网络安全防护分析

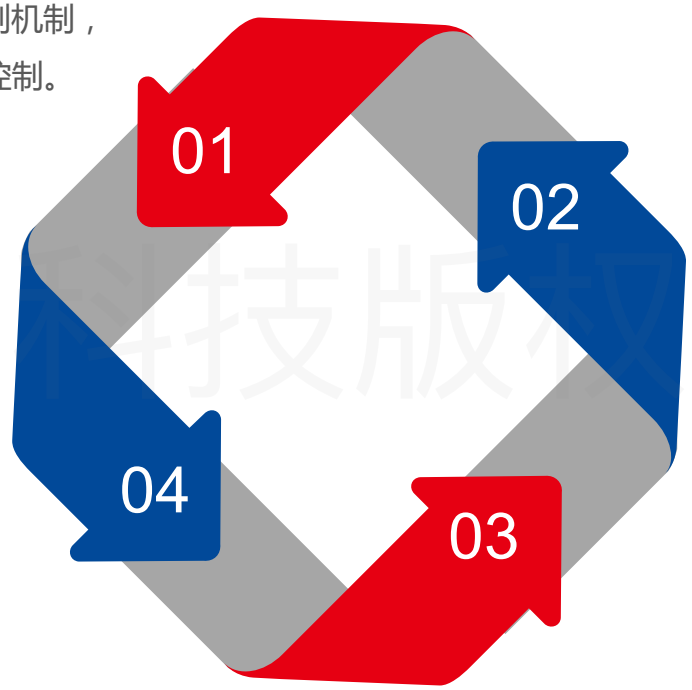
2019护网专项培训

NSFOCUS

为什么要做网络防护分析

提升安全防御能力

1. 进不来，阻止非授权用户进入网络；
2. 利用不了，通过安全域隔离和访问控制机制，实现对用户的权限控制。



落地法律法规

1. 《中华人民共和国网络安全法》
2. 《关键信息基础设施安全保护条例》
3. 以查促建、以查促管、以查促改、以查促防。

加强安全监控能力

使用监控、审计、防抵赖等安全机制，记录下非法人员的攻击行为，使得非法人员“走不脱”。

快速安全处置能力

对安全事件获取、分析和处置进行闭环管理，实现安全事件的一键应急处置。

NSFOCUS

常见网络系统的现状与问题

常见的信息系统现状

- 网络系统规模大、结构复杂，组网方式随意性强，缺乏统一规划，扩展性差。
- 不同的网络区域之间边界不清晰，互连互通缺少统一控制策略；
- 业务系统各自为政，与外网存在多个外网出口，没有统一管理。
- 安全防护策略不统一，安全防护手段部署原则不明确；
- 对访问关键业务的相对不可信终端接入网络的情况比较混乱，缺乏有效控制。

造成的安全隐患

- 无法有效隔离不同业务系统，跨业务系统的非授权互访难于发现和控制；
- 无法及时有效控制入侵行为和网络病毒对业务区域的影响；
- 缺乏7*24小时的事件监测，用户担心重保中一旦发生安全事故，不能快速响应及处置；
- 关键服务器、信息资产的缺乏重点防护；
- 向主管领导及相关部门进行汇报，需要能够针对重保前后的工作进行复盘。

CONTENTS 目 录

01

网络防护分析内容

1.1

安全域

指导思想

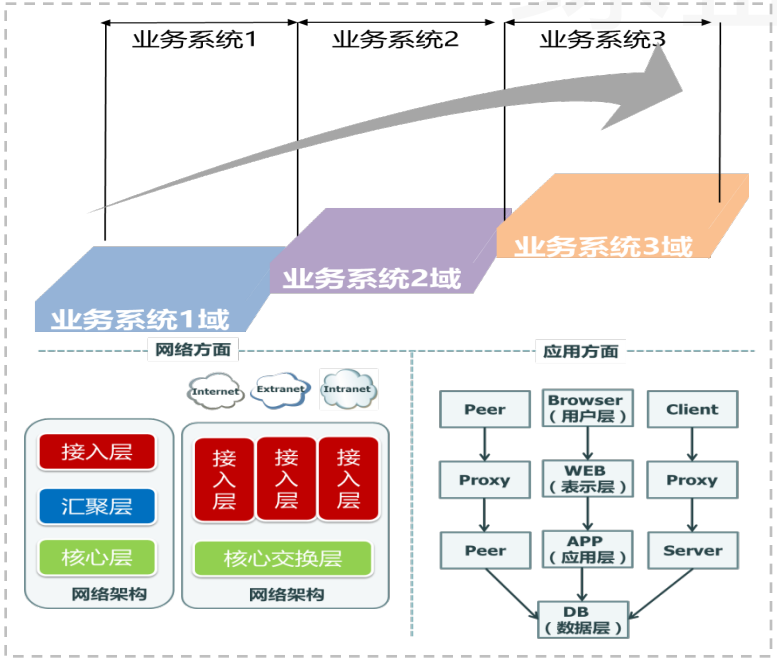
- 以业务为中心，流程为导向
- 规范和优化系统结构
- 有效的控制信息安全风险
- 符合相关标准、要求
  - SOX、COSO、ISO27001、等保
  - 企业标准

网络安全域设计方法

1.划系统拆结构

按照业务系统的不同，首先将不同的业务系统进行拆分。可以拆分为：XXX业务系统、YYY业务系统。

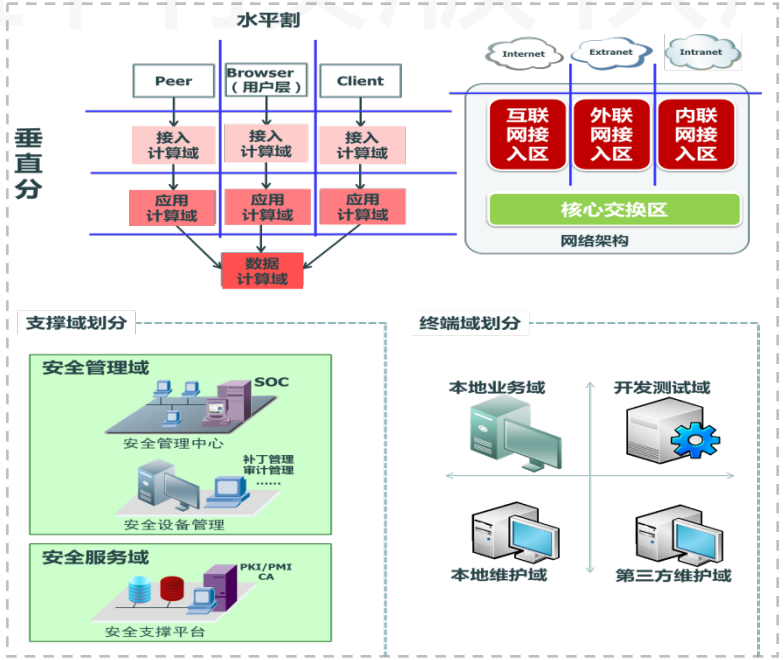
对单一信息系统功能、应用架构、网络承载等的分析和拆解，把单一信息系统拆分成基本的安全域类型。



