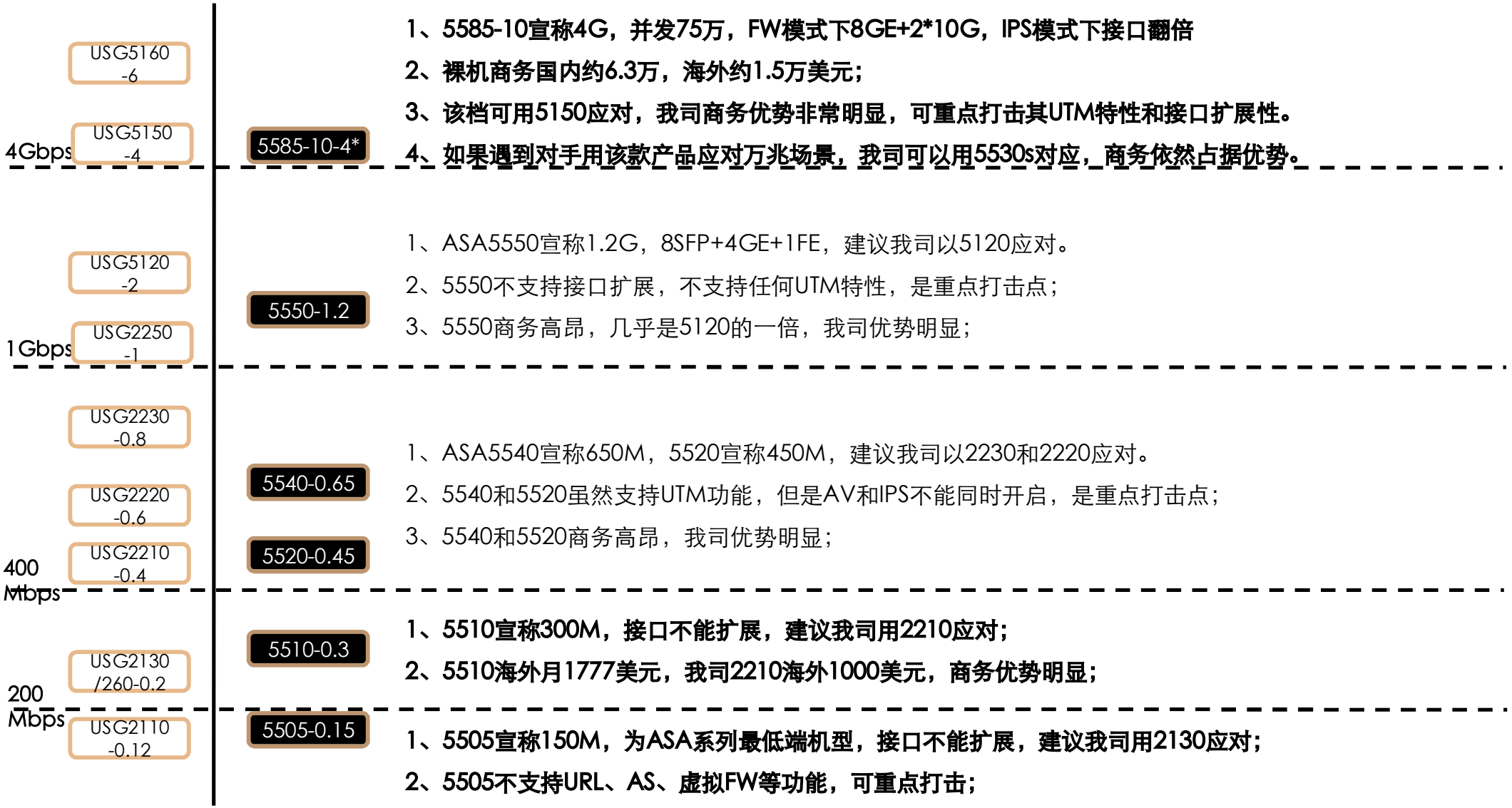
USG5530S

ASA5585-20*

1、5585-20宣称10G，并发100万，FW模式下8GE+2*10G，IPS模式下接口翻倍
2、裸机商务国内约13万，海外约3万美元；
3、该档可用5530（S）应对，我司商务优势非常明显，可重点打击其UTM特性和接口扩展性。

