



网络应用审计专家
(证券代码 300311)

任子行WEB应用防火墙

(SURF - WAF)

任子行网络科技股份有限公司
SURFILTER NETWORK TECHNOLOGY CO.,LTD.

1

应用背景

2

产品介绍

3

技术优势

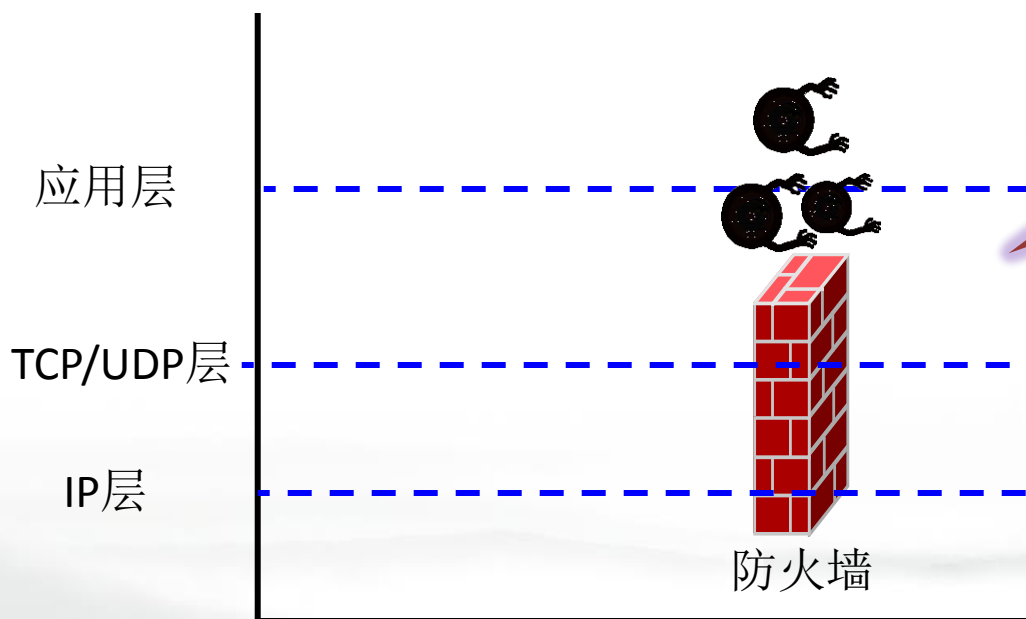
4

部署方式

IPS vs UTM vs FW vs WAF

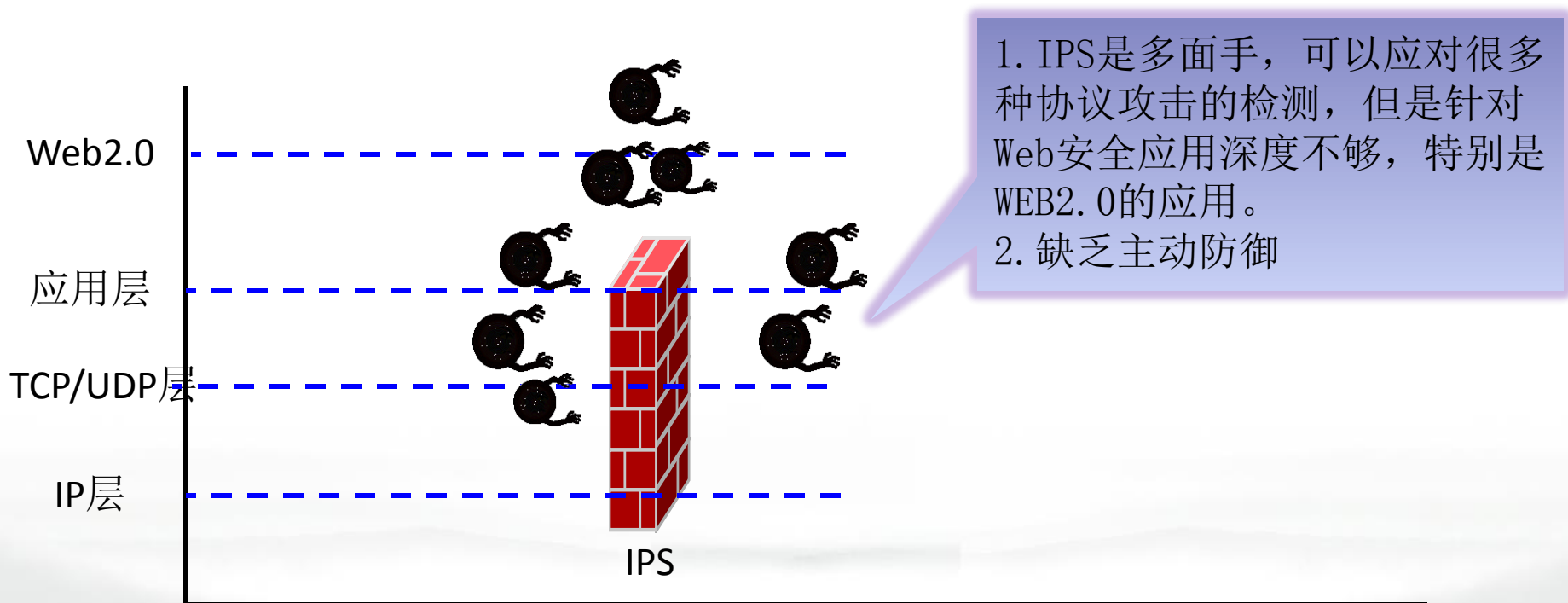
一个争吵了好久的问题.....

