数据中心安全方案设计

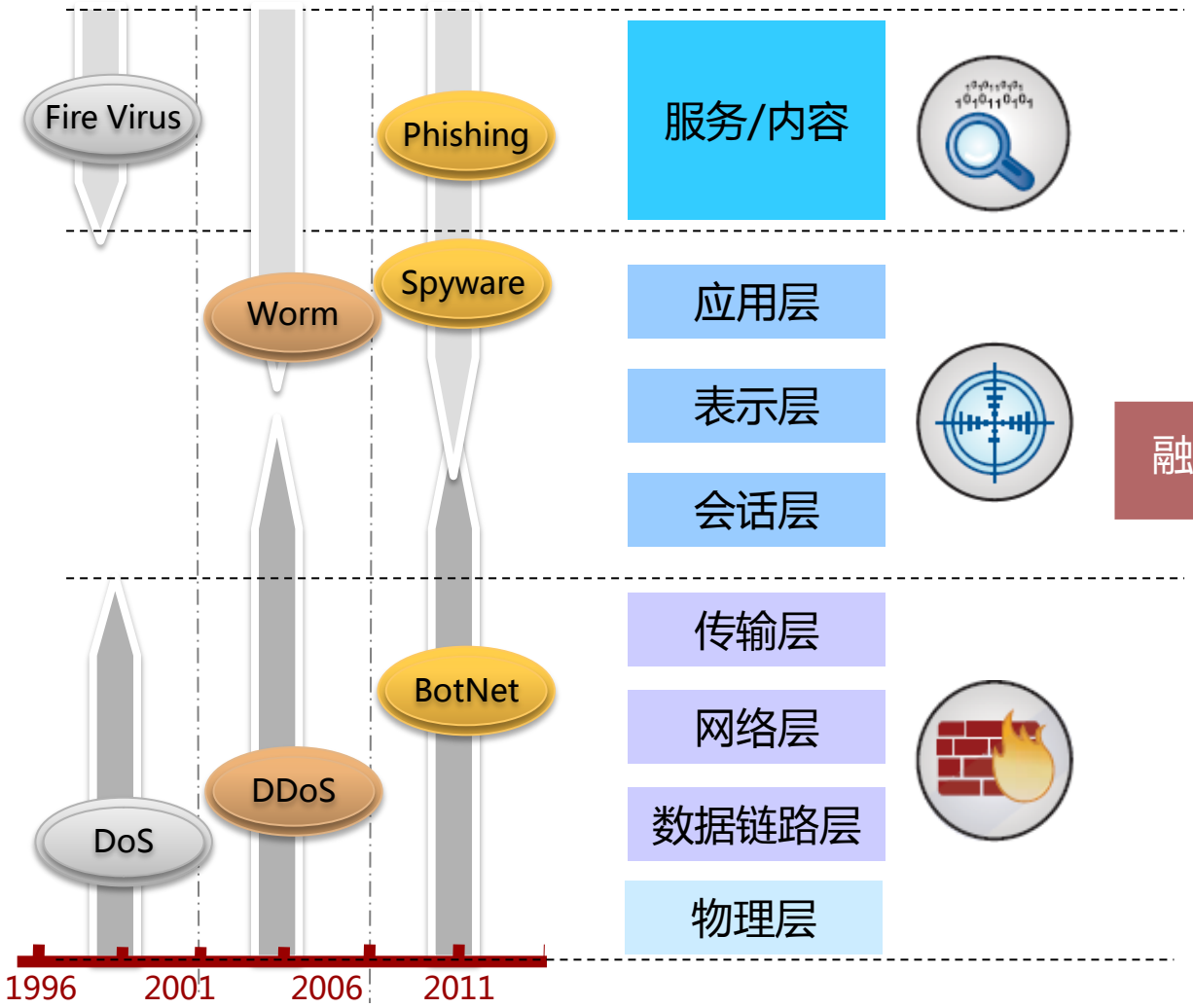
www.huawei.com/enterprise

HUAWEI TECHNOLOGIES CO., LTD.

