Huawei Enterprise A Better Way

华为Secoway USG2000&5000
统一安全网关
主打胶片

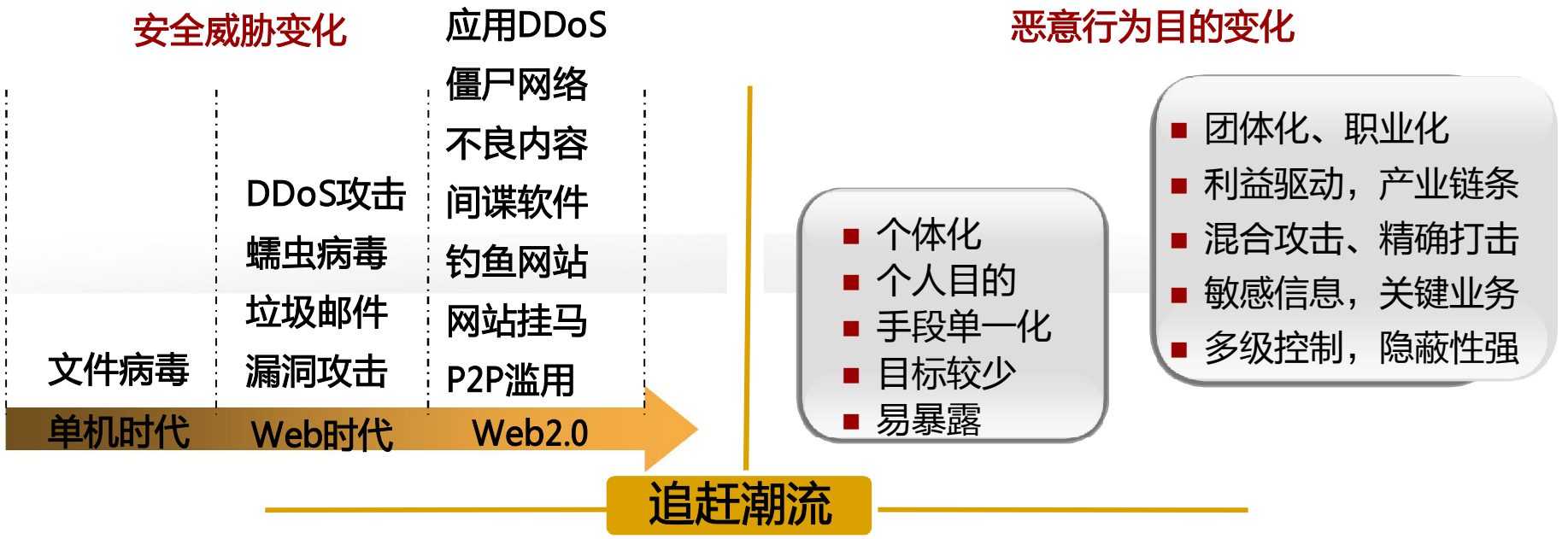
enterprise.huawei.com

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Content

安全风险发展与变化

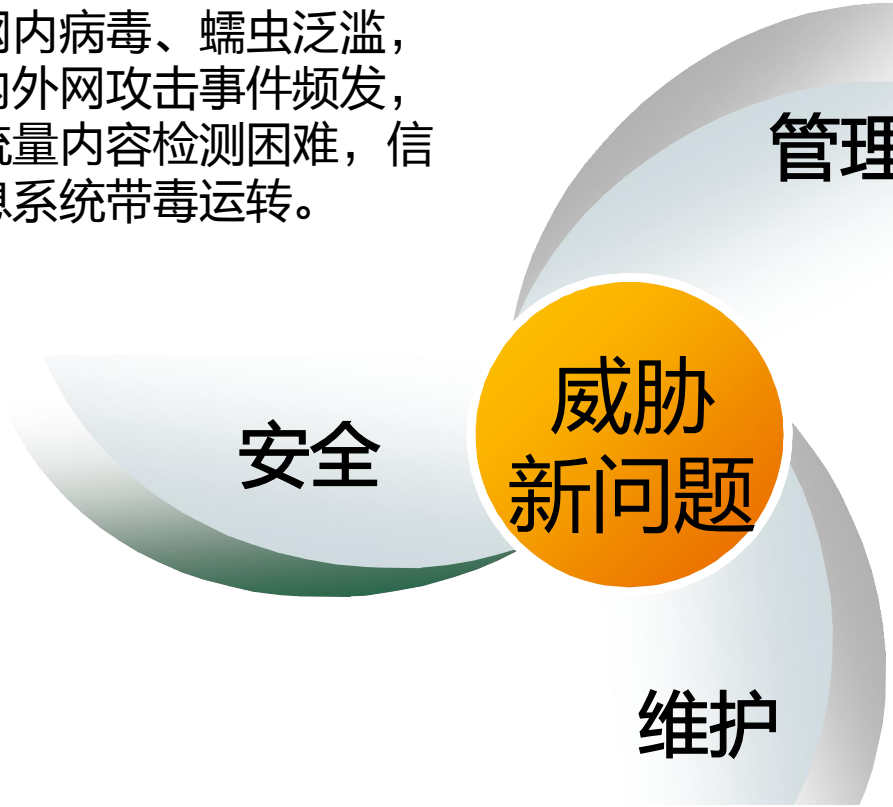


各类安全产品各自为战

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。



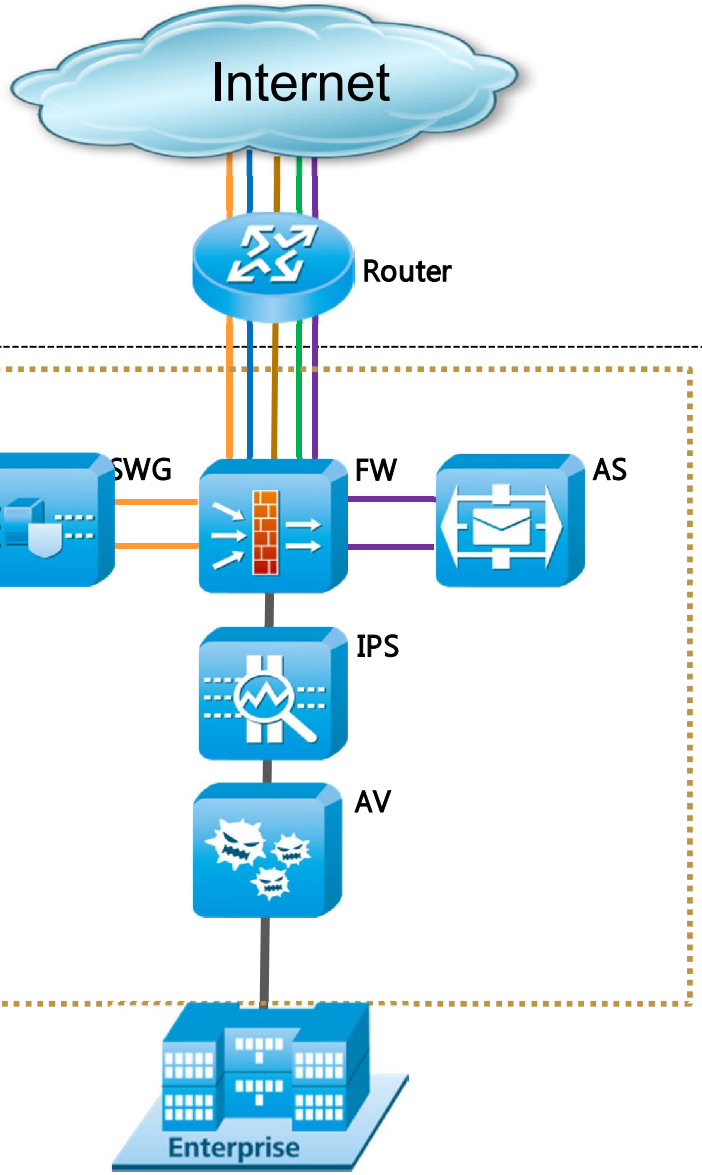
缺乏安全意识，随意浏览下载，极易中招；
滥用网络，关键业务无法保障，效率低下；
应用控制薄弱，难以准确管理网络应用；
用户难以识别，无法精确管理用户行为。