- 防火墙 (Firewall) 的不足

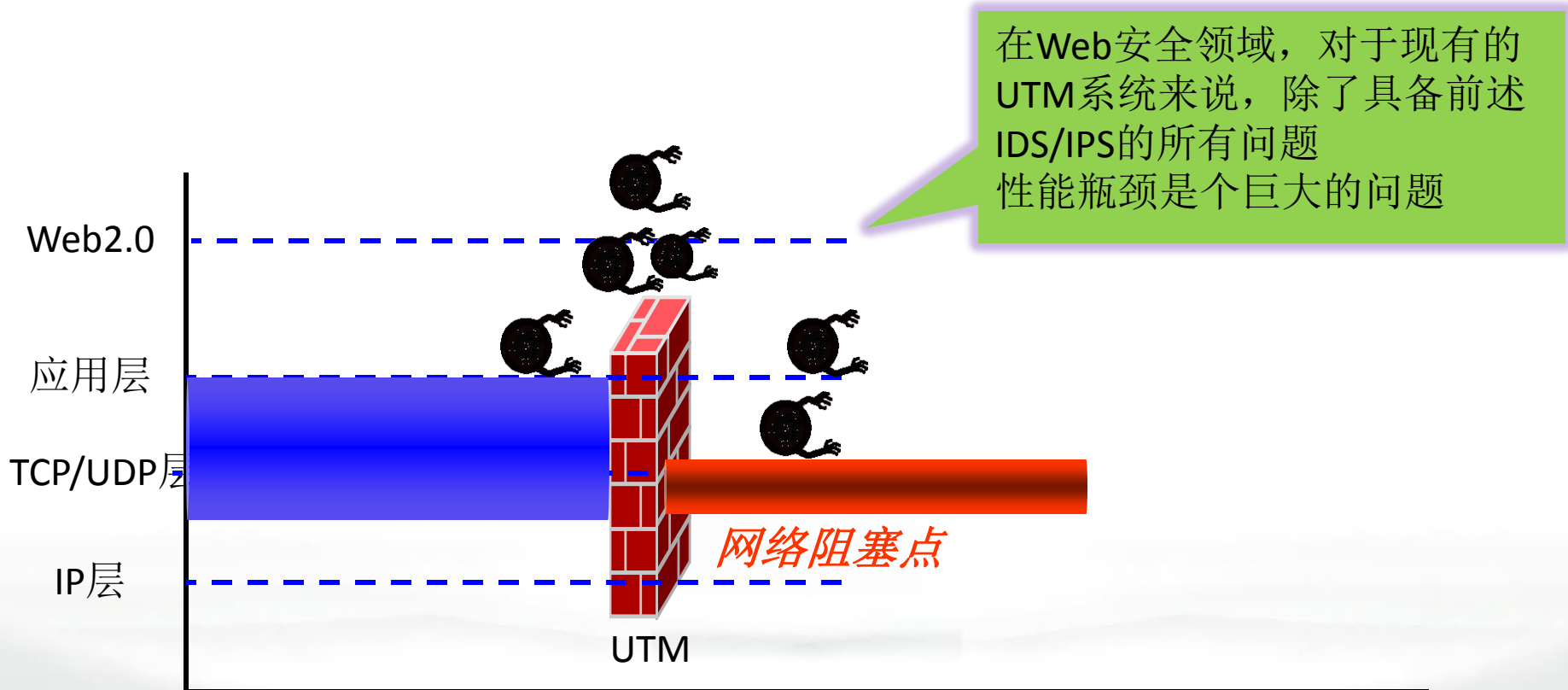


防火墙对于3, 4层进行访问控制。不对应用层进行分析, 无法防范大多数的基于Web的攻击。

- 入侵保护系统 (IDS/IPS) 的不足



- 统一威胁管理 (UTM) 的不足



现有产品形态分析 - FW/IPS/UTM/WAF

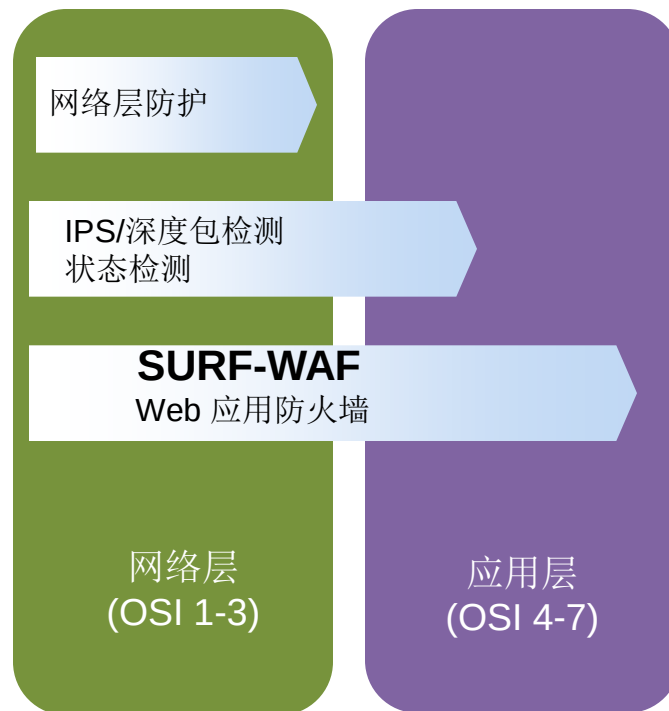
网络应用审计专家

技术	原理	工作机制	不足
传统网络防火墙	网络层、传输层 访问控制	✓端口阻断 ✓UDP/TCP状态感知	✓仅对网络层进行保护，不能对应用层保护
传统入侵防御IPS	基于规则的网络保护	✓基于规则的检测 ✓阻断连接 ✓UDP/TCP状态感知	✓ 分析深度不够 ✓ 不适应WEB2.0 ✓ 缺乏主动防御
综合安全网关（UTM）	集成了IPS,AV，防火墙等多种安全功能	✓集成IPS ✓集成AV ✓集成防火墙	✓处理性能不足 ✓WEB分析深度不足 ✓缺乏主动防御

应用安全需要新的解决方案

网络应用审计专家

- 网络防火墙检测网络攻击
 - 检查ip地址和端口
- IPS 只能检测到已知攻击
 - 规避这种检测方法是非常可能的
 - 无法保护SSL流量
 - 不能真正理解HTTP(如：HTTP头，参数等等)
 - 没有应用识别能力
 - 无法识别用户
 - 误判率较高