2.垂直分水平隔

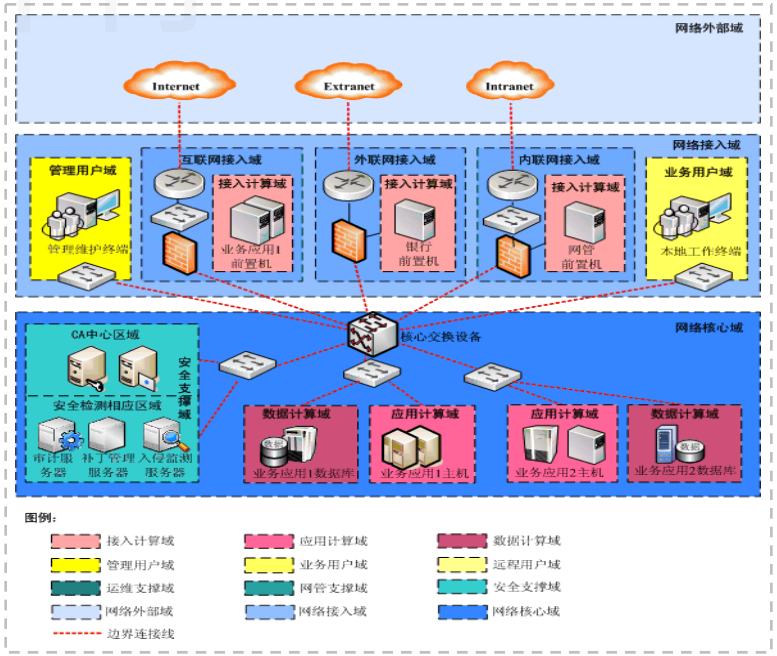
在上一步划分的基础上，按照“先应用后网络”的顺序对系统进行安全域的细分。

- 应用层面包括了计算域、用户域、支撑域；
- 网络层面包括网络域。



3.细分合精优化

根据各个细分后的安全域的防护需求的不同，进行安全域的深入划分和合并调整，并进行相应的优化处理。



网络安全域设计步骤

识别网络区域
- 根据应用系统类型，形成基于应用类型的网络区域。

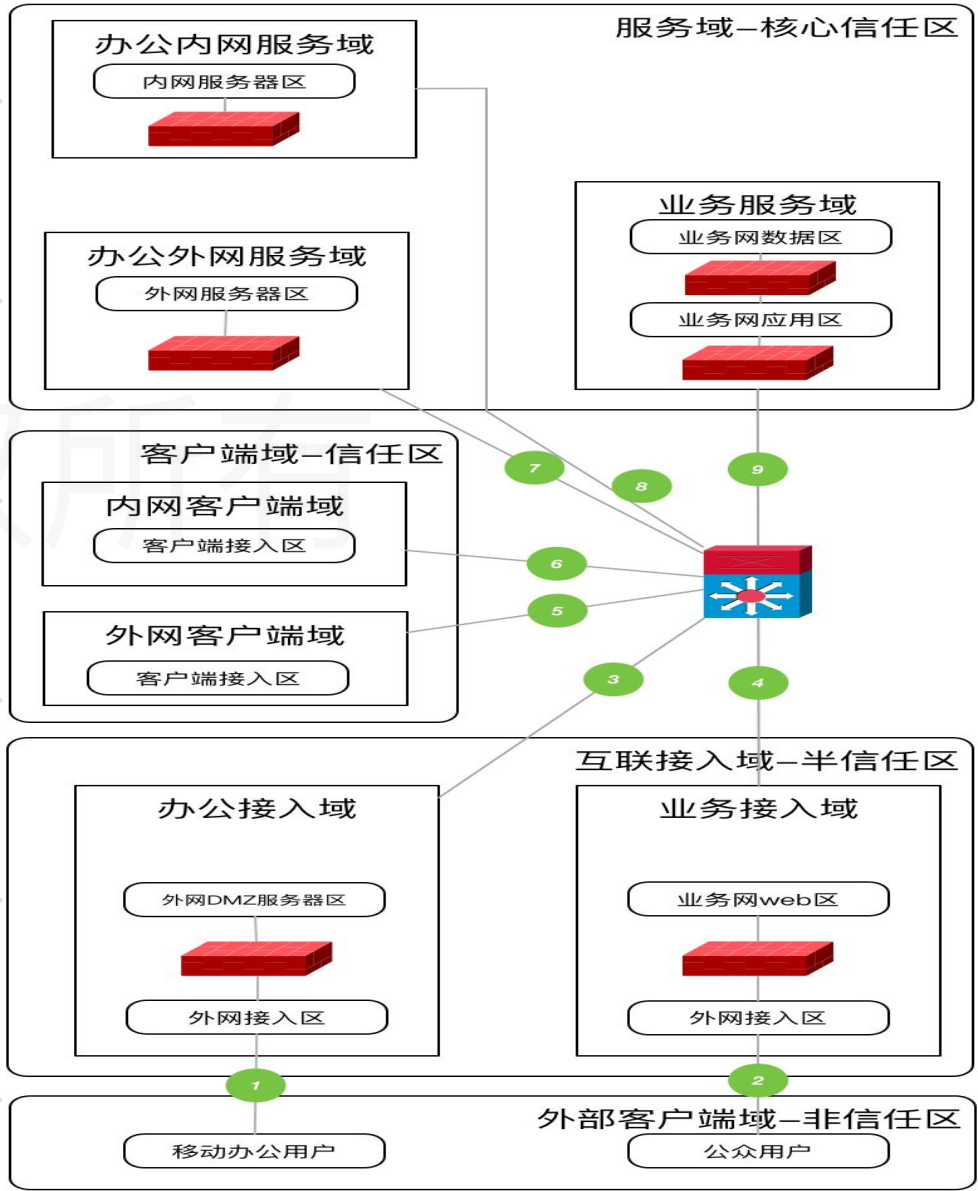
拆分网络子区域
- 根据应用系统应用类型和应用架构，拆分出网络子区域。

推导二级域
- 区域内子区域整合形成区域二级域，区域间二级域整合形成安全域二级域。