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

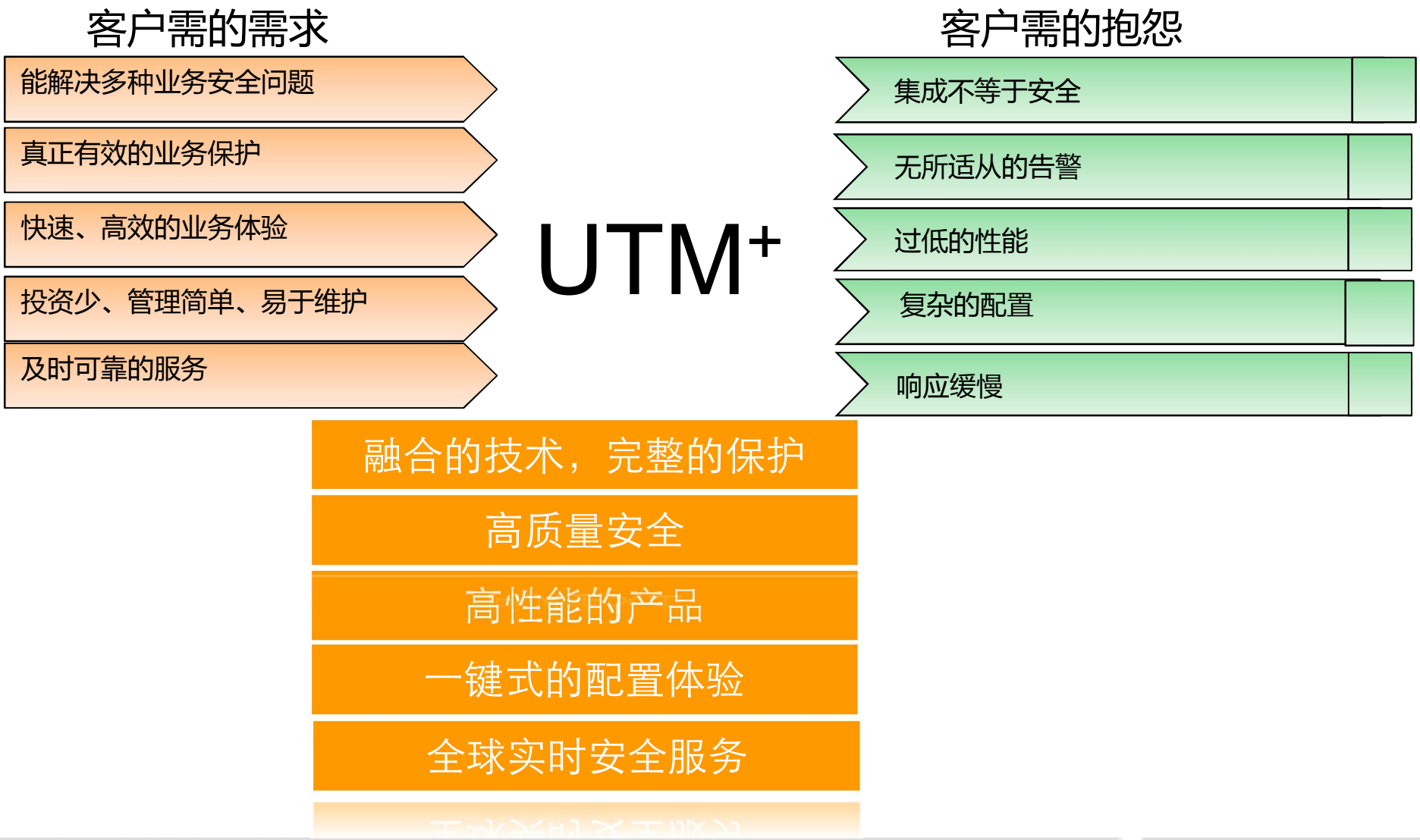
- 安全方案日趋复杂
- 运维成本日趋庞大

投入增加，收益减少

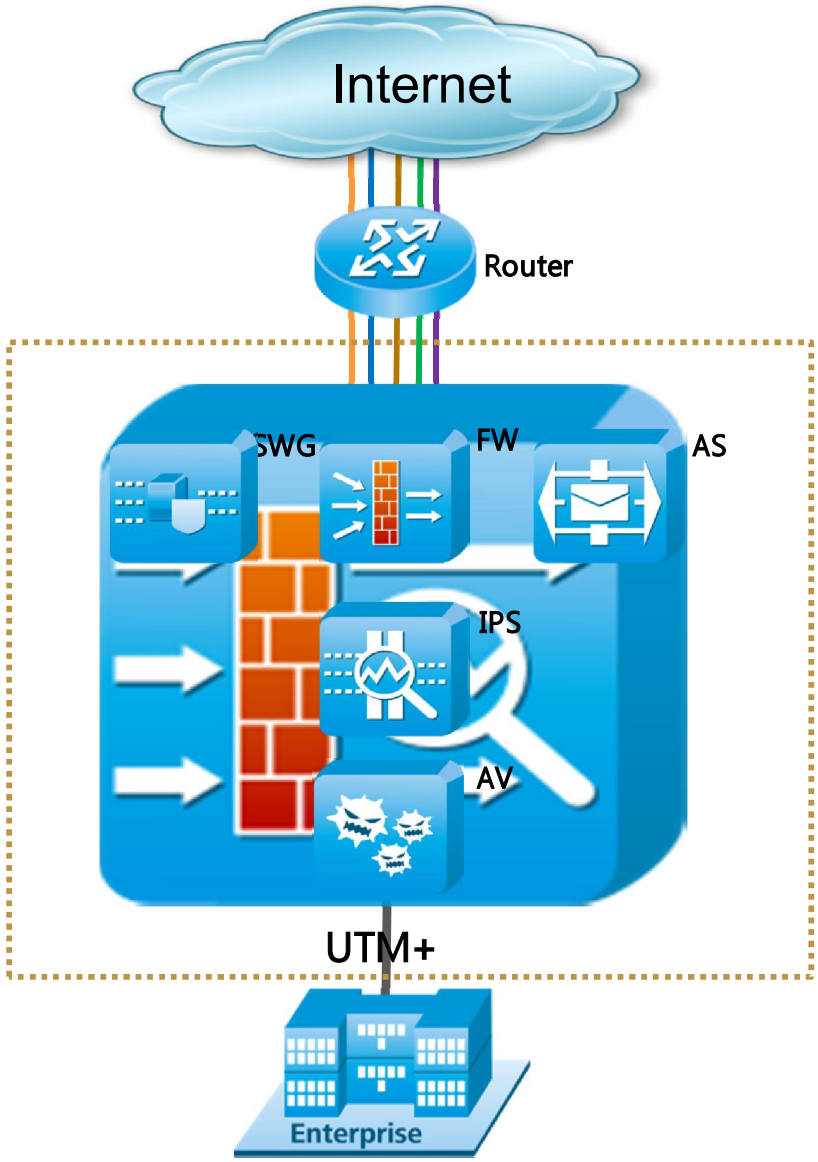


Content

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：

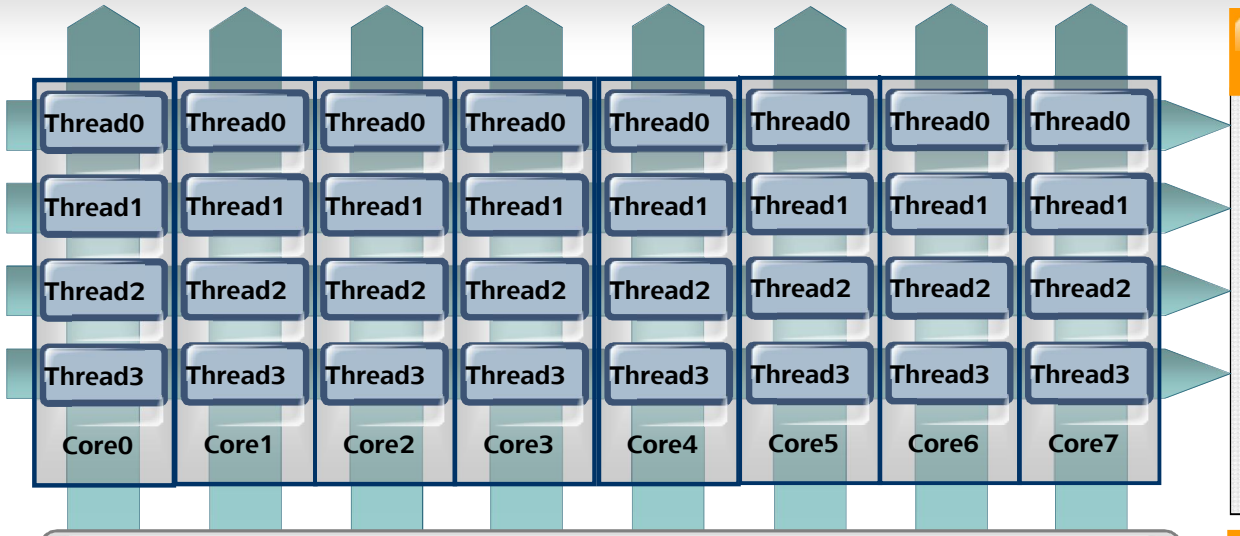
- Firewall
- UTM
- 内容过滤
- 流量控制
- 上网行为管理

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。

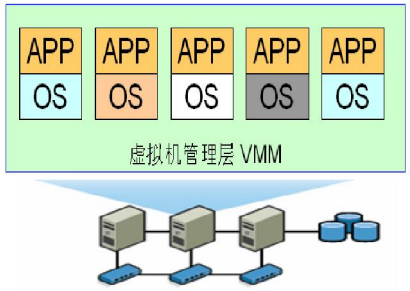
流程优化

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。

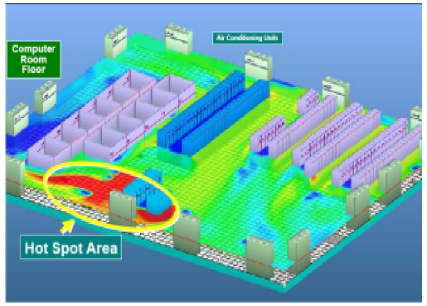
多核的优势

软件灵活性高

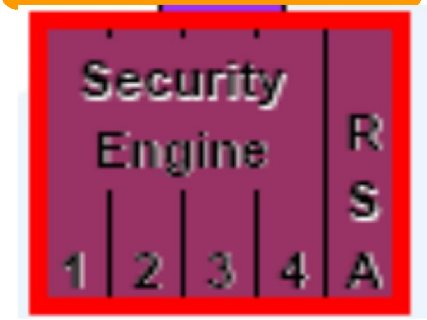


处理性能高

单位功耗低



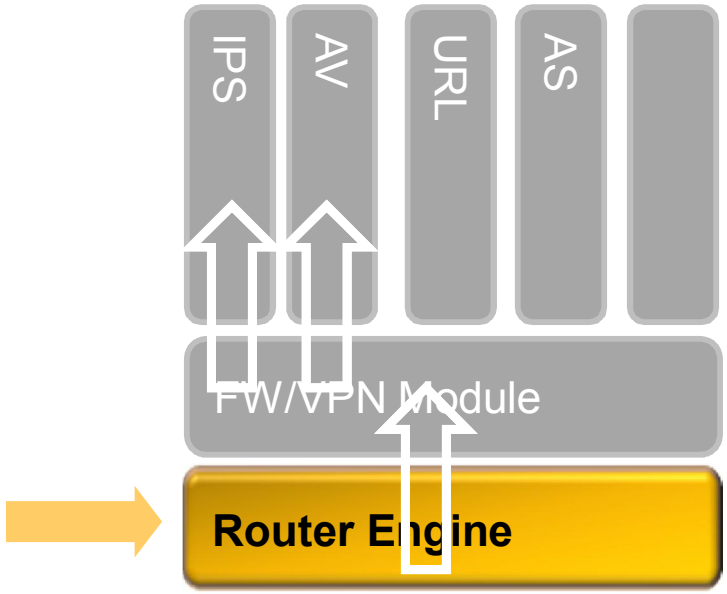
硬件加速引擎



架构-高效软件