**只有web应用防火墙可以
检测并拦截应用攻击**

目录

网络应用审计专家

1

应用背景

2

产品介绍

3

技术优势

4

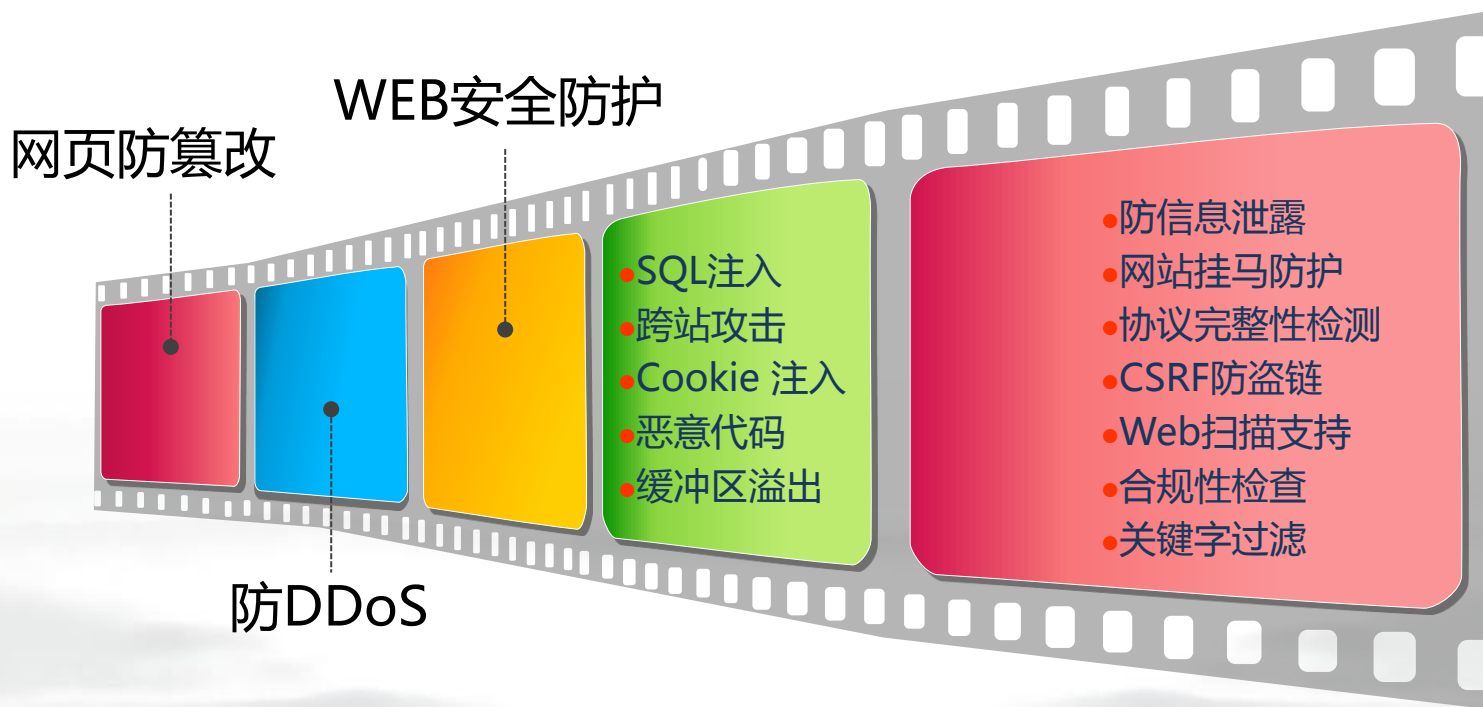
部署方式

任子行WEB应用防火墙介绍

网络应用审计专家

• SURF-WAF :

任子行SURF-WAF应用防火墙是任子行公司在多年应用安全技术积累的基础上，自主研发的新一代安全产品，作为网关设备，防护对象为Web、WebMail等应用服务器，可针对安全事件发生时序进行安全建模，分别针对安全漏洞、攻击手段及最终攻击结果进行扫描、防护及诊断，提供综合Web应用安全解决方案。



SURF-WAF功能概览

网络应用审计专家



WEB应用防火墙 - WAF

加固web应用站点帮助客户实现合规需求



Web漏洞扫描

扫描，分析，检查web应用漏洞



网络加速

应用加速

加速确保实时提交web应用站点支付内容



负载均衡Load Balancing

保证可持续的性能高可用的web应用



加固WEB应用

保护web服务

优化web业务提交

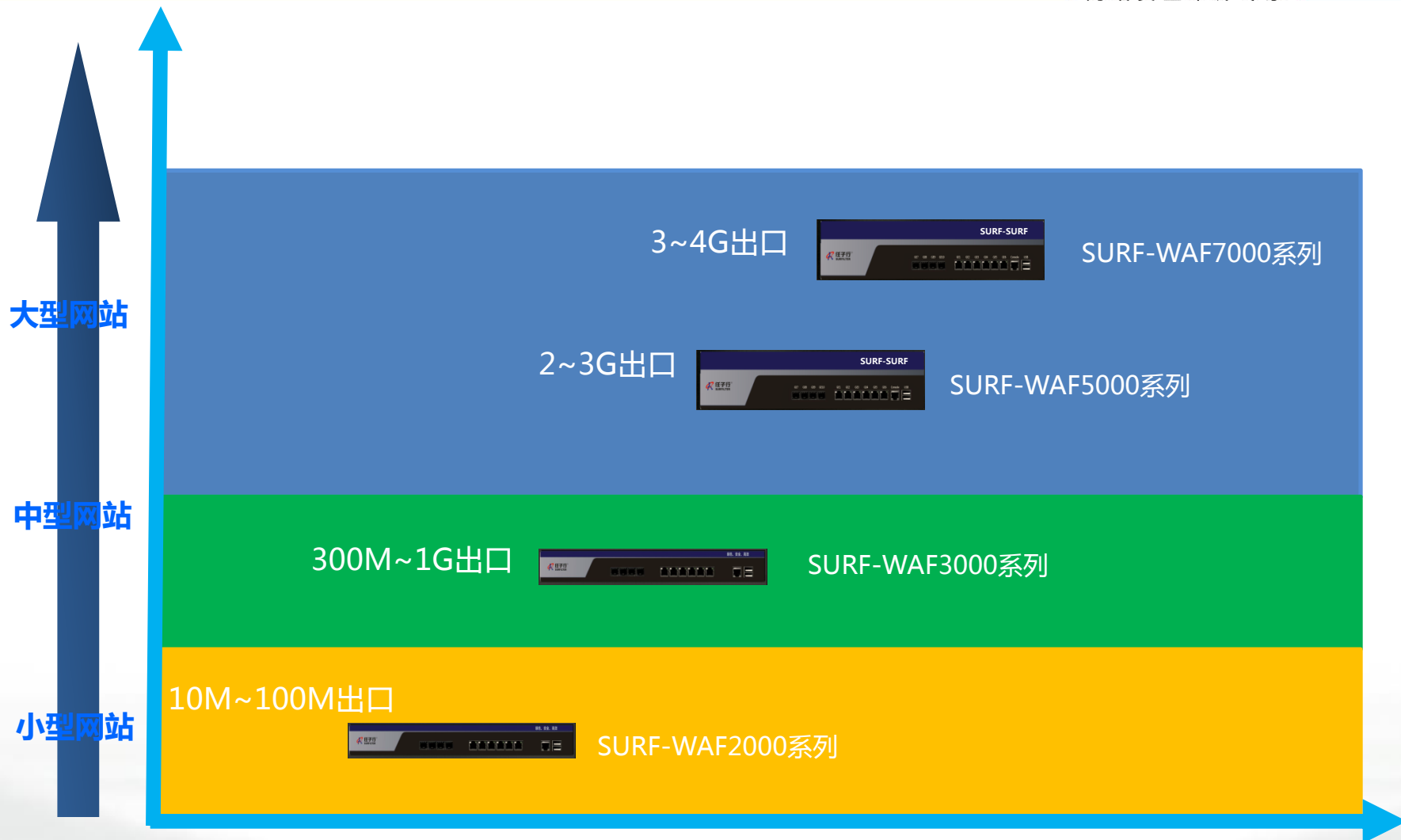
工作流程图

网络应用审计专家



任子行WEB应用防火墙概览

网络安全审计专家



设备扩展能力、处理能力、高可用性

目录

网络应用审计专家

1

应用背景

2

产品介绍

3

技术优势

4

部署方式



高级保护 - 自定义的安全策略

- 自定义策略来匹配多个元素 - URL, 源IP, HTTP头类型和值, 阈值



上传文件的进行病毒扫描和数据泄漏防护

- 对上传文件进行病毒和恶意软件扫描 (RZXGenter的更新)
- 检测信息泄露, 信用卡和PII (Personally Identifiable Information) 泄漏



