启明星辰远程办公安全解决方案

安全咨询顾问-舒江宁

目录

一、需求概述

1.1 远程办公场景模型

1.2 远程办公安全需求

1.3 启明星辰解决方案

1.4 解决方案覆盖行业

1.1 远程办公场景模型

远程办公定义：通过虚拟专用网，在公用网络中建立一个临时的、安全的连接，形成一条稳定的加密隧道，帮助远程用户、分支机构等接入内网办公。这种方式能够支持用户全方位的日常办公需求，包括获取公司内部邮件、访问局域网中的文件服务器、内部数据库、OA系统、ERP等等。上图是一个典型的远程办公场景的模型。

2020年初冠状病毒疫情推动了远程办公的发展。

一、需求概述

1.1 远程办公场景模型

1.2 远程办公安全需求

1.3 启明星辰解决方案

1.4 解决方案覆盖行业

1.2 远程办公安全需求

安全事件需相应	持续的可用性监控 重大安全事件告警与响应
攻击行为需防护	网络层攻击——DDoS、违规访问 应用层攻击——恶意爬虫、账号爆破、恶意注入等 恶意的操作——进入内网拖库、违规运维
异常状态可识别	行为异常状态识别——泄密、违规、超出基线的行为 恶意流量识别——病毒木马、勒索软件、漏洞利用等 系统异常识别——漏洞、可用性降低、被挂马等
身份权限需甄别	身份识别——防冒用 权限甄别——防滥用
网络通信防窃密	隧道传输安全保障——加密传输