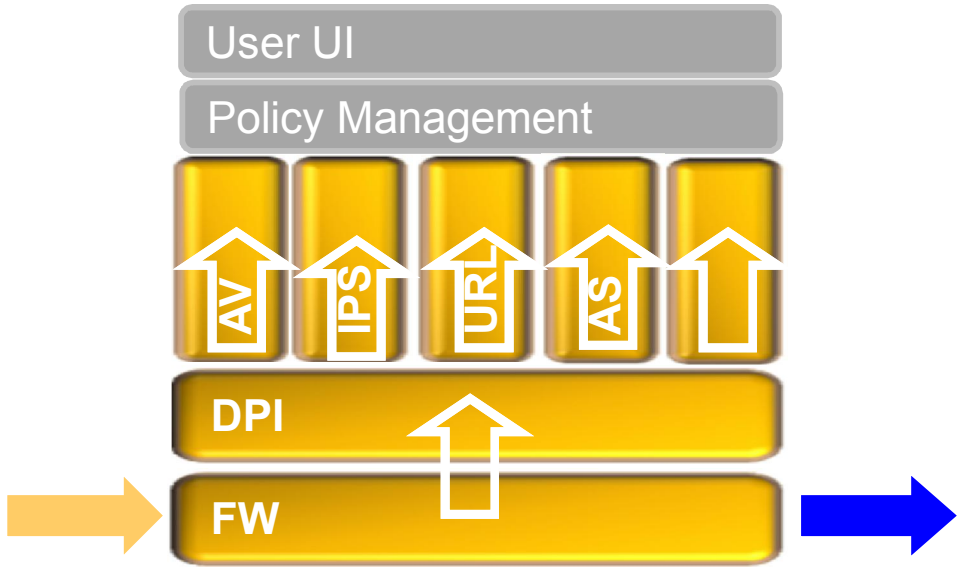
领先架构 | 丰富功能

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

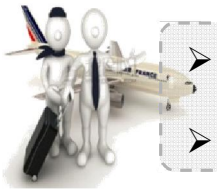
用户认证	安全策略	用户管理
➢ 本地/第三方认证 ➢ 事前/会话认证 ➢ Web/AD/Radius/LADP多认证方式	➢ 基于用户的策略 ➢ 基于用户的审计	➢ 本地/第三方用户管理 ➢ 组织架构管理&同步 ➢ 用户状态管理

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

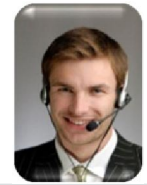
灵活性

- 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

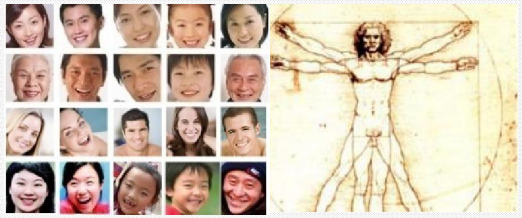
可识别超过240种协议

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

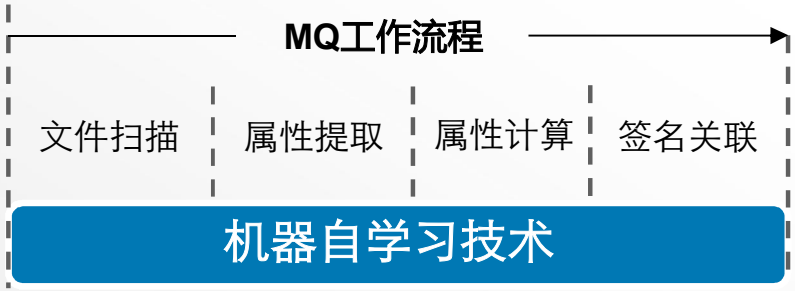
- 基于漏洞的签名，有效防止攻击变种、所有签名都可开启，并具有极低误报率
- 独特的识别能力，无需低效率的盲扫
- 新增漏洞签名到2000+种