推导一级域
- 将具有相同安全服务要求的二级域整合，形成安全域一级域。

识别安全域边界
- 梳理需要通讯的二级域访问关系，识别出安全域边界。

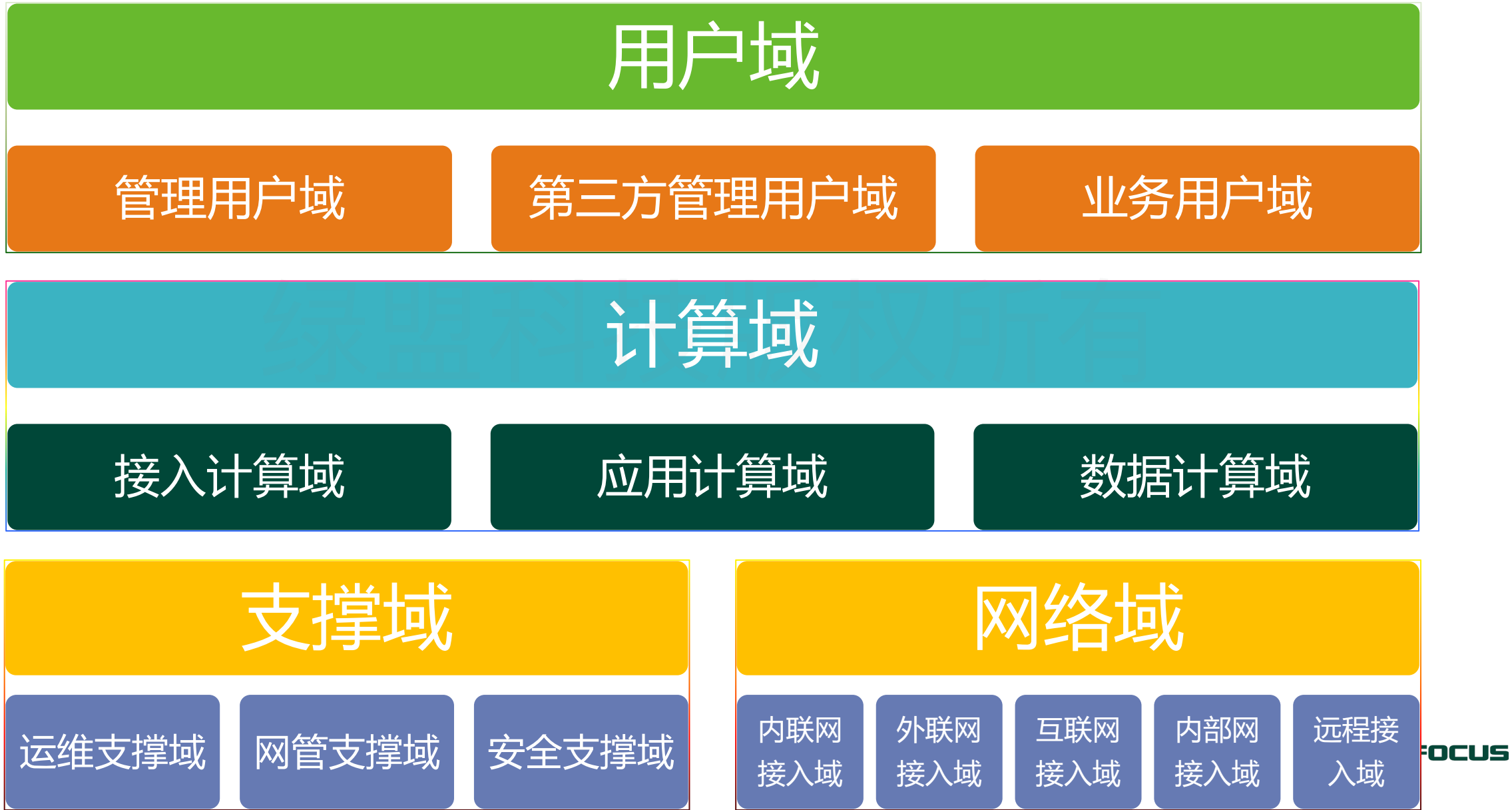
设计访问控制策略
- 根据安全域设计和安全域边界编制安全访问控制策略



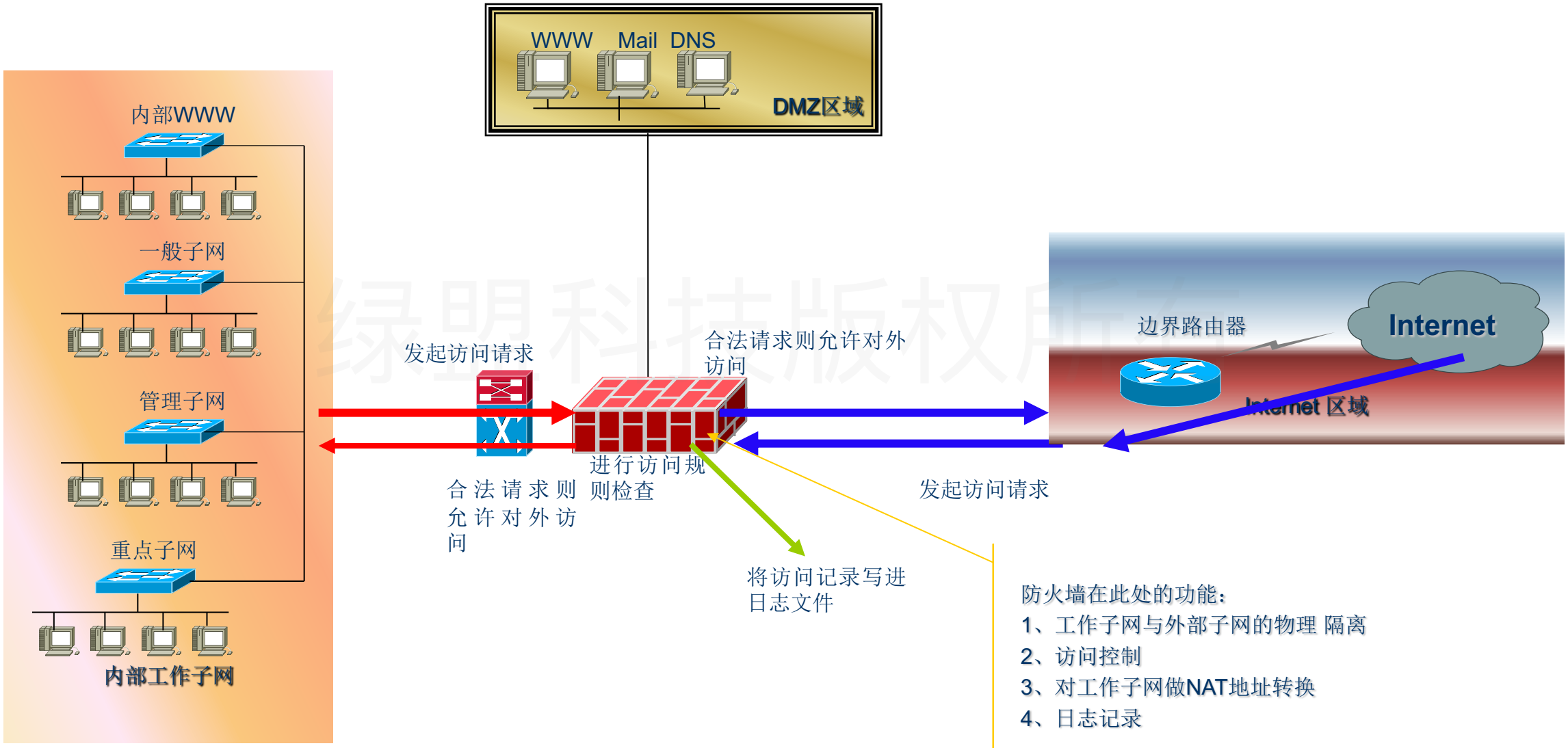
1.2

访问控制

网络安全域


用户域
管理用户域
第三方管理用户域
业务用户域
计算域
接入计算域
应用计算域
数据计算域
支撑域
运维支撑域
网管支撑域
安全支撑域
网络域
内联网接入域
外联网接入域
互联网接入域
内部网接入域
远程接入域