一、需求概述

1.1 远程办公场景模型

1.2 远程办公安全需求

1.3 启明星辰解决方案

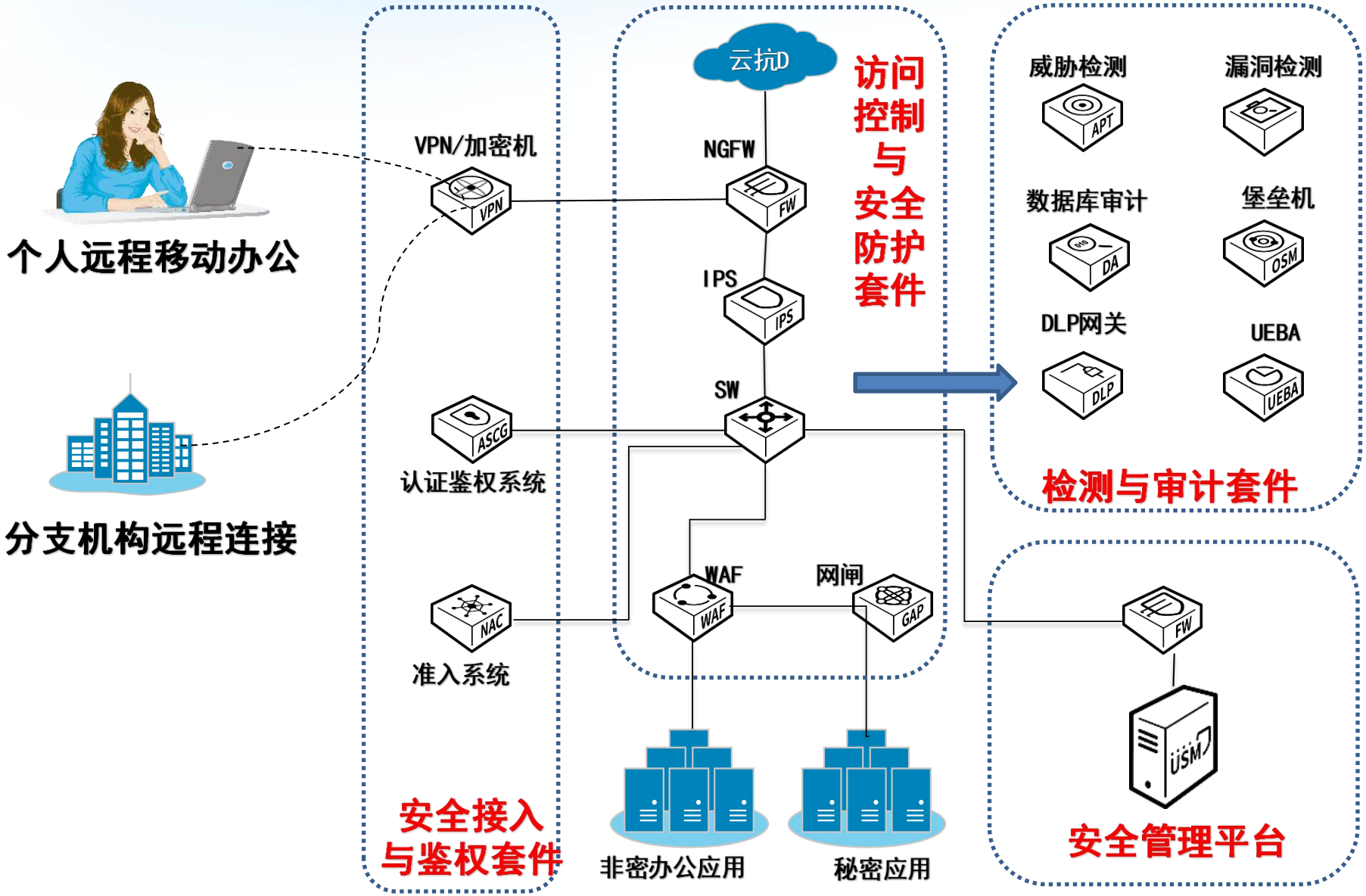
1.4 解决方案覆盖行业

1.3 启明星辰解决方案——远程接入的全面安全管控

启明星辰集团针对远程办公场景，推出了安全远程办公解决方案：

由四组安全套件，
形成五大安全能力，
提供六重安全防护。
全面保障远程办公环境安全

1.3 启明星辰解决方案——架构设计



一、需求概述

1.1 远程办公场景模型

1.2 远程办公安全需求

1.3 启明星辰解决方案

1.4 解决方案覆盖行业

1.4 解决方案覆盖行业

二、建设方案

2.1 安全远程接入

2.2 身份识别准入

2.3 边界安全防护

2.4 内外安全检测

