HUAWEI ENTERPRISE A BETTER WAY

未雨绸缪、主动防御
外部边界和内网安全一体化解决方案

华为USG2200TSM终端安全一体机主打胶片

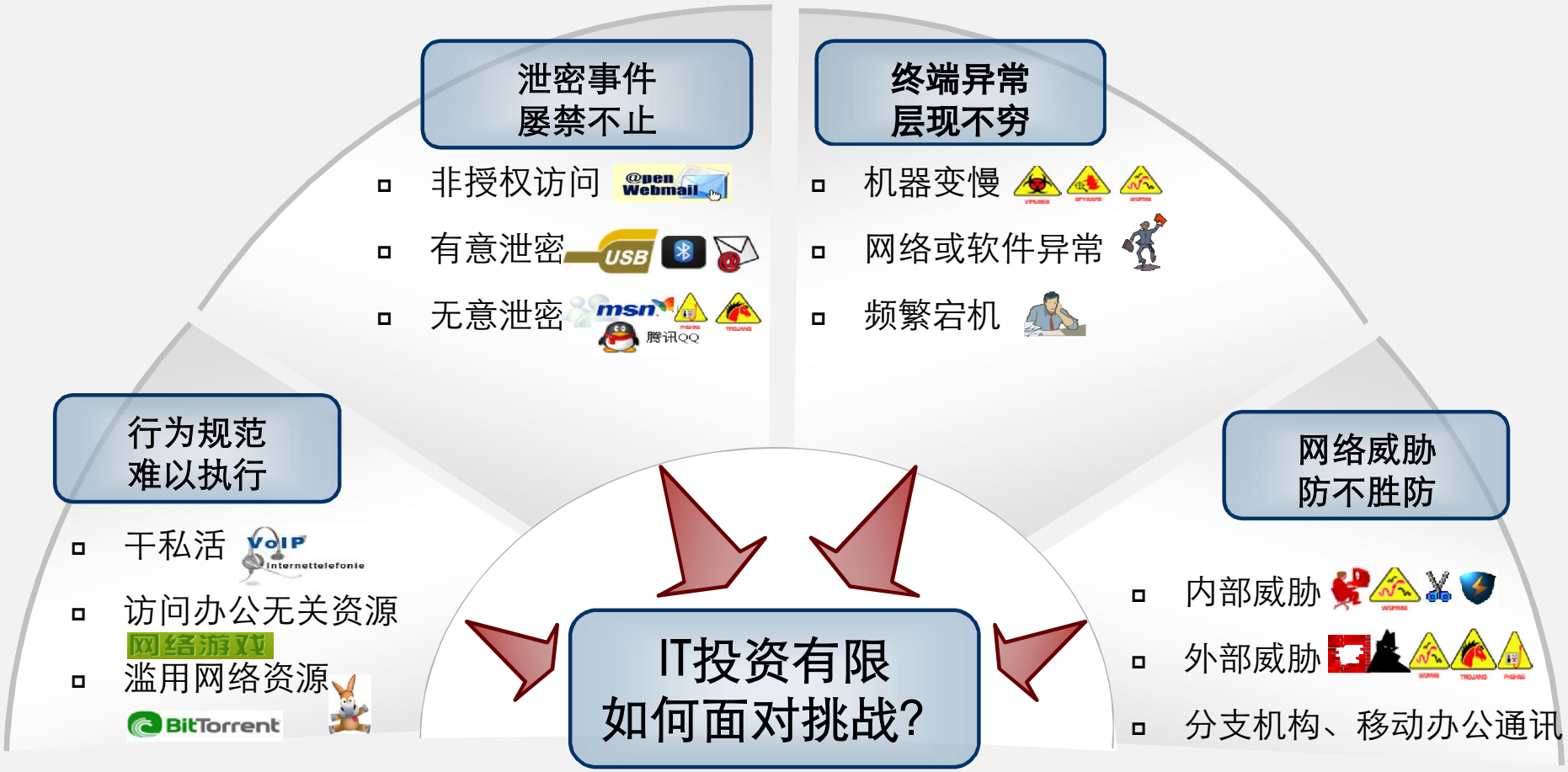
enterprise.huawei.com

HUAWEI TECHNOLOGIES CO., LTD.

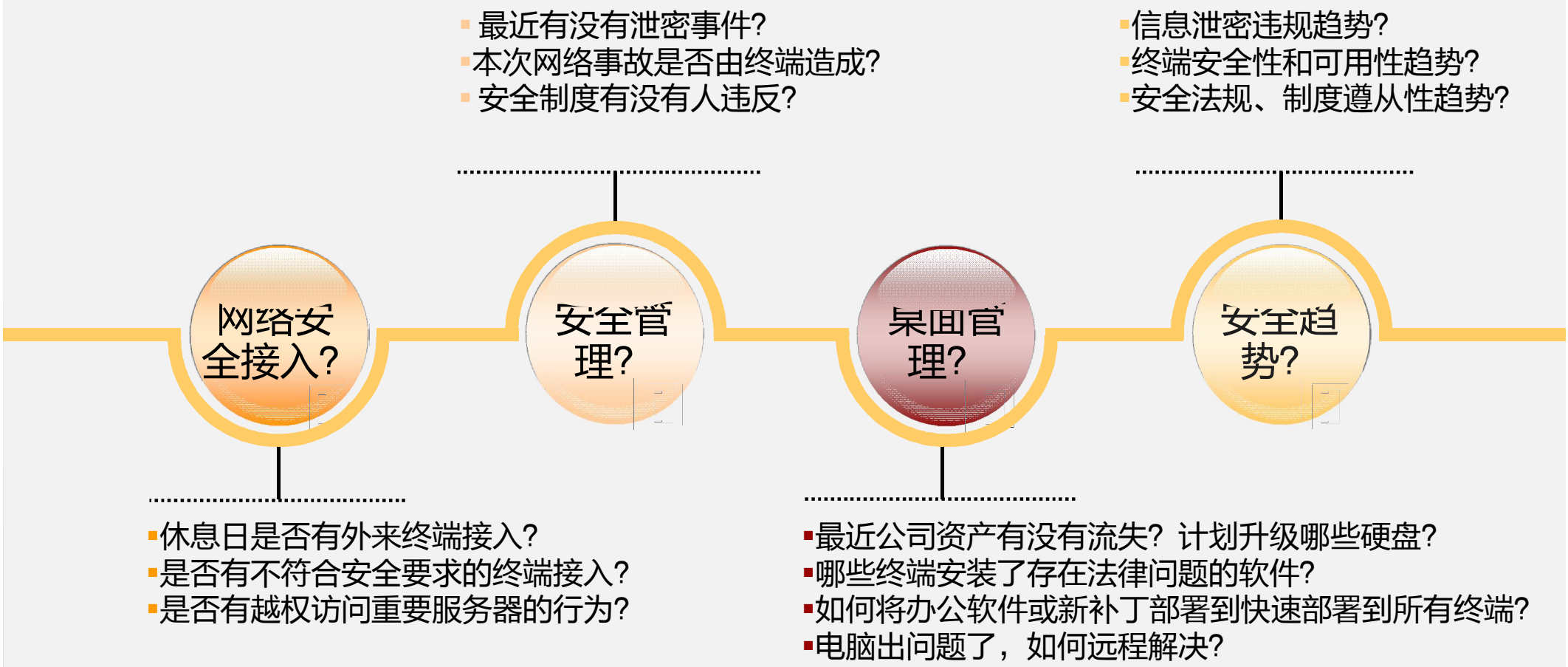
HUAWEI

Content

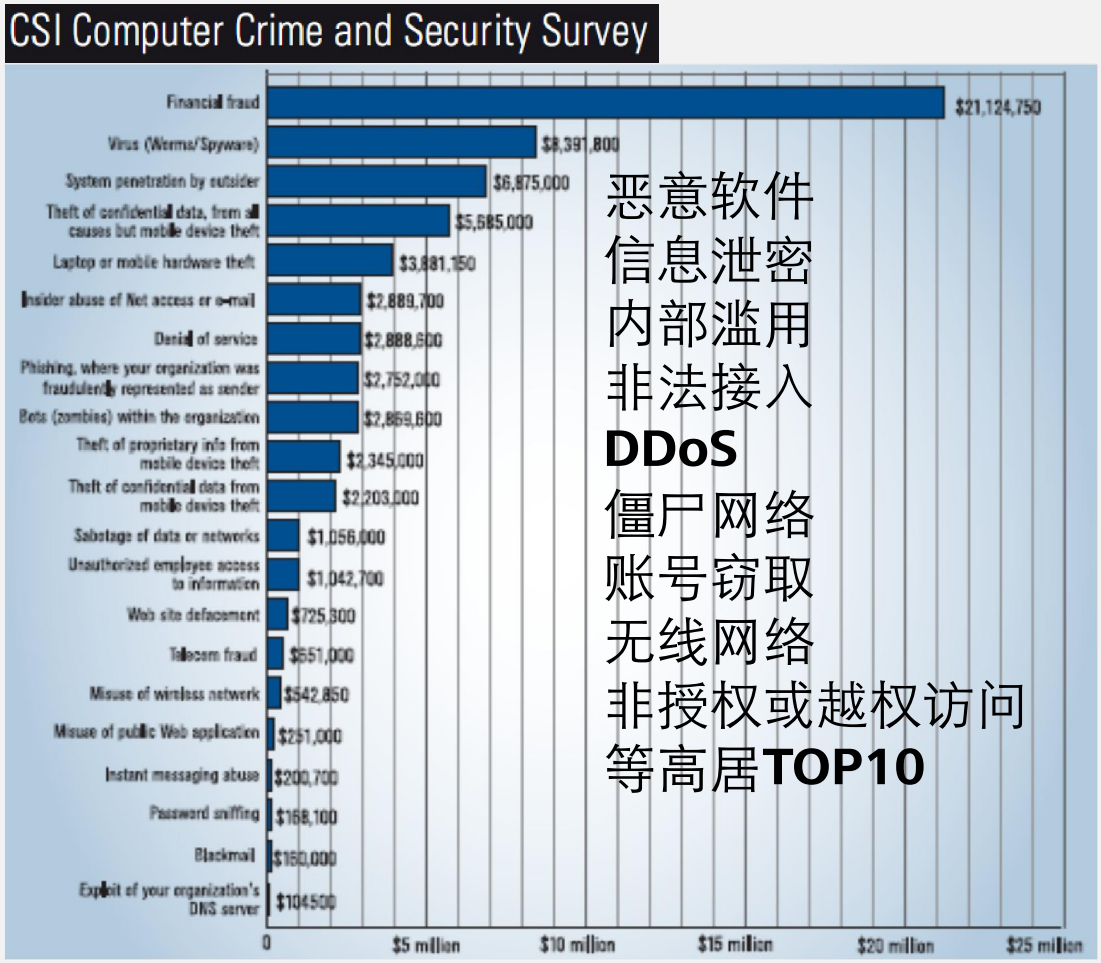
企业网络安全危机四伏


泄密事件
屡禁不止
非授权访问
有意泄密
无意泄密
终端异常
层现不穷
机器变慢
网络或软件异常
频繁宕机
行为规范
难以执行
干私活
访问办公无关资源
滥用网络资源
网络威胁
防不胜防
内部威胁
外部威胁
分支机构、移动办公通讯
IT投资有限
如何面对挑战?

内网安全状况无法统一掌控



美国CSI计算机安全方面的调查



恶意软件
信息泄密
内部滥用
非法接入
DDoS
僵尸网络
账号窃取
无线网络
非授权或越权访问
等高居**TOP10**

CSI COMPUTER SECURITY INSTITUTE

根据加利福尼亚州旧金山的计算机安全协会(CSI)的观点，
大约60%到80%的网络滥用事件起源于内部网络。

- 威胁不仅仅来自于外部，内部威胁损失更加严重
- 如何从容应对如此众多的威胁， 成为困扰CTO们的难题

HUAWEI

Content

安全一体机的解决思路

USG2200

- **防火墙**

  NAT/包过滤/安全域/ASPF/攻击防范

  有效阻止威胁扩散

- **VPN**

  L2TP/GRE/IPSEC

  构建安全的数据传输通道

- **流量控制和QoS**

  支持P2P/IM/IP-CAR/QoS

  …

TSM

- **提供完整的终端安全解决方案**

  支持准入控制、安全管理、桌面管理，确保入网终端安全、合规、受控，降低企业IT风险、提升IT效率、降低IT成本

  …

整合、优化、集成

- 借助防火墙和VPN，抵御外部威胁和内部攻击，确保移动办公安全性
- 借助准入控制、安全管理和桌面管理，提升终端防御能力，确保终端不成为攻击源

内网安全的解决思路

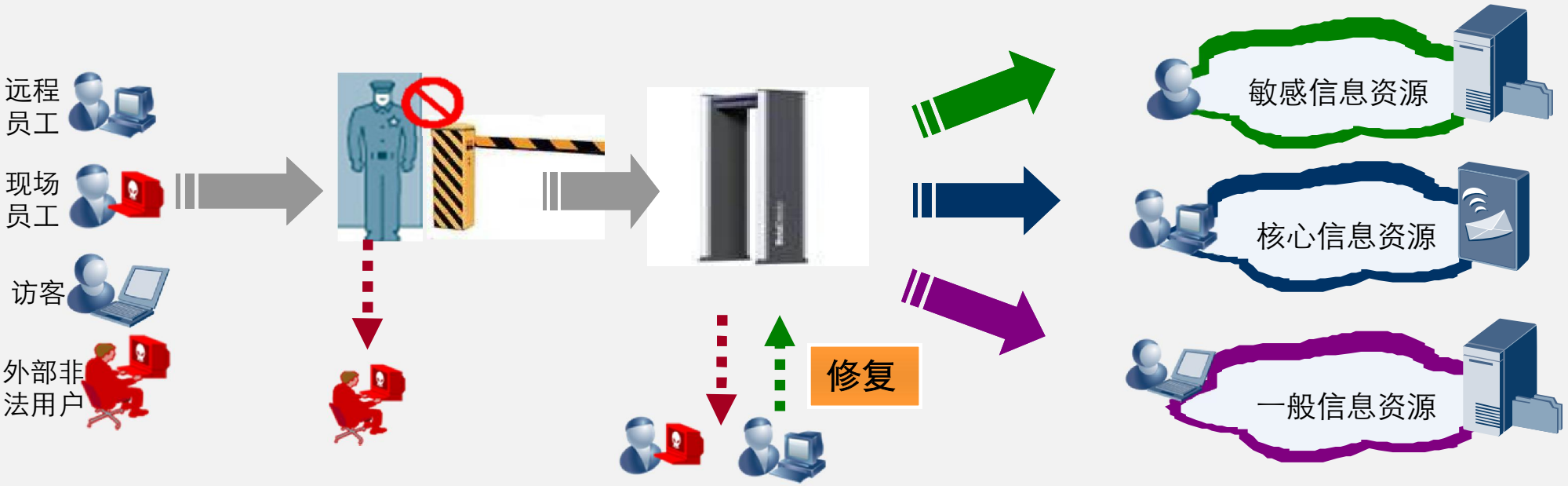
- 以网络身份识别为基础，以准入控制为手段，以桌面管理为补充，构建一体化的内网安全解决方案
- 主动防御，从源头消除漏洞和威胁；确保终端合规、受控