内部子网与互联网的访问控制



防火墙在此处的功能：

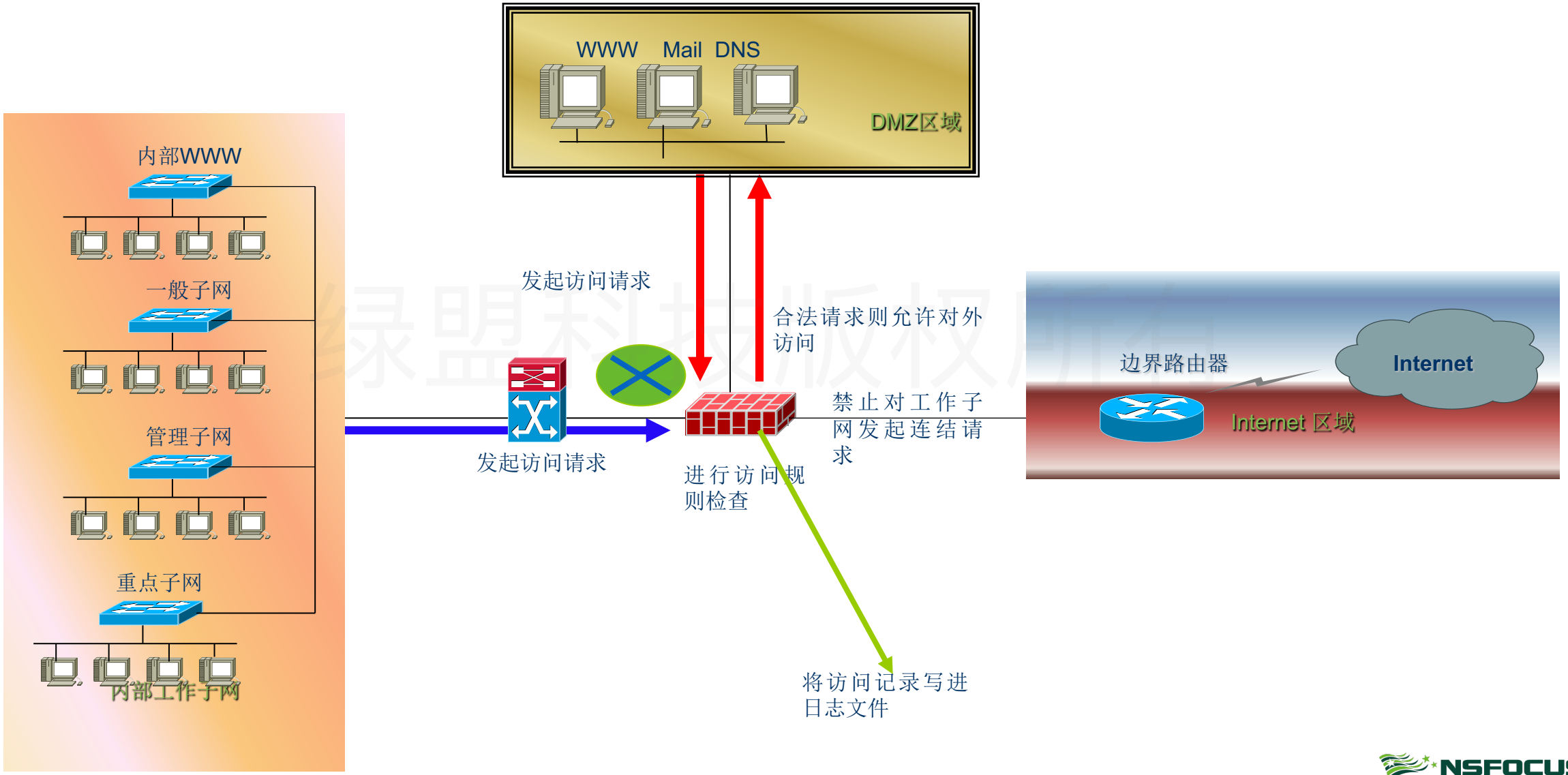
1、工作子网与外部子网的物理 隔离

2、访问控制

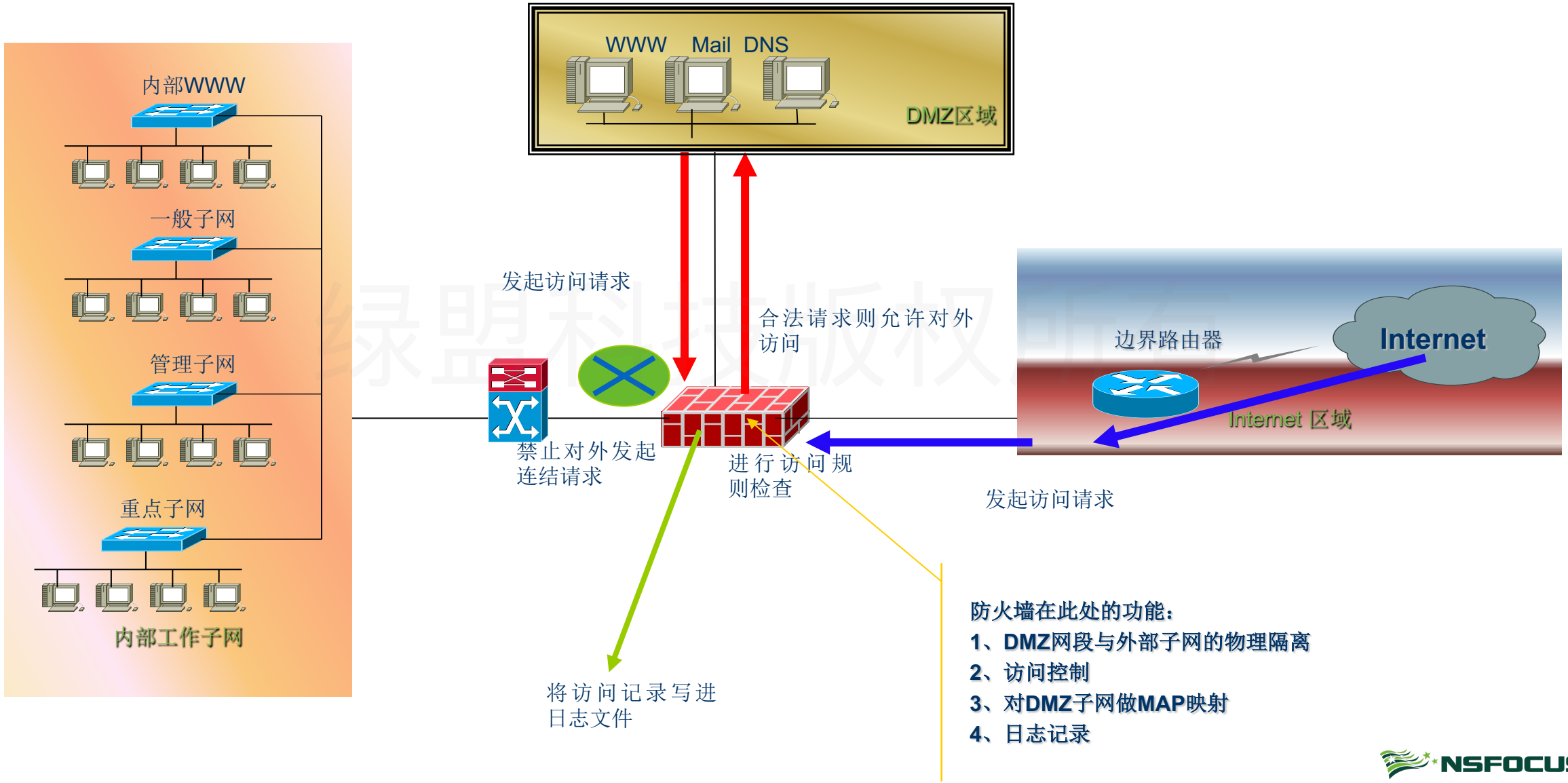
3、对工作子网做NAT地址转换

4、日志记录

内部子网与DMZ区的访问控制



DMZ区与互联网的访问控制



访问控制基本原则

●突出重点 ●就高原则 ●最小权限 ●层层防护 ●严进宽出？

安全策略（客体） / 安全策略（主体）		内部网		互联网		
		重要区域（互联网接入区域，专线接入区域，外联区域，核心交换区域，生产应用区域，核心数据区域）	一般区域（用户接入区域，管理区域，DMZ区域，异地灾备，测试区）	第三方区域	分支区域	互联网区域
内部网	重要区域	通过部署防火墙，制定安全策略实现最小权限控制。	原则上不允许	原则上不允许	原则上不允许	原则上不允许
	一般区域	通过部署防火墙，制定安全策略实现最小权限控制，并且对访问的范围做到IP地址，端口级限制。	根据实际系统运行需要，通过部署防火墙，制定安全策略，实现最小权限控制。	原则上不允许	原则上不允许	此处主要是指用户区域访问互联网。
互联网	第三方区域	通过部署防火墙，制定安全策略实现最小权限原则。同时对源IP地址和目的IP地址进行限制。	——	——	——	——
	分支区域	通过部署防火墙，制定安全策略实现最小权限原则。同时对源IP地址和目的IP地址进行限制。	——	——	——	——
	互联网区域	原则上不允许	此处的安全策略主要是针对互联网访问DMZ区。通过部署防火墙，制定安全策略实现最小权限控制。	——	——	——