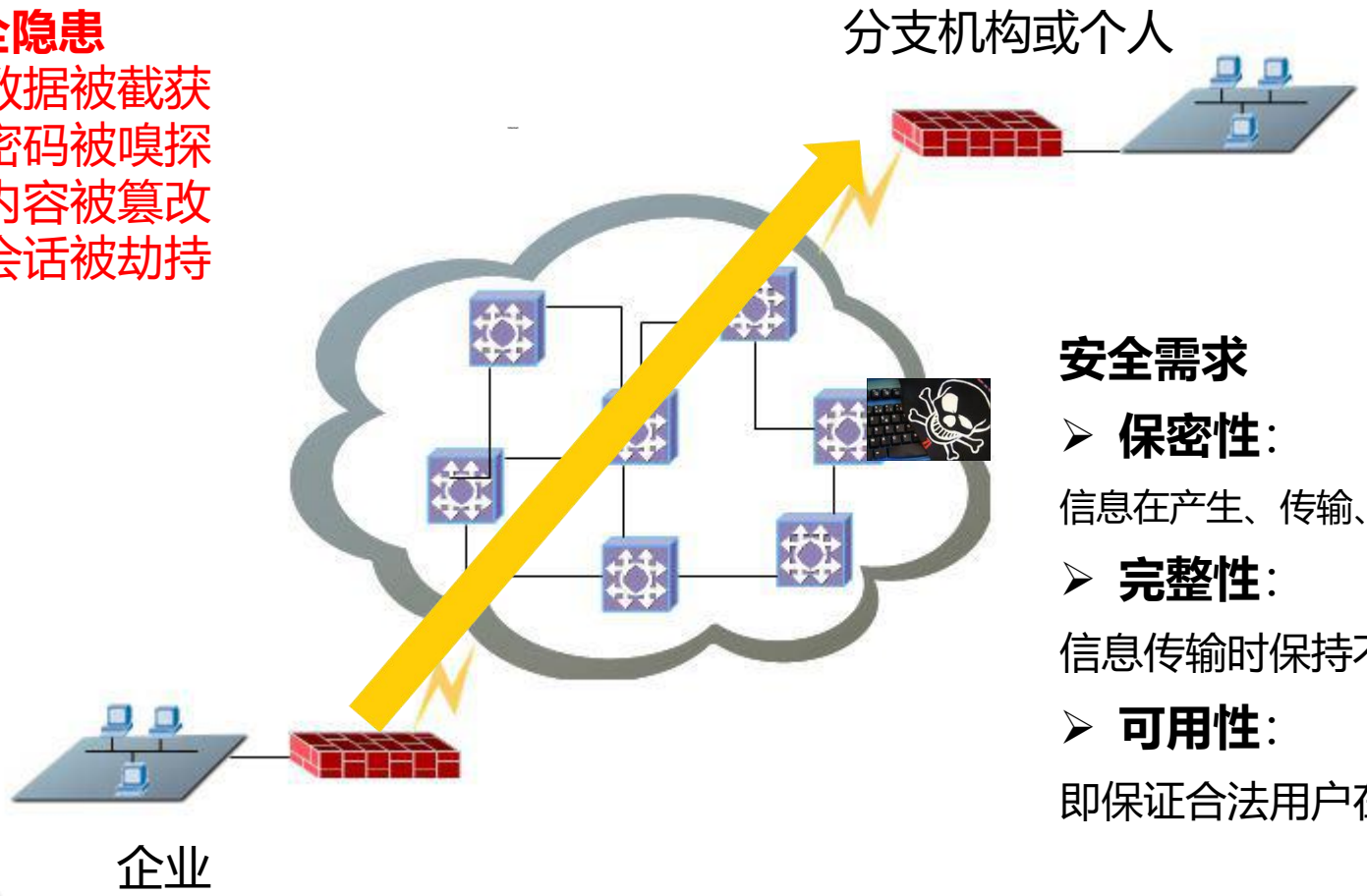
2.5 安全管理响应

2.1 安全远程接入——远程办公风险

企业在与分支机构或个人进行远程通信时，需要经过Internet，因此不可避免的会存在以下安全威胁：

安全隐患

- 数据被截获
- 密码被嗅探
- 内容被篡改
- 会话被劫持



安全需求

- **保密性**：

信息在产生、传输、处理的环节中不泄漏给非授权的个人和实体。

- **完整性**：

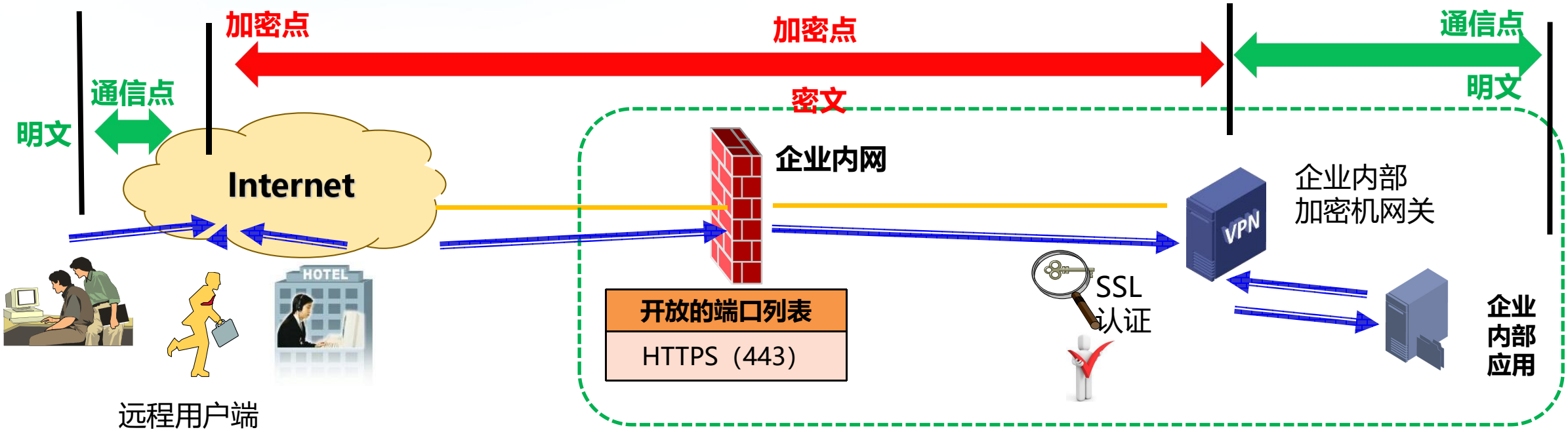
信息传输时保持不被修改、不被破坏、不乱序和不丢失的特性。

- **可用性**：

即保证合法用户在需要时可以使用所需信息。

2.1 安全远程接入——SSLVPN加密传输组网