8Gbps

How to Beat Cisco-产品维度

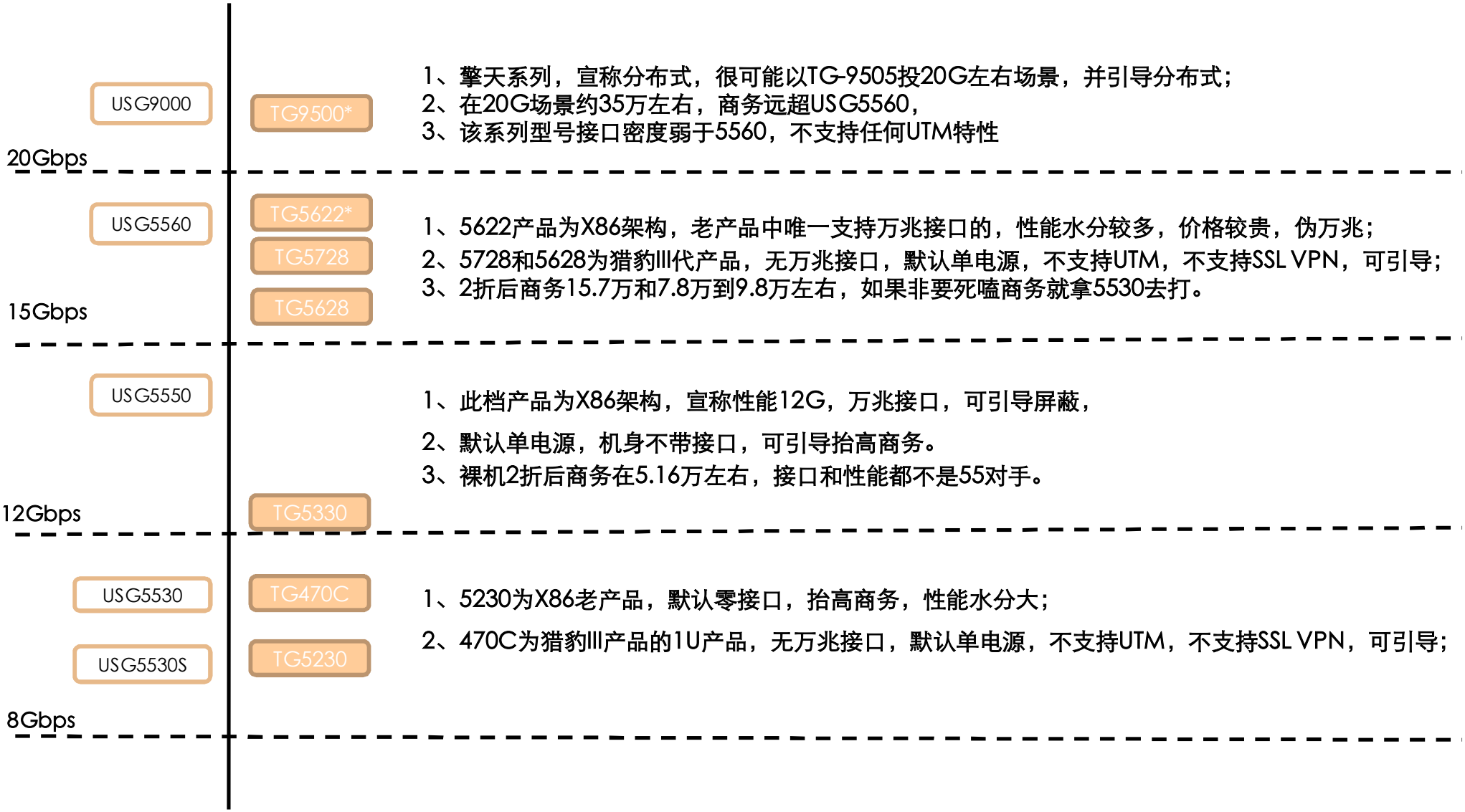


How to Beat Topsec-厂商维度

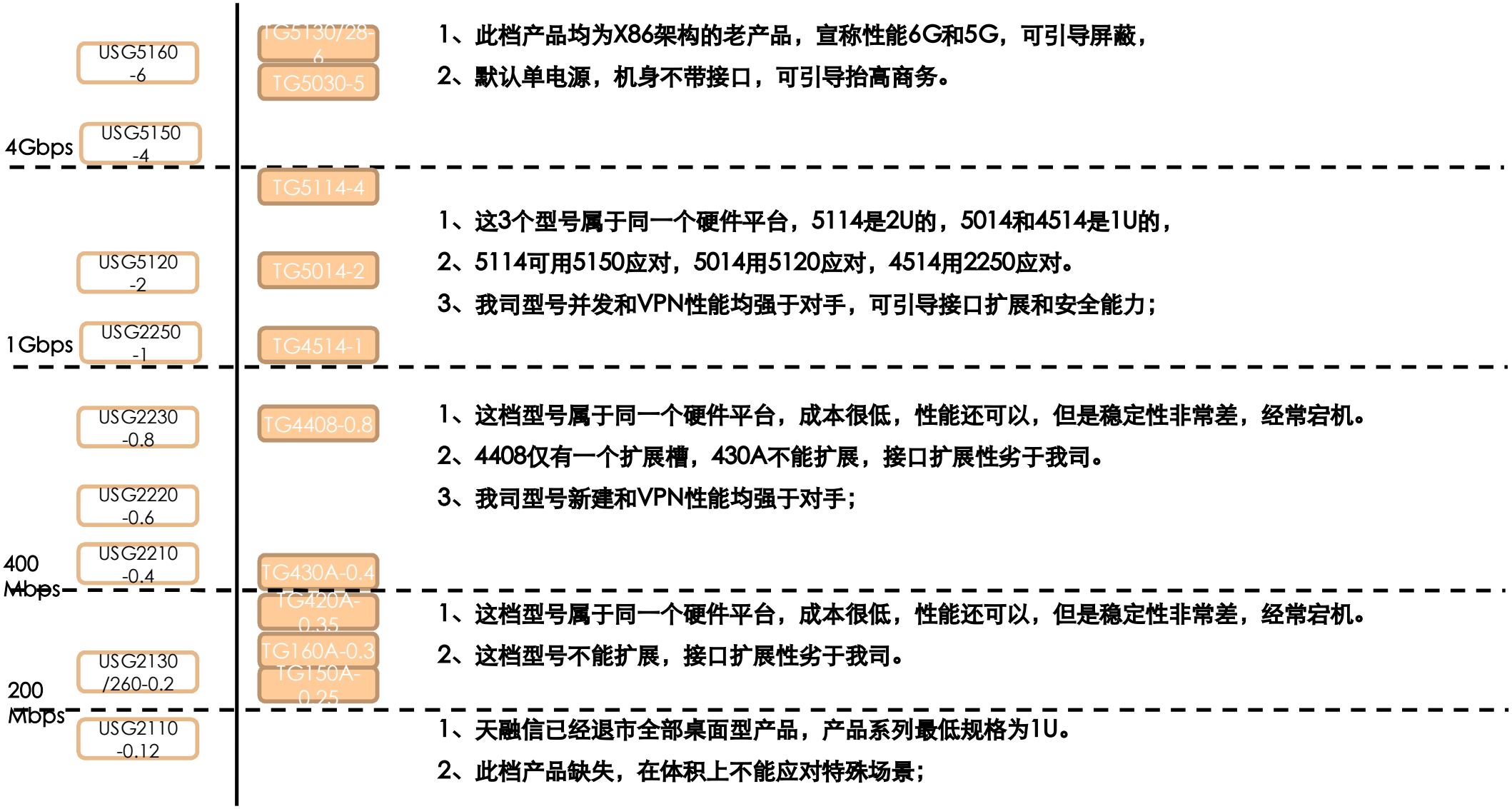
通用打击方式	基于行业的打击点					
	政府	公共事业	金融	能源	教育	企业
基于产品选择要素/厂商选择要素的打击点						
•**打击点-性能差**：天融信x86产品真实性能很低，但宣称性能水分很大，大包吞吐量、小包吞吐量、并发连接数都有较大的夸大，可以引导实测。 •**打击点-无领先技术**：天融信始终以防火墙份额居首，在UTM产品、专业安全网关领域的技术积累较差。 •**打击点-代码开源的GPL风险**：产品基本都是采用开源代码，存在GPL约束，代码一旦开源后，对客户存在厂商信誉度降低和产品漏洞被曝光的风险。 •**打击点-猎豹系列功能缺失**：不支持SSL、IPS、AV、URL和AS。 •**打击点-安全能力差**：天融信的URL过滤仅有500万，AV病毒特征库只有300万，DPI识别能力只支持150+种，比我司产品差很远；	•**通用打击点。** •**特性打击点-外资背景**：天融信网络安全公司属于外资，但其注册了天融信科技，进行规避。		•**通用打击点。** •**特性打击点-可靠性**：天融信的千兆系列基本都是采用x86架构，稳定性和可靠性比起专用的多核架构差别很大。 •**特性打击点-数通特性的客户信赖度差**：天融信是做安全起家的，客户对数通特性的信赖度差。	•**通用打击点**	