安全防护策略

防火墙策略合规

对标分析（目的IP范围过大、目的端口范围过大、源IP范围过大；策略包含；策略顺序）

防火墙策略有效

使用扫描工具对靶机进行端口扫描，扫描端口与开放端口一致。

安全设备策略有效

使用扫描工具对靶机进行漏洞扫描，安全设备能正常检测扫描行为，并产生日志记录。

日志管理

能否正常采集防火墙、安全设备的日志

1.3

入侵防范

不同的安全域需求不同

在划分安全域之后，我们对不同安全域内的关键设备进行安全加固，依据是：各安全域内部的设备由于不同的互联需求，面临的威胁也不同，因此其安全需求也存在很大差异。

互联网

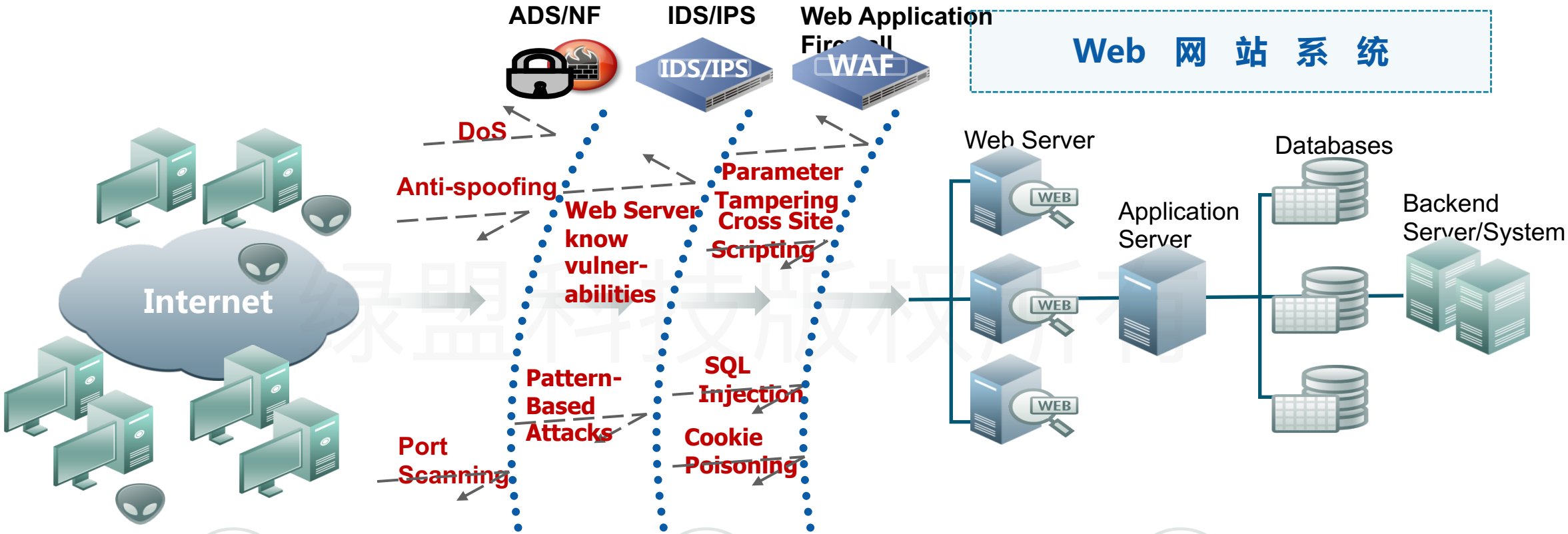
- 面临着黑客入侵、病毒扩散等威胁，主要的安全需求是入侵检测、病毒防护、数据过滤等。
- 可以在互联网出口侧部署流量清洗系统，可以迅速对DDoS攻击流量进行过滤，确保正常业务的可用性。
- 可以在边界部署网络入侵检测系统，对网络边界处入侵和攻击行为进行检测，并在最重要的区域和易于发生入侵行为的网络边界进行网络行为监控，在核心交换机上部署双路监听端口IDS系统，IDS监听端口类型需要和核心交换机对端的端口类型保持一致。

不同的安全域需求不同

第三方、合作伙伴

- 对业务系统的软、硬件进行远程维护或现场维护，其操作很难控制，面临着病毒、漏洞、攻击、越权或滥用、泄密等威胁，安全需求主要是接入控制，包括IP / MAC地址绑定、访问控制、病毒防护、行为审计等。
- 可以在边界部署防病毒网关，对进出网络的数据进行扫描，可以把病毒拦截在外部，减少病毒渗入内网造成危害的可能。通常部署在防火墙和中心交换机之间，可以在病毒进入网络时对它进行扫描和查杀。
- 可以在边界部署行为审计，对网络数据的采集、分析、识别，实时动态监测通信内容、网络行为和网络流量，发现和捕获各种敏感信息、违规行为。

入侵的检测及防御



1
- 网络端口访问控制
- UDP/TCP状态感知

2
- 基于规则的异常检测
- 入侵防护
- 已知漏洞管理

3
- HTTP/S应用保护
- 会话管理（Cookie安全）
- 内容控制
- 数据泄露管理

4
- Web漏洞扫描
- 防篡改
- 漏洞管理、漏洞验证

5
- Web网站风险评估
- Web网站检测服务
- 应急响应

NSFOCUS

1.4

策略优化

安全防护策略优化

策略命中率分析

识别高命中的策略，便于运维人员进行策略调优。

策略冗余

识别出现网中的垃圾冗余策略，提高设备策略的合理性。

策略风险分析

识别出现网中的风险，对有风险策略提供修正建议，提高设备策略的合规性和安全性。

策略综合分析

集中了策略冗余分析、策略风险分析、策略命中率分析，给设备策略的健康度进行综合评估，客观的反应设备的运维健康情况。

02

网络防护分析实施

NSFOCUS

实施流程

01
评估准备

- 成立评估组
- 获取网络相关文档
- 制定分析规范&计划

02
组织实施

- 依据输入开展评估
- 现场评估

03
评估总结

- 召开总结会议
- 确认评估结果
- 形成评估报告

04
整改复核

- 实施风险整改
- 形成整改报告
- 提交评估组复核

05
试运行

- 优化改进

评估准备

- **成立评估组**：当满足启动条件时，各单位应及时组织成立评估组，启动安全评估。评估组由安全、网络、相关厂商等方面专家组成。
- **获取业务文档**：业务运营团队应向评估组提供开展评估需要的文档、资料和信息。

通用	逻辑设计实施文档类	安全设计和负载均衡设计文档类	高可用性设计类	管理文档
• 数据中心分区网络详细拓扑 • 网络资产清单 • 数据中心网络系统设计文档 • 数据中心网络系统实施文档、实施结果总结文档 • 数据中心路由实施方案 • 数据中心路由、交换机配置	• vlan划分文档 • IP地址和VLan分配文档 • 路由设计实施方案 • 地址转换设计文档	• 网络系统安全设计实施文档（通信安全、安全区域设计、数据安全设计、防火墙防病毒网关等安全设备上线实施文档等） • 数据中心网络系统安全策略文档 • 负载均衡设计实施文档	• 包含链接冗余、机箱冗余、STP设计、FHRP设计、路由协议冗余设计、防火墙冗余、负载均衡冗余、通信流设计	• 数据中心命名规范（主机名、标签等） • 用户账号的管理制度 • 备份和修复设计 • SNMP相关文档 • CDP/LLDP设计 • 网络设备进行资产登记制度 • 机房、线缆、配电等物理安全方面周期检查制度档

组织实施

网络架构

1

通信传输

2

边界防护

3

访问控制

4

入侵防范

5

恶意代码防范

6

安全审计

7

集中监控

8

检查维度	检查点	
网络架构	1. 保证网络设备的业务处理能力具备冗余空间，满足业务高峰期需要	1) 访谈网络管理员，询问边界和主要网络设备的性能（CPU、Memory、会话连接数等）以及目前业务高峰流量情况
	2.应保证网络中各个部分的带宽满足业务高峰期需要	1) 访谈网络管理员，询问网络的带宽情况；询问网络中带宽控制情况以及带宽分配的原则
		2) 检查网络设计/验收文档，查看是否有边界和网络设备业务处理能力、网络接入及核心网络的带宽满足业务高峰期的需要以及不存在带宽瓶颈等方面的设计或描述
		3) 检查边界和网络设备，查看是否有对带宽进行控制的策略（如路由、交换设备上的QOS策略配置情况，专用的带宽管理设备的配置策略等），这些策略能否保证在网络发生拥堵的时候优先保护重要业务（如重要业务的主机的优先级要高于非重要业务的主机）
	3.网络应划分不同的网络区域，并按照方便管理和控制的原则，为各网络区域分配地址空间	1) 访谈网络管理员，询问网段划分情况以及划分原则
		2) 访谈网络管理员，询问网络设备的路由控制策略措施有哪些，这些策略设计的目的是什么
		3) 检查网络拓扑图，查看其与当前运行情况是否一致
		4) 检查网络设计/验收文档，查看是否有根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网和网段分配地址段的设计或描述
		5) 检查边界和网络设备，查看是否配置路由控制策略（如使用静态路由等）建立安全的访问路径
	4.避免将重要网络区域部署在网络边界处且没有边界防护措施	1) 应访谈安全管理员，询问重要业务的网络区域有哪些，是否将重要网段部署在网络边界处，边界和网络设备的保护策略措施有哪些
		2) 应检查边界和网络设备，重要网段和其它网段之间应配置安全策略进行网络边界隔离
	5.应提供通信线路、关键网络设备的硬件冗余，保证系统的可用性	1) 应检查设计/验收文档，查看其是否有关于网络单点故障的处理描述以及网络设备、通信线路的高可用性采用的技术描述
		2) 应访谈网络管理员，询问网络设备是否提供数据本地和异地备份与恢复功能，完全数据备份的周期；备份介质是否场外存放
		3) 应检查网络拓扑结构是否不存在网络单点故障
		4) 应检查网络设备、通信线路是否采用硬件冗余、软件配置等技术手段提供系统的高可用性
		5) 应检查冗余测试文档，查看是否有开展冗余测试，以及冗余测试的完整性和有效性
	6.网络建设应具有规范性，网络设备命名、设备标签、线缆标签、端口描述等应具备一定的规范性	1) 访谈网络管理员，询问网络设备配置是否遵循相关的规范，设备上架、线缆铺设时是否按要求设立响应的标签信息
		2)检查设备配置，查看设备命名方式、端口描述信息，设备标签、线缆标签等是否统一规范，是否清晰描述对应的功能信息