应用层和网络层DoS防护 (DoS/DDoS 防护)

- 检测和聚合来自多方的DoS攻击



自动学习和验证规则

- 偏离正常用户行为, 自动化和自定义规则的访问行为



应用攻击特征库

- 检测已知的应用程序的攻击
- RZXGenter更新



协议验证

- 验证HTTP的RFC合规性

• OWASP Top 10

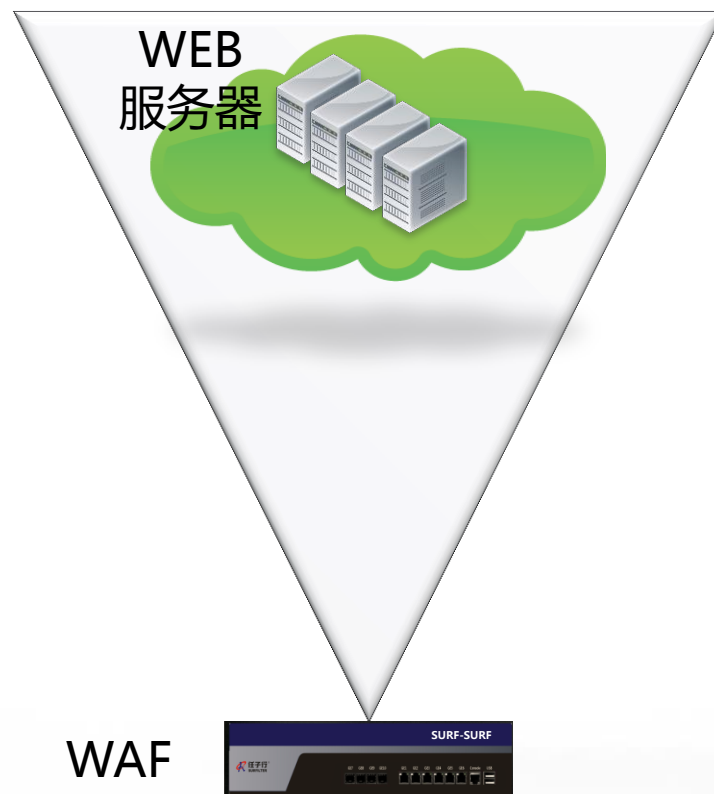
- 注入攻击
- 跨站脚本
- 失效的验证和会话管理
- 不安全的直接对象引用
- 跨站请求伪造
- 安全性配置错误
- 非安全的加密存储
- 未能限制URL访问
- 不足的传输层保护
- 未经验证的重定向和转发

• SURF-WAF

- 使用多个安全层来防止OWASP Top 10
- 正向和反向安全模块
- 预置了很多保护策略可以满足很多需求
- 复杂的自动学习功能帮助识别正常行为和清除访问服务器配置错误和不安全的对象引用
- 预定义的DLP防止敏感信息的泄露
- 不安全的密码存储泄漏
- Cookie中毒保护、会话管理和流控制防止失效的身份验证和会话攻击