SSLVPN的组网，只需在企业端有专用加密机设备，而用户端只需软件形式的客户端。适用于PC和手机移动端。

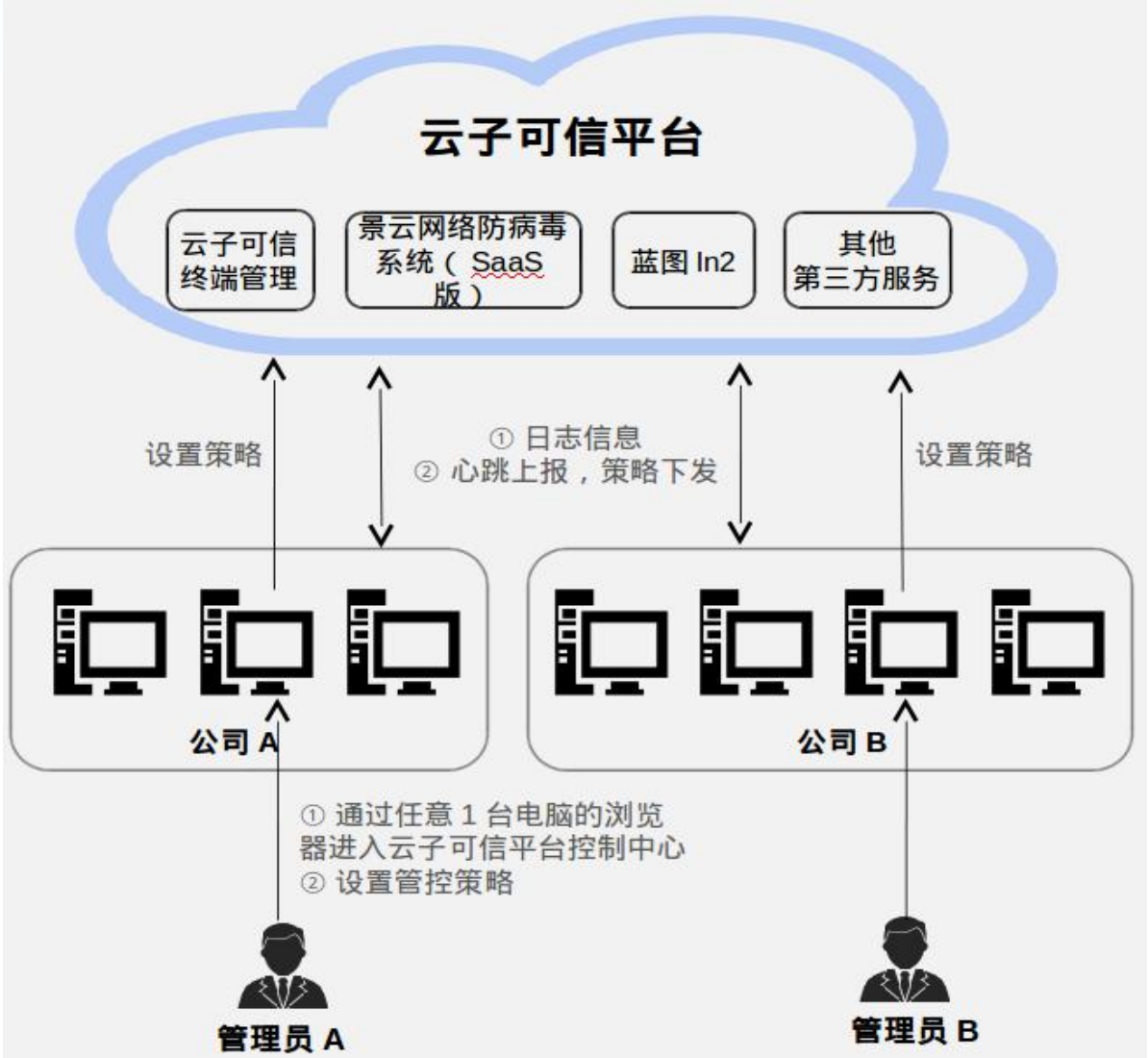


SSLVPN的场景，可以用于个人远程接入。隧道加密连接，隔离办公两不误！

保障了个人与企业内部网络间隧道的加密传输，防止被窃密监听。此外，更安全的做法是加强的多因子认证（账户+U盾、账户+短信验证码）。

2.1 安全远程接入——SaaS平台

在企业没有远程办公环境，但是又需要有简单的终端接入与管理，远程协助、公告与文件分发的场景下，启明星辰还提供了基于SaaS平台的可信云环境，实现分布式办公设备集中管理，无需部署服务器或硬件网关，提供轻量级客户端，操作简单易用，无需专业IT人员维护。实现消息一键“通达”、终端管理实时统一、文件共享清晰明了的效果。