HUAWEI

终端安全管理设计思路

策略 → 身份认证 → 安全检查 → 修复

安全检查 → 授权访问 → 监控 → 响应 → 审计



阻止非授权用户

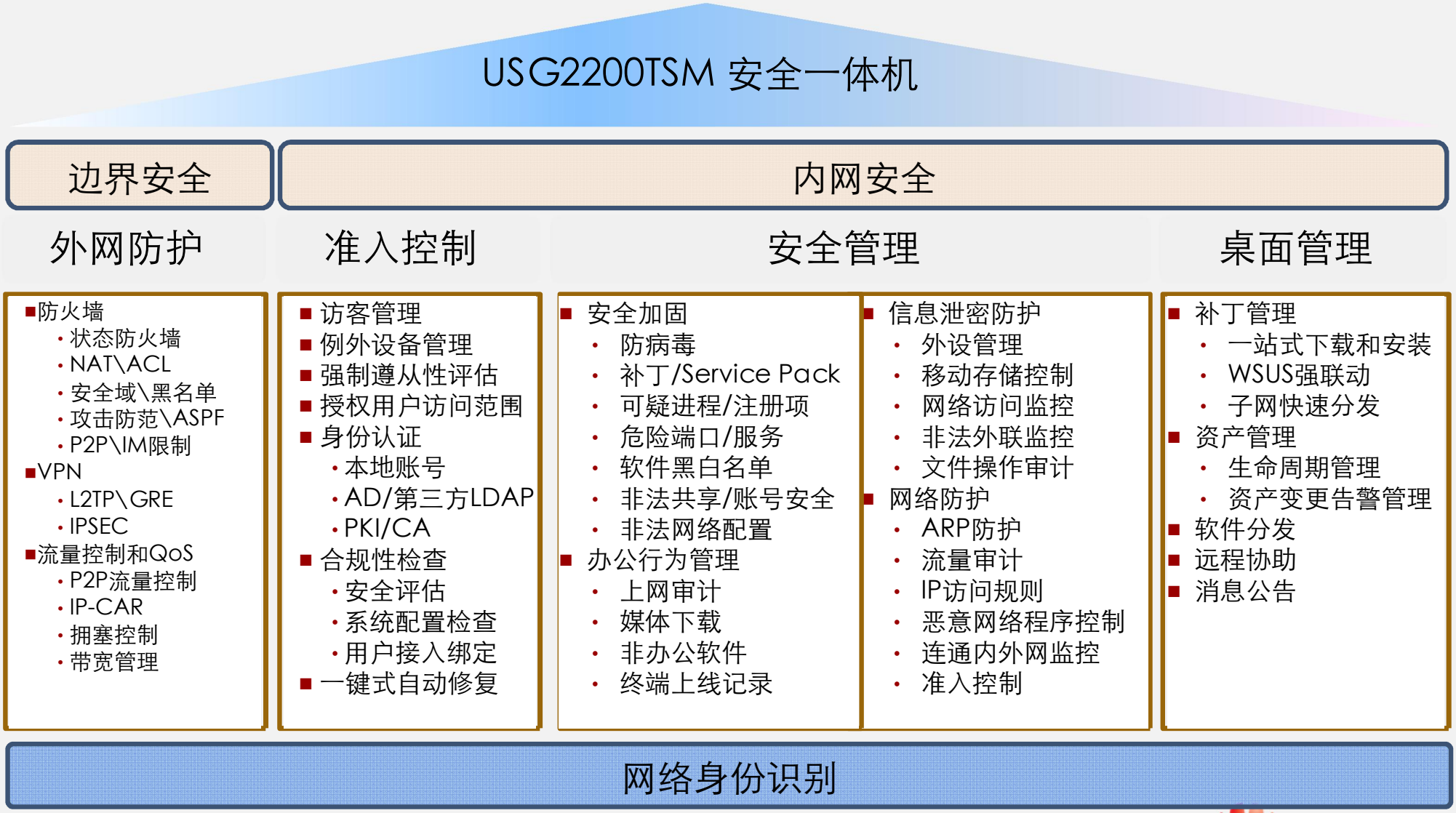
隔离修复不安全用户

授权用户访问范围

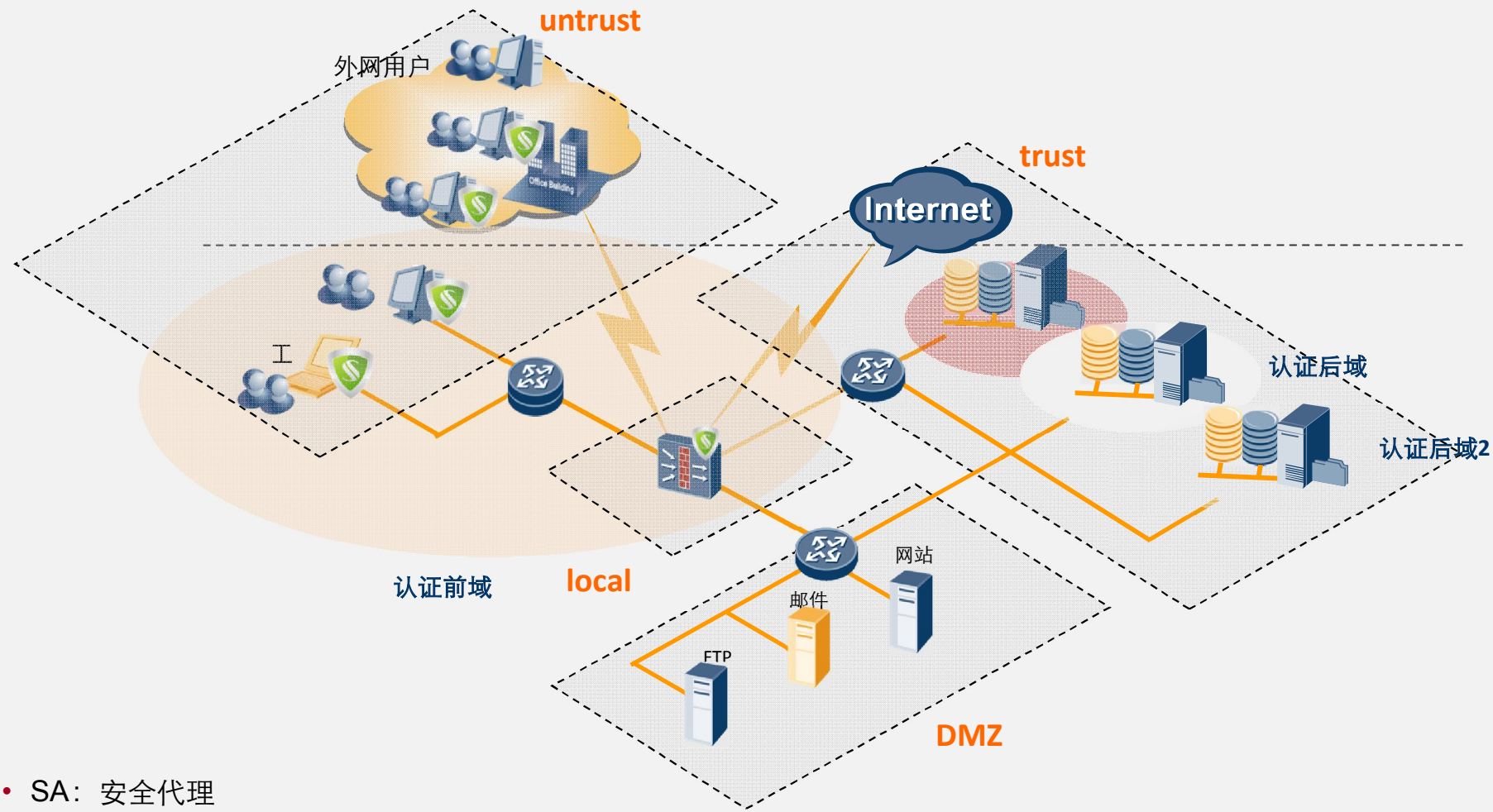
监控行为审计取证

Content

安全一体机功能架构

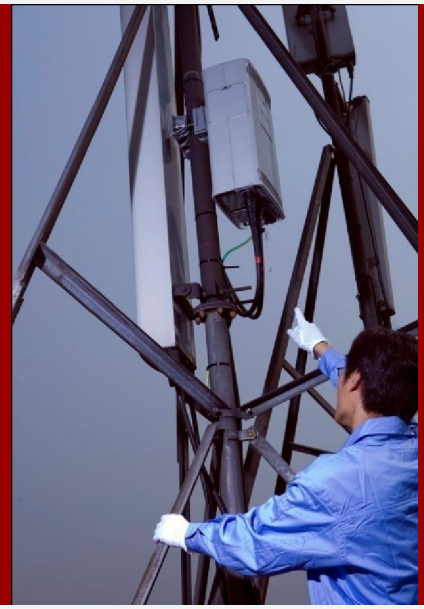


安全一体机系统组成

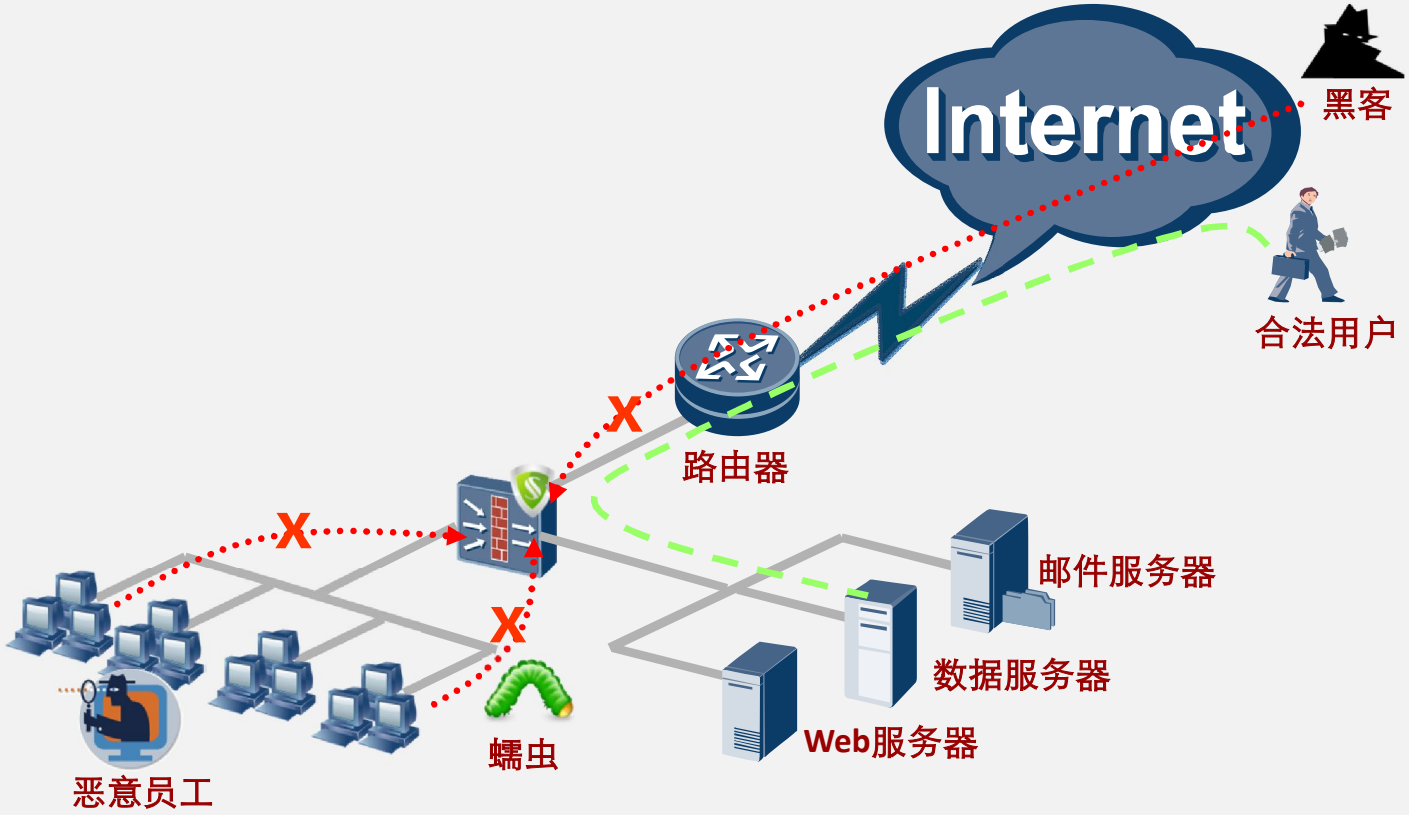


- SA：安全代理

消除内外网威胁，构筑安全边界

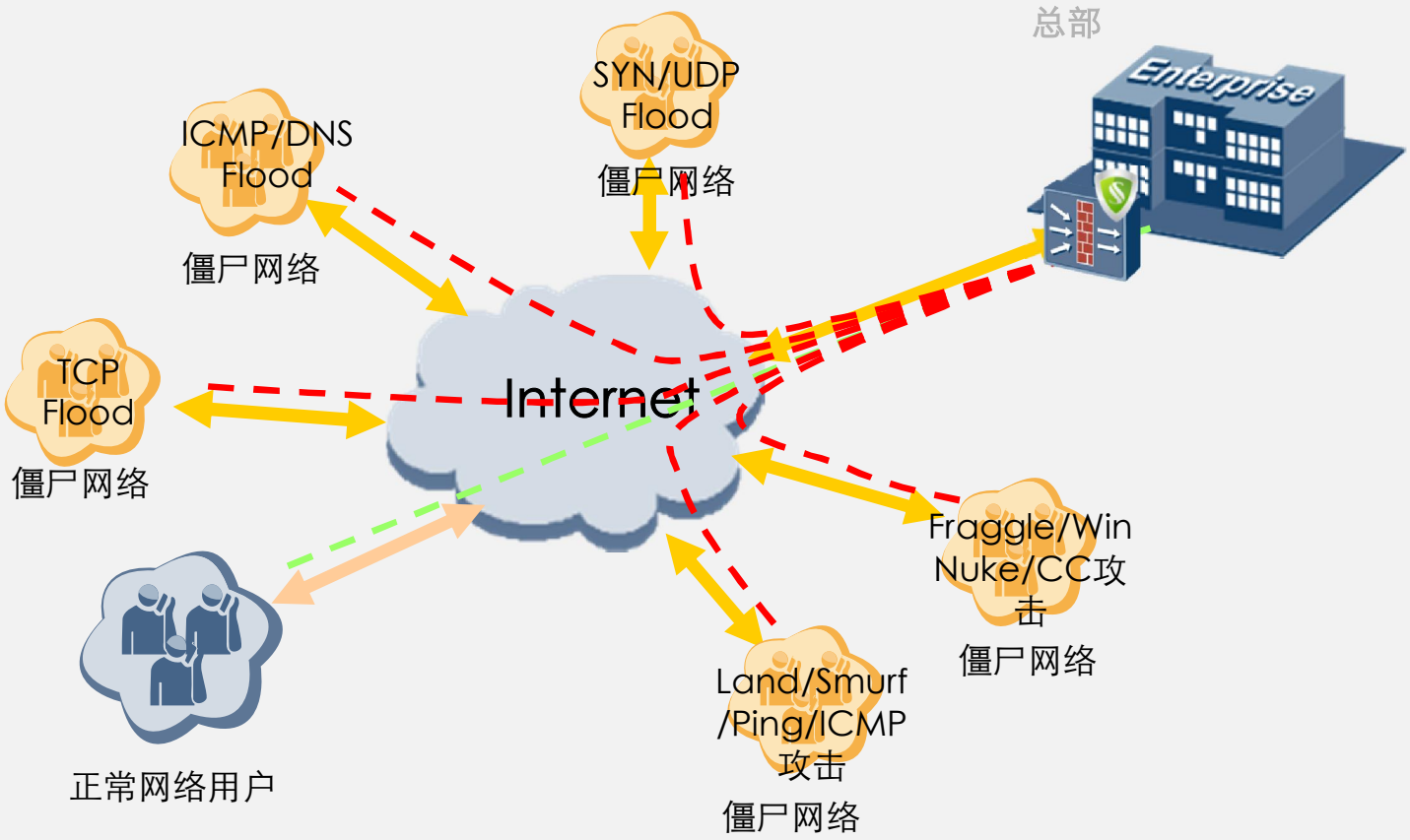


阻断网络入侵和攻击



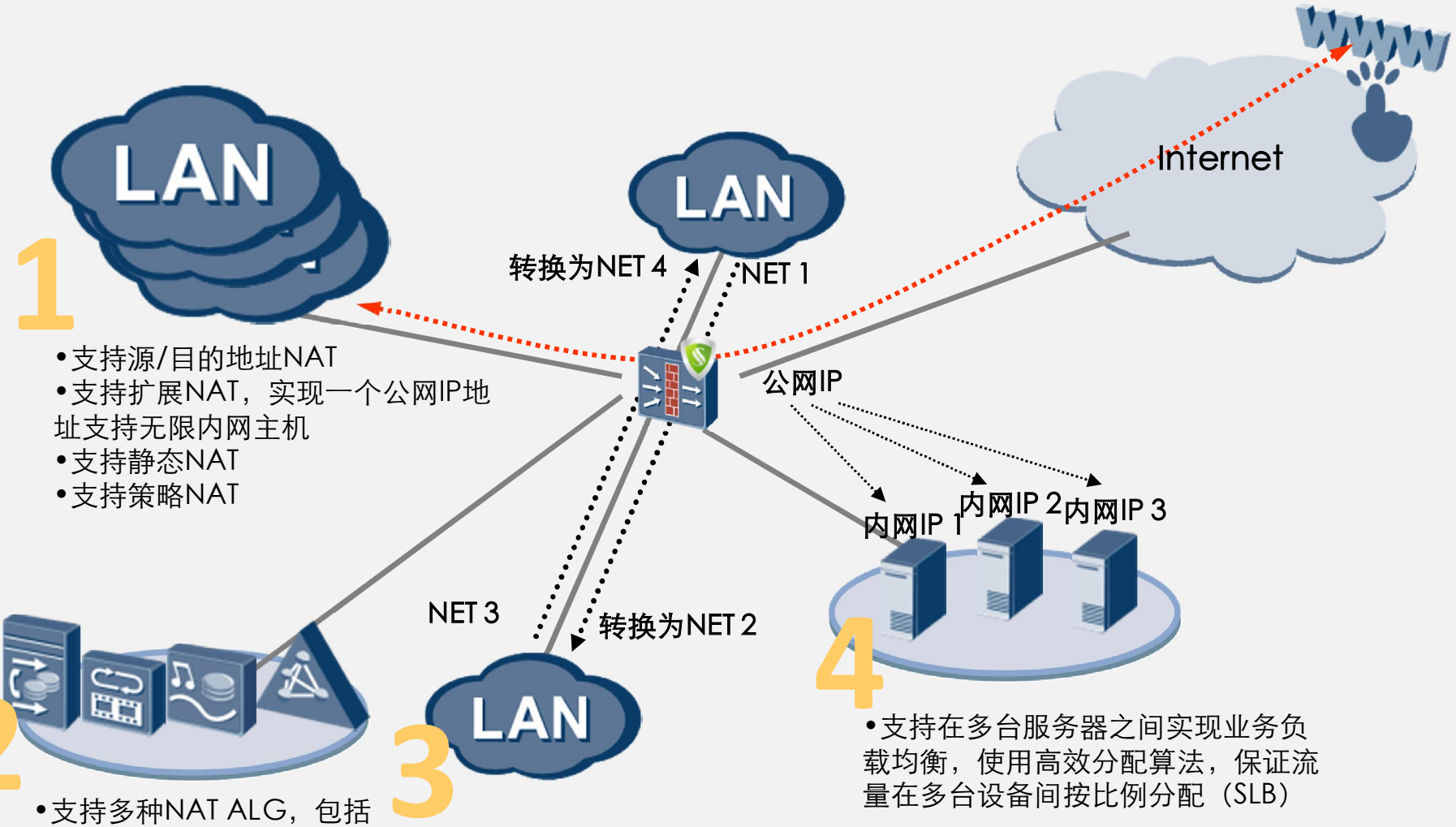
- 防止外部黑客和内部恶意员工针对服务器的入侵和攻击
- 防止蠕虫病毒的传播

强大的DDoS防御能力



- 网络规模和网络带宽不断增加，导致攻击流量指数级增长