通用规避方式	基于行业的规避点					
	政府	公共事业	金融	能源	教育	企业
基于产品选择要素/厂商选择要素的规避点						
•**规避点-不对等竞争**：天融信经常以低打高，所以经常出低价，要引导用户进行测试，去确保竞争对等，以抬高友商商务。	•**通用规避点。** •**特性规避点-售后服务能力**：天融信常年跟踪政府项目，并形成了针对性极强的售后服务模式及队伍，规避时要强调我司售后能力强。 •**特性规避点-合规性**：天融信在等保、分保方面投入的时间和精力都较大，贴近对政府项目的要求。 •**特性规避点-已应用该品牌产品**：天融信在政府行业的应用案例较多，要注意引导用户关注当前项目。		•**通用规避点。**	•**通用规避点。** •**特性规避点-内容过滤**：天融信支持基于关键字的过滤，要引导用户认识到基于关键字的内容过滤的实用价值不高，应该去使用基于URL库过滤的价值更高。	

How to Beat Topsec-产品维度



How to Beat Topsec-产品维度



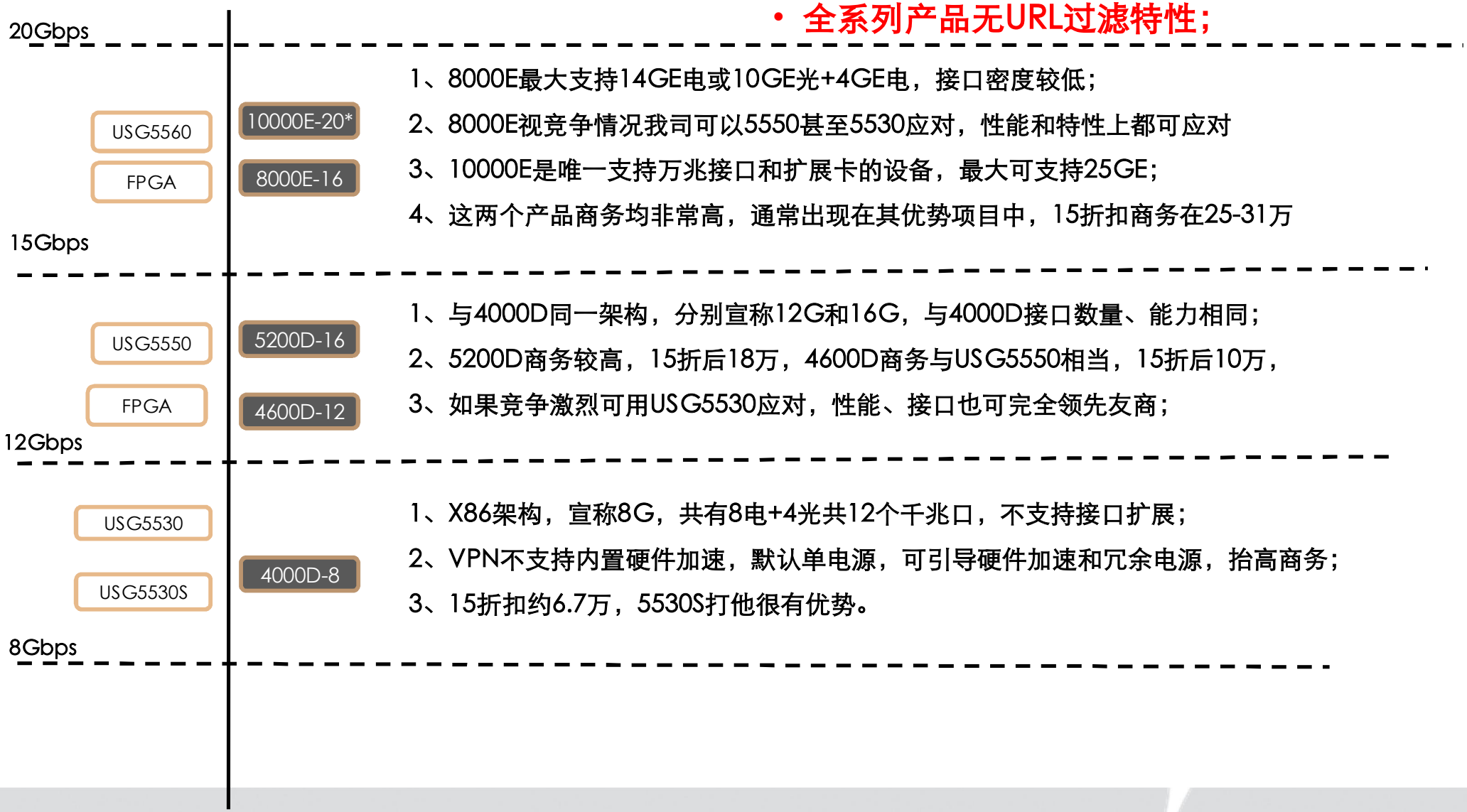
How to Beat启明星辰-厂商维度

通用打击方式	基于行业的打击点					
	政府	公共事业	金融	能源	教育	企业
基于产品选择要素/厂商选择要素的打击点						
•**打击点-产品落后**：天晴汗马USG产品即启明成功上市后就没有新特性，产品陈旧； •**打击点-性能低**：天清汉马USG系列普遍性能较低。 •**打击点-可靠性差**：天清汉马USG的千兆系列基本都是采用x86架构，相比网络多核架构可靠性要差。 •**打击点-代码开源的GPL风险**：产品基本都是采用开源代码，存在GPL约束，代码一旦开源后，对客户存在厂商信誉度降低和产品漏洞被曝光的风险。 •**打击点-安全能力差**：启明没有URL库，仅支持Web页面过滤，AV病毒特征库只有60万，	•**通用打击点。**		•**通用打击点。** •**打击点-数通特性的客户信赖度差**：启明星辰是做安全起家的，客户对数通特性的信赖度差。		•**通用打击点。** •**打击点-认证支持差**：仅支持本地、Web、redius、LDAP，不支持Radius、Tacacs等认证方式	