二、建设方案

2.1 安全远程接入

2.2 身份识别准入

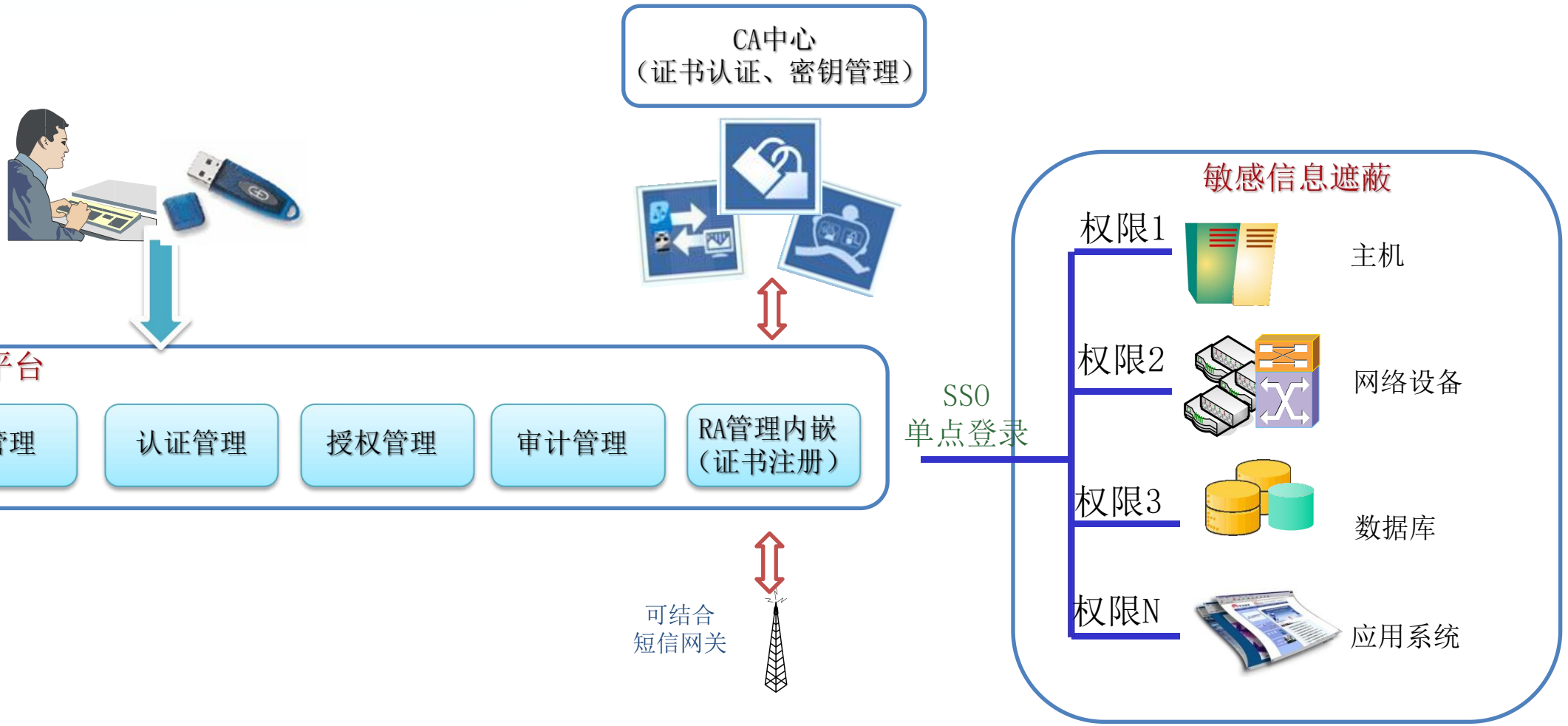
2.3 边界安全防护

2.4 内外安全检测

2.5 安全管理响应

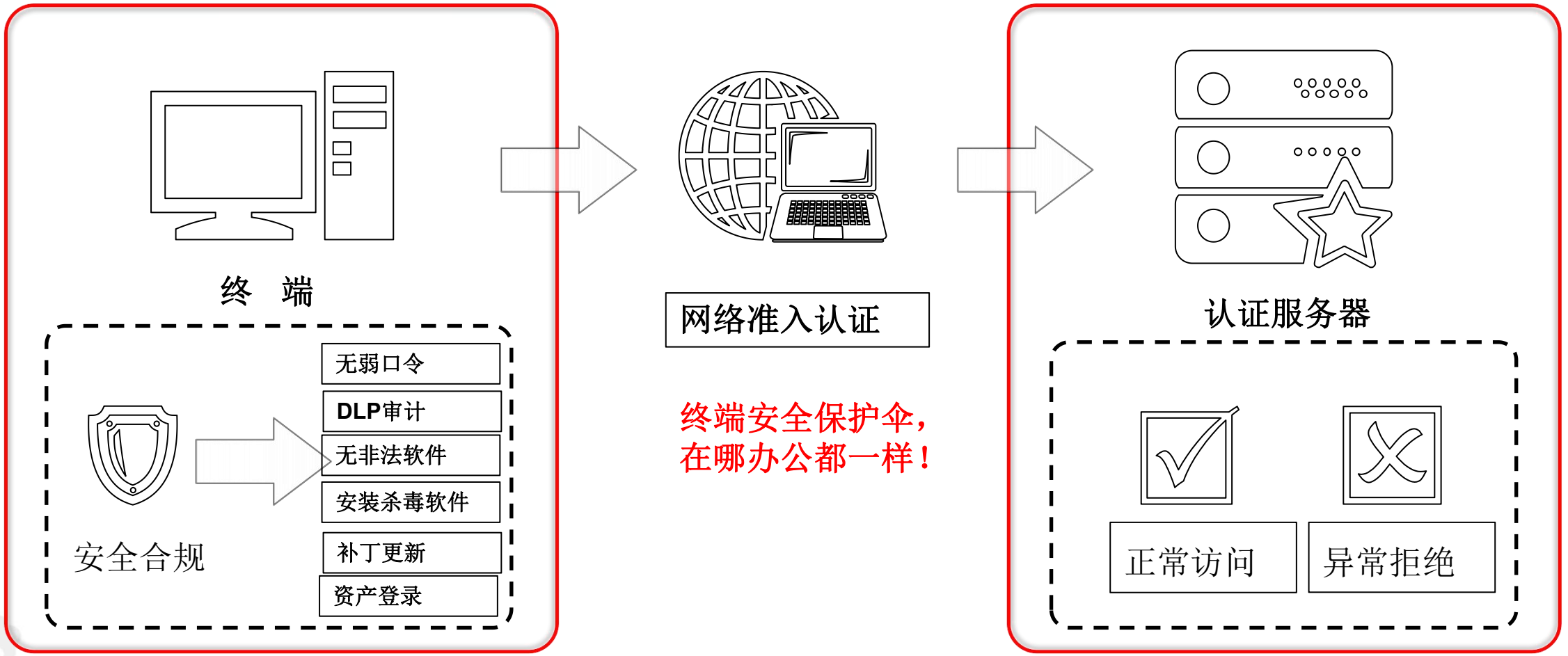
2.2 身份识别准入——应用安全网关

身份标识与权限鉴别，作为访问控制的基础，是解决主动攻击威胁的重要防御措施之一。通过SSO单点登录功能：可以实现身份可知，身份可信，权限可控，账号可管！并且针对敏感信息，可以做到遮蔽化屏蔽（例如身份证号用※代替），应用URL访问限制等。并且可以全程访问审计，甚至录屏归档。



2.2 身份识别准入——终端准入

在远程办公场景下，不仅要识别用户，如有可能，还需对用户接入的设备进行标识，对接入的终端设备进行管理与准入。最终实现对终端的资产识别与登录、防病毒、补丁分发、软件/进程黑白名单、移动防拷贝、终端防泄密