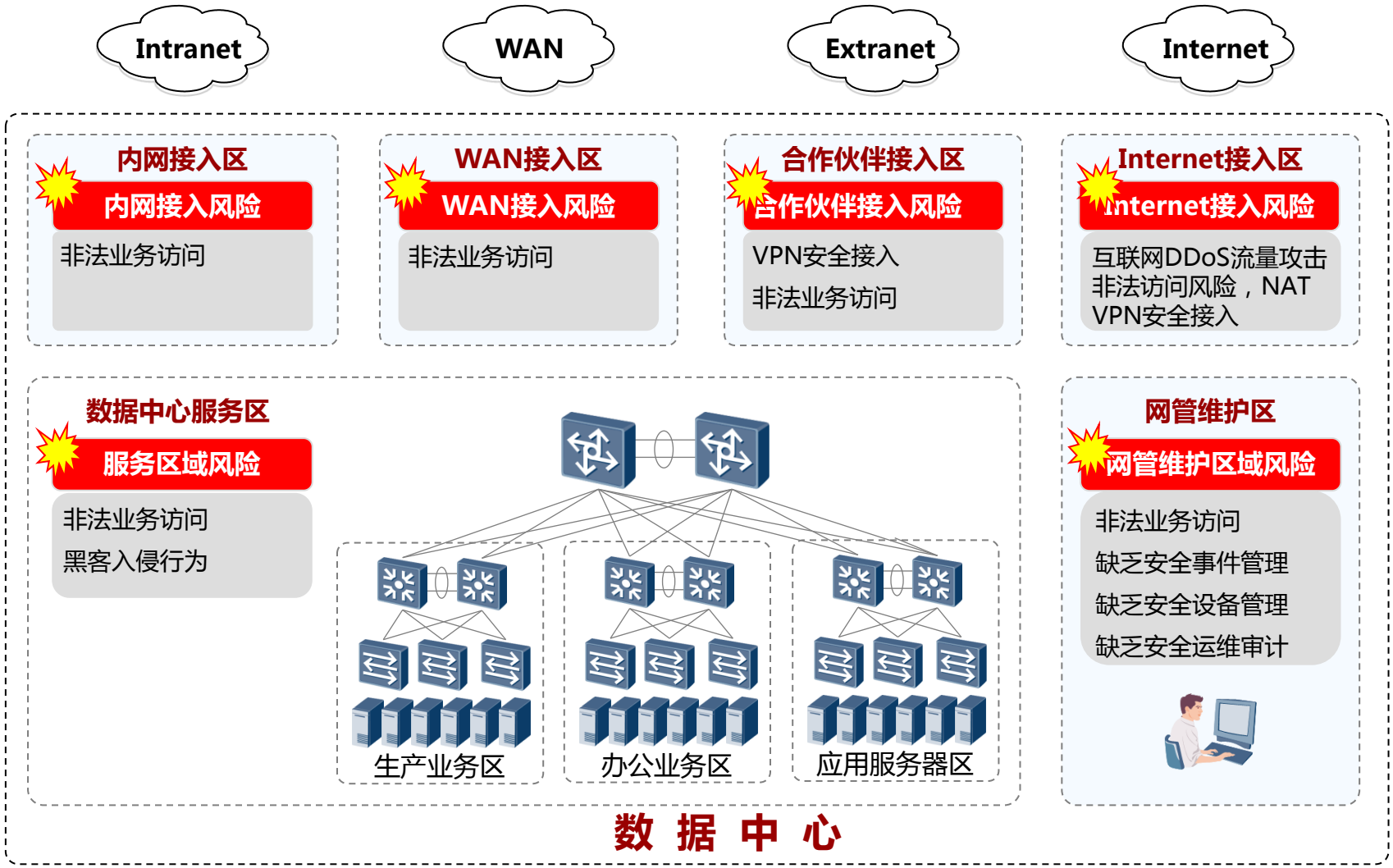
HUAWEI

目录

安全趋势分析


Fire Virus
Phishing
Worm
Spyware
BotNet
DDoS
DoS
1996
2001
2006
2011
服务/内容
应用层
表示层
会话层
传输层
网络层
数据链路层
物理层
融合趋势
内容深度防御
L2-L7全方位
安全防范
访问控制
协议栈安全
L2-4攻击防范
威胁趋势
网络分层
安全趋势

数据中心安全风险分析


Intranet
WAN
Extranet
Internet
内网接入区
内网接入风险
非法业务访问
WAN接入区
WAN接入风险
非法业务访问
合作伙伴接入区
合作伙伴接入风险
VPN安全接入
非法业务访问
Internet接入区
Internet接入风险
互联网DDoS流量攻击
非法访问风险，NAT
VPN安全接入
数据中心服务区
服务区域风险
非法业务访问
黑客入侵行为
生产业务区
办公业务区
应用服务器区
网管维护区
网管维护区域风险
非法业务访问
缺乏安全事件管理
缺乏安全设备管理
缺乏安全运维审计
数 据 中 心

数据中心安全应对之道

安全维度	安全需求	安全技术与方案
边界防护	防护DDoS攻击	Anti-DDoS
	分支安全接入	IPSec VPN网关
	远程用户安全接入	SSL VPN网关
深度防御	防护非法业务访问	防火墙
	NAT地址转换	防火墙
	黑客入侵行为	IPS入侵防御网关
统一安全管理	安全设备管理	安全设备管理
	运维审计	统一运维审计
	安全事件管理	安全管控中心