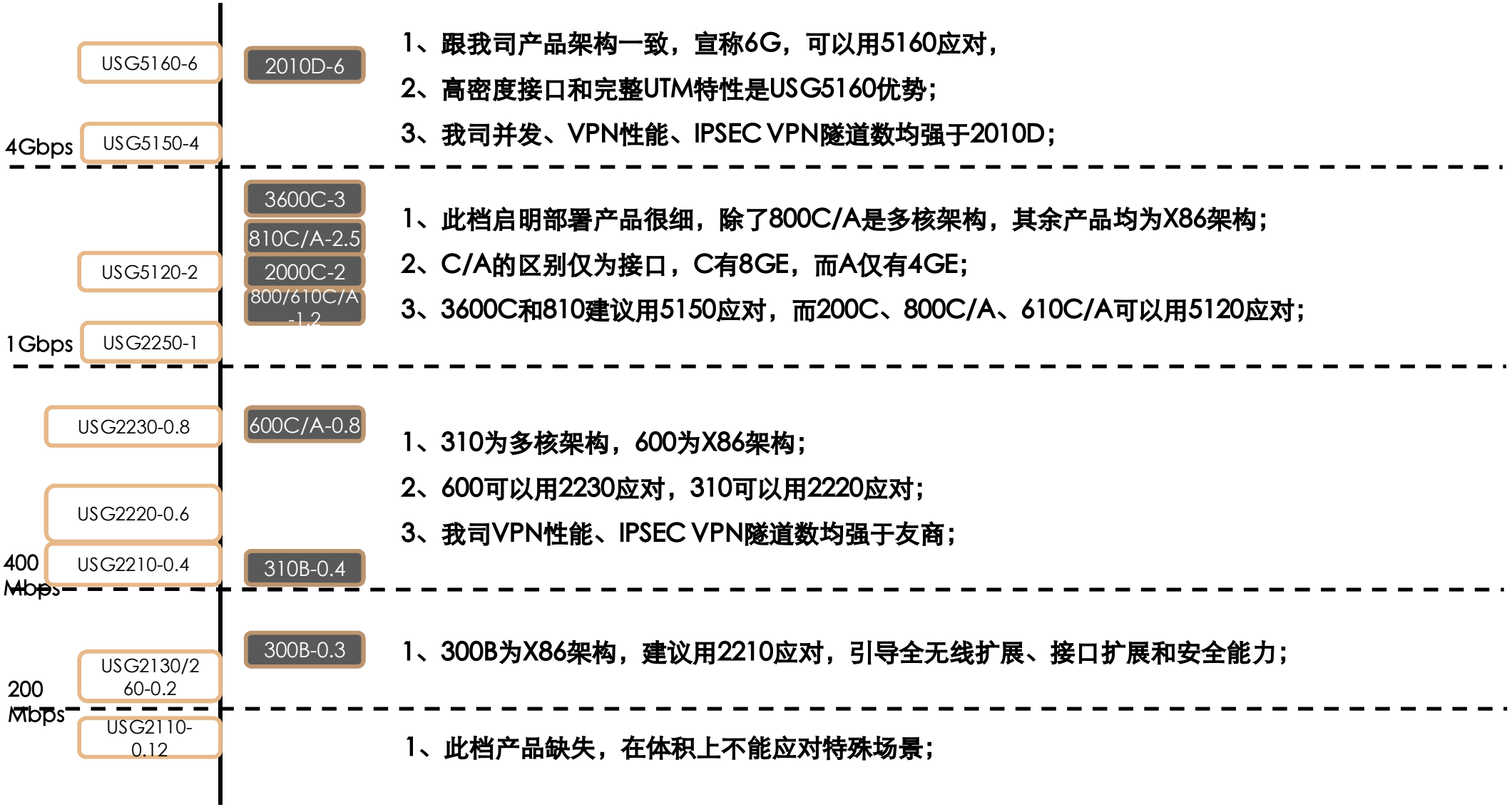
通用规避方式	基于行业的规避点					
	政府	公共事业	金融	能源	教育	企业
基于产品选择要素/厂商选择要素的规避点						
•**规避点-IPS能力强**：启明星辰主要依赖IDS产品起家，所以在攻防方面的技术积累较深。要注意引导用户放在防病毒、URL等UTM特性上。 •**规避点-不对等竞争**：启明星辰经常以低打高，所以经常出低价，要引导用户进行测试，去确保竞争对等，以抬高友商商务。	•**通用规避点。** •**特性规避点-已应用该品牌产品**：启明星辰在政府行业的应用案例较多，要注意引导用户关注当前项目。 •**特性规避点-合规性**：启明星辰在等保、分保方面投入的时间和精力都较大，贴近对政府项目的要求。 •**特性规避点-售后服务能力**：启明星辰的政府项目经验丰富，服务能力针对性强，规避时要强调我司售后能力强。		•**通用规避点。**		•**通用规避点。** •**特性规避点-内容过滤**：启明星辰支持基于关键字的过滤，要引导用户认识到基于关键字的内容过滤的实用价值不高，应该去使用基于URL库过滤的价值更高。	

How to Beat启明星辰-产品维度

- 除10000E外，全系列产品不支持万兆接口；
- 全系列产品无URL过滤特性；



How to Beat启明星辰-产品维度



How to Beat Hillstone-厂商维度

通用打击方式	基于行业的打击点					
	政府	公共事业	金融	能源	教育	企业
基于产品选择要素/厂商选择要素的打击点						
•**通用打击点-病毒查杀率极低**：Hillstone采用流扫描引擎，AV查杀率极低。AV特征库只有40w。 •**通用打击点-DPI协议识别低**：Hillstone仅支持300+种应用协议识别。 •**通用打击点-URL过滤库数量少**：Hillstone仅支持2000万Url网址，我司支持6500万； •**通用打击点-不支持反垃圾邮件**：Hillstone仅支持邮件关键字过滤。 •**通用打击点-售后服务能力差**：Hillstone公司目前规模较小（200人左右），但面向全国行业市场，售后服务能力差。 •**通用打击点-扩展能力差**：SG6000部分产品扩展槽较少，最大接口数较低，例如G6100只有13GE。	•**通用打击点。**		•**通用打击点。** •**特性打击点-新进入厂商，无成功案例**：Hillstone为新进入厂商，对于较为看重成功案例的行业客户，Hillstone呈现劣势。		•**通用打击点。** •**特性打击点-新进入厂商，无成功案例**：Hillstone为新进入厂商，对于较为看重成功案例的行业客户，Hillstone呈现劣势。	

通用规避方式	基于行业的规避点					
	金融	能源	政府	公共事业	教育	企业
基于产品选择要素/厂商选择要素的规避点						
•**通用规避点-技术积累强**：Hillstone的Founder为Netsrceen的高层，对于FW的硬件积累较为深厚。 •**通用规避点-AV性能高**：Hillstone采用独立AV加速卡把性能加速到1.2G，在业界领先，需要强调AV检出率。	•**通用规避点。** •**特性规避点-FW性能高**：SG6000采用Cavium多核架构，FW性能在业界集中式产品种算是较高的，与我司产品基本持平。		•**通用规避点。** •**特性规避点-FW性能高**：SG6000采用Cavium多核架构，FW性能在业界集中式产品种算是较高的，与我司产品基本持平。			

How to Beat Hillstone-产品维度

20Gbps

SG-X6150

1、10年发布的高端设备，宣称分布式，最大支持100G，不支持UTM特性；
2、我司最好以9000系列应对，如果以5560应对注意引导UTM特性；
3、目前暂无商务信息

15Gbps

USG5560
FPGA

SG-X5100

1、 X5100宣称20G，标配1GE+12SFP+2XFP，不支持扩展；
2、防火墙吞吐性能一般，但加速后并发可达1000万，企业用户很难用到；
3、特价商务22.6万，我司优势明显，可重点打击其接口扩展性