二、建设方案

2.1 安全远程接入

2.2 身份识别准入

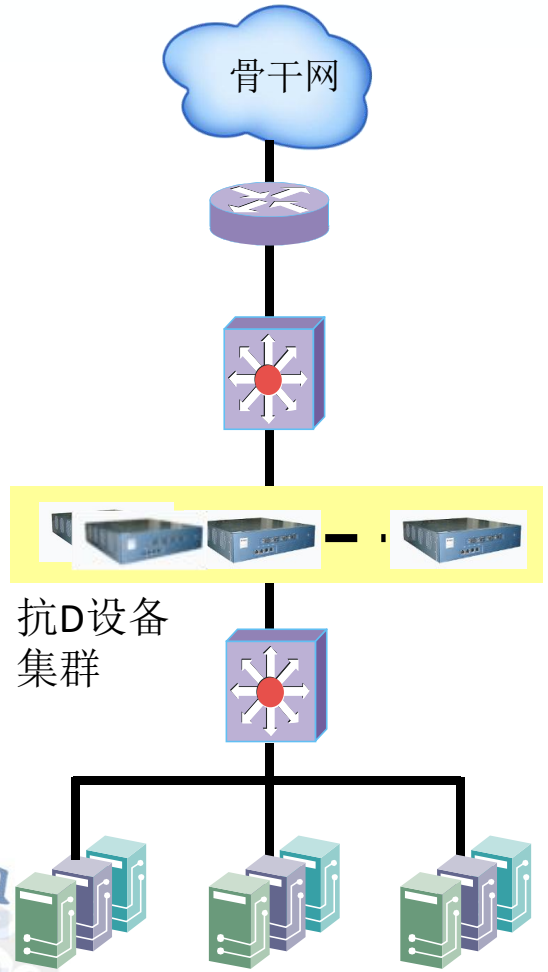
2.3 边界安全防护

2.4 内外安全检测

2.5 安全管理响应

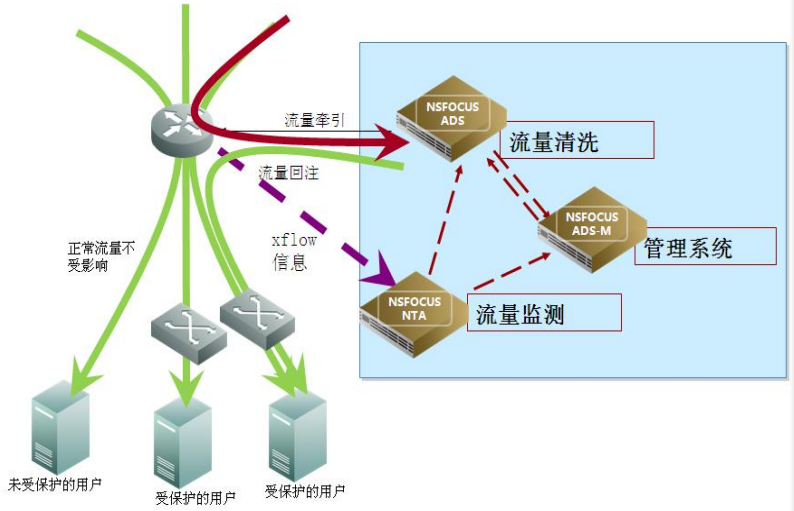
2.3 边界安全防护——DDoS流量清洗

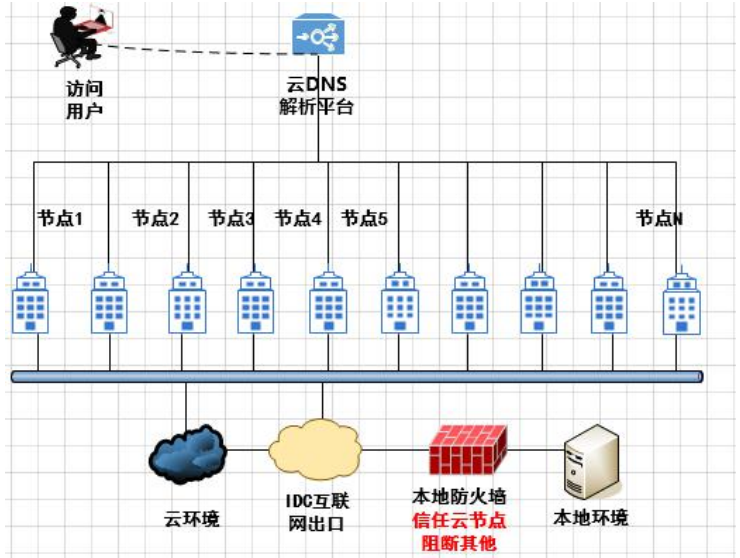
可用性是在线办公的第一道门槛，而DDoS是成本最低，最简单有效的破坏可用性的手段。因此，进行DDoS流量清洗，保障办公网边界的流量可信是首要任务。DDoS防护部署场景主要有三种方式，各有优缺点。