数据中心安全设计原则

最小授权

控制访问权限，解决非法访问

可靠稳定

安全设备避免单点故障

可扩展性

采用模块化体系架构

分区管理

不同区域采用不同安全策略

运维审计

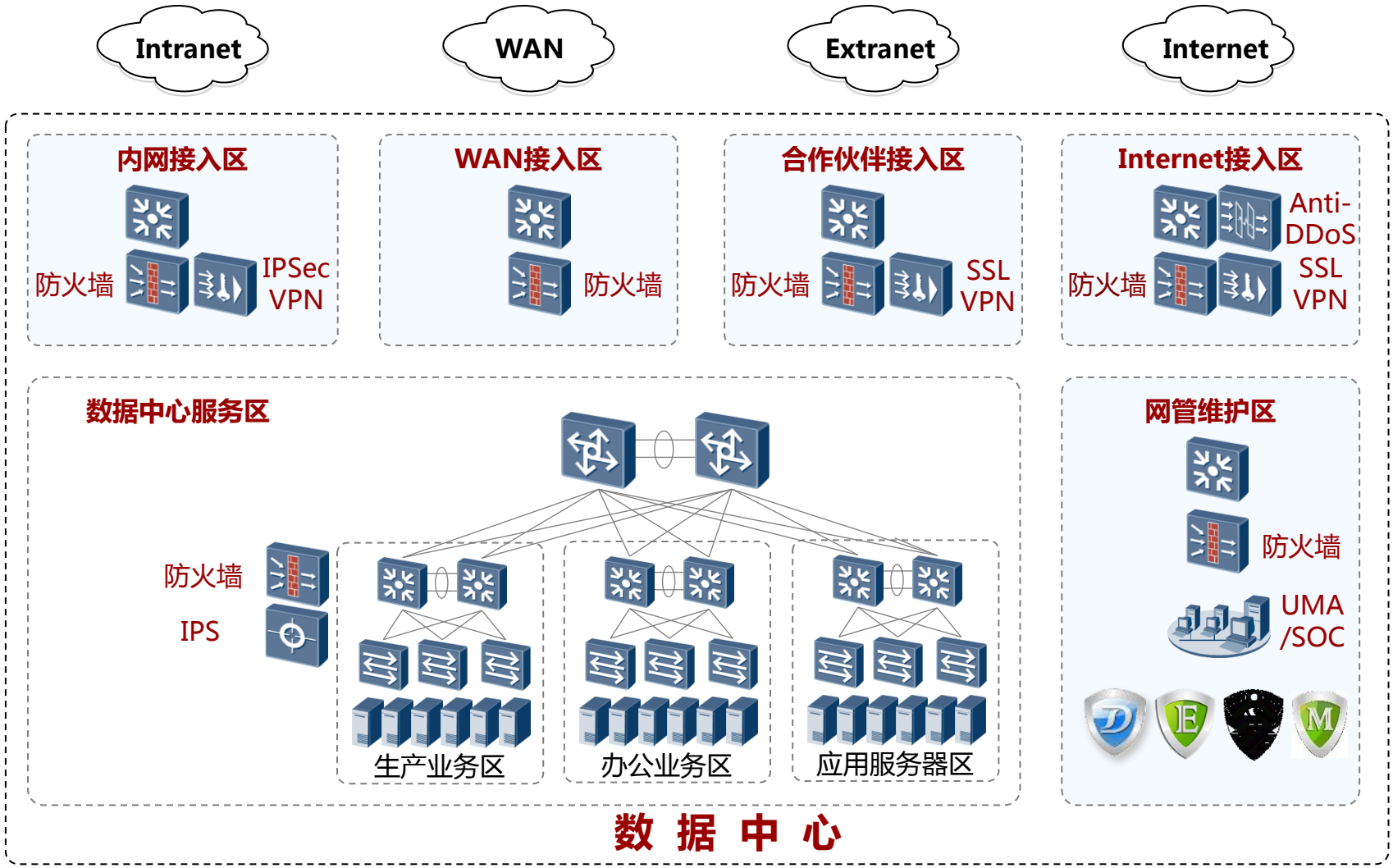
降低资源风险完善责任认定

安全管理

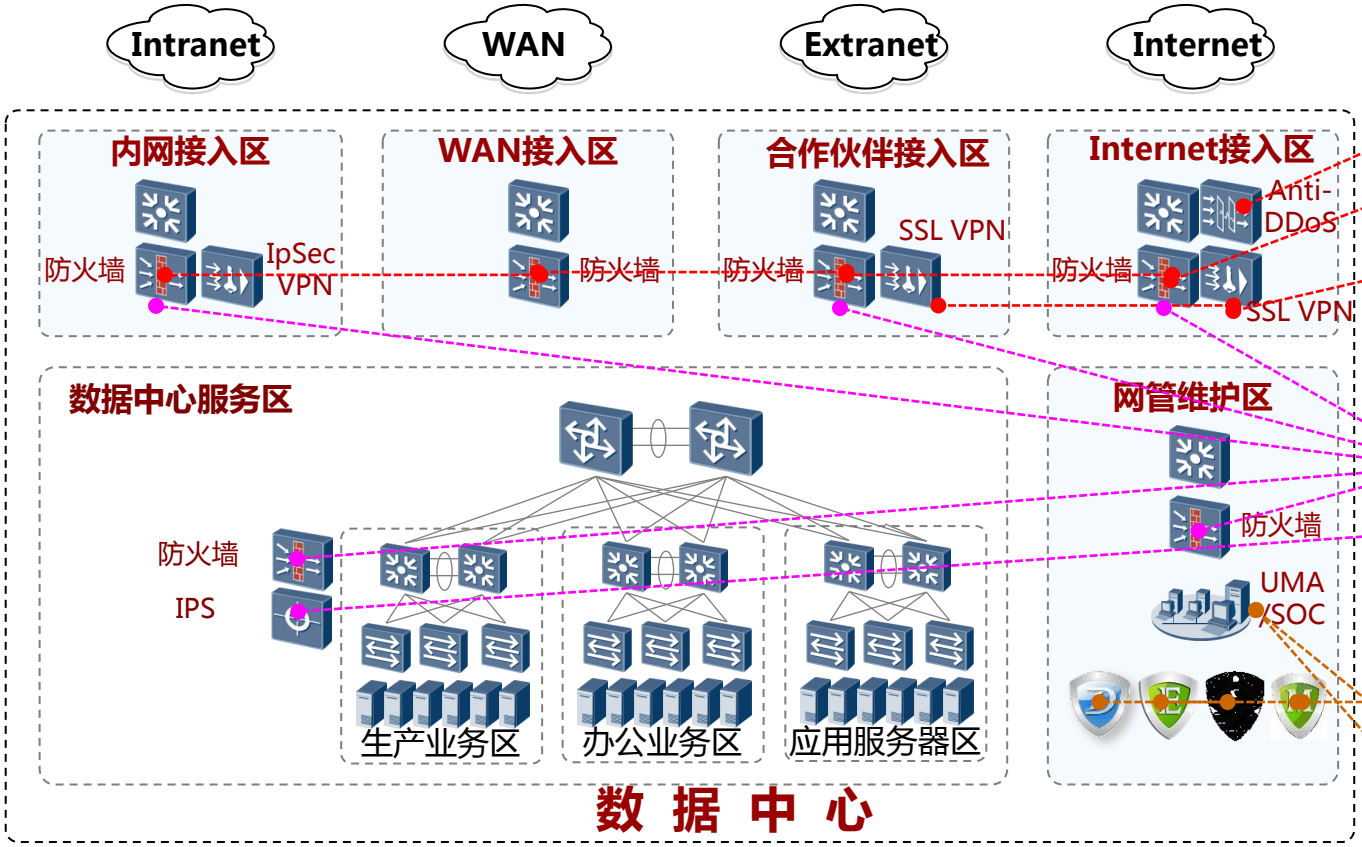
关联事件分析评估安全状态

目录

数据中心安全方案


Intranet
WAN
Extranet
Internet
内网接入区
防火墙
IPSec VPN
WAN接入区
防火墙
合作伙伴接入区
防火墙
SSL VPN
Internet接入区
防火墙
Anti-DDoS
SSL VPN
数据中心服务区
防火墙
IPS
生产业务区
办公业务区
应用服务器区
网管维护区
防火墙
UMA /SOC
数 据 中 心