12Gbps

USG5550
FPGA

1、 此档产品缺失，友商很可能以低打高（加速后）；

8Gbps

USG5530

SG-G6100

USG5530S

SG-G5150

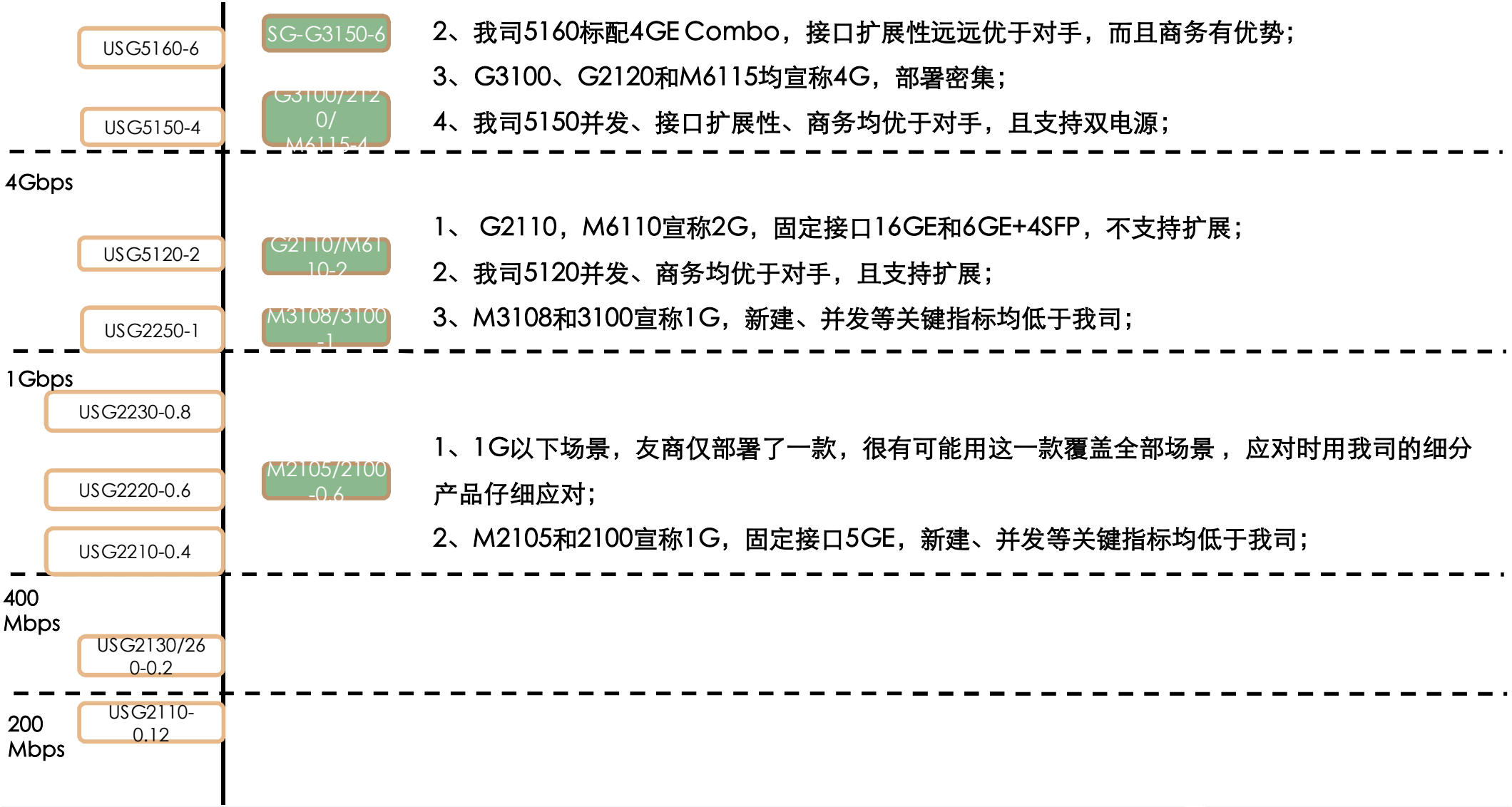
1、5150宣称8G加速可至10G，标配4GE+8SFP，4扩展槽，支持万兆
6100宣称10G，标配1GE+12SFP，不能扩展，不支持万兆，
两个型号都为多核/双电，加速后并发链接数很高，注意引导其必要性
2、5150特价商务约9.1万，加速需3万，6100特价商务约13.8万，加速需4.8万。
3、性能、接口5530均可覆盖，商务优势明显，6100不支持上网行为管理

USG5150

SG-G3150

1、多核，宣称6G加速可至8G，单电源，标配4GE+8SFP，4扩展槽，最多8GE/槽
2、裸机特价商务可达6.2万（6G）/8.3万（8G），该机不支持万兆口；
3、5530S应对8G优势明显，应对6G可以持平，如果引导双电源，我司优势更加明显。