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

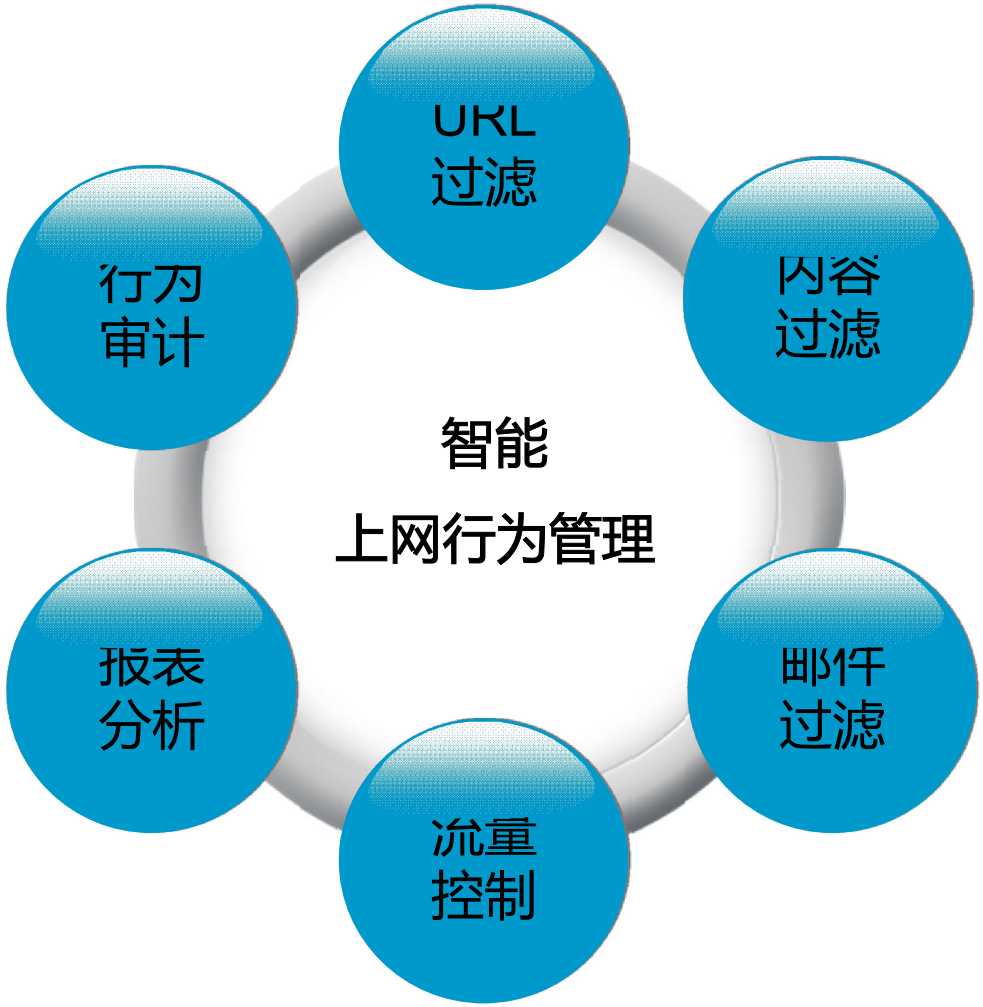
精细预分类：130种
支持用户自定义分类
细

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

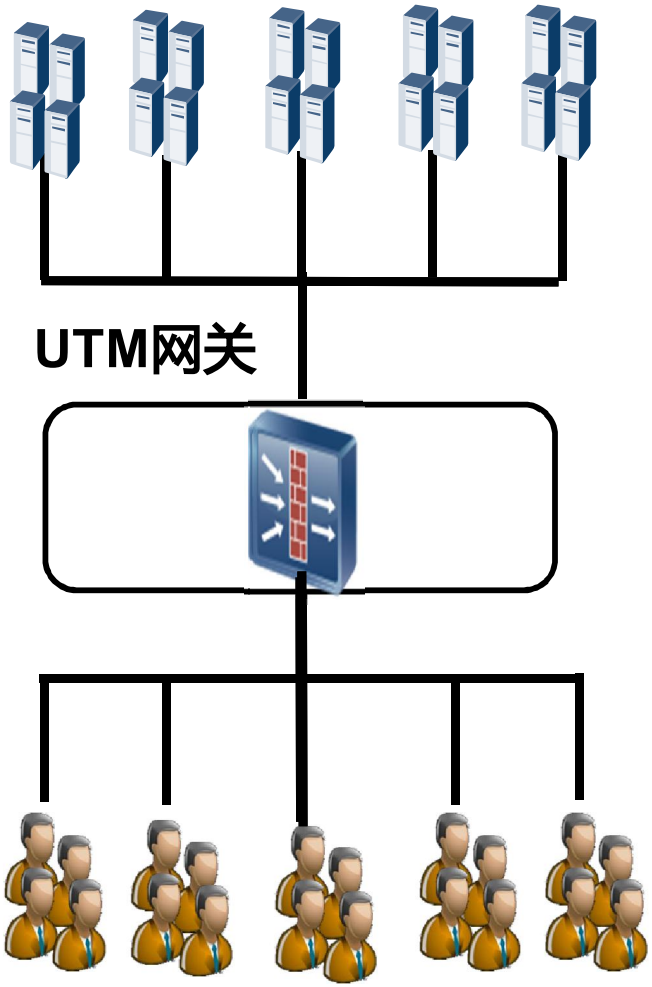
- FW、NAT、VPN、IPS、AV、URL、DPI、AS、Content Filter