- 有效抵御大流量的DDoS攻击，可识别多种攻击类型，轻松应对网络攻击

全面的NAT技术，完备的NAT ALG功能



1

- 支持源/目的地址NAT
- 支持扩展NAT，实现一个公网IP地址支持无限内网主机
- 支持静态NAT
- 支持策略NAT

2

- 支持多种NAT ALG，包括FTP、RAS、H323、QQ、MSN、MGCP、SIP、TFTP、RTSP、PPTP、HWCC、Netbios、用户自定义等

3

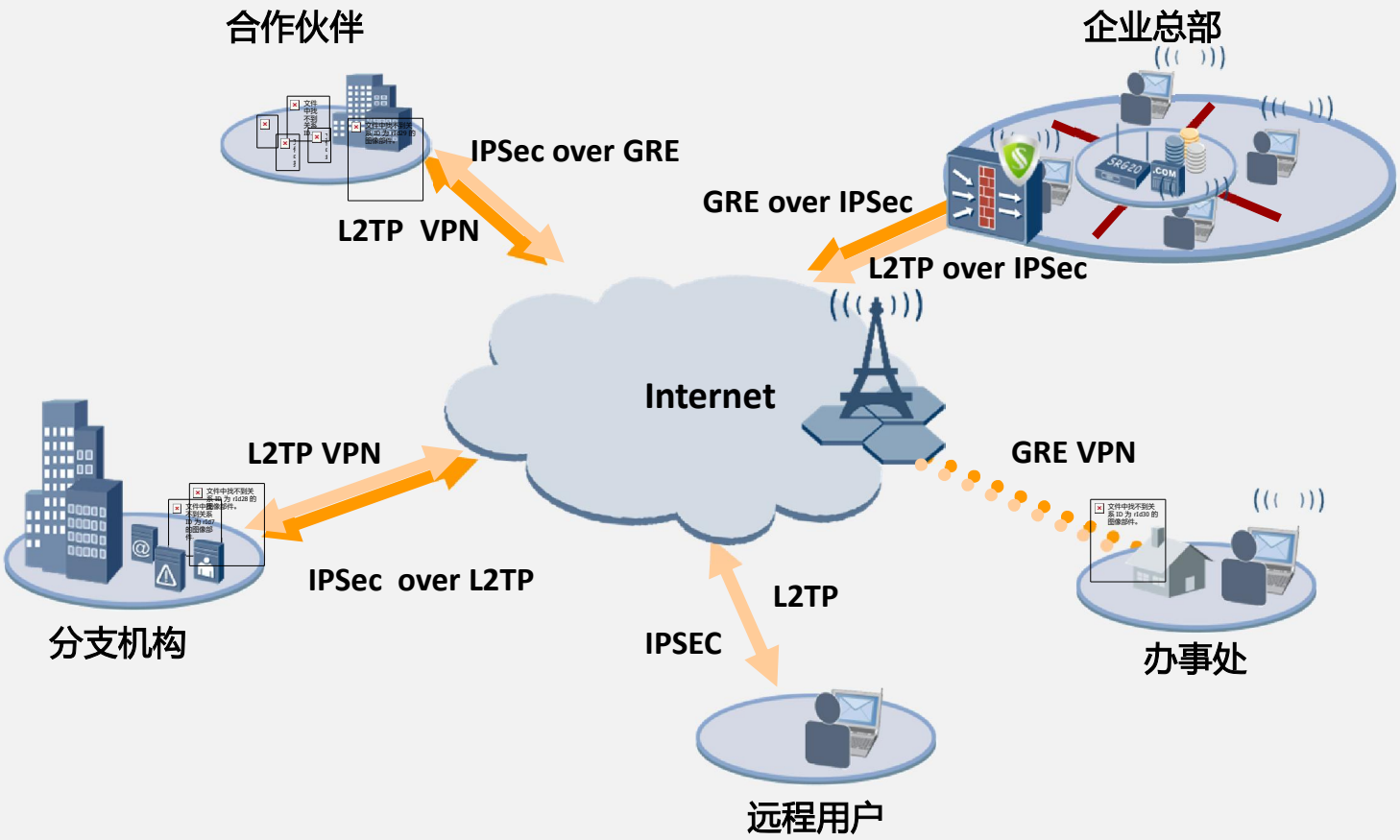
- 支持双向NAT，实现两侧网络同时转换

4

- 支持在多台服务器之间实现业务负载均衡，使用高效分配算法，保证流量在多台设备间按比例分配（SLB）

HUAWEI

丰富的VPN接入方式



- 为高度分散企业网络和远程用户提供安全互联，确保通讯安全
- 支持DES、3DES、AES等多种加密算法，提供高强度传输保障

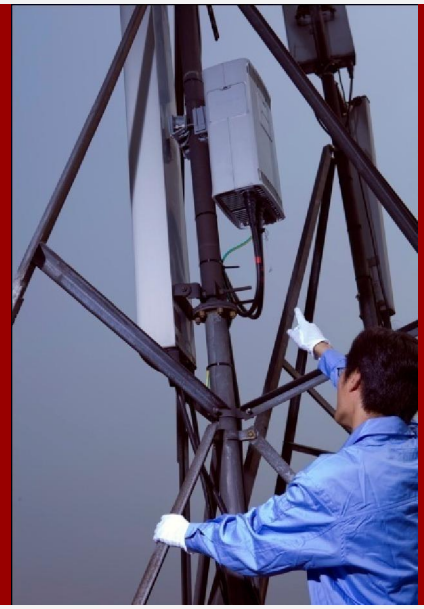
功能强大的P2P/IM阻断和限流功能

X 阻断(IM)

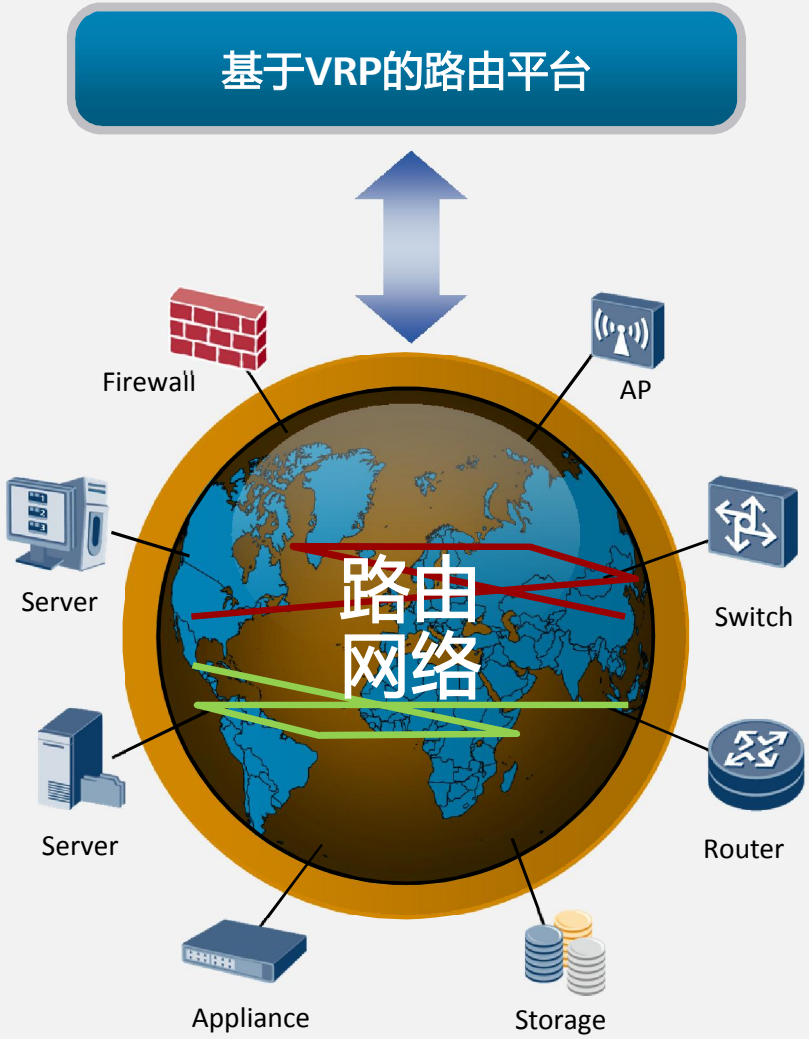
10 限制流量(P2P)