How to Beat Hillstone-产品维度



1、 G3150，标配4GE+8SFP，最大可扩展到32GE，宣称6G；

2、我司5160标配4GE Combo，接口扩展性远远优于对手，而且商务有优势；

3、G3100、G2120和M6115均宣称4G，部署密集；

4、我司5150并发、接口扩展性、商务均优于对手，且支持双电源；

1、 G2110，M6110宣称2G，固定接口16GE和6GE+4SFP，不支持扩展；

2、我司5120并发、商务均优于对手，且支持扩展；

3、M3108和3100宣称1G，新建、并发等关键指标均低于我司；

1、1G以下场景，友商仅部署了一款，很有可能用这一款覆盖全部场景 ，应对时用我司的细分产品仔细应对；

2、M2105和2100宣称1G，固定接口5GE，新建、并发等关键指标均低于我司；

目录

典型应用-政务专网出口安全防护

存在的问题

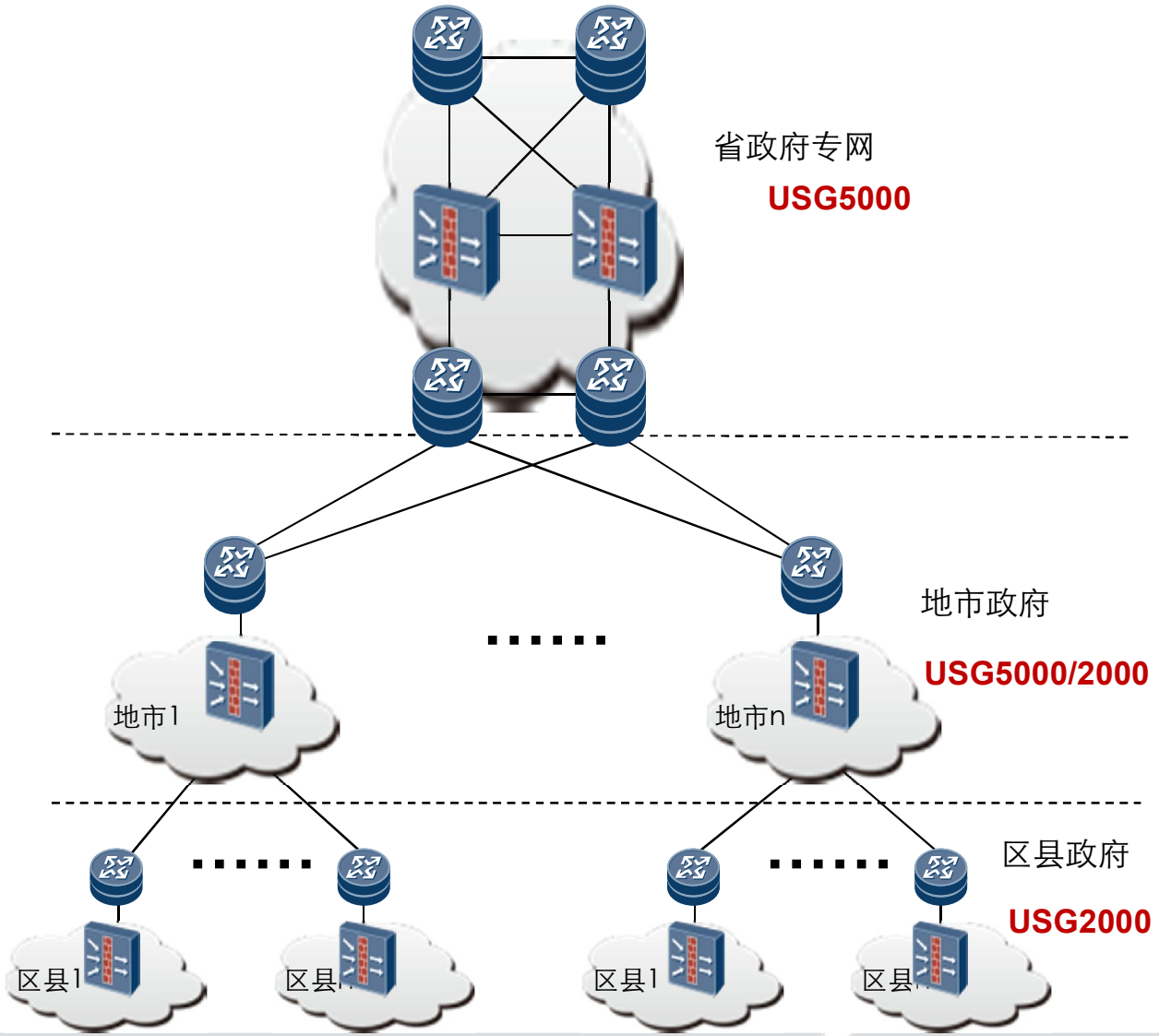
- 政府专网之间缺乏隔离