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

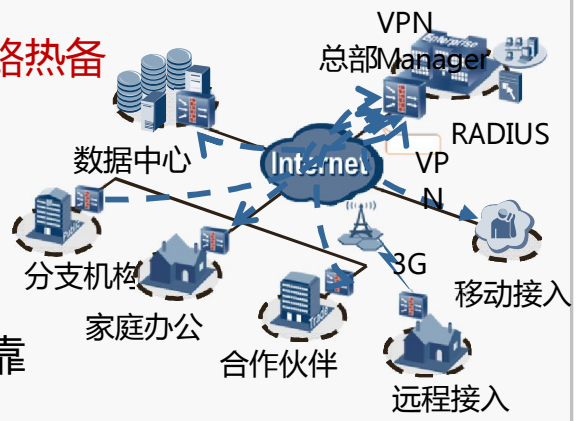

基于应用的选路


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

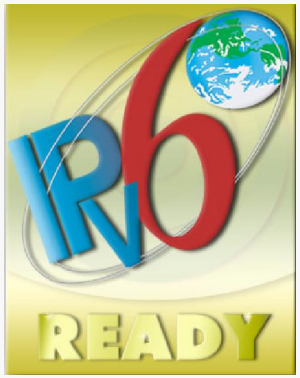


IPv6过渡技术

- 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

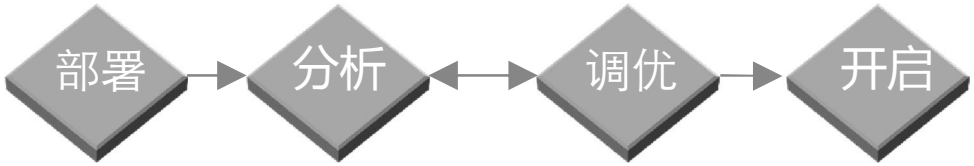


UTM+功能-一键配置

领先架构 | 丰富功能

- 传统UTM配置复杂，人为因素多，费时费力

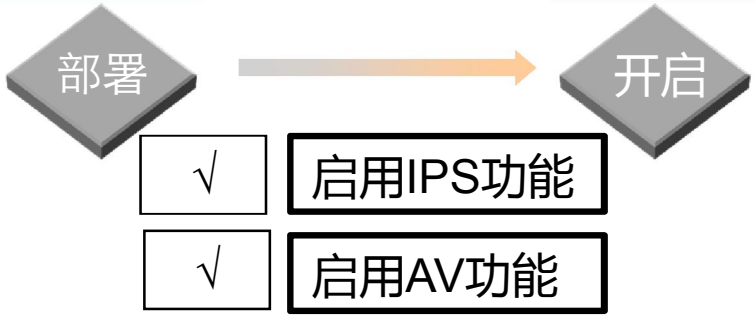
Step1 Step2 Step3 Step4



- 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

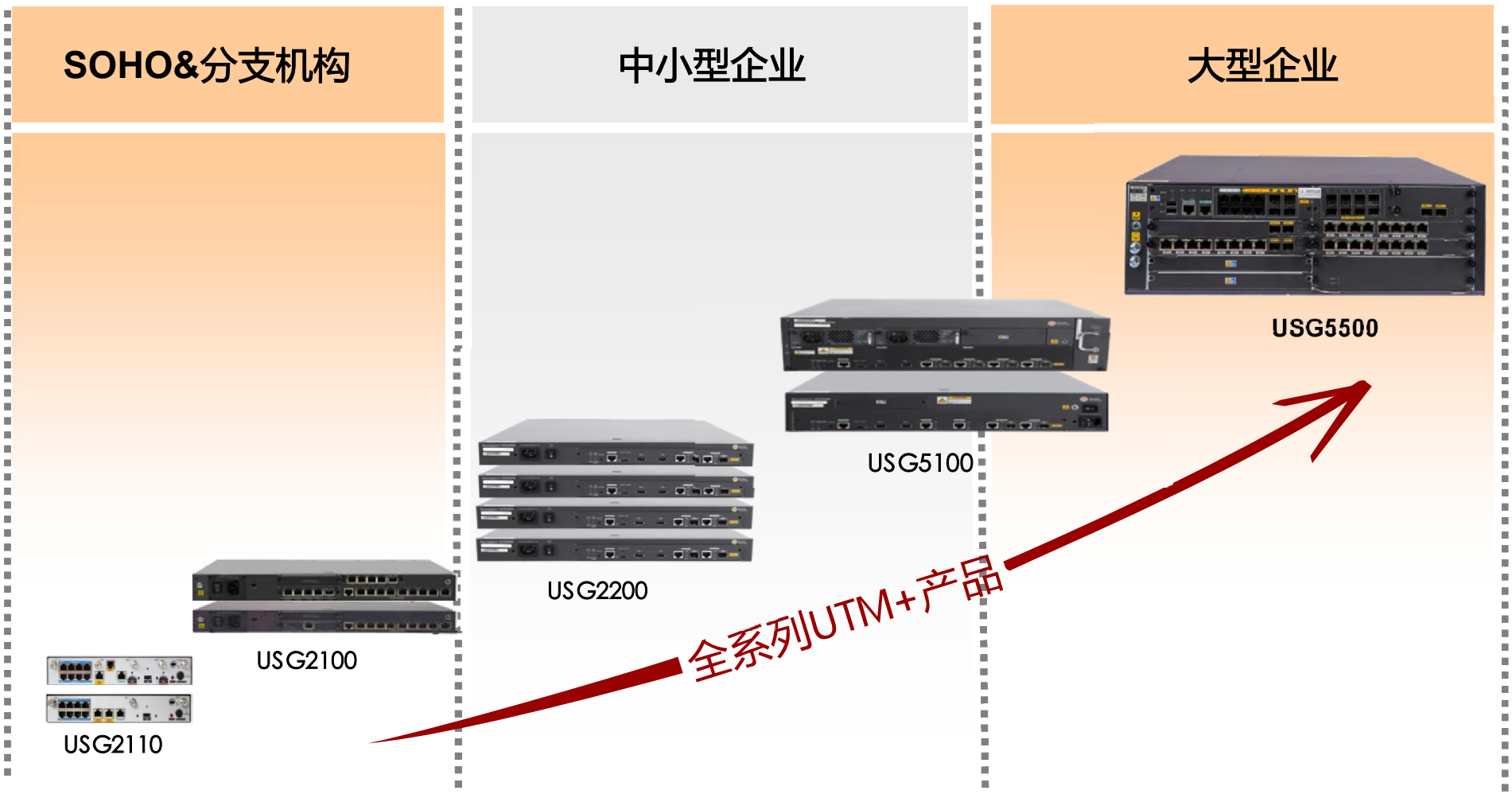
用户关键字命中排行

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)

Content

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；

  高达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	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；
  高达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；
  高达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）

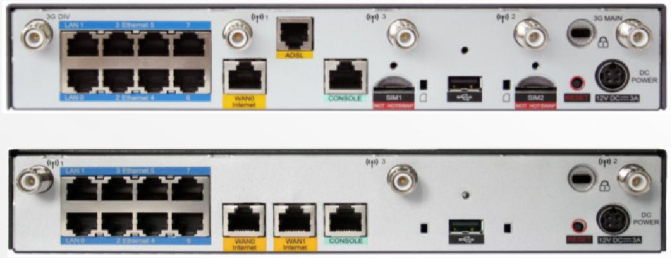
- 定位： 入门级百兆UTM
- 功能： 支持USG V3R1版本特性；
  高达200M FW性能，基于用户的安全策略，增强UTM功能，基于内容的安全过滤；
  强大的上网行为管理，支持IPv6 ，提供直流机型；
- 接口： 1FE+8 FE 固定，1 / 2 x 扩展插槽(2130/2160），
  丰富的广域网接口卡 Serial /E1 / ADSL2+ / FE / GE /3G / G.SHDSL，内置WIFI（-W机型）。