网络防护分析方法

顾问访谈	• 业务功能、应用结构和网络拓扑、安全现状调查 • 系统分析和系统安全分析情况的分角色沟通和确认 • 运维管理情况的分角色访谈
文档审核	• 现有系统设计方案、实施记录收集和分析 • 安全技术策略、管理制度、运维纪录收集和分析 • 进行适用性检查
调查问卷	• 信息资产调查 • 系统基本情况调查
工具使用	• RSAS、Nmap、IPS • 抽样采集技术脆弱性数据
人工检查	• 网络现状收集和分析 • 网络设备、安全产品、操作系统和应用系统安全抽样检查

评估总结

评估总结会

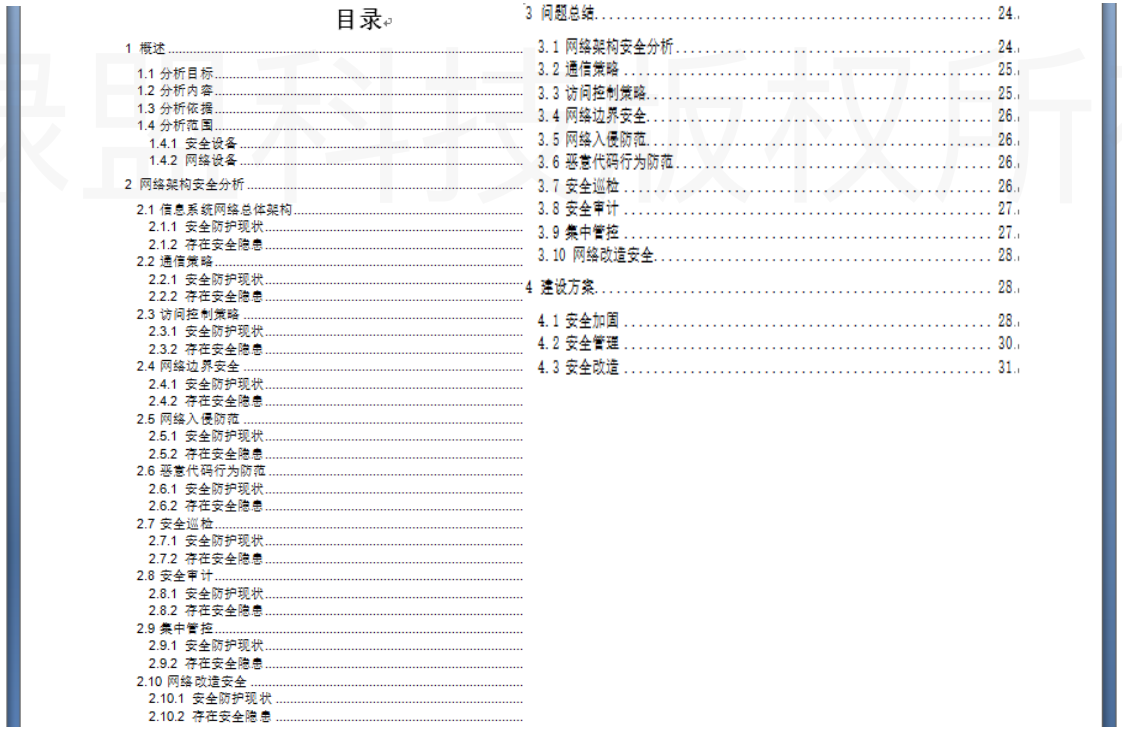
- 现场评估完成后，由评估组组织召开评估工作总结会议，对评估结果进行确认，并形成评估报告。

评估报告

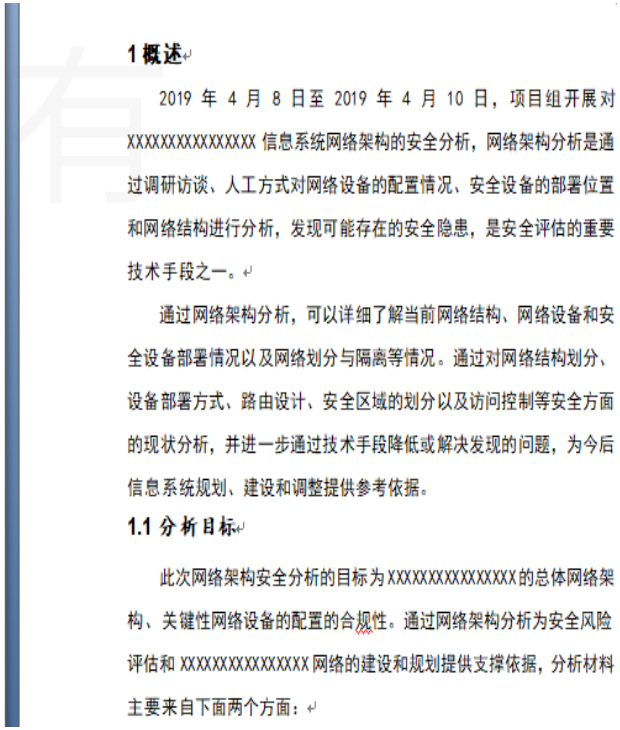
- 网络架构分析报告：包括检查概况、不符合安全要求、安全建议。

XXXXXXXXXXXXXXXX
网络架构分析报告

绿盟科技
2019 年 4 月



目录



1 概述

2019 年 4 月 8 日至 2019 年 4 月 10 日，项目组开展对 XXXXXXXXXXXXXXX 信息系统网络架构的安全分析，网络架构分析是通过调研访谈、人工方式对网络设备的配置情况、安全设备的部署位置和网络结构进行分析，发现可能存在的安全隐患，是安全评估的重要技术手段之一。

通过网络架构分析，可以详细了解当前网络结构、网络设备和安全设备部署情况以及网络划分与隔离等情况。通过对网络结构划分、设备部署方式、路由设计、安全区域的划分以及访问控制等安全方面的现状分析，并进一步通过技术手段降低或解决发现的问题，为今后信息系统规划、建设和调整提供参考依据。