- 内外网缺乏安全保护
- 内部多业务系统存在漏洞

解决方案

- 边界安全防护加防病毒隔离
- 网络安全统一管理

方案价值

- 政府专网之间实现安全隔离
- 专业高效防病毒保护
- 有效控制安全事件的范围
- 统一管理实现漏洞和补丁升级



典型应用-数据中心安全隔离

存在的问题

- 大流量安全隔离
- 业务连续性保障
- DDoS安全防御
- 应用可视化管理

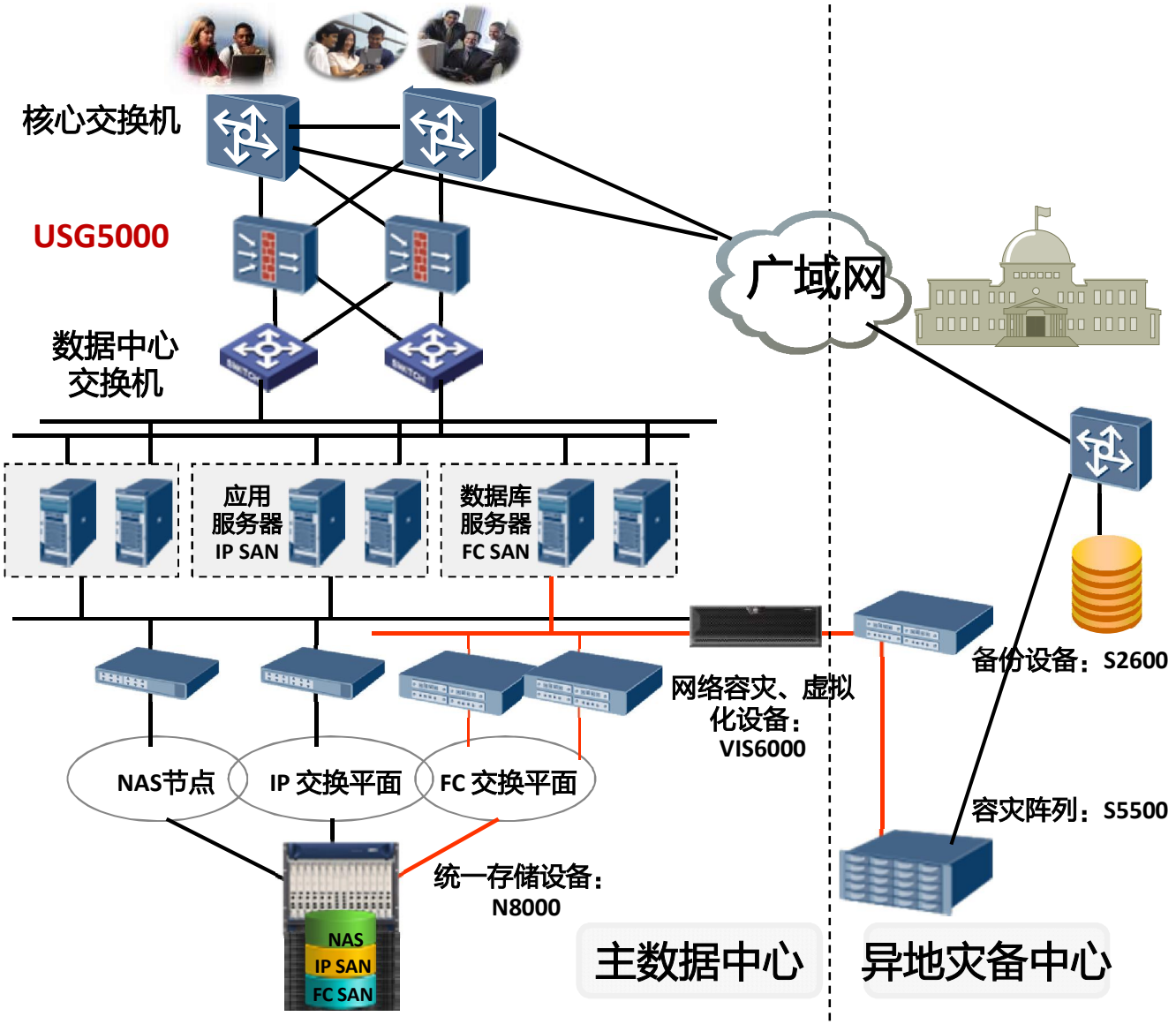
解决方案

- 数据中心万兆安全隔离
- 部署双机热备

方案价值

- 单机32Gbps流量安全隔离
- 10Gbps专业DDoS安全防御
- 微秒级时延、双机热备

  零丢包率，保障业务连续
- 实现业务可视化管理



典型应用-网络准入安全防护

存在的问题

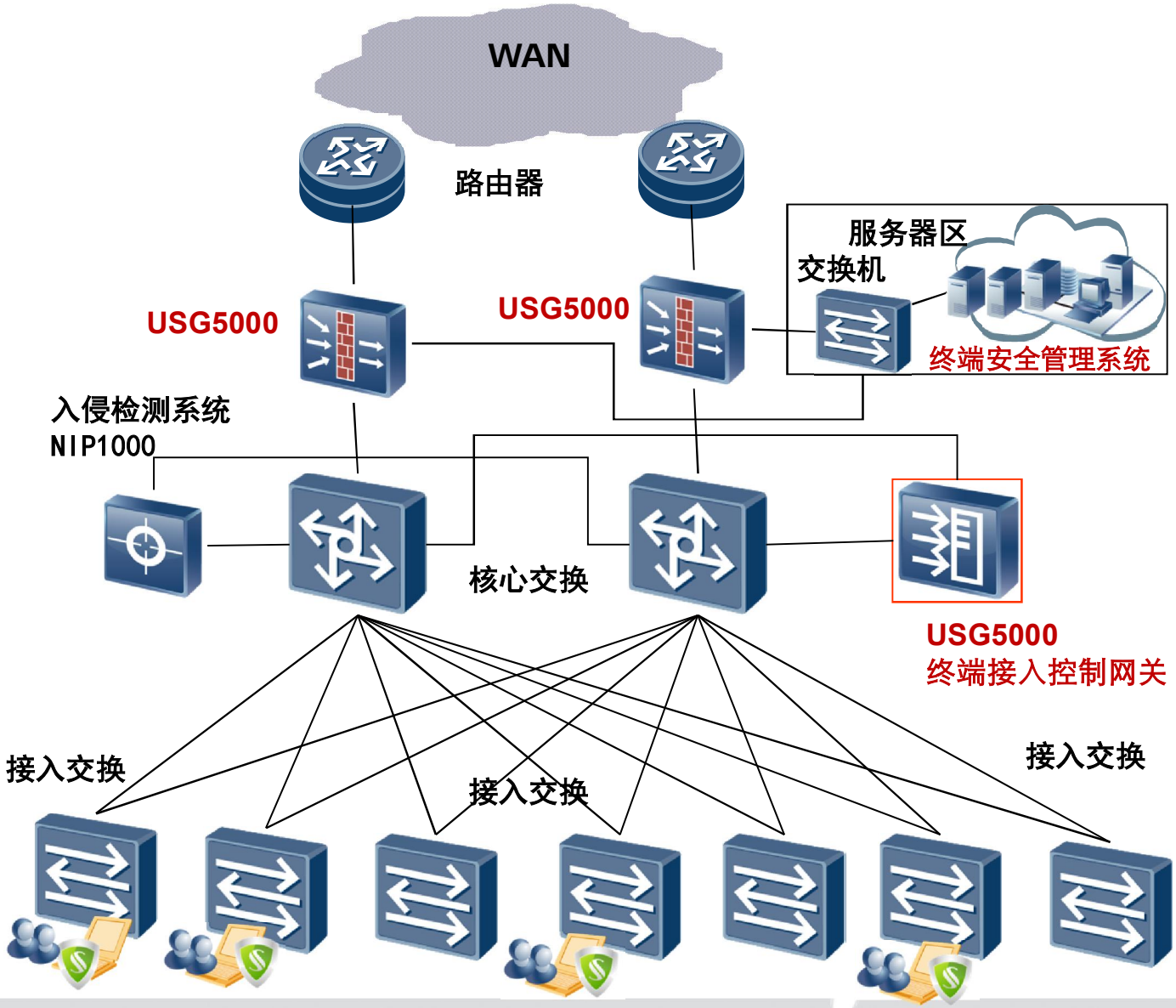
- 终端存在安全漏洞
- 合法用户非法访问
- 非法用户接入无法控制
- 终端众多难以管理