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；

  高达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

典型应用-政务专网出口安全防护

存在的问题

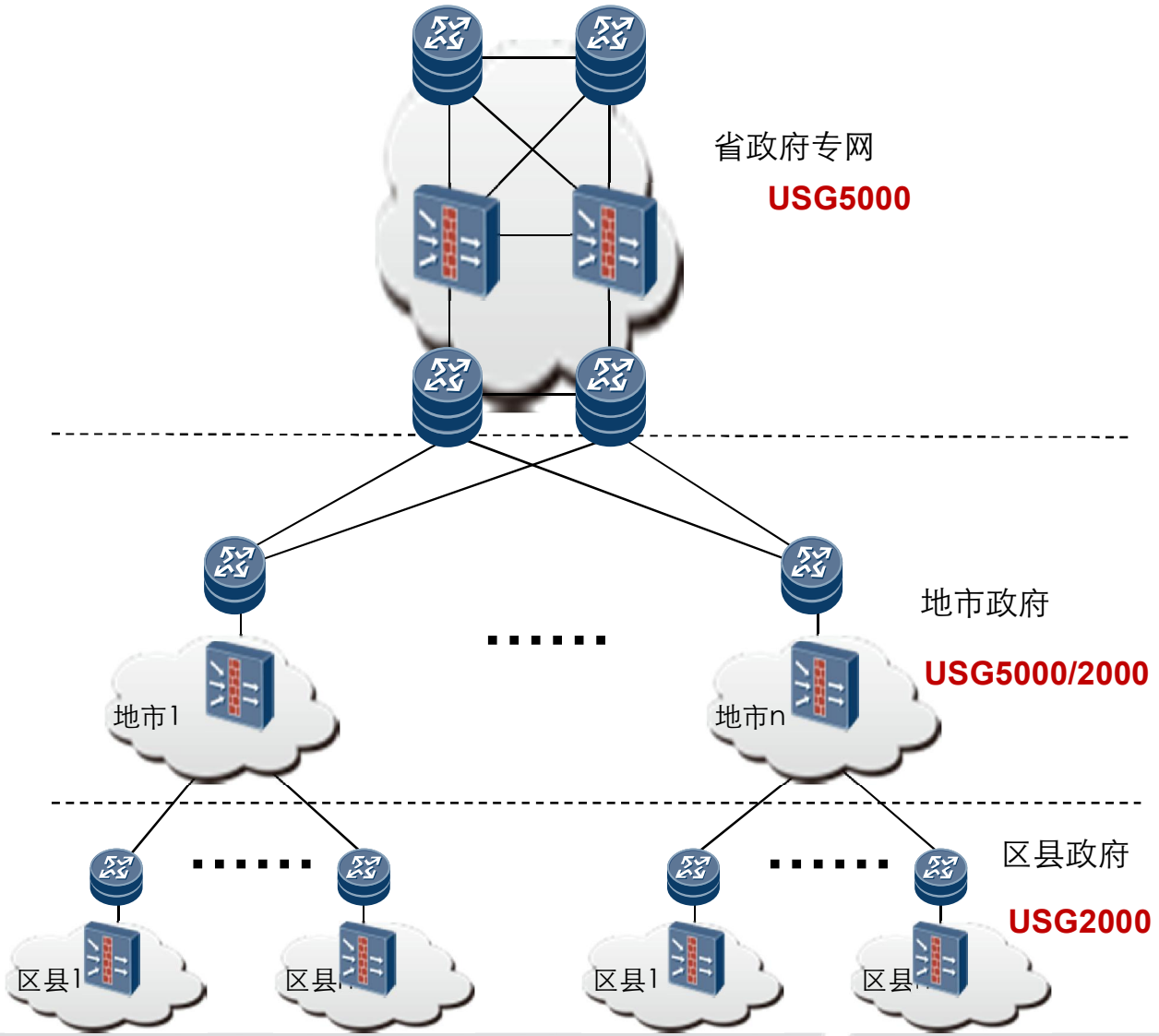
- 政府专网之间缺乏隔离
- 内外网缺乏安全保护
- 内部多业务系统存在漏洞

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

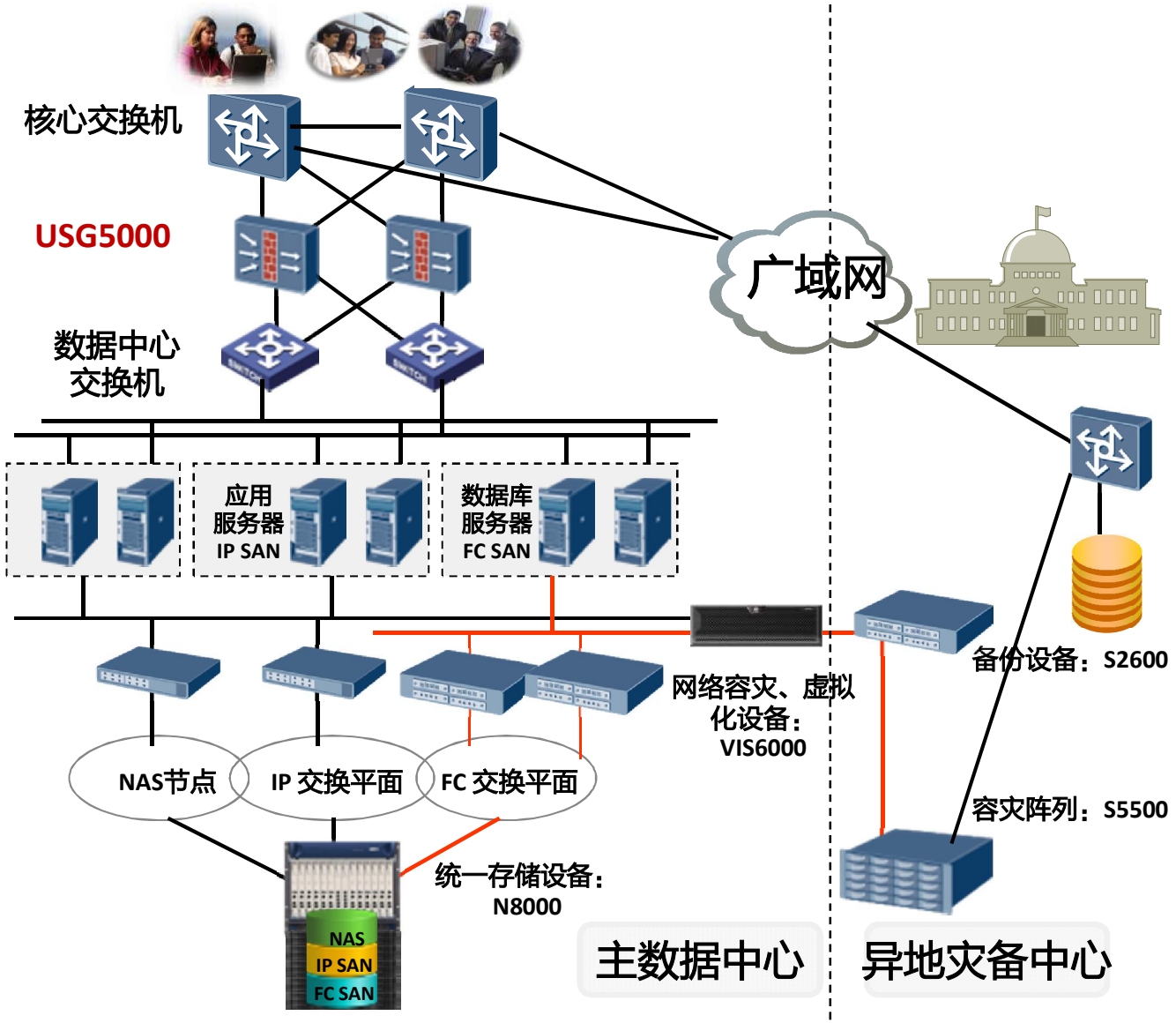
解决方案