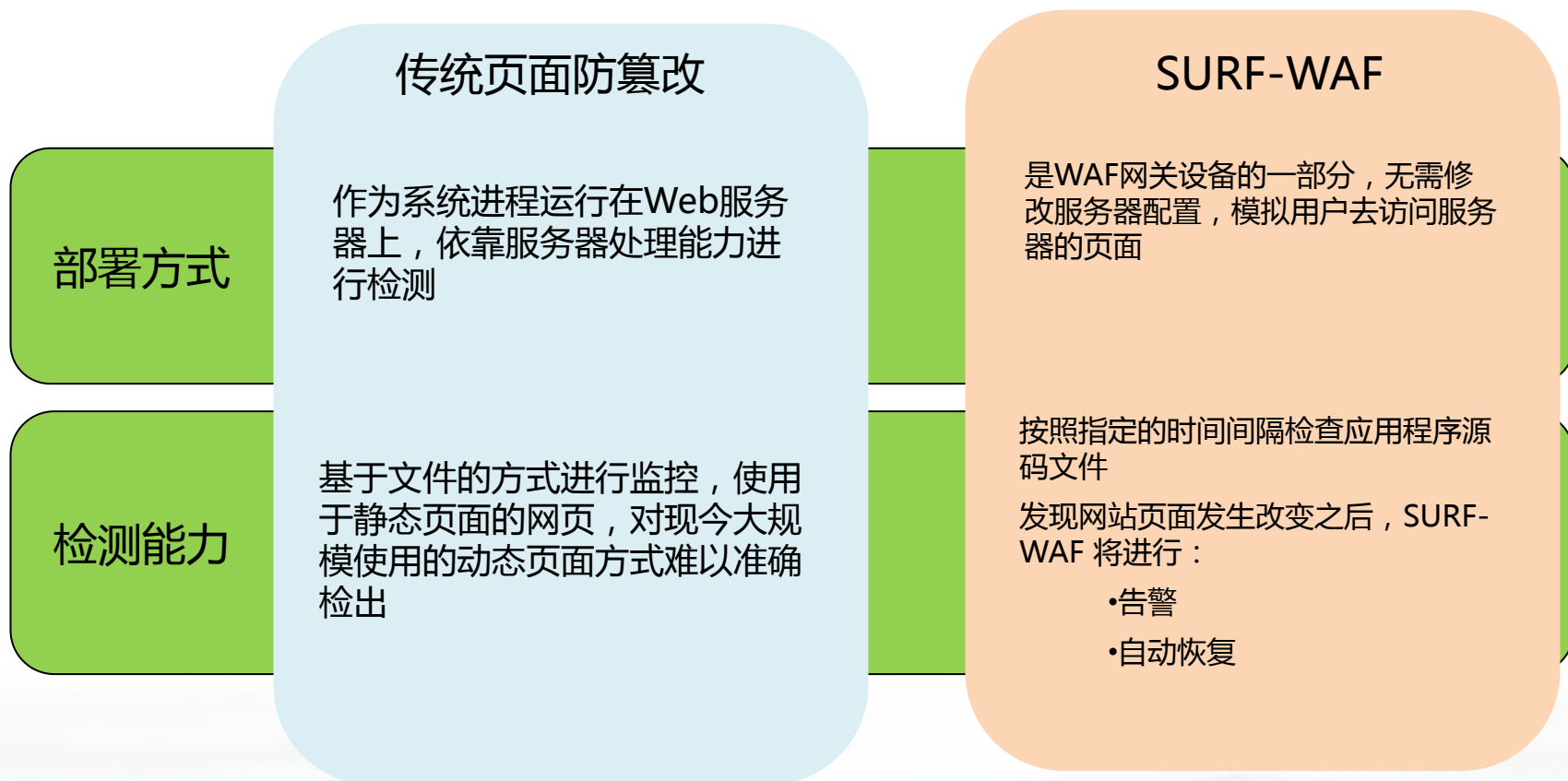


- 轻松扫描你的应用程序Web漏洞
 - 常见漏洞
 - SQL 注入
 - 跨站攻击
 - 源码泄露
 - OS 命令漏洞
- 增强型/标准模式
- 认证选项
- 精细控制扫描范围
- 计划扫描和按需扫描



网页防篡改-虚拟用户检测方式

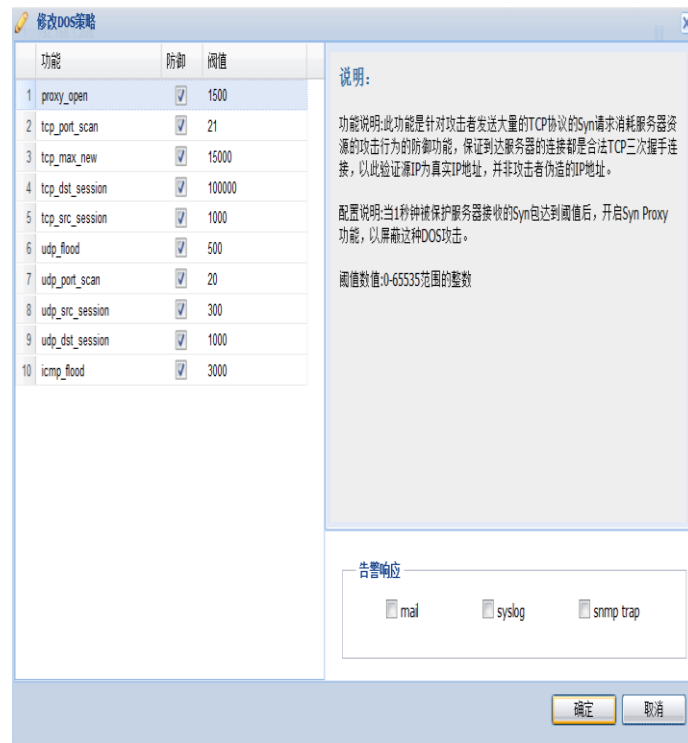
网络应用审计专家



基于应用和网络的DoS/DDoS防护

网络应用审计专家

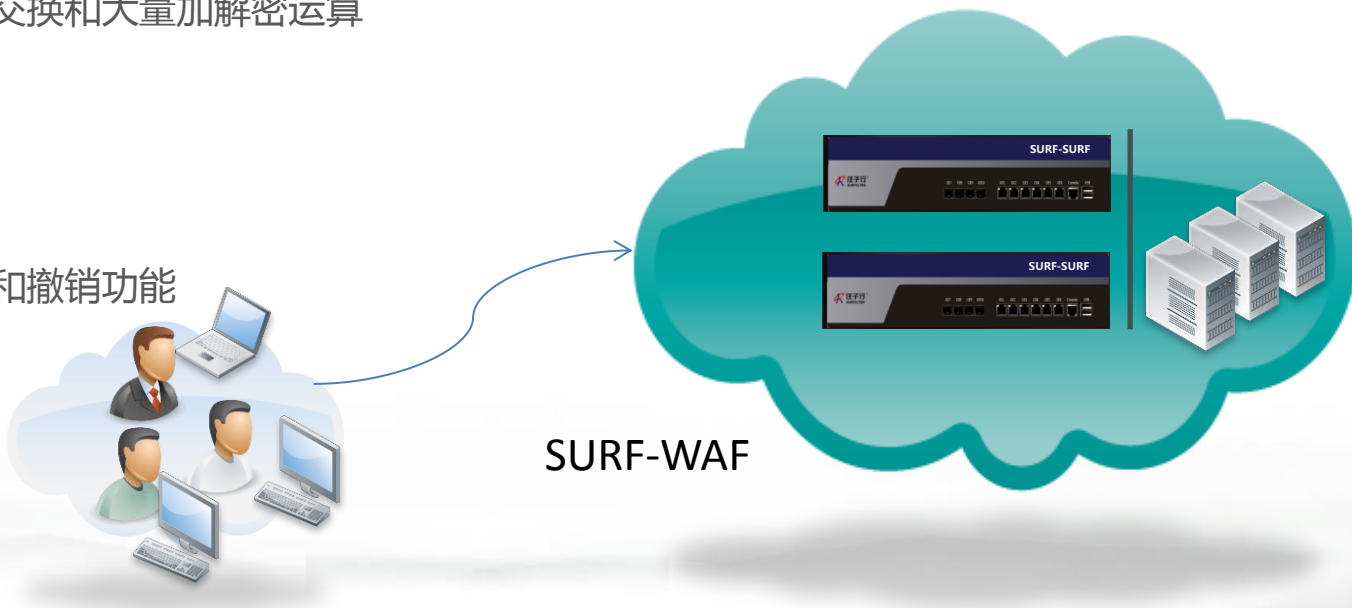
- 基于用户的不同特征来分析请求数据如IP 和Cookie
- 通过复杂的机制综合判断这些请求是真正的用户请求还是自动工具的攻击 (HOIC, LOIC tools)
- **应用层- 4种不同的策略**
 - **HTTP 访问限制**– 限制某个ip地址每秒钟发起的HTTP请求数量
 - **恶意攻击** – 限制具有相同Session cookie的TCP连接的数量
 - **HTTP Flood 洪水** – 相同session cookie每秒钟发出的HTTP请求
 - **真实浏览器访问限制** – 设置一秒内每个TCP连接中对某个URL发送的HTTP请求数量，一旦超过这个限制，SURF-WAF将发送一个脚本到客户端已验证客户端是浏览器还是一个自动化工具。
- **网络- 2种不同策略**
 - **TCP Flood 洪水** –限制 同一个源ip地址发起的TCP连接的数量
 - **SYN Cookie** – 防御SYN flood攻击