解决方案

- 专业网关方案，适应性强
- 集中管理，快速部署
- 终端支持广泛
- 可靠性高，控制灵活

方案价值

- 强制终端保护业务系统
- 提升网络安全性和可用性
- 提高效率，节约费用



典型应用-分支机构VPN安全接入

存在的问题

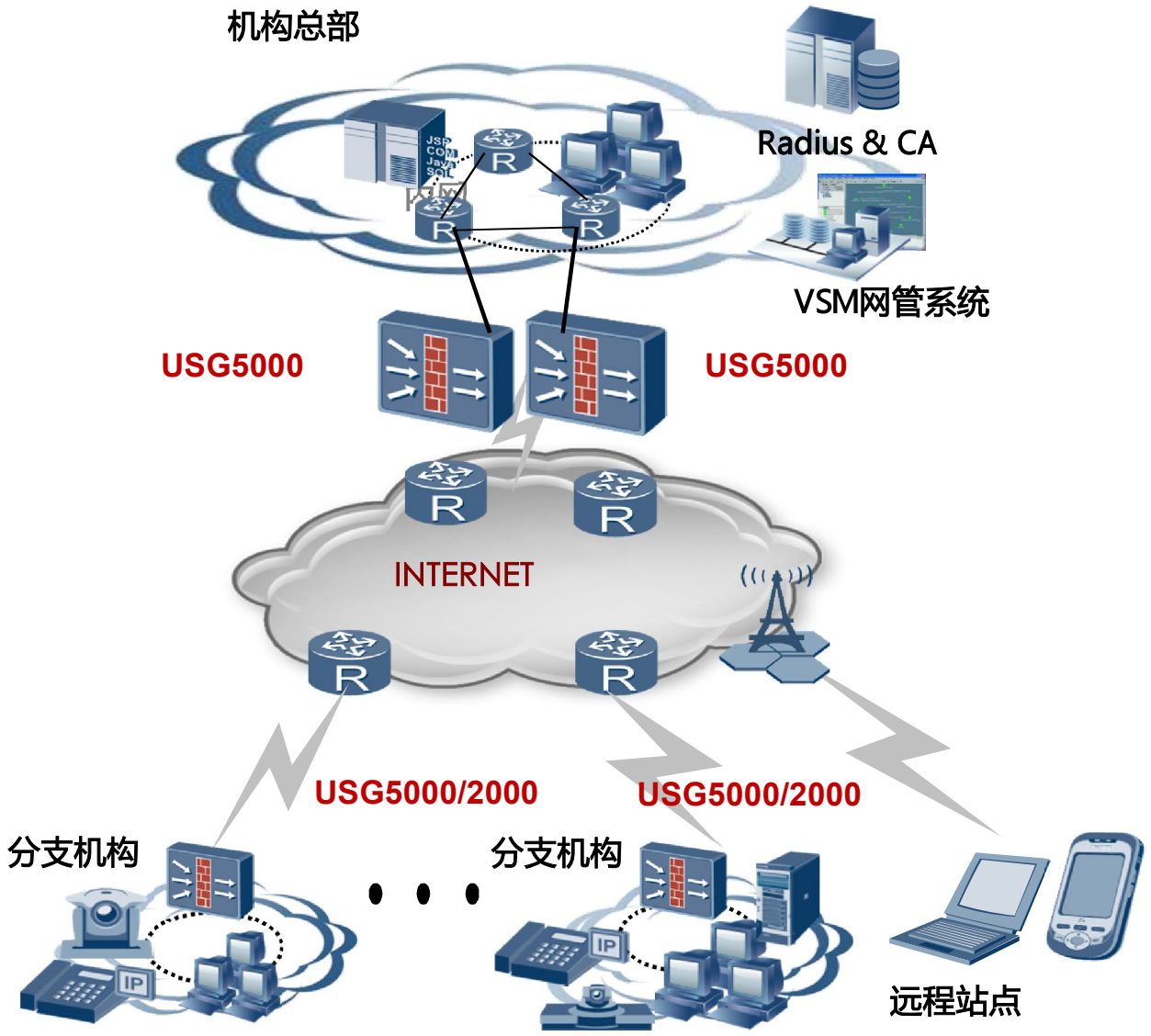
- 分支机构、移动办公安全接入
- 跨互联网数据安全传输

VPN解决方案

- 支持IPSec/L2TP/GRE/ SSL/ MPLS多种VPN技术
- 支持隧道数在线扩展
- 电信级高可靠性

方案价值

- 安全、灵活、可靠VPN接入
- 业务集中管理



目录

成功案例-中国中央电视台

挑战

- 数据中心大流量安全隔离
- 数据中心应用可视化管理

特点

- 4台USG5560提供双机热备，1台冗余后备
- 单机最高32Gbps吞吐
- 10Gbps硬件DDoS安全防御
- 1000+应用识别能力

价值

- USG5500实现零时延、双机零丢包，为业务连续性实现高可靠的保障

成功案例-黑龙江财政厅

挑战

- 专网频遭恶意攻击，时有病毒爆发
- 要求安全产品高性能+高检出率

特点

- 13台USG5530S，66台USG5320，搭建专网防御
- AV检出率高达99%
- 专业DDoS安全防御

价值

- UTM产品政府专网安全防护

中低端USG产品典型案例-湖南地税第二网络建设

挑战

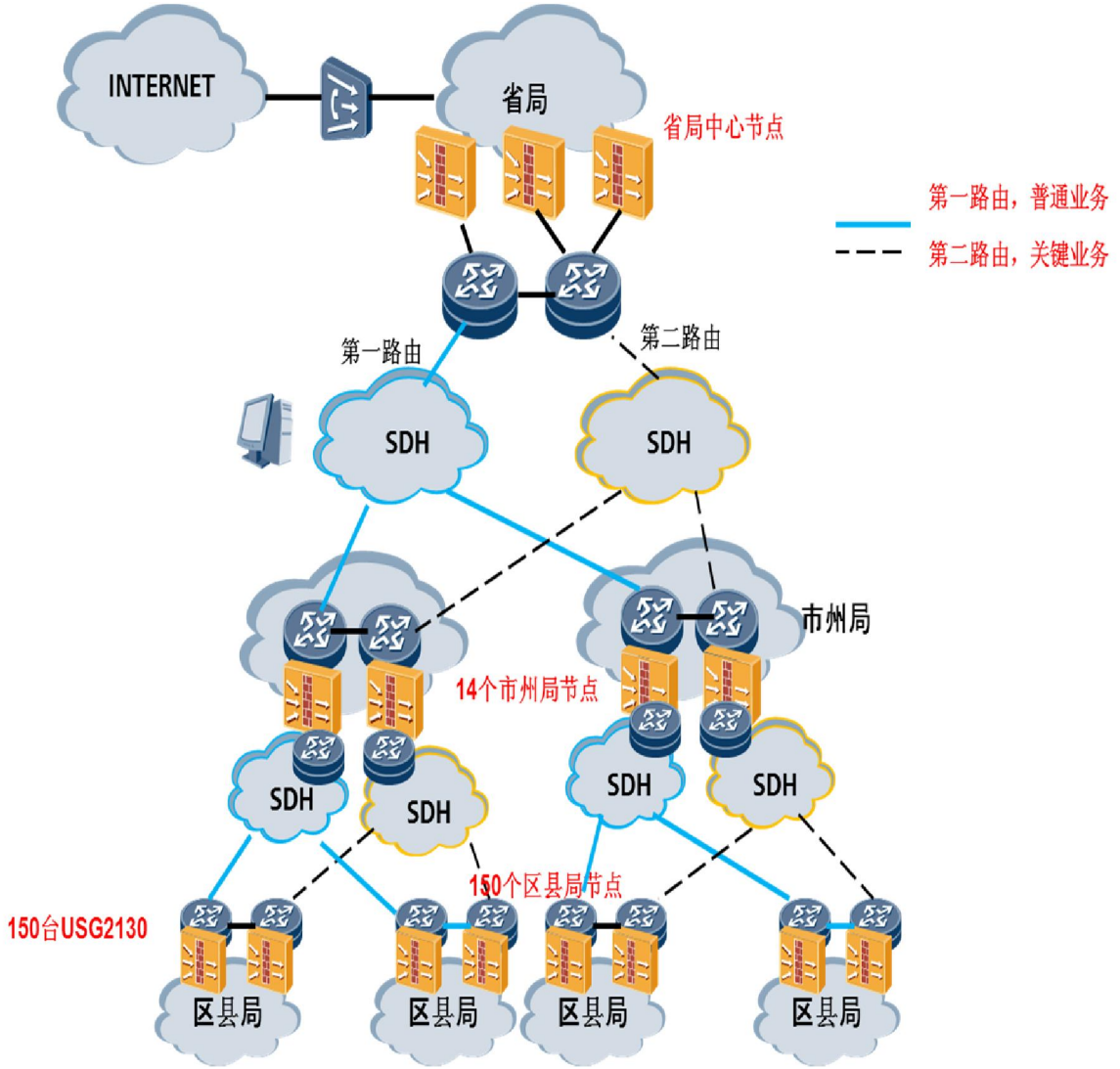
- ✓ 多出口，多安全隐患高
- ✓ 层次化网络，纵深防御

特点

- ✓ 在全省150个县部署USG2130
- ✓ 安全区域划分，设置安全级别，制定安全策略

价值

- ✓ 统一安全网关**USG2130**，丰富的产品特性和极高的性价比为客户带来了高效的收益，有效降低了客户的**TCO**



Huawei Enterprise A Better Way