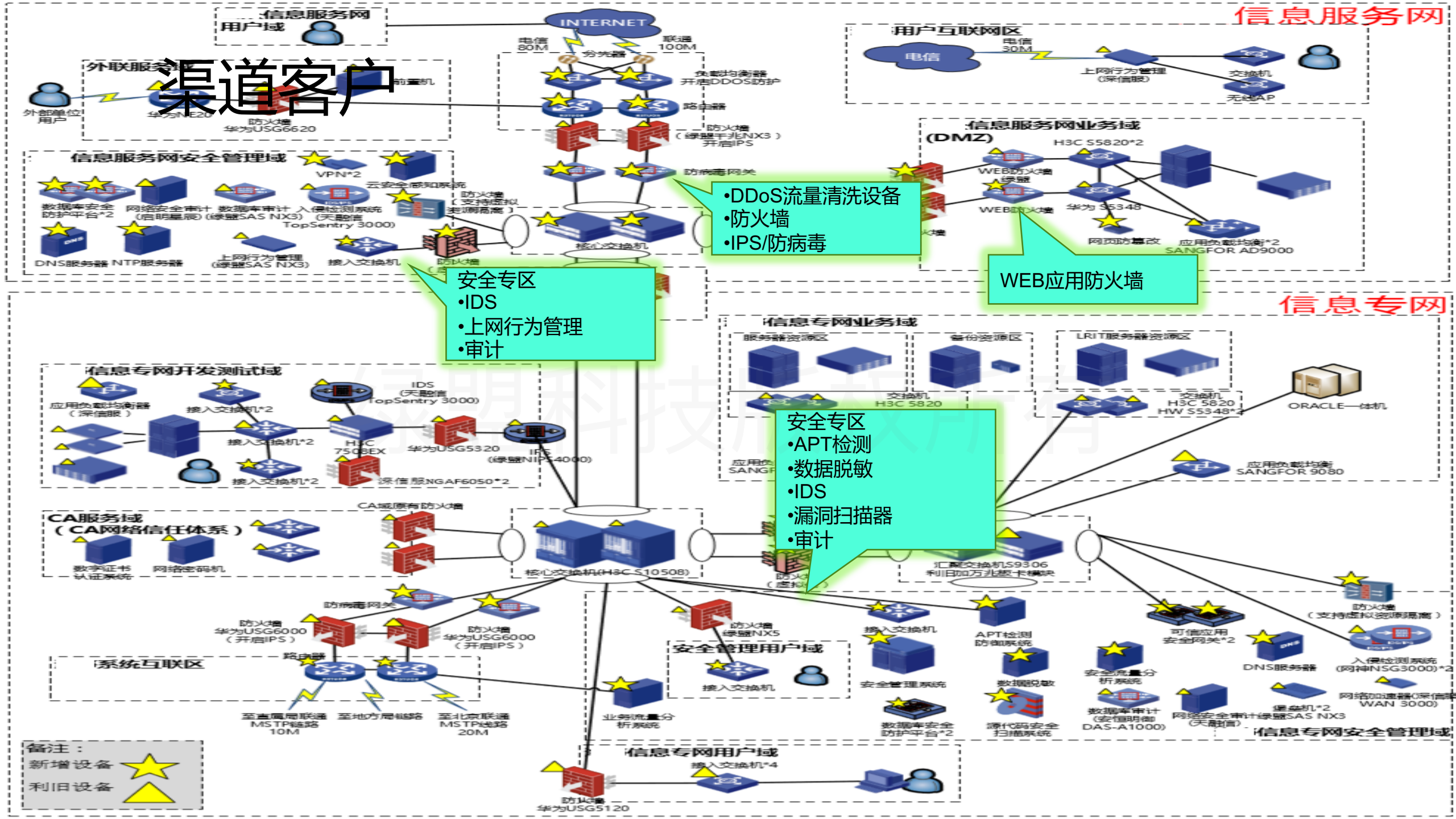
1.1 分析目标

此次网络架构安全分析的目标为 XXXXXXXXXXXXXXX 的总体网络架构、关键性网络设备的配置的合规性。通过网络架构分析为安全风险评估和 XXXXXXXXXXXXXXX 网络的建设和规划提供支撑依据，分析材料主要来自下面两个方面：