- NGFW-WAF监控所有出站流量，并防止：
 - 信息泄露
 - 信用卡被盗用/滥用



- 集成ASIC硬件芯片加速及硬件Bypass
- SSL卸载- 卸载对服务器性能影响较大的SSL加解密运算负担
 - 基于硬件的密钥交换和大量加解密运算
 - 建立SSL处理
 - 完整的证书管理
 - 高级认证的验证和撤销功能
- TCP连接复用



HTTPS 加速

网络应用审计专家

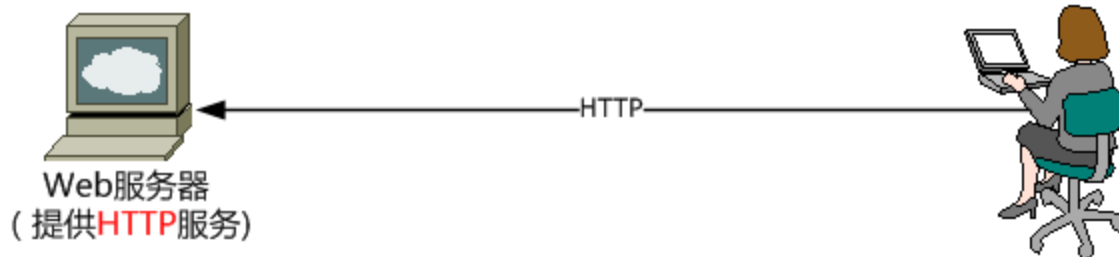


图1：客户原始配置，对外提供HTTP服务

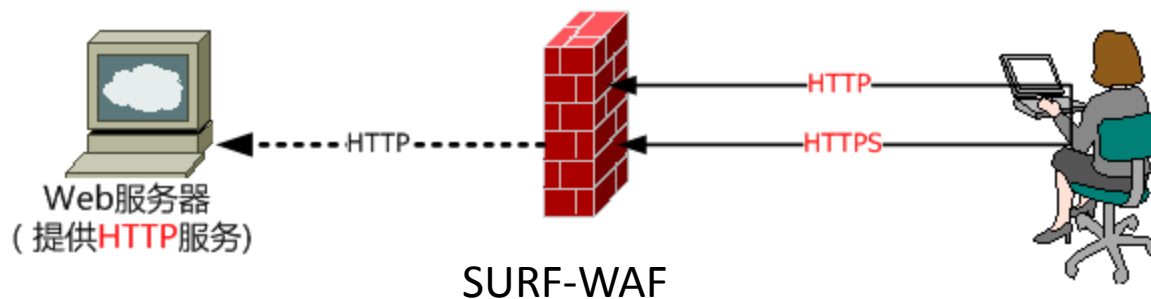


图2：WAF工作在HTTPS卸载模式，客户Web服务器配置不变，WAF充当HTTPS网守，提供加密功能，从而保证客户安全。

图：WAF作为HTTPS网守应用

HTTPS卸载

网络应用审计专家

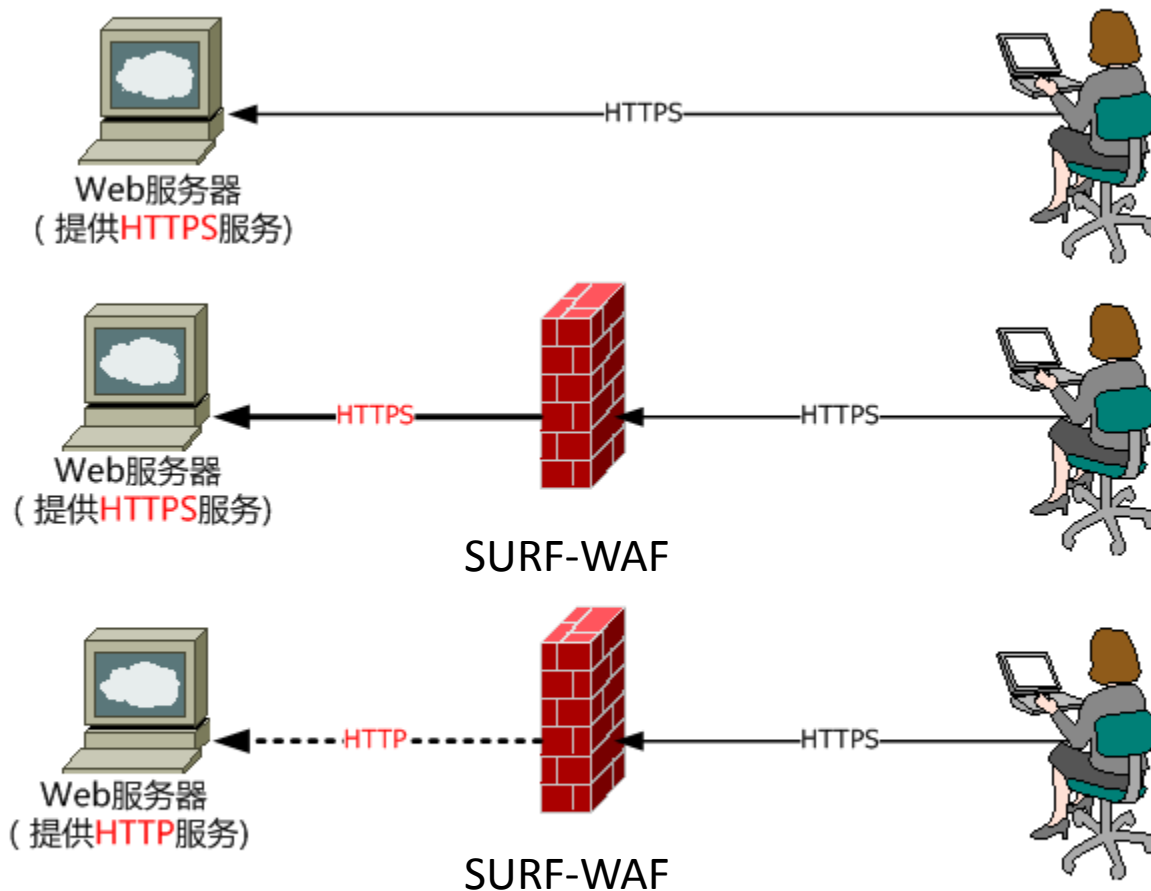


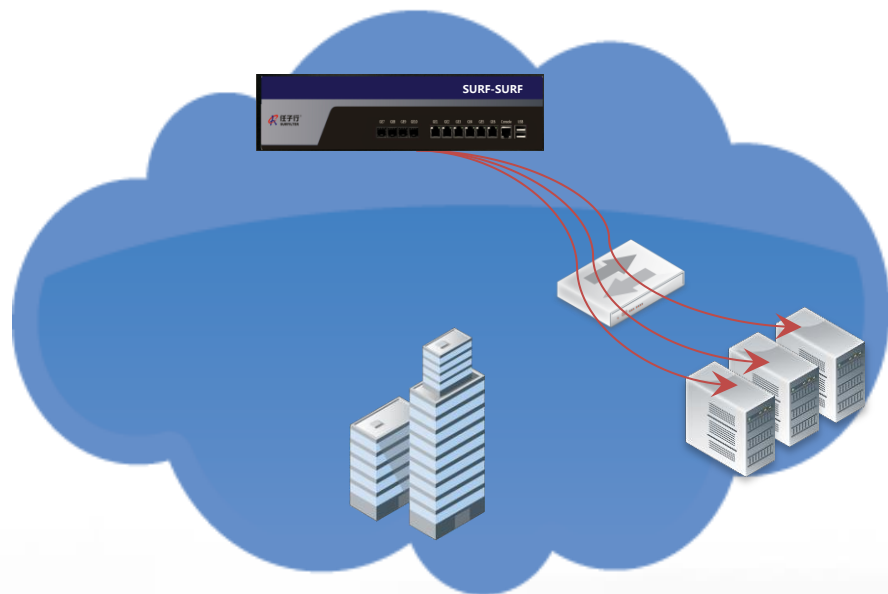
图1: 客户原始配置, 对外提供HTTPS服务

图2: WAF工作在HTTPS应用加速模式下, 客户Web服务器不用更改

图3: WAF工作在HTTPS卸载模式, 客户Web服务器改动由HTTPS服务转为HTTP服务