- 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

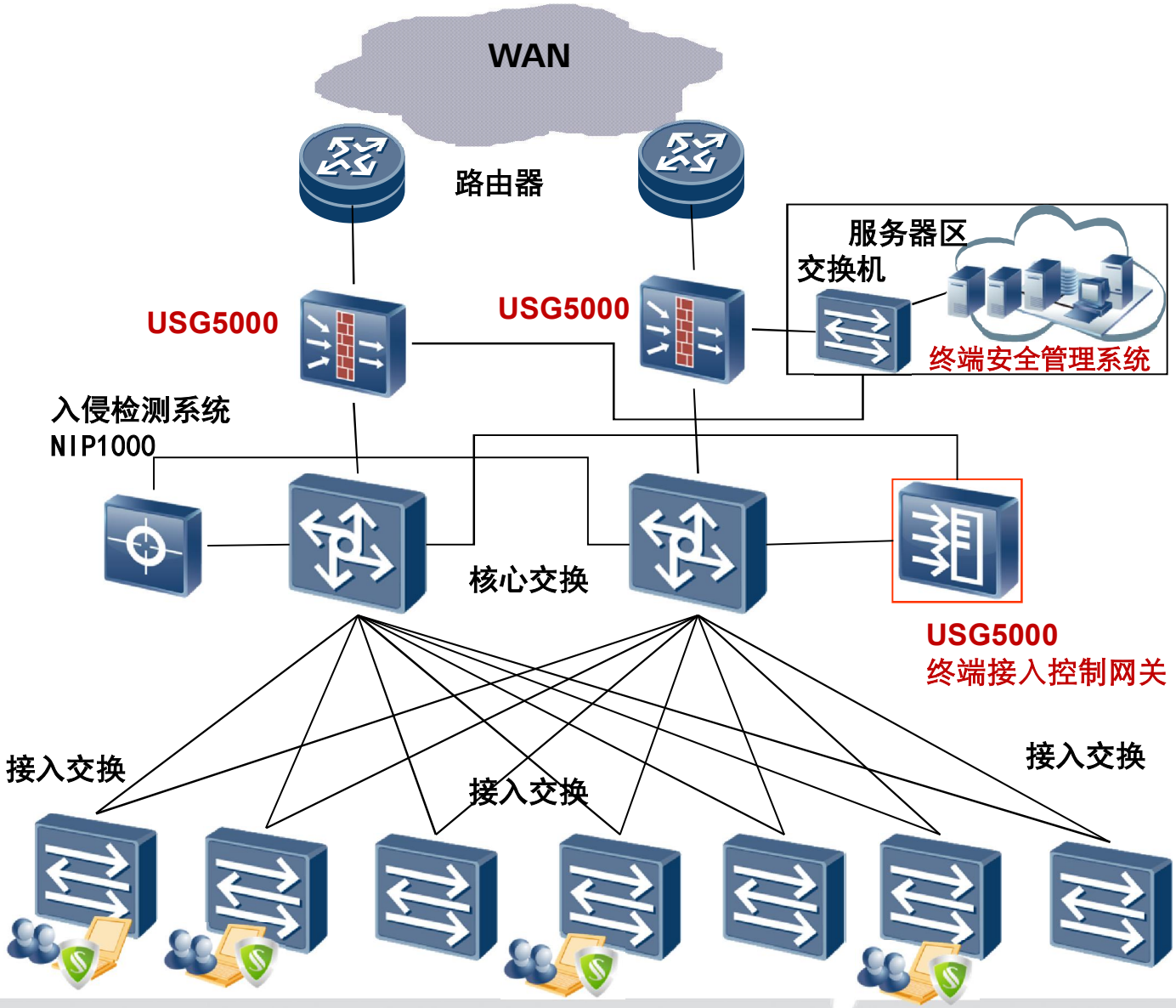
- 终端存在安全漏洞
- 合法用户非法访问
- 非法用户接入无法控制
- 终端众多难以管理

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

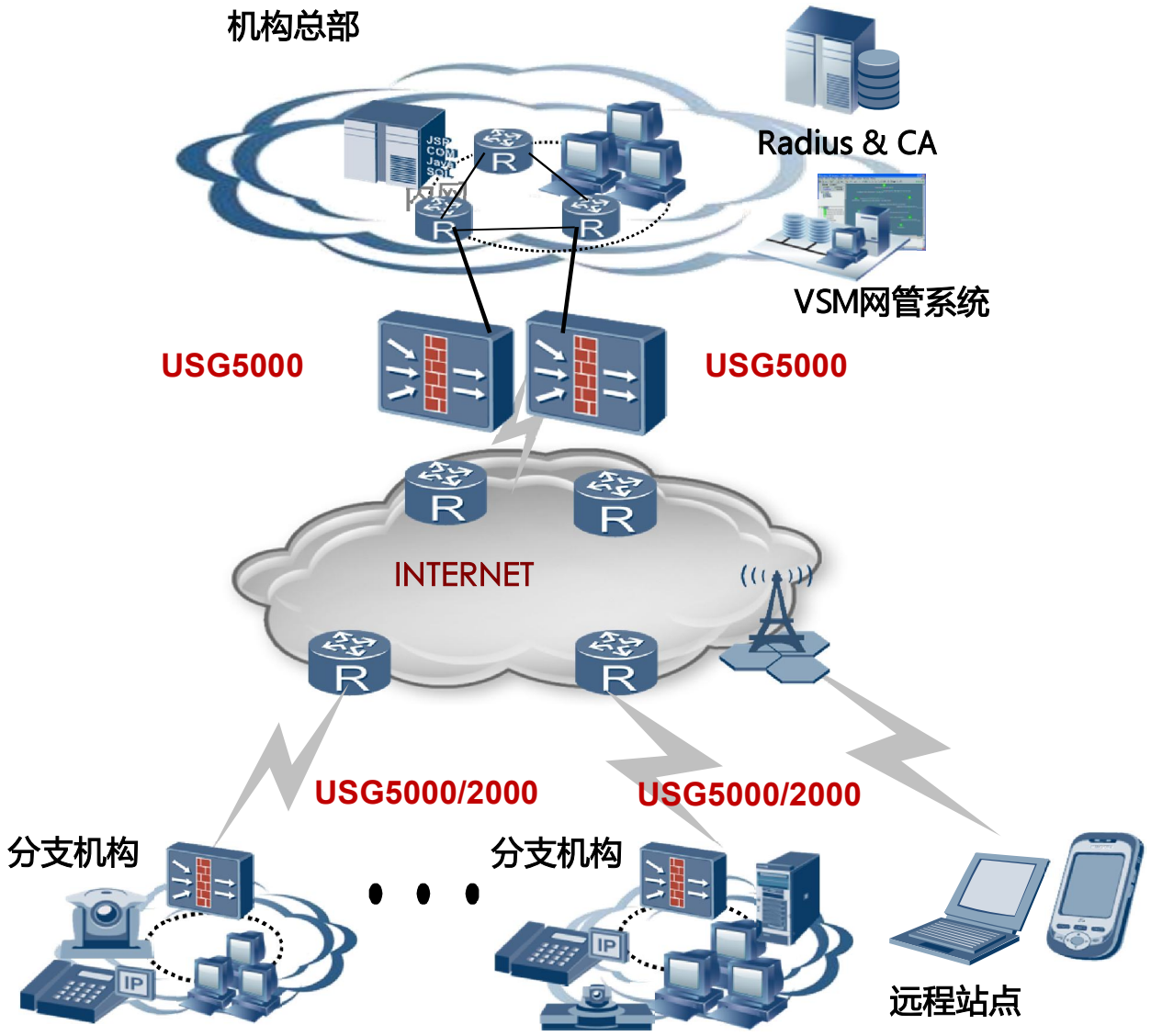
- 分支机构、移动办公安全接入
- 跨互联网数据安全传输

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



Content

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台冗余后背
- 单机最高32Gbps吞吐
- 10Gbps硬件DDoS安全防御
- 850+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

成功案例-马来西亚肯德基

挑战

- ✓ 门店分散，互联网接入安全风险高
- ✓ 服务响应要求快

特点

- ✓ 高性能、3G灵活接入
- ✓ 安全、灵活的VPN特性
- ✓ 多业务融合

价值

- ✓ 最佳性价比的高品质解决方案

Huawei Enterprise A Better Way