- 先进的P2P/IM检测算法
- 支持丰富的P2P/IM协议，包括QQ，MSN， PPLIVE，PPstream，BT（比特精灵和比特彗星），EDEM（edonkey和emule），UUSee，poco，bbsee，feidian，qqlive，kugoo音乐盒，风行网络电视，PP365，SOPCAST，TVU，PPFILM，QQDownload，迅雷看看等
- 多达7个限流级别，可根据不同ACL范围分别配置不同的限流级别
- 每个限流级别可基于不同时间段进行限流控制
- 完备的P2P流量日志，支持报表统计、审计
- 可结合基于IP的限流达到更好的P2P限流效果

灵活的组网适应能力、无限自由的接入

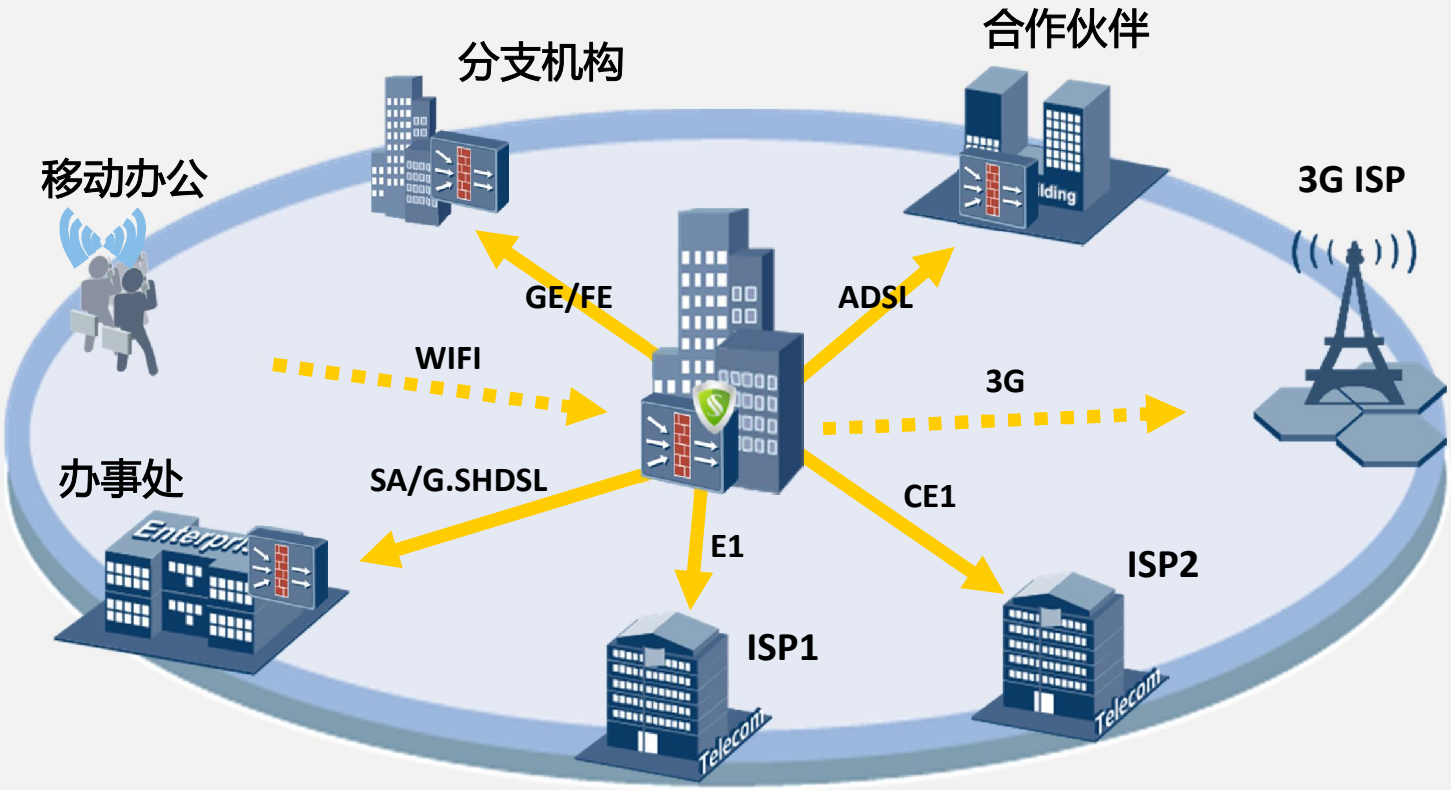


丰富的路由交换特性



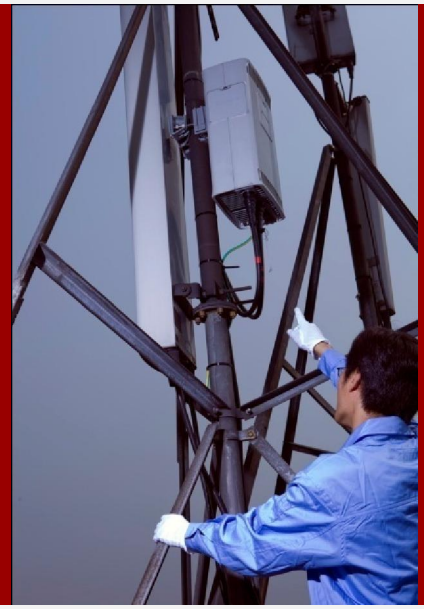
- **静态路由与动态路由**
  - Static/RIPv2/OSPFv2/BGPv4
- **灵活的设置管理**
  - 路由策略&路由迭代&路由管理
- **基于会话流的策略路由**
  - 使得策略路由与安全特性(如NAT、ASPF等)协同工作达到接口级负载分担。当一条链路故障时，流量将切换到其它正常的链路中
- **快速的2层交换**
  - 内置快速2层转发芯片保证快速2层交换能力
  - 通过扩展插槽支持10个二层交换接口，最多提供10个二层下行接口

接口丰富，提供多种互联

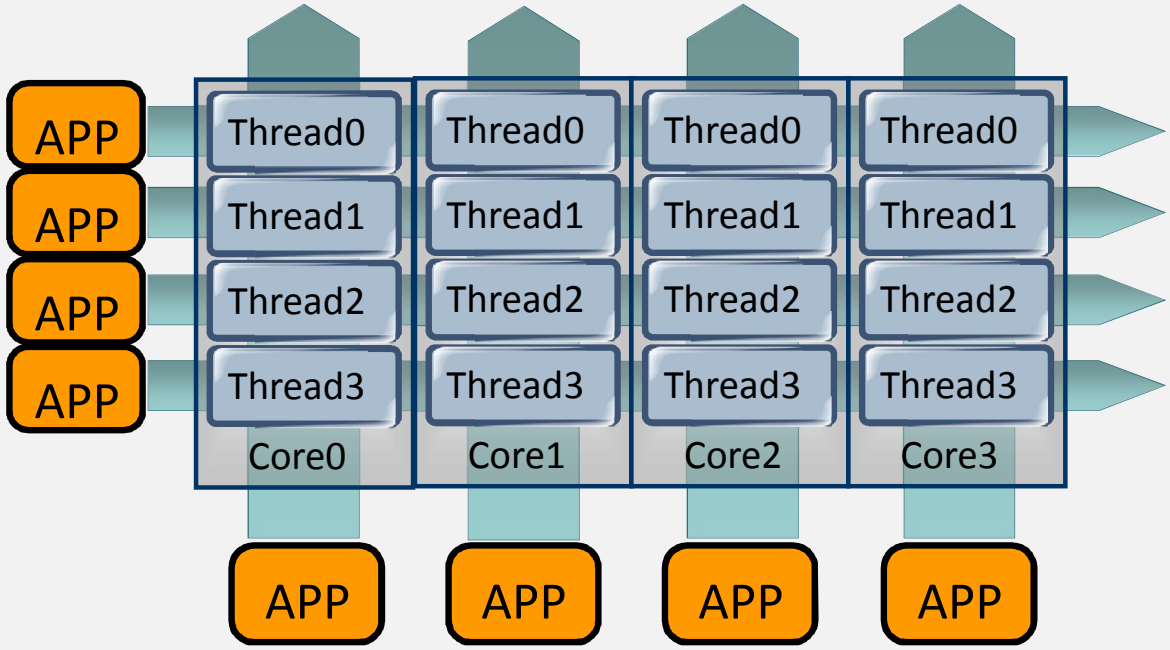


- 多ISP链路支持：多种WAN接口支持以及多种3G技术链路备份使得企业网络能够无损伤的从链路故障中得以恢复
- 方便的业务扩展：丰富的接口类型（LAN\WLAN\WAN\WWAN）使得企业在业务扩展时可以自由选择