图: WAF作为HTTPS 卸载/加速应用

- 智能7层应用负载分担
- 只支持HTTP/HTTPS
- 丰富的负载均衡算法
 - 轮循
 - 权重轮循
 - 最少连接
 - 基于HTTP会话轮循
- 持久性连接
 - 连接超时时间
- 灵活的健康检查
 - 物理服务器检查支持HTTPS, HTTP, TCP, Ping
 - 支持利用正则表达式进行内容健康检查
- Web Services负载均衡
 - WSDL 或者内容路由



无与伦比的增值产品

网络应用审计专家



- 大幅降低企业数据丢失的风险。
 - 精准的保护与多层防御
 - 集成的Web漏洞扫描功能
 - 有效防御 OWASP Top 10攻击
- 使用自动学习基线的自动化管理
- 在任何环境中易于部署
 - 提供多种部署模式
- 应用加速
 - 应用负载均衡
 - 压缩
 - 基于ASIC芯片的 SSL加速
- 帮助PCI合规

目录

网络应用审计专家

1

应用背景

2

产品介绍

3

技术优势

4

部署方式

■ 二层 – 透明检测和纯粹透明代理

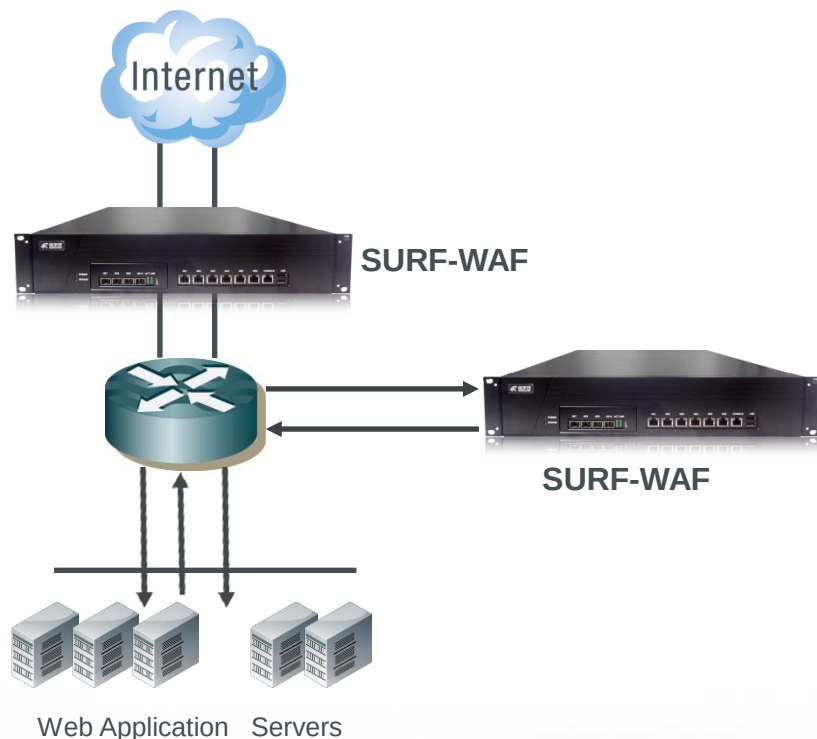
- 易于部署 – 对现有网络结构物任何影响，实现完全透明无缝接入
- 出现故障时实现硬件BYPASS