数据中心安全方案逻辑设计



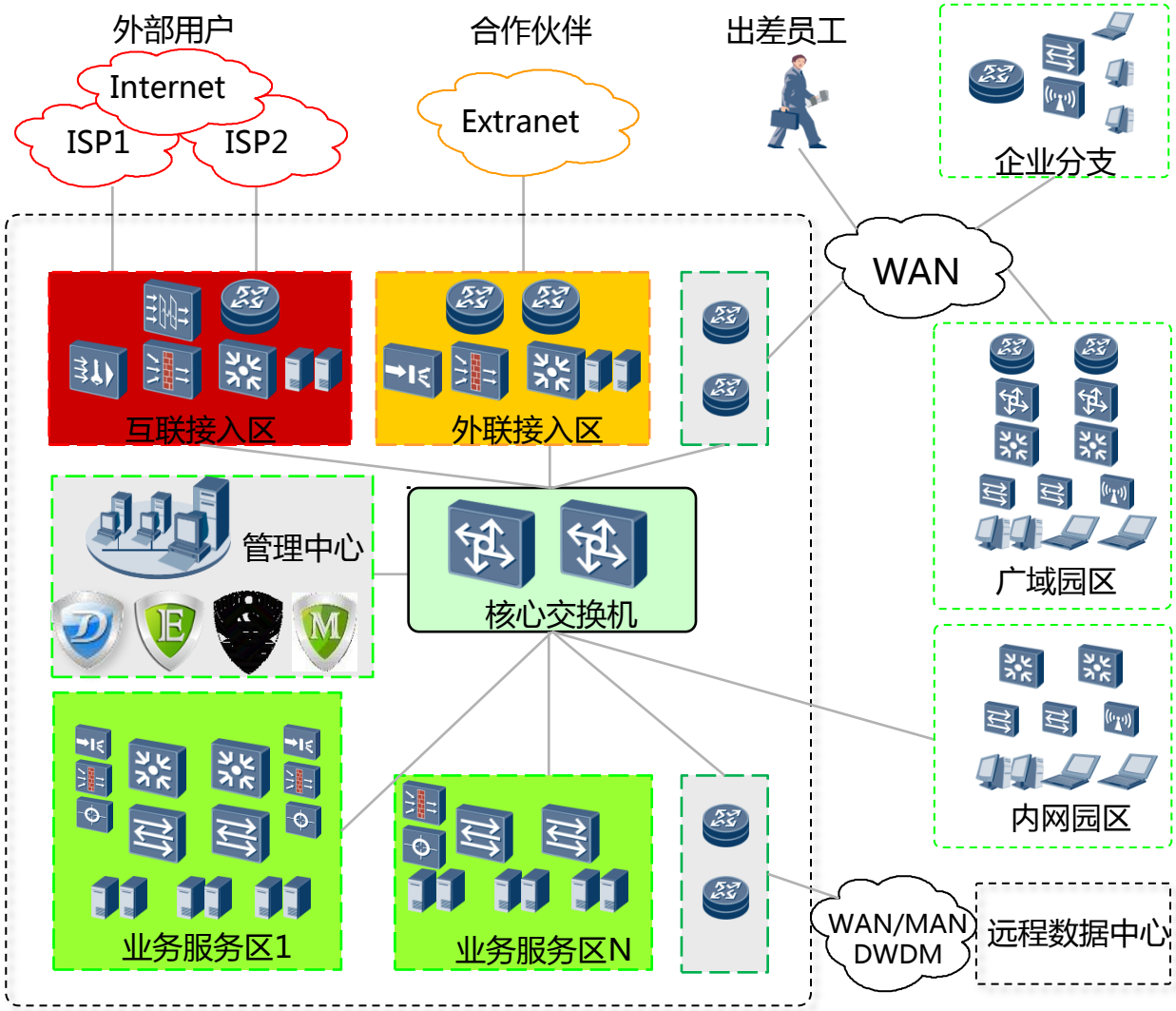
边界防护
- DDoS防御外界攻击
- FW控制外界访问
- 远程分支、员工、合作伙伴通过IPSec SSL VPN安全接入