电信级专业硬件设备



多核多线程安全平台提升安全性能



领先的架构平台

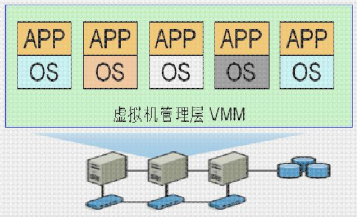
软硬件有机结合

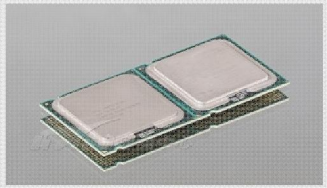
先进多核硬件架构，多线程并行处理与实时多任务安全操作系统VSP完美融合。

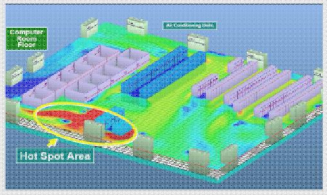
流程优化

优化安全处理流程，特别是针对首包的处理，具备业界第一的每秒新建数。

多核的优势



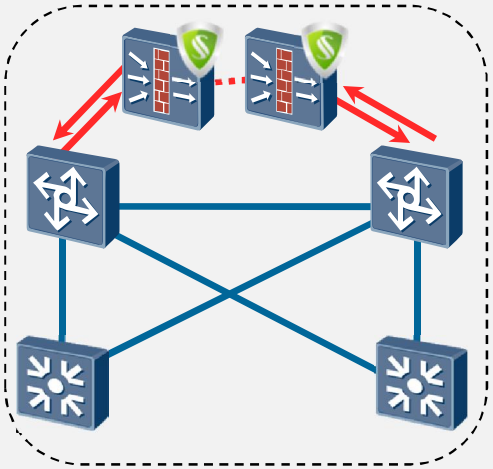




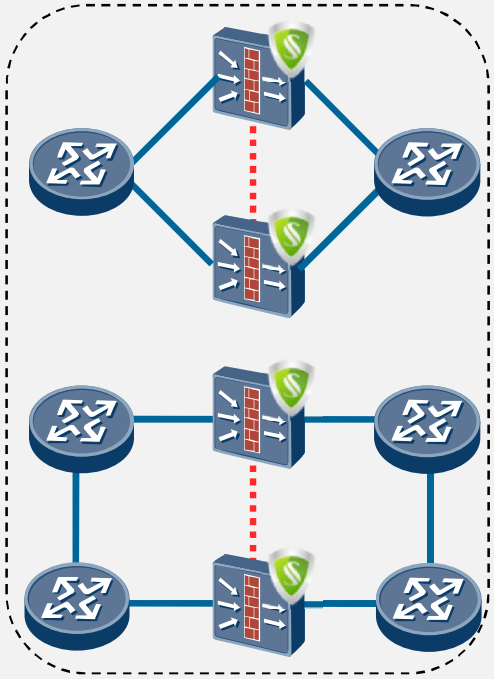
HUAWEI

双机备份提高网络稳定性

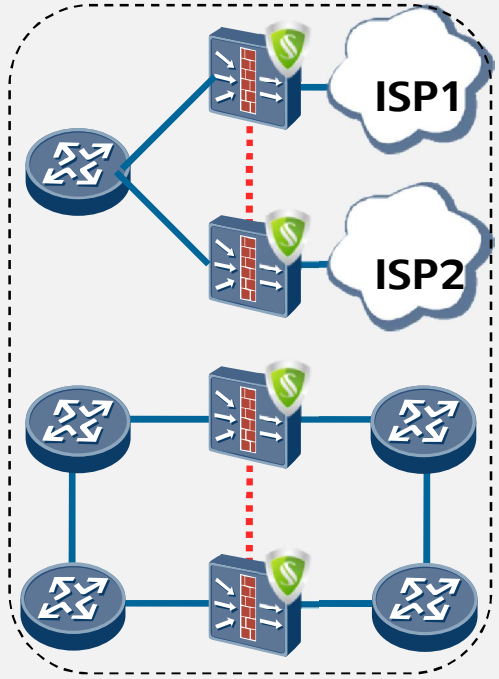
侧挂（路由模式）



直挂（混合模式）



直挂（路由模式）



双机备份特性

- 完善的组网环境适应性
  - 交换、路由环境双机备份
  - 交换、路由混合环境双机备份
- 成熟的链路倒换机制
  - 物理链路触发倒换

最易用、最可靠

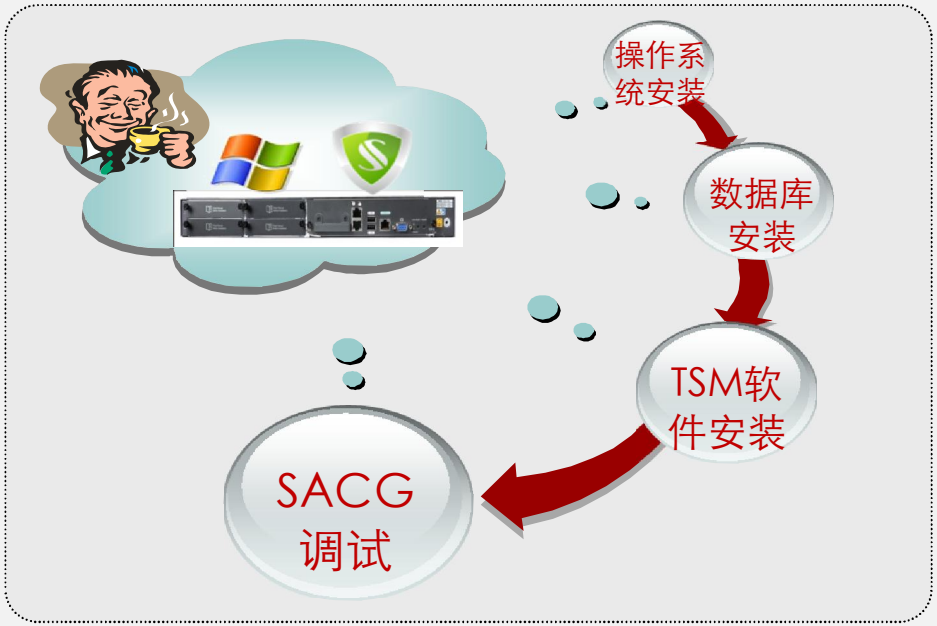
最易用

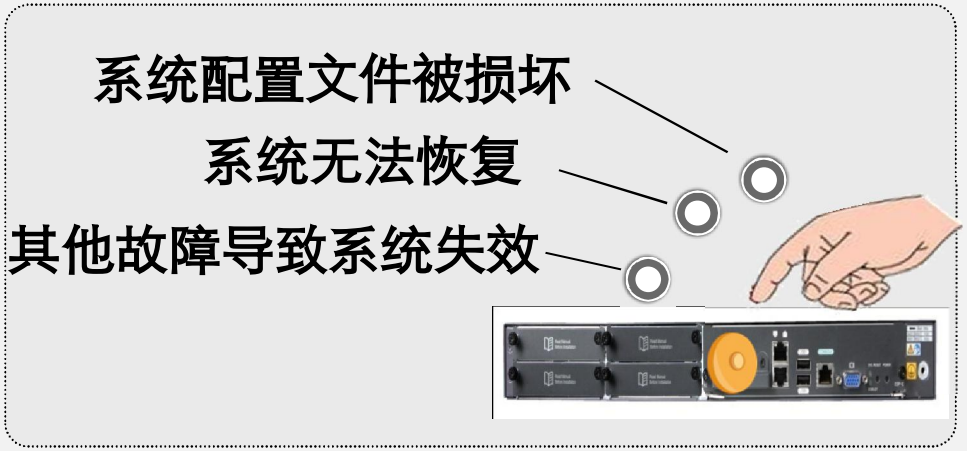
- 上电即部署

  部署简单，出厂时在x86板卡里预装好操作系统、数据库以及TSM服务器，服务器端部署时间降低40%以上

- 开机即使用

  预置策略模板，TSM系统默认配置好“高、中、低”策略模板，免除客户自定义策略的繁琐





最可靠

- 一键备份

  自带CF数据卡，服务器后台自动备份重要数据；

- 一键恢复

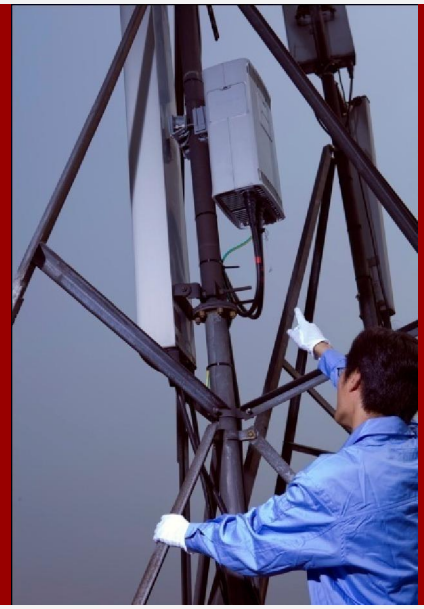
  现场复原管理，Reset按钮一键还原系统；

- 自我监控

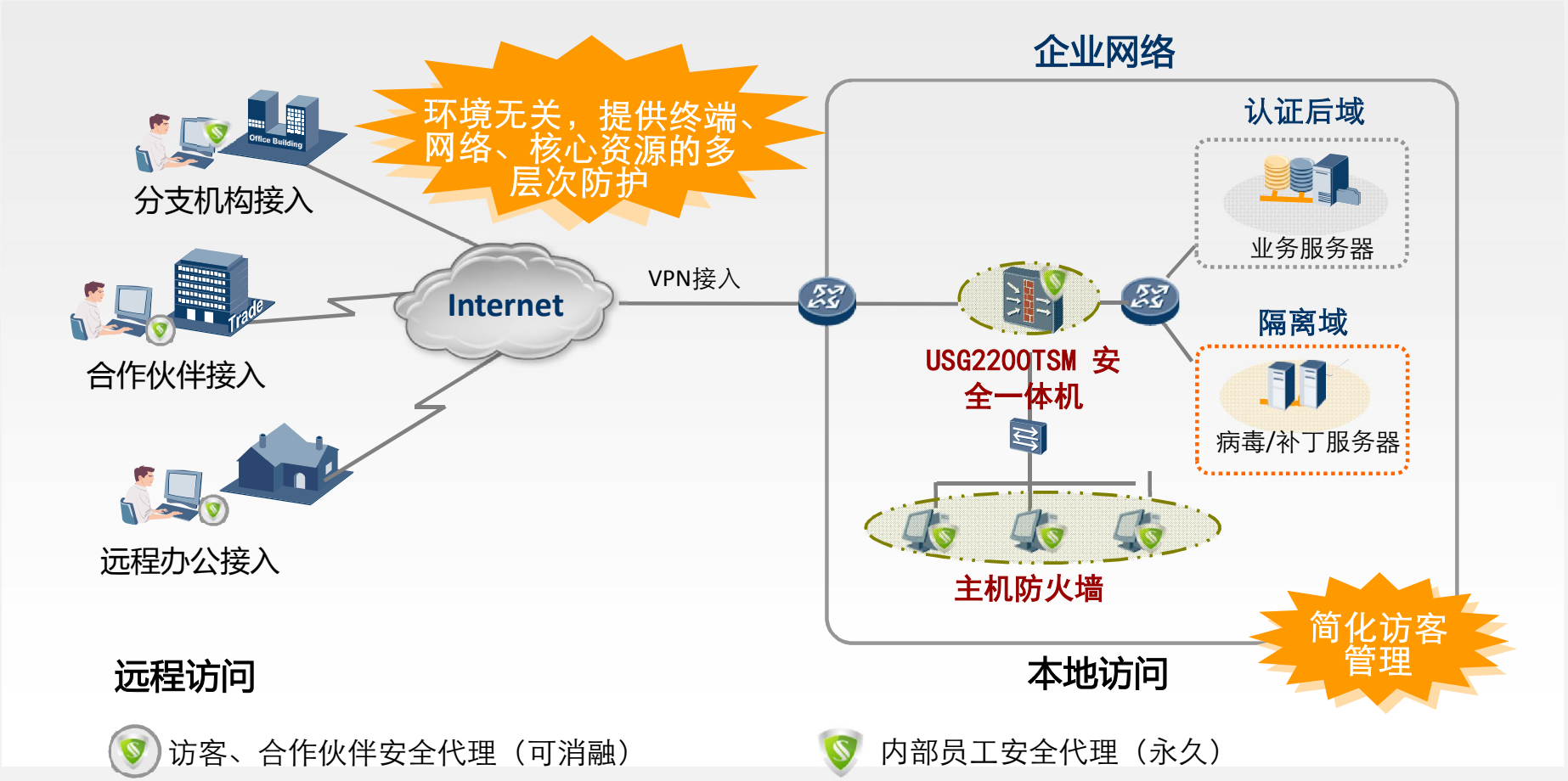
  提前预警、故障报警、自动逃生，最大程度减轻运维压力

HUAWEI

安全可靠、易于部署和管理的准入控制技术

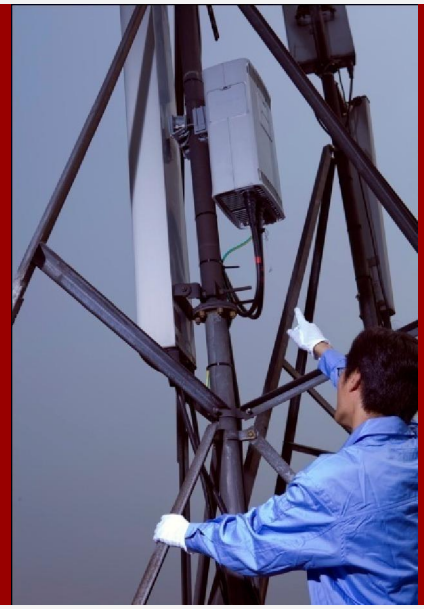


安全可靠、易于部署和管理的准入控制技术



- 专用硬件方案，环境适应性强
- 部署维护成本最低：集中管理，快速部署
- 管理力度强：可强制安装客户端
- 场景支持好：支持各种接入方式
- 可靠性高：设备冗余、自动逃生
- 控制灵活：可以细分服务器访问权限

强制评估遵从性，提升内网安全性和可用性



确保接入终端满足企业要求

合规性检查 | 一键式自动修复

财务部

严格

财务部安全检查策略模板

- ✗ 检查防病毒软件
- ✓ 检查补丁/Service Pack
- ✗ 检查可疑注册项/进程
- ✗ 检查软件黑白名单
- ✓ 检查非法端口使用
- ✓ 检查开启不安全服务
- ✓ 检查非法共享
- ✗ 检查账号安全性
- ……
- ✓ 强制DHCP
- ✓ 同时使用多网卡
- ✓ 用户接入绑定

认证后域

安检不通过
禁止接入网络

SM

产生违规接入记录

总裁办

宽松

总裁办安全检查策略模板

- ✓ 检查防病毒软件
- ✓ 检查补丁

认证后域

安检通过
授权接入网络

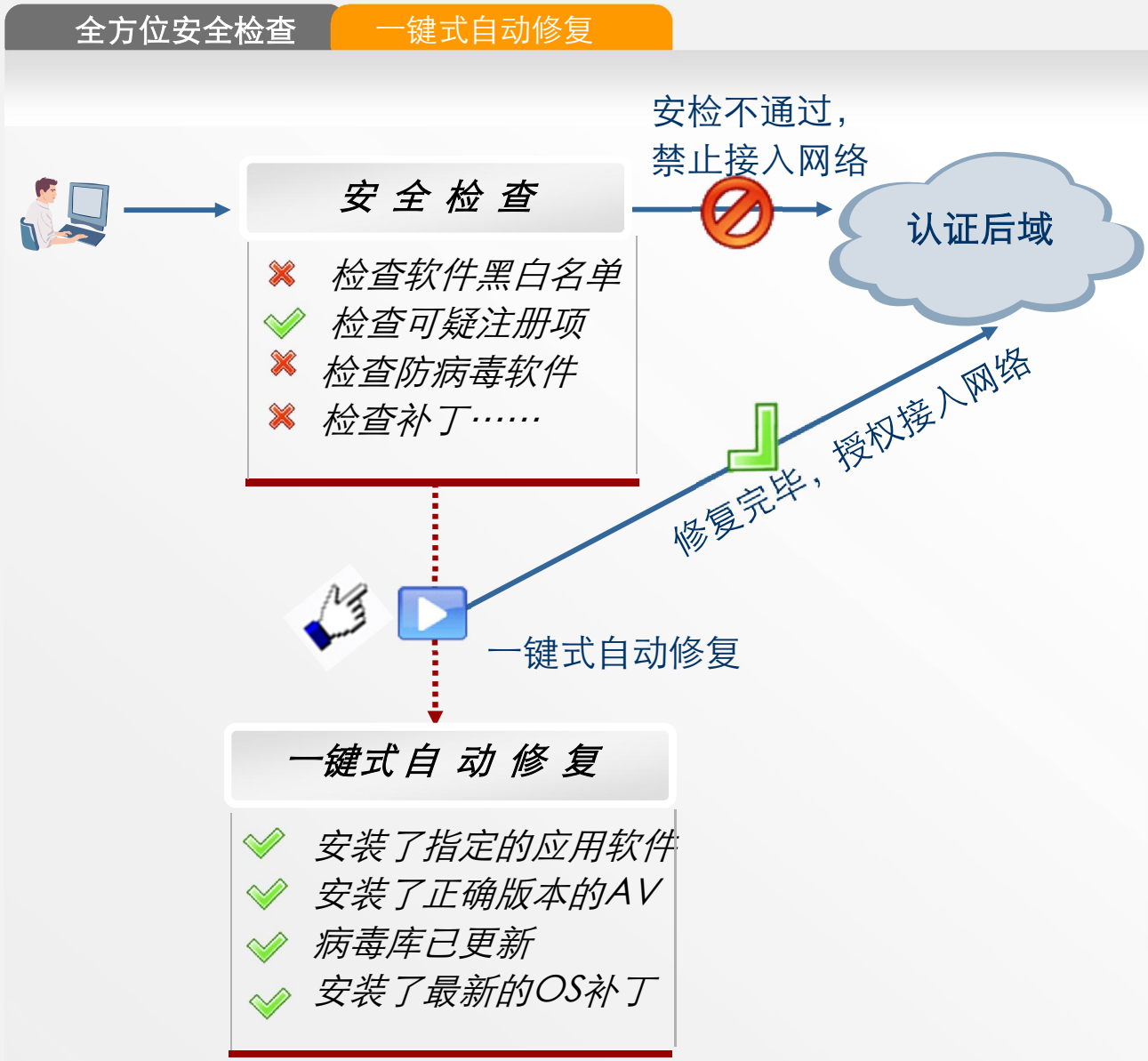
业界最丰富的安全检查策略，强制终端遵从

- 保护AV等安全产品的投资价值
- 减少恶意代码传播，提升资源可用性，减少服务中断风险
- 减少信息泄密风险
- 降低终端威胁网络的风险
- 提供准确实时的企业遵从信息