■ 反向代理

- 支持更改请求和响应内容
- 提供高级URL重写功能
- HTTPS 卸载
- 强大的HTTP负载均衡功能

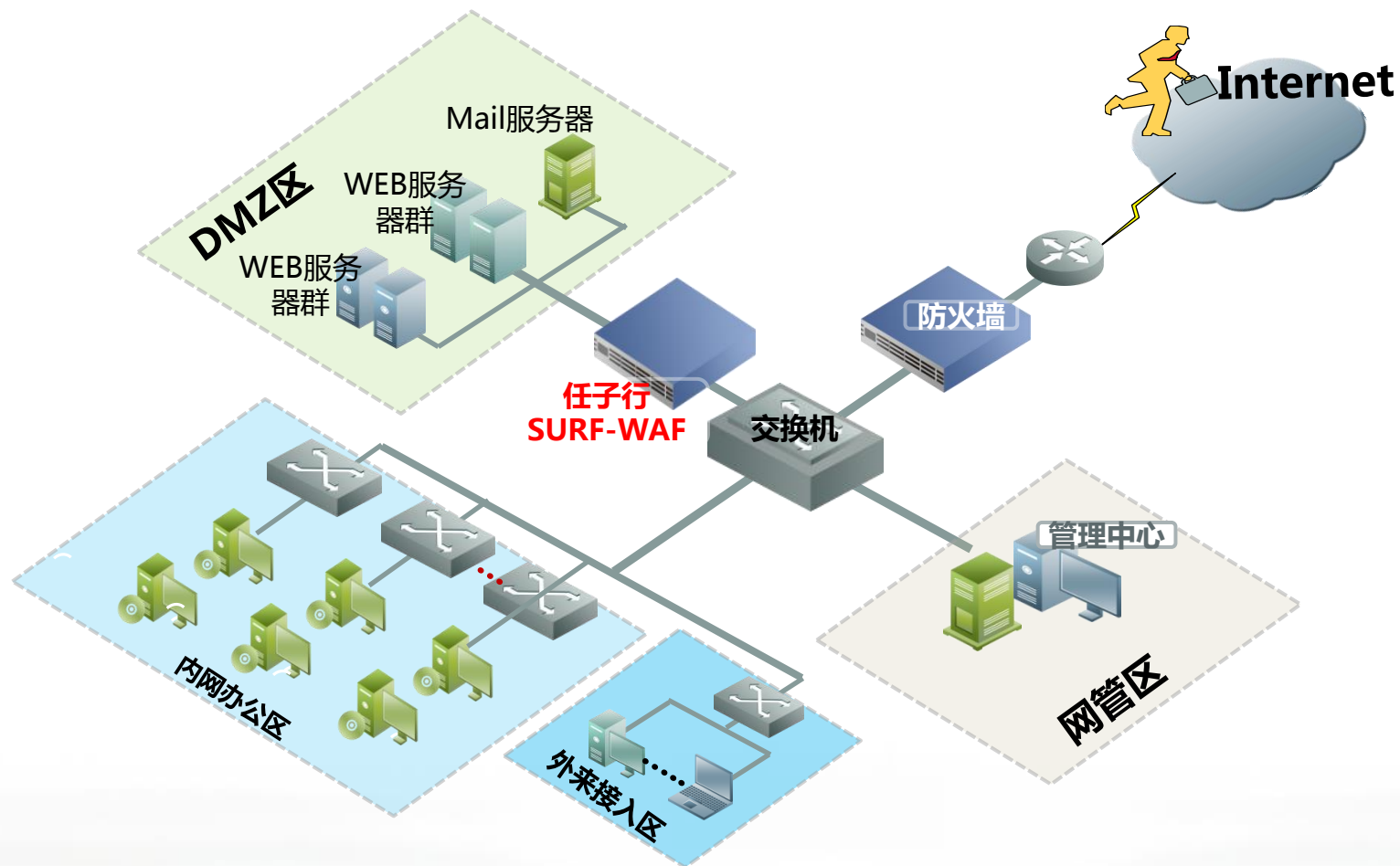
■ 离线检测– SPAN port

- 零网络延迟Zero network latency
- 使用TCP reset进行拦截攻击
- 非侵入性网络部署，产品评估理想部署模式



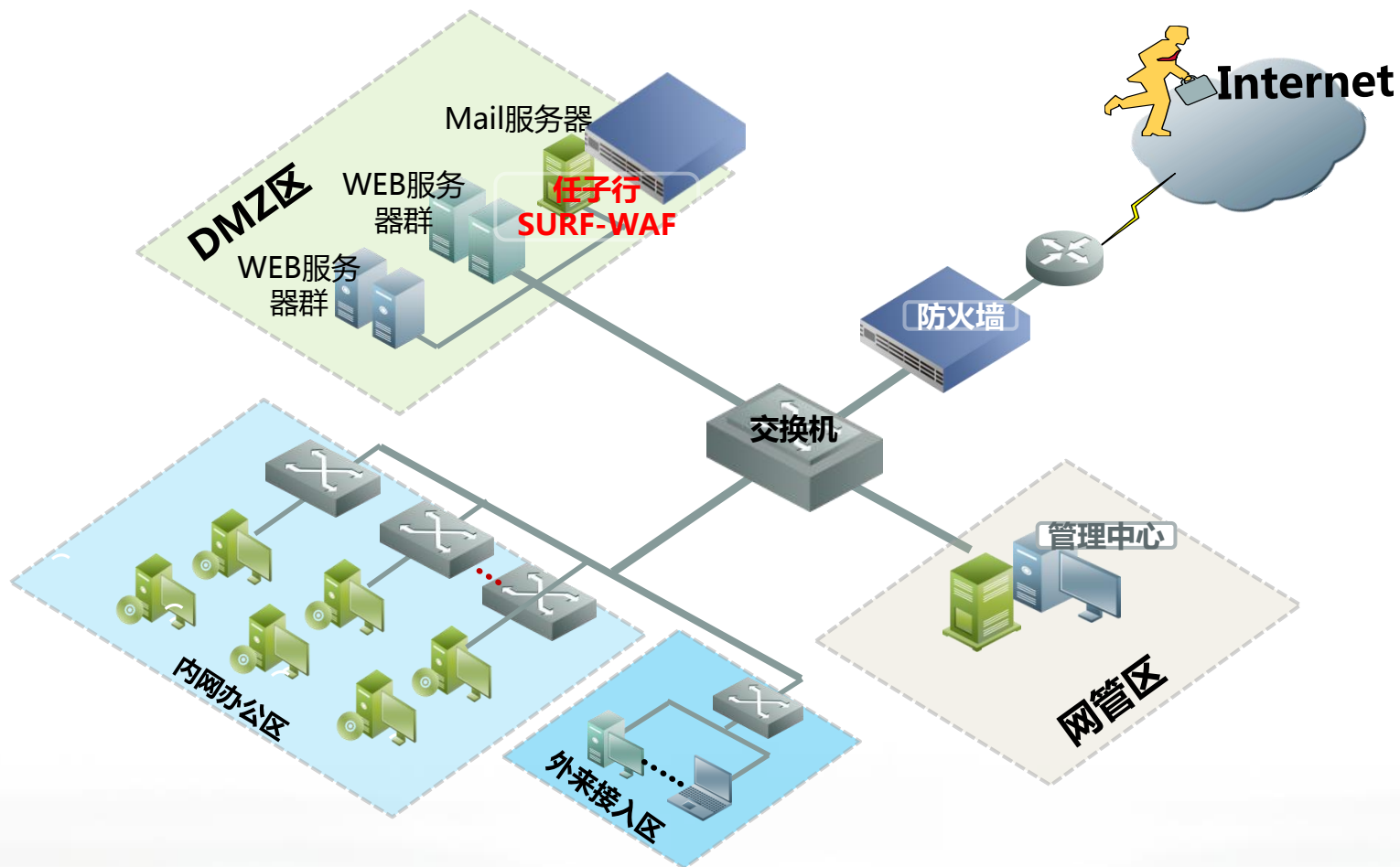
网桥部署

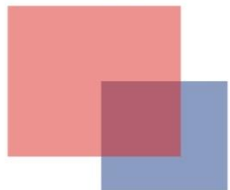
网络应用审计专家



反向代理

网络应用审计专家





Thanks

全国统一服务热线：400 700 1218

 **任子行[®]** | 网络应用审计专家
SURFILTER (证券代码 300311)