深度防御
- FW控制内部访问
- IPS对流量深度防御

统一安全管理
- 终端安全管理
- 运维审计
- 安全事件管理

通过Anti-DDoS，IPSec SSL VPN网关、防火墙、IPS入侵防御网关、安全设备管理、运维审计和安全管理中心等设备和软件充分配合，确保数据中心安全

数据中心分区安全设计



分区安全等级：

企业分支	高
广域园区	高
内网园区	高
出差员工	较高
合作伙伴	中
Internet用户	低

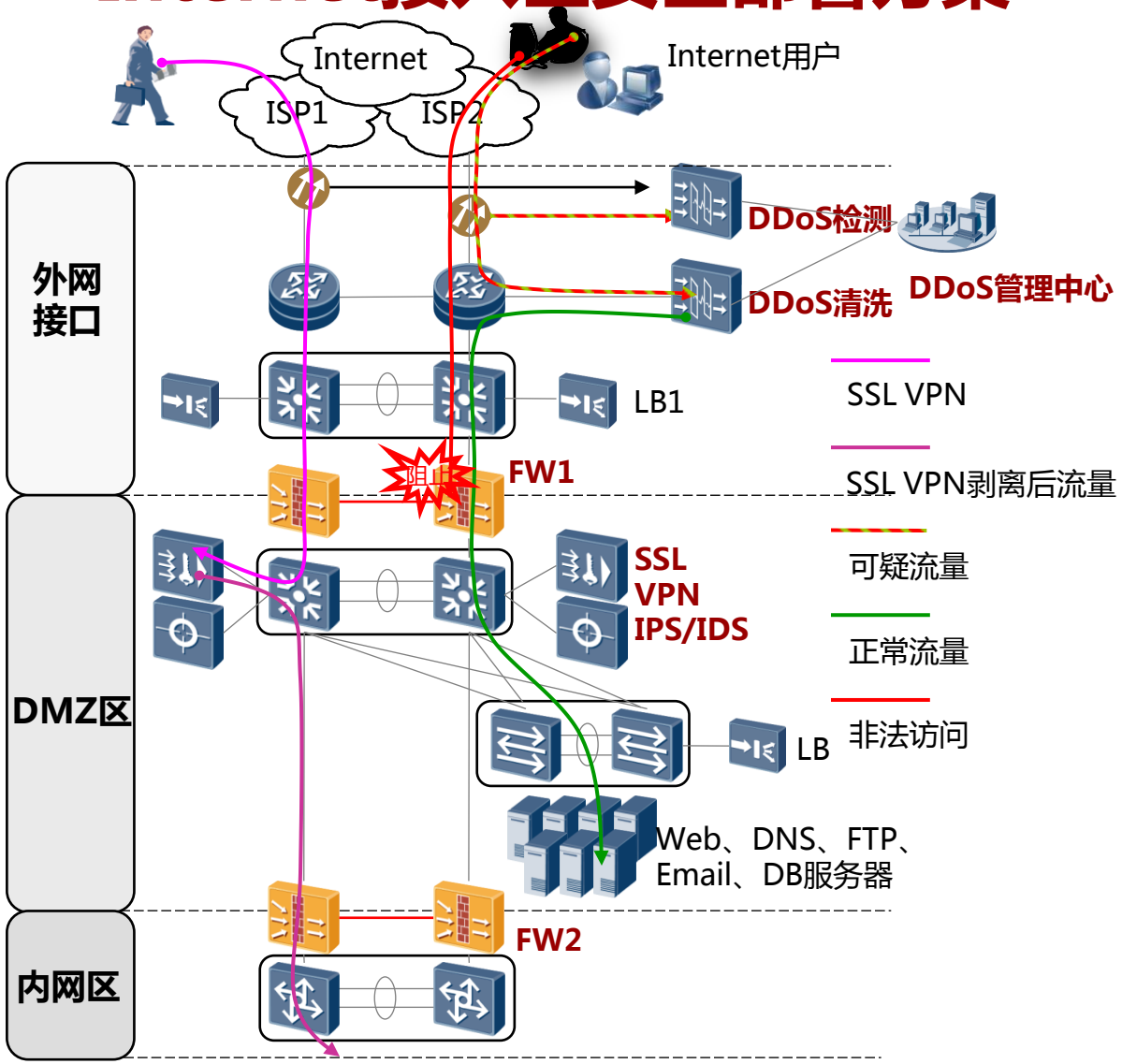
互联网客户最不可信，单独有互联业务区对应。

合作伙伴可信度居中，企业的中心仅开放部分业务给合作伙伴，部署Extranet Server区

企业分支和出差员工，根据访问方式的不同，给予不同的业务范围。

内部园区和广域园区都是企业的内部，可信度最高，根据不同部门和业务，访问数据中心的不同业务服务区。

Internet接入区安全部署方案



安全风险/需求

DDoS流量攻击

非法业务访问

NAT地址转换

VPN安全网关

安全方案

出口部署Anti-DDoS设备，清洗异常攻击流量

防火墙直路部署，控制外网访问内网的流量

交换机旁挂SSL VPN设备，满足远程用户安全接入，访问内部的需求

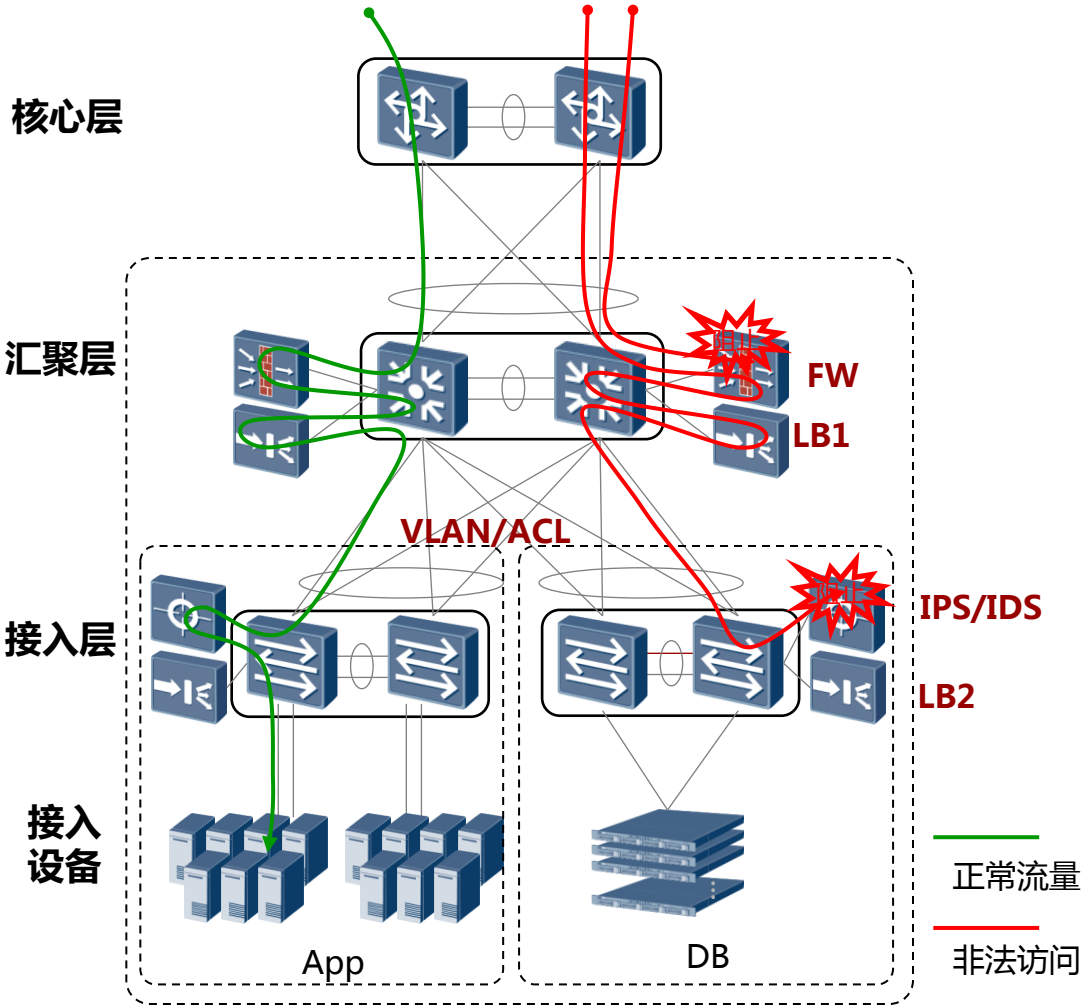
方案价值

高安全性：通过Anti-DDoS和防火墙策略保证数据中心区域安全性

高可靠性：防火墙、SSL VPN设备采用双机备份

灵活接入：SSL VPN网关，满足远程用户安全接入需求

业务服务区安全部署方案



安全风险/需求

非法业务访问

黑客攻击行为