量体裁衣，基于角色的动态策略控制

- 基于用户角色或部门自定义不同安全规则，针对不同点控制点采取不同安全策略
- 支持企业安全管理制度的演进

降低终端管理维护成本



一键式智能自动修复，实现终端自我管理

- 自动部署指定版本的防病毒软件
- 防病毒软件强联动，自动更新病毒库
- 自动修复补丁
- 根据链接指导安装指定备软件
- 注册表键值自动修复
- 屏保设置自动修复
- 共享目录自动删除
- ……

规范终端行为，创造合规价值

提升效率、降低病毒感染风险

规范行为 | 信息泄密防护

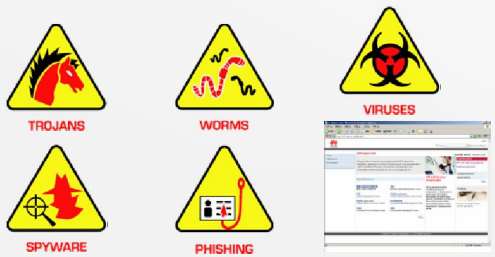
控制非办公软件使用

控制各类IM、炒股、网游、媒体下载

行为管理

- 实时阻断
- 40 限速
- 基于时间阻断
- 事后审计

控制Web访问



- 过滤各种恶意、可疑网站URL

HUAWEI

降低信息泄密和病毒感染风险

规范行为 | 信息泄密防护

移动存储控制

文件操作

- 增加、删除、编辑、复制、重命名操作监控
- 选择指定文件或动作监控

控制各类 IM、P2P软件

信息泄密防护

准入控制

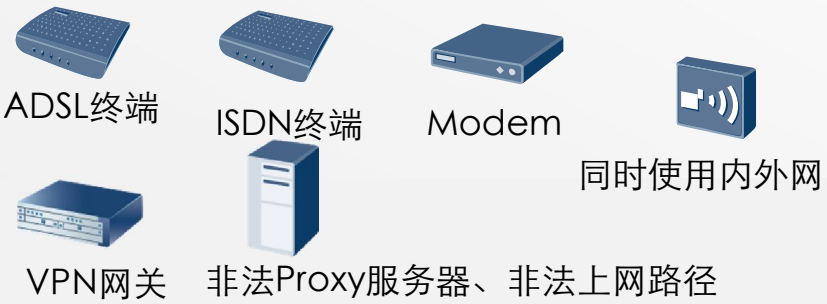
- 身份认证和合规性检查
- 杜绝访客、不安全终端、无权用户非法访问

网络程序、网络流量控制和审计

- 基于协议的监控
- 基于端口的监控
- 基于网络程序的监控

外设接口管理

控制各种非法外联行为



HUAWEI

消除内部威胁、构建绿色网络

降低入网设备对网络的威胁

网络接入防护 | 终端网络异常检测

网络安全准入控制

禁止接入网络

安全检查

- ✗ 检查防病毒软件
- ✓ 检查补丁/ Service Pack
- ✗ 检查可疑注册项/进程
- ✗ 检查软件黑白名单
- ✓ 检查非法端口使用
- ✓ 检查开启不安全服务
- ✓ 检查非法共享
- ✗ 检查账号安全性
- ……
- ✓ 强制DHCP
- ✓ 同时使用多网卡
- ✓ 用户接入绑定

财务人员

财务部检查策略

- ✓ 检查防病毒软件
- ✓ 检查补丁

安检通过，授权访问财务资源

财务资源

研发资源

- 实时阻断
- 基于时间阻断
- 事后审计

HUAWEI

杜绝终端攻击网络

网络接入防护 | 终端网络异常检测

终端网络异常检测

攻击防范

- ARP攻击检测
- ARP攻击防护
- 防范蠕虫病毒
- 防范 food\单包\tcp全连接等攻击
- 防范扫描窥探攻击
- 防范其它攻击

控制大流量下载

BitTorrent BitComet skype

网络程序、网络流量控制和审计

- 基于协议的监控
- 基于端口的监控
- 基于网络程序的监控

同时使用内外网

同时使用内外网

控制恶意Web访问、IP访问

TROJANS WORMS VIRUSES SPYWARE PHISHING

SMTP,HTTP,TELNET,FTP,
NETBIOS控制

- 过滤各种恶意、可疑网站URL
- 配置主机防火墙IP规则，控制终端上、下行访问

实时阻断 40 限速
基于时间阻断
事后审计

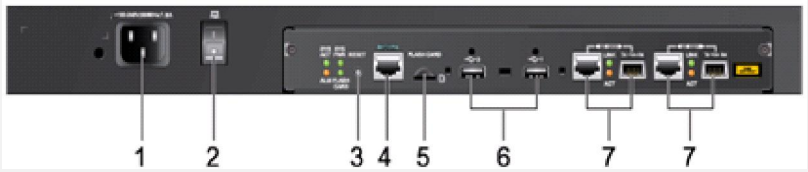
HUAWEI

产品规格介绍

USG2200TSM 安全一体机 整体概览

整体规格	USG2200TSM 安全一体机500	EUSG2200TSM 安全一体机1000
支持终端数	500个	1000个
固定WAN	2*GE Combo	
扩展插槽	4MIC	
WAN接口种类	FE, GE, ADSL2+, G. SHDSL, E1/CE1, SA, 3G	
WiFi功能	支持	
3G功能	支持	
USB接口	2 (v2.0)	
尺寸	1RU	

USG2200TSM 安全一体机前面板



1.交流电源插孔	2.电源开关	3.一键恢复	4. Console接口
5.闪存接口	6. USB2.0接口	7. GE Combo接口	

USG2200TSM 安全一体机后面板

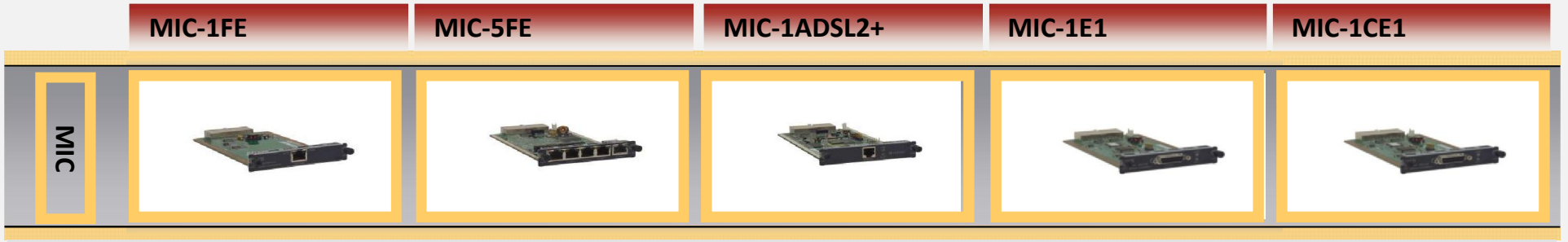
1/3. MIC插槽	2/4. MIC插槽	5. 2*FE
8. VAG口	7. Console口	6. 2*USB

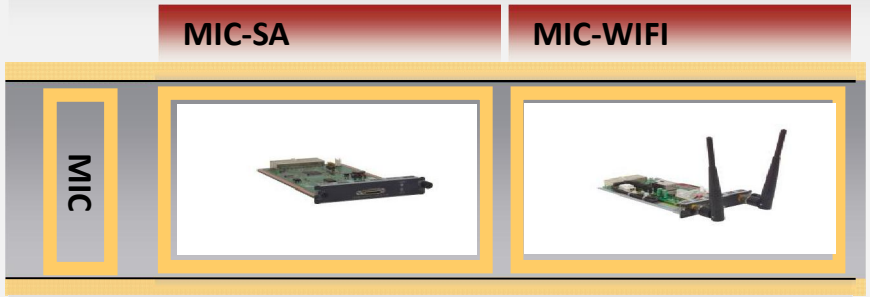
HUAWEI

USG2200TSM 安全一体机特性参数

特性/产品	USG2200TSM 安全一体机500	USG2200TSM 安全一体机1000
最大吞吐量(bps)	600M	1G
VPN吞吐量(bps)	350M	500M
最大并发连接数	1,000,000	1,000,000
最大新建连接数	20,000	20,000
高可用性	主-主/主-备	
最大功率	100W	100W
电源模块	AC：100～240V 1.5A 50/60Hz	

可扩展硬件模块（按需选购）





MIC/USB		USG2200TSM 安全一体机
MIC	1ADSL over POTS	☑
	1/2/4G.SHDSL	☑
	1E1/CE1	☑
	1FE(WAN)/5FE(LAN)	☑
	5FSW	☑
	1/2SA	☑
	3G	☑
	Wi-Fi	☑

硬件规格

软件功能		USG2200TSM 安全一体机
交换	VLAN	☑
	端口隔离	☑
	端口镜像	☑
路由	静态路由	☑
	RIP/OSPF/BGP	☑
	策略路由/路由策略	☑
安全	NAT/NAT ALG	☑
	包过滤	☑
	安全域	☑
	黑名单	☑
	攻击防范\ASPF	☑
	P2P/IM	☑
SACG	SACG	☑
VPN	L2TP	☑
	GRE	☑
	IPSec	☑

软件功能		USG2200TSM 安全一体机
流量控制和QoS	P2P流量控制	☑
	IP-CAR	☑
	拥塞控制	☑
	带宽控制	☑

软件规格

软件功能		USG2200TSM 安全一体机
网络身份识别	本地账号	☑
	第三方LDAP	☑
	PKI/CA	☑
准入控制	合规性检查	☑
	授权用户访问范围	☑
	一键式自动修复	☑
安全管理	安全加固	☑
	办公行为管理	☑
	信息外泄防护	☑
	网络防护	☑
桌面管理	补丁管理	☑
	资产生命周期管理	☑
	软件分发	☑
	远程协助	☑
	消息公告	☑

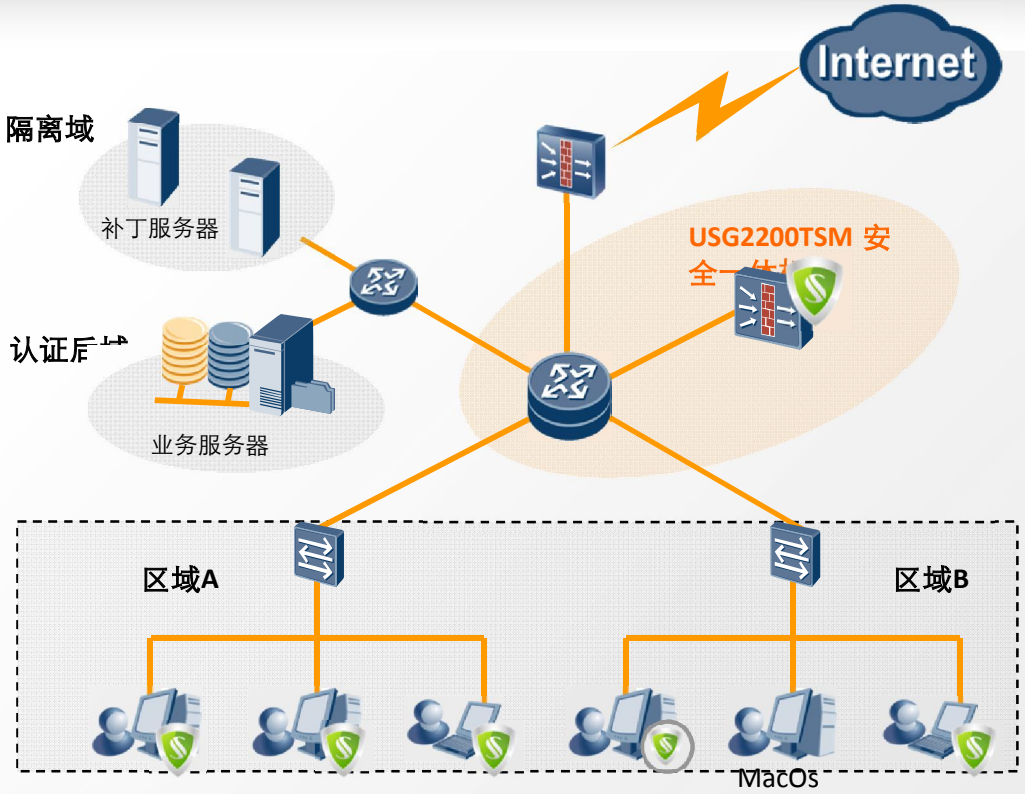
软件功能		USG2200TSM 安全一体机
策略管理	分权分域	☑
	策略模板	☑
可运维报表	预置统计报表	☑
	预置趋势报表	☑
	自定义报表	☑