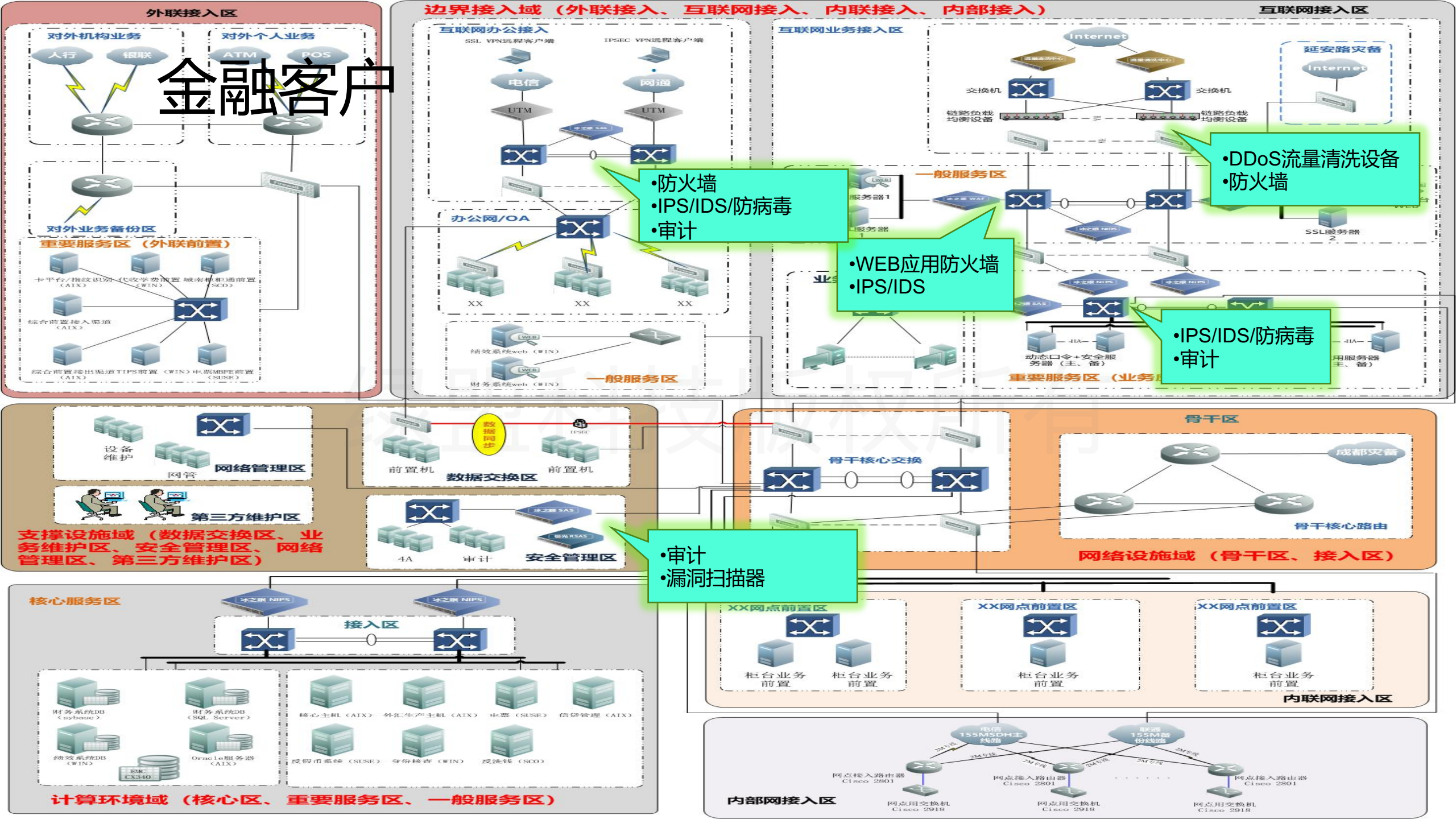
NSFOCUS

03

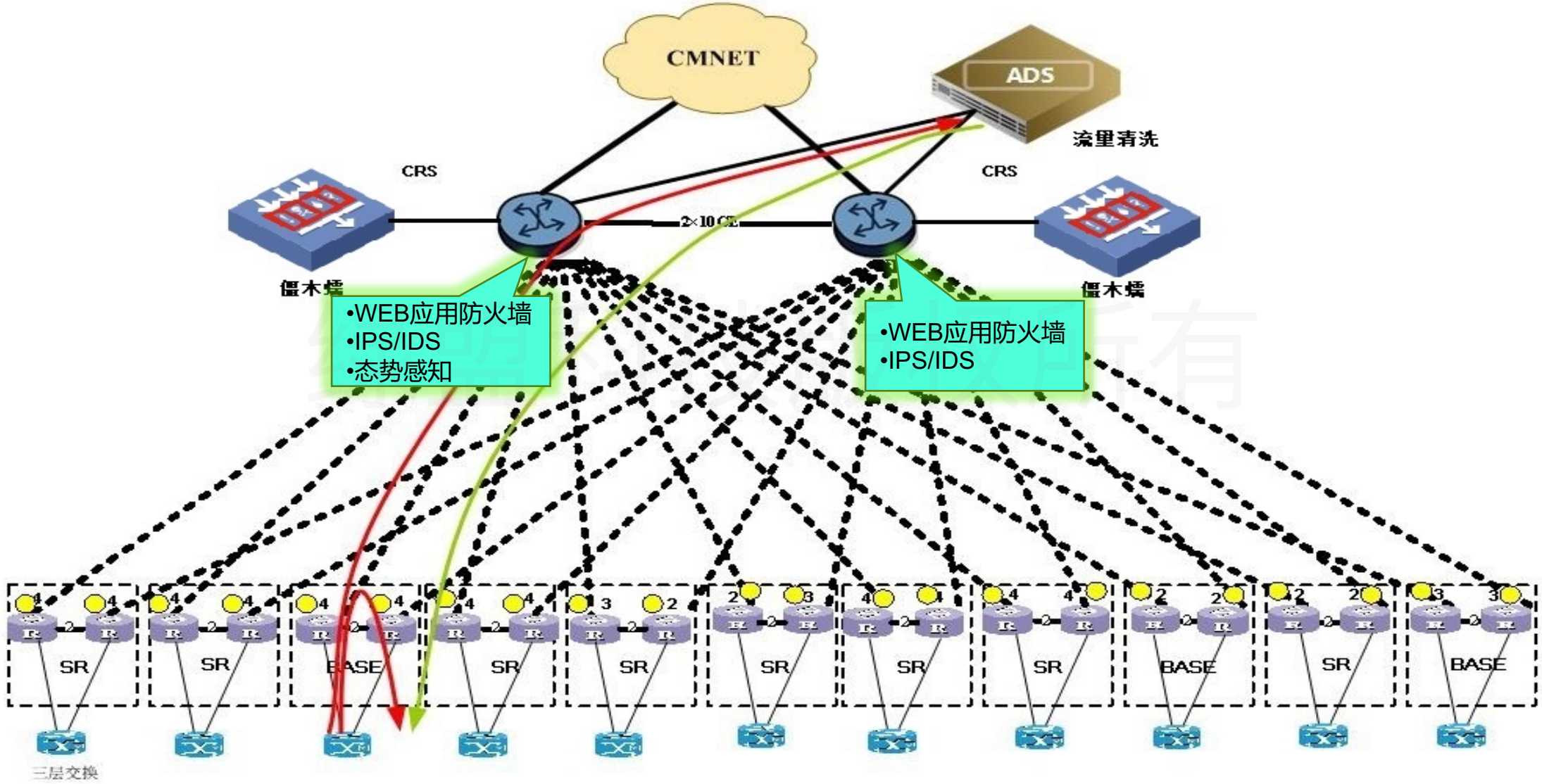
网络防护分析案例


渠道客户
信息服务网
信息专网
INTERNET
信息服务网用户域
外联服务域
用户互联网区
电信
电信 80M
联通 100M
分光器
负载均衡器 开启DDOS防护
路由器
防火墙 华为USG6620
防火墙（绿盟千兆NX3）开启IPS
防病毒网关
信息服务网安全管理域
VPN*2
云安全感知系统
数据库安全防护平台*2
网络安全审计（启明星辰）
数据库审计（绿盟SAS NX3）
入侵检测系统（天融信TopSentry 3000）
防火墙（支持虚拟资源隔离）
DNS服务器
NTP服务器
上网行为管理（绿盟SAS NX3）
接入交换机
核心交换机
防火墙
上网行为管理（深信服）
交换机
无线AP
信息服务网业务域（DMZ）
H3C S5820*2
WEB防火墙 绿盟
WEB防火墙
华为 S5348
网页防篡改
应用负载均衡*2 SANGFOR AD9000
•DDoS流量清洗设备
•防火墙
•IPS/防病毒
WEB应用防火墙
安全专区
•IDS
•上网行为管理
•审计
信息专网开发测试域
应用负载均衡器（深信服）
接入交换机*2
IDS（天融信TopSentry 3000）
H3C 7503EX
华为USG5320
IPS（绿盟NIPS4000）
深信服NGAF6050*2
信息专网业务域
服务器资源区
备份资源区
LRIT服务器资源区
交换机 H3C 5820
交换机 H3C 5820 HW S5348*4
ORACLE一体机
应用负载均衡 SANGFOR 9080
安全专区
•APT检测
•数据脱敏
•IDS
•漏洞扫描器
•审计
CA服务域（CA网络信任体系）
数字证书认证系统
网络密码机
CA域原有防火墙
核心交换机H3C S10508
汇聚交换机S9306 利旧加万兆板卡模块
防病毒网关
防火墙 华为USG6000（开启IPS）
防火墙 绿盟NX5
接入交换机
安全管理用户域
安全管理系统
APT检测防御系统
数据脱敏
源代码安全扫描系统
安全流量分析系统
数据库审计（安恒明御DAS-A1000）
数据库安全防护平台*2
可信应用安全网关*2
DNS服务器
堡垒机*2 绿盟SAS NX3
网络加速器（深信服WAN 3000）
入侵检测系统（网神NSG3000）*2
防火墙（支持虚拟资源隔离）
系统互联区
路由器
至直属局联通MSTP链路 10M
至地方局链路
至北京联通MSTP链路 20M
业务流量分析系统
信息专网用户域
接入交换机*4
防火墙 华为USG5120
信息专网安全管理域
备注：
新增设备
利旧设备

金融客户


外联接入区
对外机构业务
人行
银联
对外个人业务
ATM
POS
对外业务备份区
重要服务区（外联前置）
综合前置接入渠道（AIX）
综合前置接出渠道TIPS前置（WIN）
电票MBFE前置（SUSE）
边界接入域（外联接入、互联网接入、内联接入、内部接入）
互联网接入区
互联网办公接入
SSL VPN远程客户端
IPSEC VPN远程客户端
电信
网通
UTM
办公网/OA
XX
一般服务区
绩效系统web（WIN）
财务系统web（WIN）
互联网业务接入区
Internet
交换机
链路负载均衡设备
延安路灾备
一般服务区
SSL服务器
重要服务区（业务
动态口令+安全服务器（主、备）
用服务器（主、备）
•防火墙
•IPS/IDS/防病毒
•审计
•DDoS流量清洗设备
•防火墙
•WEB应用防火墙
•IPS/IDS
•IPS/IDS/防病毒
•审计
设备维护
网管
网络管理区
第三方维护区
支撑设施域（数据交换区、业务维护区、安全管理区、网络管理区、第三方维护区）
前置机
数据同步
IPSEC
数据交换区
4A
审计
安全管理区
•审计
•漏洞扫描器
骨干区
骨干核心交换
成都灾备
骨干核心路由
网络设施域（骨干区、接入区）
核心服务区
接入区
财务系统DB（sybase）
财务系统DB（SQL Server）
绩效系统DB（WIN）
Oracle服务器（AIX）
核心主机（AIX）
外汇生产主机（AIX）
电票（SUSE）
信贷管理（AIX）
反假币系统（SUSE）
身份核查（WIN）
反洗钱（SCO）
计算环境域（核心区、重要服务区、一般服务区）
XX网点前置区
柜台业务前置
内联网接入区
电信155MSDH主线路
联通155M备份线路
网点接入路由器 Cisco 2801
网点用交换机 Cisco 2918
内部网接入区

运营商客户



NSFOCUS

谢谢！

NSFOCUS