安全方案

防火墙旁路部署

核心服务器上游部署IPS进行应用层攻击防御

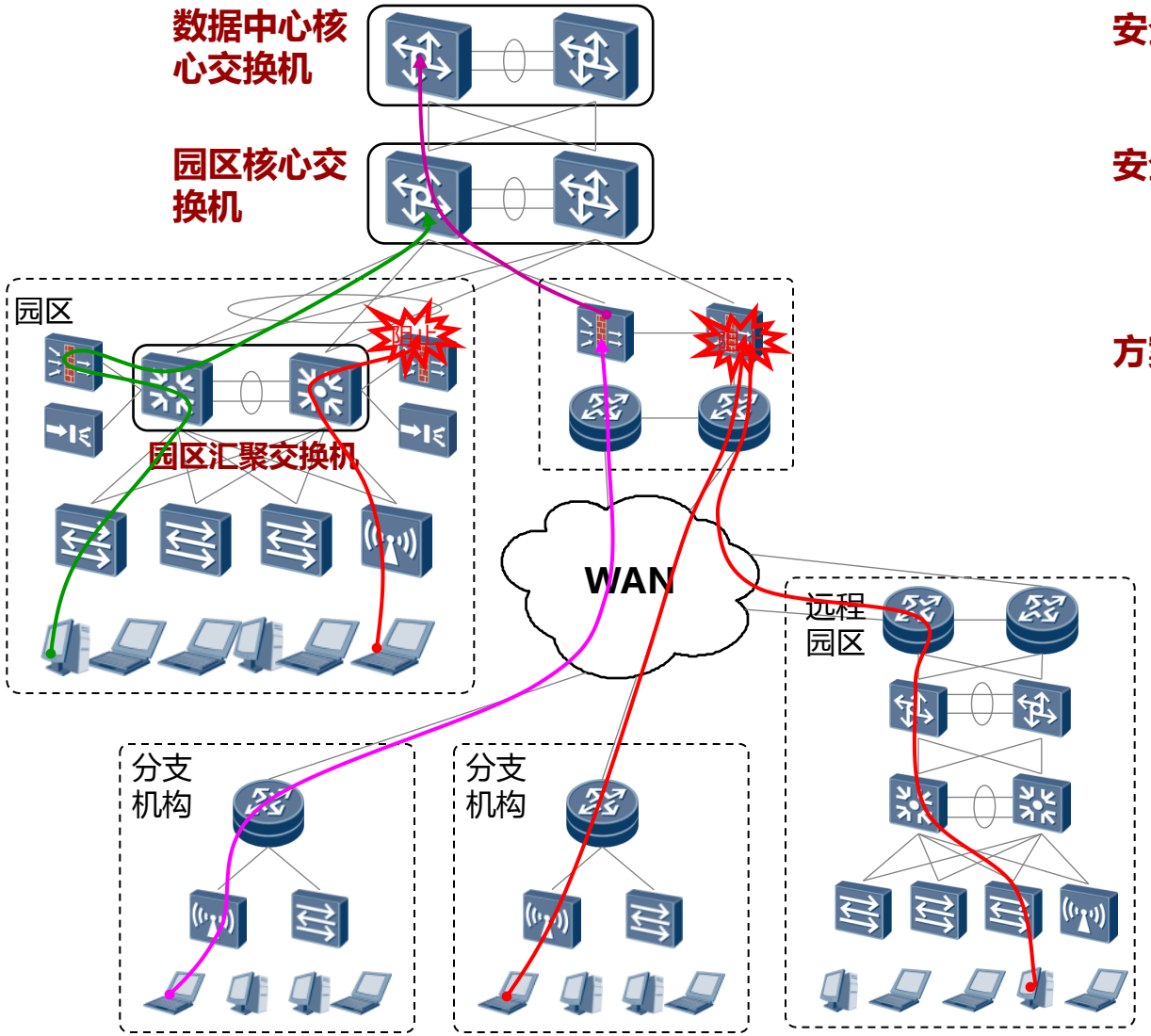
方案价值

高安全性：通过防火墙策略保证不同服务器区合法互访、IPS保障服务器免受黑客攻击

高可靠性：防火墙、 IPS采用双机备份方式

灵活接入：防火墙旁挂，按需引入流量进行策略控制，可信流量直接通过交换机转发

内网接入区安全设计



安全风险/需求

非法业务访问

安全方案

防火墙可采用直路或者旁路方式，推荐直路部署，双机热备

方案价值

高安全性：通过防火墙策略保证内网用户与数据中心区域交互的高安全性

高可靠性：采用双机备份方式

灵活接入：防火墙作为VPN网关，满足分支安全接入需求

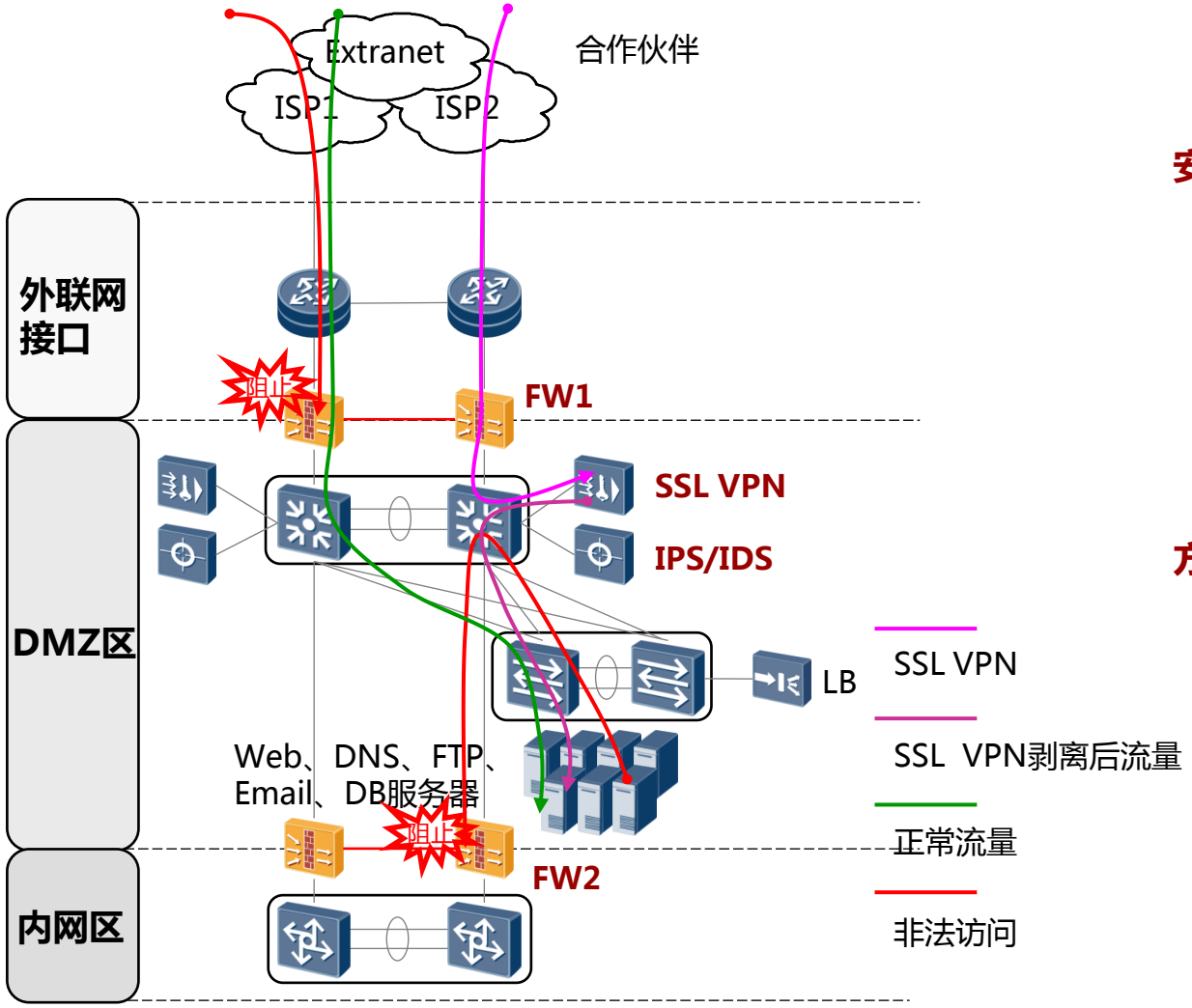
IPSec VPN

IPSec VPN剥离后流量

正常流量

非法访问

合作伙伴接入区安全部署方案



安全风险/需求

VPN安全接入

非法业务访问

安全方案

防火墙设备直路部署，部署双层

外层防火墙1隔离合作伙伴到前置机的非法访问流量，同时具备VPN功能，实现合作伙伴的安全VPN接入需求。

内层防火墙2隔离前置机到内部业务服务区间的非法访问流量。

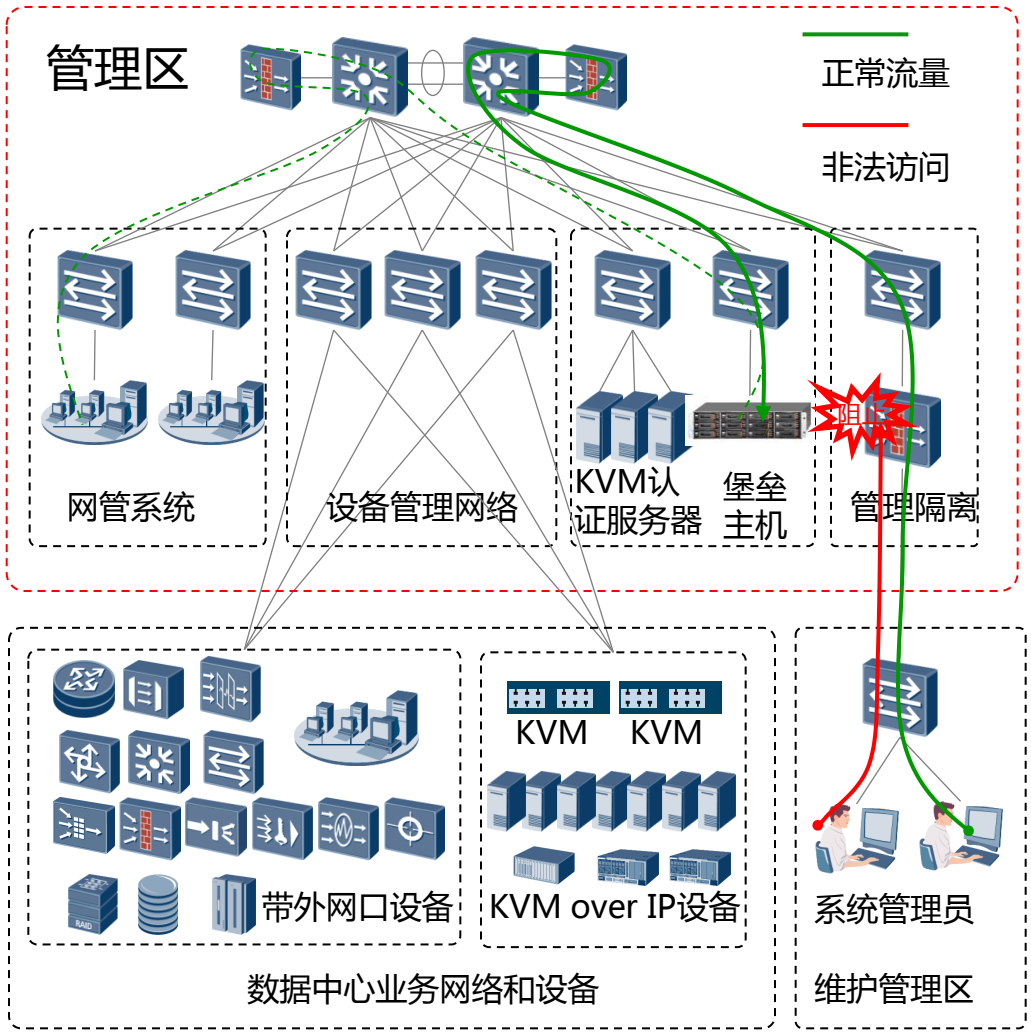
方案价值

高安全性：通过双层防火墙策略保证合作伙伴接入区企业访问数据中心内部业务的安全性，外层防火墙具备VPN网关功能，提供VPN安全接入能力

高可靠性：采用双机备份方式，出现故障不会对网络业务产生影响

高效性：防火墙直路部署避免流量迂回，提高转发效率