HUAWEI

灵活部署，方便管理

旁挂核心交换机，组网方便

旁挂核心交换机 | 直挂核心交换机前 | 直挂网络出口 | 分布式部署



客户价值：

- 防止不安全的终端直接访问企业的业务系统和互联网
- 强制终端合规，保护企业业务系统
- 提升网络安全性和可用性
- 提高效率、节约IT预算、保证遵从性

适应场景：

- 组网中存在核心路由器或者核心交换机
- 旁挂设备支持策略路由或者报文重定向
- 选用旁挂方式

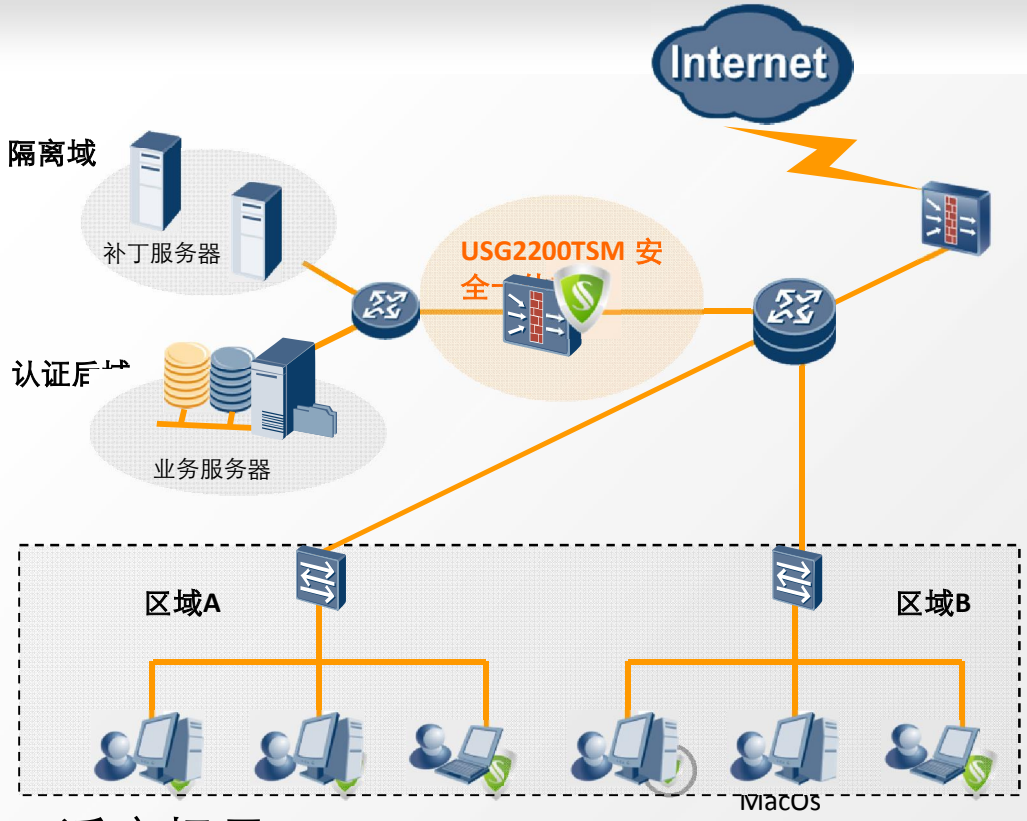
增值特性：

- 黑名单、安全域
- 流量控制和QOS
- 无线接入（外购模块）

HUAWEI

直挂核心交换机前，组网简单、增值应用

旁挂核心交换机 | 直挂核心交换机前 | 直挂网络出口 | 分布式部署



适应场景：

- 组网中存在核心路由器或者核心交换机
- 旁挂设备不支持策略路由或者报文重定向
- 选用直挂方式

客户价值：

- 防止不安全的终端直接访问企业的业务系统
- 强制终端合规，保护企业业务系统
- 提升网络安全性和可用性
- 提高效率、节约IT预算、保证遵从性
- 防止服务器被内外网攻击

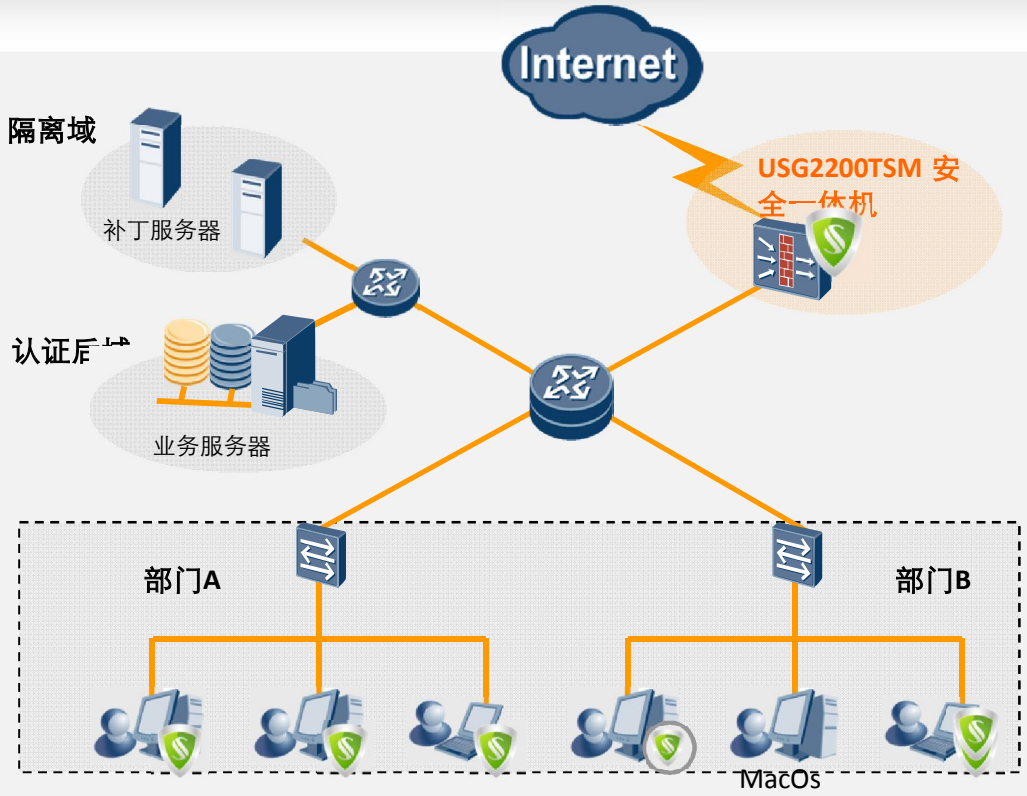
增值特性：

- 黑名单、安全域
- 攻击防范、ASPF
- 端口映射、SLB
- 流量控制和QOS、IPCAR、无线（外购模块）

HUAWEI

直挂在网络出口处，功能强大

旁挂核心交换机 | 直挂核心交换机前 | 直挂网络出口 | 分布式部署



客户价值：

- 防止不安全的终端直接访问互联网
- 强制终端合规，保护企业业务系统
- 提升网络安全性和可用性
- 提高效率、节约IT预算、保证遵从性
- 防止服务器和办公电脑被外网攻击

适应场景：

- 组网中不存在核心路由器或者核心交换机
- 存在统一Internet出口
- 选用透明或路由模式

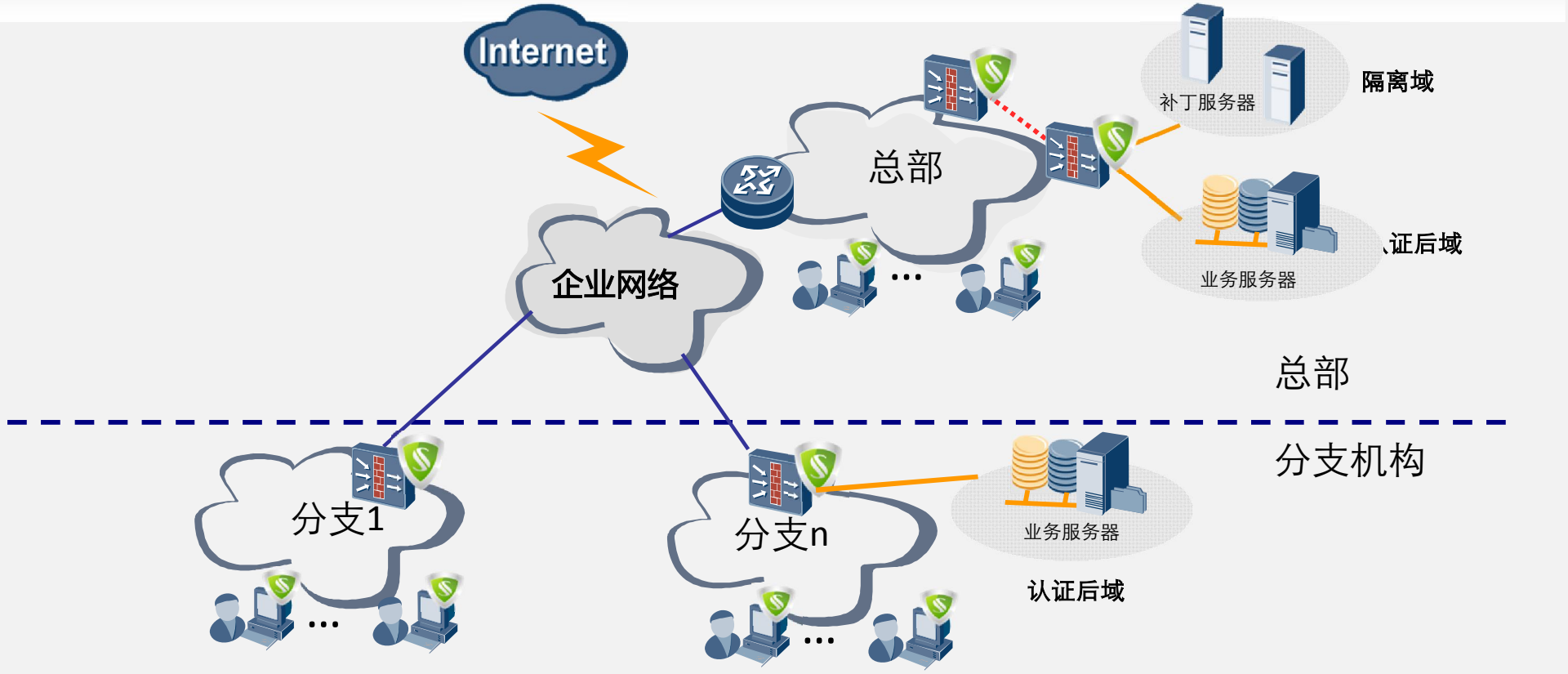
增值特性（透明模式同上述直挂）：

- 黑名单、安全域
- 攻击防范、ASPF、包过滤
- 端口映射、SLB 、NAT、VPN、高级路由
- 流量控制和QOS、IPCAR、无线（外购模块）

HUAWEI

分布式部署，集中控制

旁挂核心交换机 | 直挂核心交换机前 | 直挂网络出口 | 分布式部署



适应场景：

- 存在多个分支机构或者多个流量汇聚点

客户价值和增值特性：

- 同上述章节

业界领先的All-in-One安全解决方案

整合、优化和全面集成的服务

设备集成

路由器 交换机 Wi-Fi 3G 防火墙 VPN

TSM服务器 TSM数据库 SACG

服务集成

局域联网 广域联网 无线LAN 无线WAN VPN组网 边界安全 网络身份识别 准入控制

终端加固 办公行为管理 信息泄密防护 网络防护 补丁管理 资产管理 统一部署 集中维护

客户受益集成

解决内外网安全问题
降低IT风险
确保遵从性

提升IT效率
确保IT满意度

降低采购成本
降低运营成本
投资保护

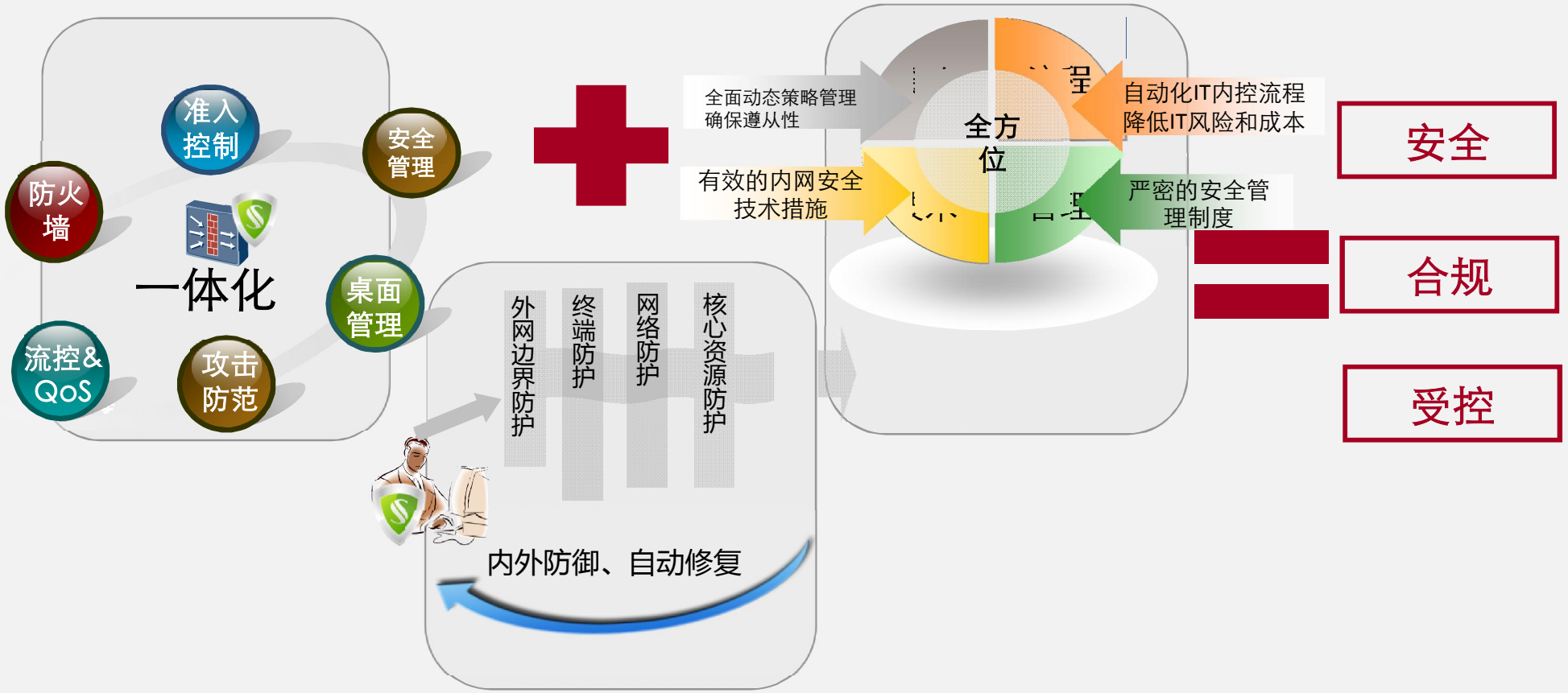
易于部署和管理

USG2200TSM 安全一体机

HUAWEI

一体化、多层次、全方位的安全保护方案

一体化 + 多层次 + 全方位 = 绿色终端，绿色网络



通过一体化、多层次和全方位的网络安全管理，实现企业从被动响应到有预见性、主动性的防御方式转变

HUAWEI

帮您达成系统建设目标

提升终端、网络、应用性能
- 减少软件故障、恶意代码传播，净化终端环境
- 减少网络资源滥用和恶意网络流量，净化网络环境
- 减少未授权访问和攻击，提升应用系统性能