网管维护区安全部署方案



安全风险

非法业务访问

共享账号问题、非法访问、操作审计问题

安全设备管理问题、安全故障快速处理

信息安全事件孤岛、海量安全日志、安全趋势分析不全面

安全方案

防火墙设备直路部署，仅允许堡垒主机、网管及SoC系统与区域外部的互访

通过部署堡垒主机，提供运维唯一入口

部署SoC安全运营中心，提供全面的安全态势分析

方案价值

高安全性：堡垒主机实现统一运维入口，集中帐号管理，实现单点登录、帐号权限严格控制

统一安全运维：通过SoC及堡垒主机系统的事前安全告警、事中安全运维、事后追踪审计输出全面准确的安全态势报告

高可靠性：防火墙采用双机备份方式，出现故障不会对网络业务产生影响

数据中心安全解决方案总述

安全区域	风险与需求	风险等级	部署建议	部署价值
内网接入区	非法业务访问	中低	防火墙	解决内网园区、远程分支、远程园区用户非法访问问题
WAN接入区域	非法业务访问	中低	部署防火墙	解决分支介入非法访问问题
Internet接入区	DDoS流量攻击 非法业务访问、NAT VPN安全接入	高	Anti-DDoS 部署防火墙 SSL VPN设备	解决DDOS攻击、业务非法访问、远程用户安全接入问题
合作伙伴接入区	VPN安全接入 非法业务访问	中	双层防火墙	解决业务非法访问问题 合作伙伴的VPN安全接入问题
业务服务区	非法业务访问 黑客攻击行为	中高	部署防火墙 IPS设备	解决业务非法访问、黑客入侵攻击问题
网管维护区	非法业务访问 缺乏安全事件管理 缺乏安全设备管理 缺乏安全运维审计	低	部署防火墙 iSoC系统 安全设备管理系统 堡垒主机	解决业务非法访问，安全事件关联、安全设备管理与运维审计问题

安全产品全景图

安全服务

能力中心

僵尸网络特征库	垃圾邮件库
应用协议分类库(DPI)	URL分类库
病毒/恶意代码特征库	入侵/漏洞特征库

服务中心

安全应急响应	安全管理中心
在线升级平台	安全管理服务
信誉评估中心	安全咨询

网络与内容安全

深度包检测 (DPI)

Bypass series

SIG1000E

SIG9280E

Inline series

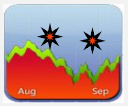
SIG9800-X

DDoS防护解决方案

Eudemon 1000E-I/D

Eudemon 8000E-X

ATIC



Mgmt Center

UTM/Firewall

Eudemon 200E-X

Eudemon 1000E-X

Eudemon 8000E-X

IDS

NIP200/1000

IPS

NIP2000/5000

SSL VPN

SVN 2000

SVN 5000

安全软件

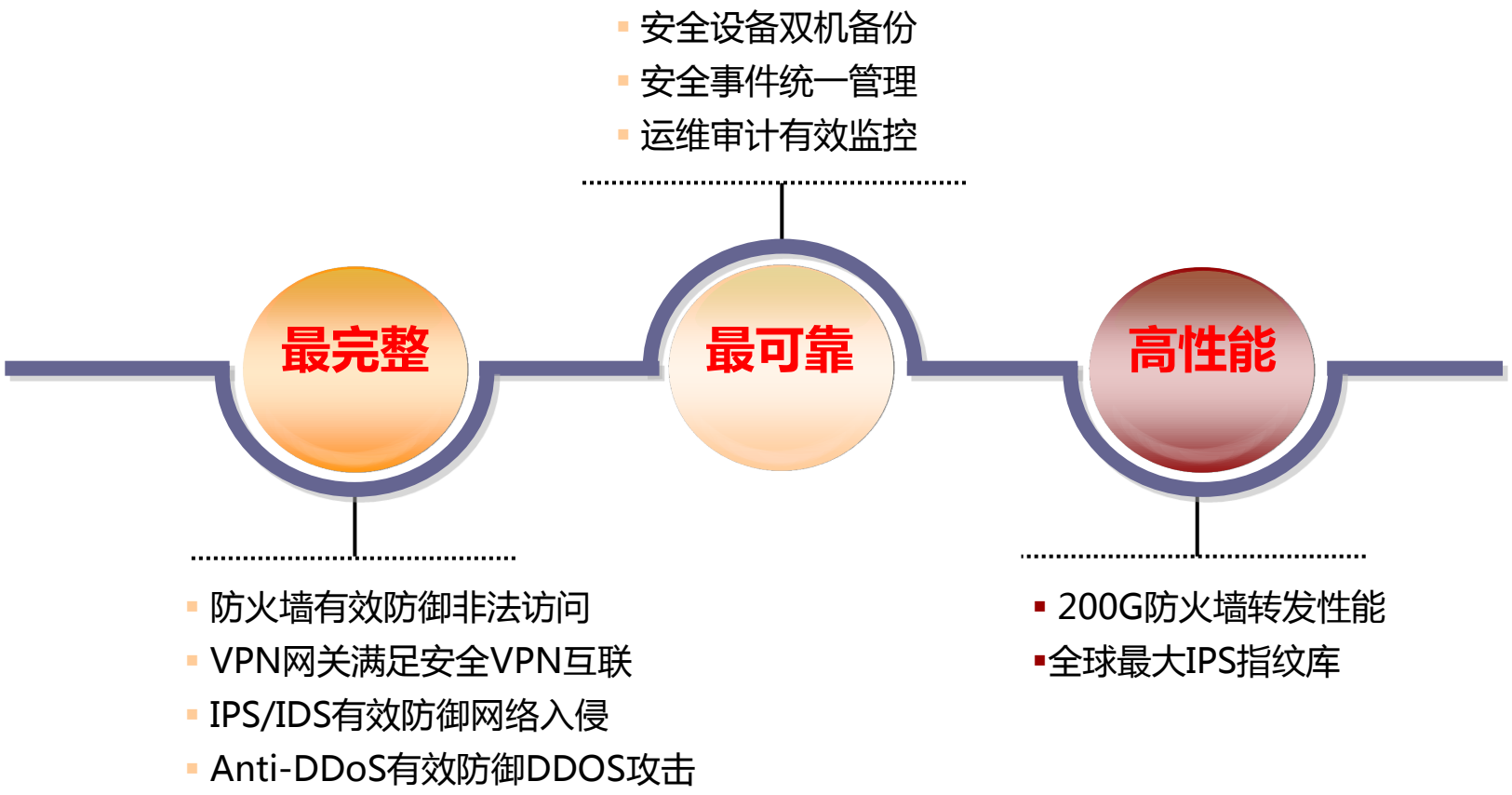
终端安全管理

TSM	DSM
终端安全管理	文档安全管理

安全管理

eLog	VSM	UMA	iSoC
日志管理和审计	设备网管	堡垒主机	安全运营中心

数据中心安全方案特点


安全设备双机备份
安全事件统一管理
运维审计有效监控
最完整
最可靠
高性能
防火墙有效防御非法访问
VPN网关满足安全VPN互联
IPS/IDS有效防御网络入侵
Anti-DDoS有效防御DDOS攻击
200G防火墙转发性能
全球最大IPS指纹库

Huawei Enterprise A Better Way