提升办公、IT运维 、决策效率
- IT性能提升、业务中断风险降低、办公行为得到规范
- 快速定位处理故障、自动化桌面管理
- 统一掌控内网状况，辅助快速决策

降低资产管理成本、资本支出CAPEX
- 降低资产总拥有成本（TCO）
- 集成设备，减低采购和安装成本

降低运营成本OPEX
- 降低故障概率、终端自动修复、自动化补丁和软件部署，减轻IT管理员的工作强度，降低IT运维成本
- 一体化方案，易于部署和管理，降低方案复杂性和成本

降低信息泄密、恶意代码传播、网络或业务中断风险
- 降低终端信息泄密的风险
- 降低终端感染病毒、被入侵的风险
- 降低内外网发起的蠕虫传播、入侵、攻击网络或业务的风险

降低遵从性风险
- 实时掌控遵从性，降低违规风险

降低资产遗失风险
- 动态掌握资产变更情况，杜绝资产遗失

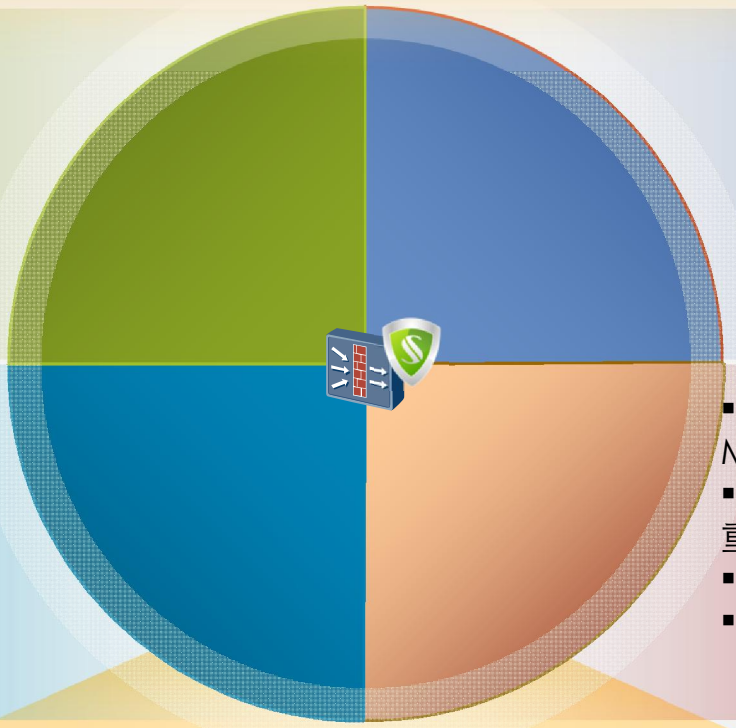
HUAWEI

USG2200TSM 安全一体机四大亮点

专业安全厂商全力打造

- 终端互访控制技术
- 业界最强的环境适应性
- 提供快速部署、访客接入管理、别和处理例外设备
- 网络身份识别，依身份授权访问
- 终端一键式自动修复，自我管理
- 支持广泛的认证源
- 稳定可靠、无法绕过

能涵盖边界和内网安全
低资本性支出CAPEX和运营支出OPEX
滑扩容、保护投资



- 上电即部署，服务器端部署时间低40%以上
- 开机即使用，预置“高、中、低策略模板，免配置使用

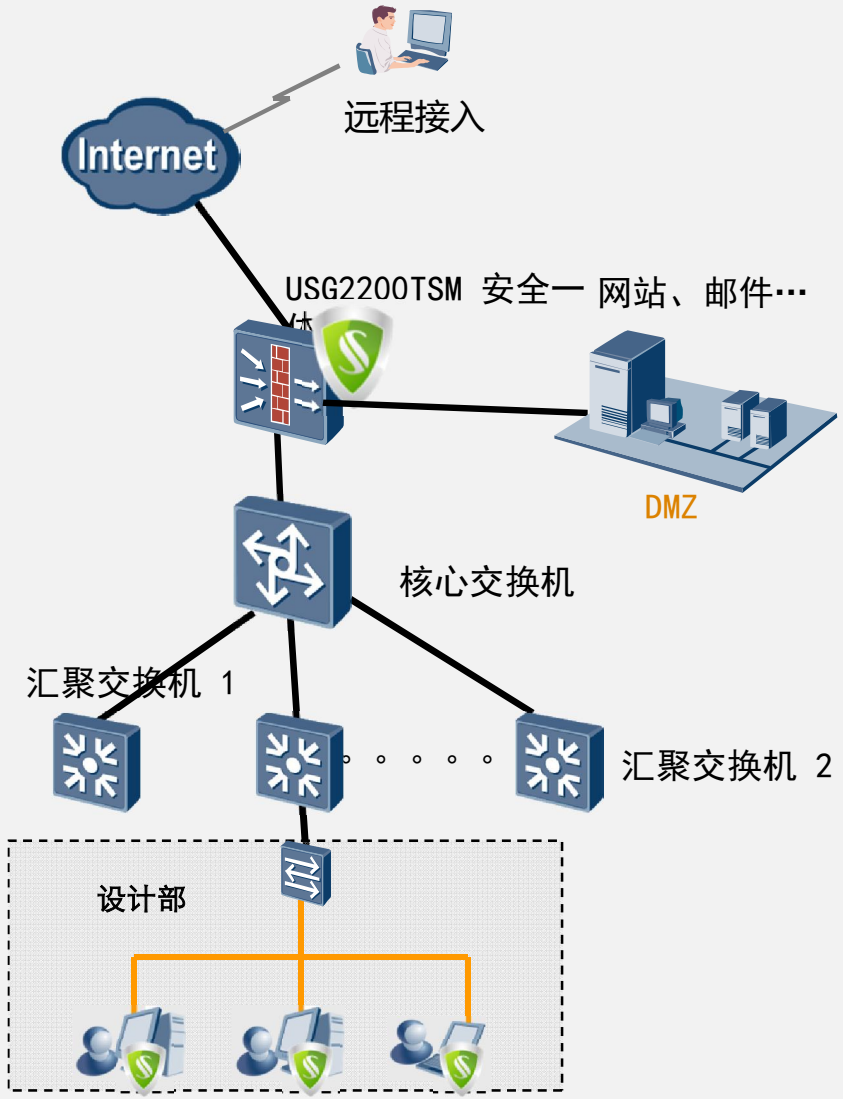
- 电信级专业硬件设备可用度>0.9999，MTBF为12.67年、MTTR为0.5小时
- 一键备份，自带CF数据卡，后台自动备份重要数据
- 一键恢复，Reset按钮一键还原系统
- 24小时自我监控，确保业务连续性

边界安全 + 内网安全

Content

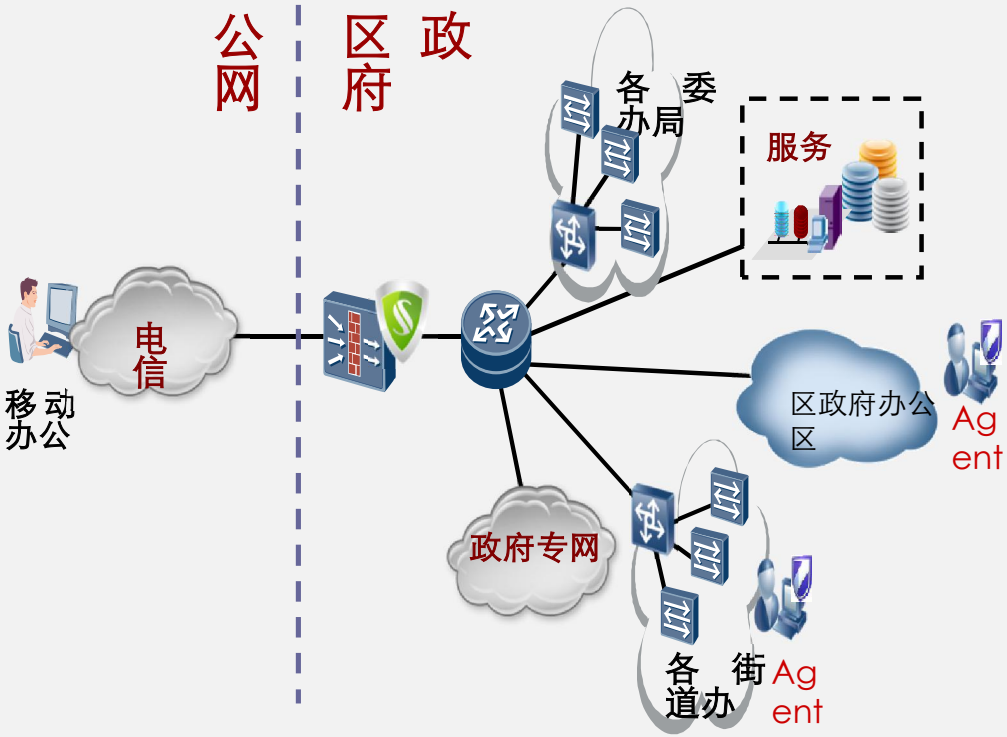
×××制造企业安全项目

- 项目背景
  - 存在一些员工爱干私活、炒股、游戏、聊天；多次发生工单、图纸外泄的事件
  - 多次被专业利益集团攻击导致服务器拒绝服务、网页被篡改被挂马，企业形象受损
  - 每月均有大量机器需要重装，需要处理上百起软件或网络异常事件，大部分机器抱怨过慢
  - 外来终端随意接入，普遍存在未授权或越权访问的行为
- 客户价值
  - 通过USG2200TSM 安全一体机，将对外服务器放到DMZ区，并对不同业务部门的服务器进行安全分域，借助准入控制、安全加固、办公行为管理、泄密防护、网络防护等措施，成功解决上述问题。



×××区政府立体安全防护解决方案

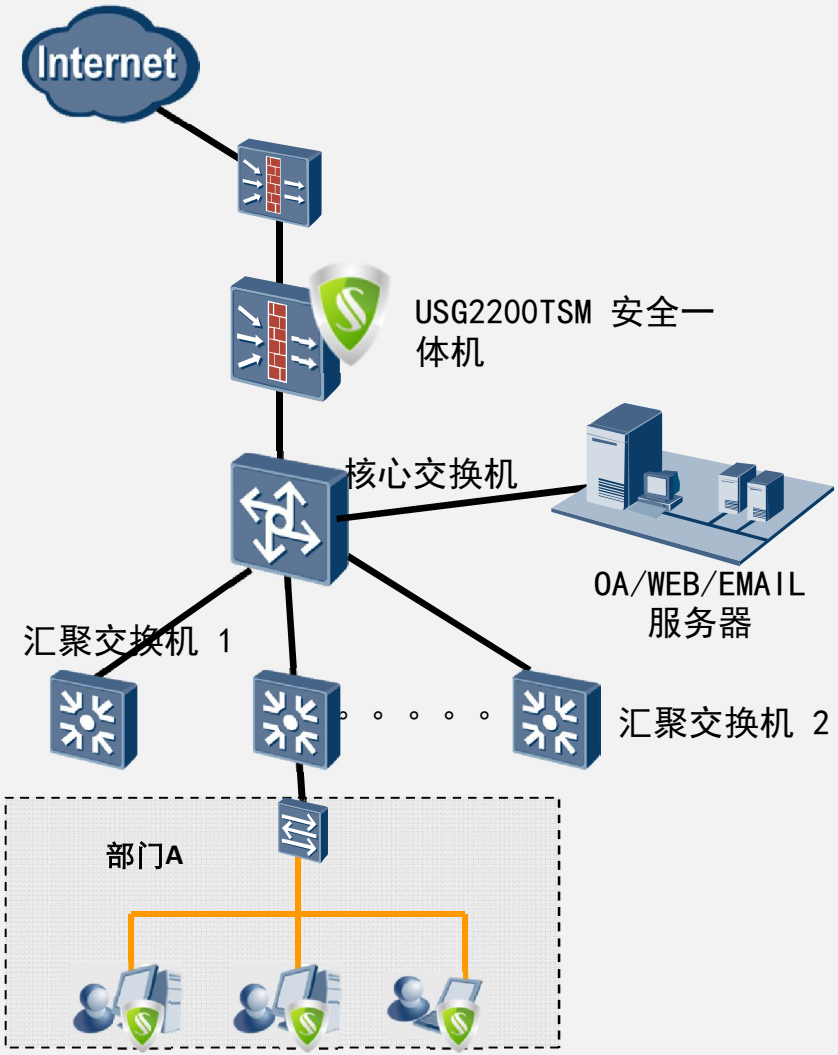
- 项目背景
  - 政府应用敏感，频繁遭受外部黑客、DOS攻击，影响政府形象
  - 内网终端非法接入、网络资源滥用、机器变慢、病毒泛滥、信息外泄、内部恶意网络攻击等使得业务中断、办公效率低下、信息安全事故频发、IT响应慢，信息部门形象受损
- 客户价值
  - 通过部署USG2200TSM 安全一体机，整体提升IT管理水平，基本达到消除外患、解决内忧的效果。在IT风险、办公效率、桌面维护方面起到了良好的效果，IT部门满意度明显改善，IT部门工作强度显著下降。



HUAWEI

×××省政协安全项目

- 项目背景
  - 终端缺乏有效管理，不能对用户上网进行控制，无法确保终端定期更新补丁、病毒防护措施难以贯彻
  - 管理员需要对每台机器安装应用软件，维护工作量较大
  - 单位每台计算机的配置如MAC地址、软硬件信息等计算机配置情况没有一个清晰的了解
- 客户价值
  - 通过部署USG2200TSM 安全一体机，整体提升IT管理水平，对用户上网和办公行为进行管理，强制部署病毒防护措施，通过补丁和软件分发减少管理员的维护工作量，动态掌握资产情况。



HUAWEI ENTERPRISE A BETTER WAY