本地三角回注方式部署

- 优点
  - 扩张容易
  - 无攻击时延迟低
- 缺点
  - 有攻击时响应时间稍慢





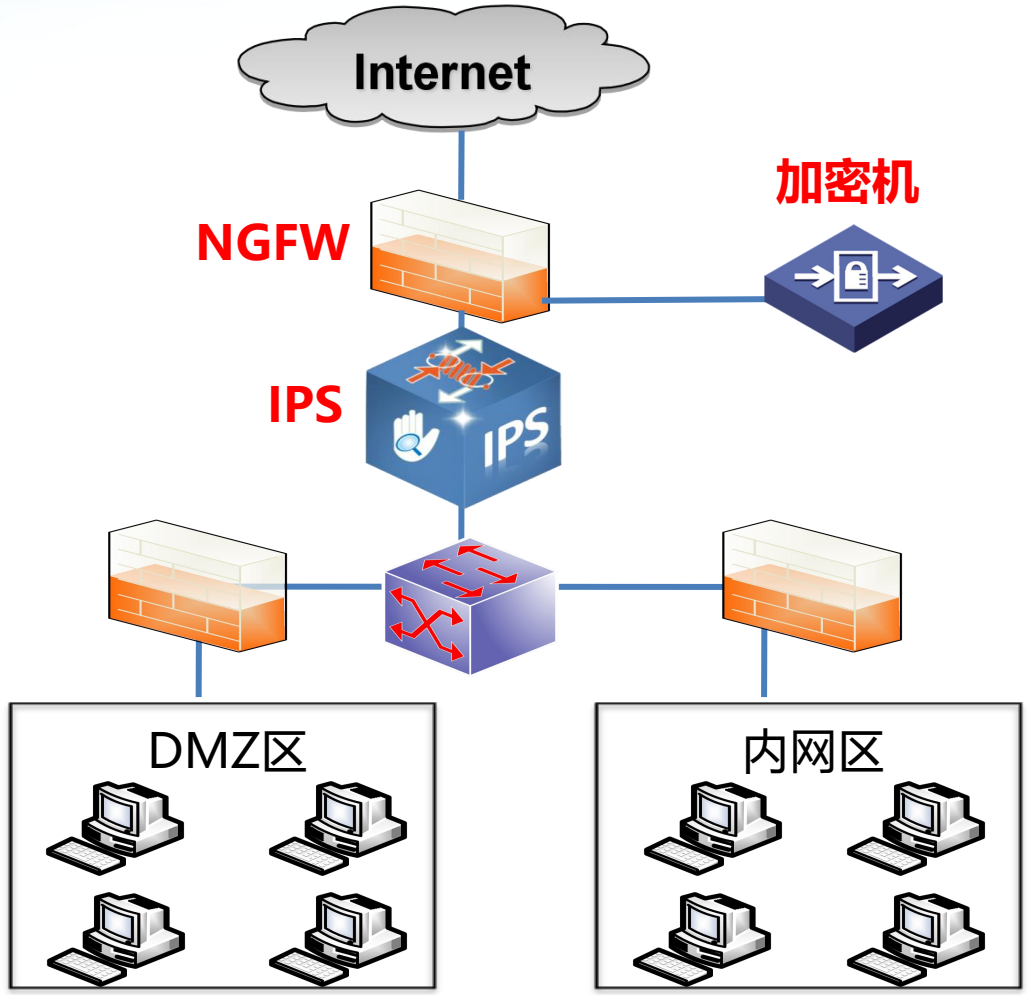
云端防护

- 优点
  - 配置工作量少
  - 扩展灵活
  - 防护能力卓越
  - 单节点宕机无影响
- 缺点
  - 成本高

2.3 边界安全防护——访问控制与入侵防御

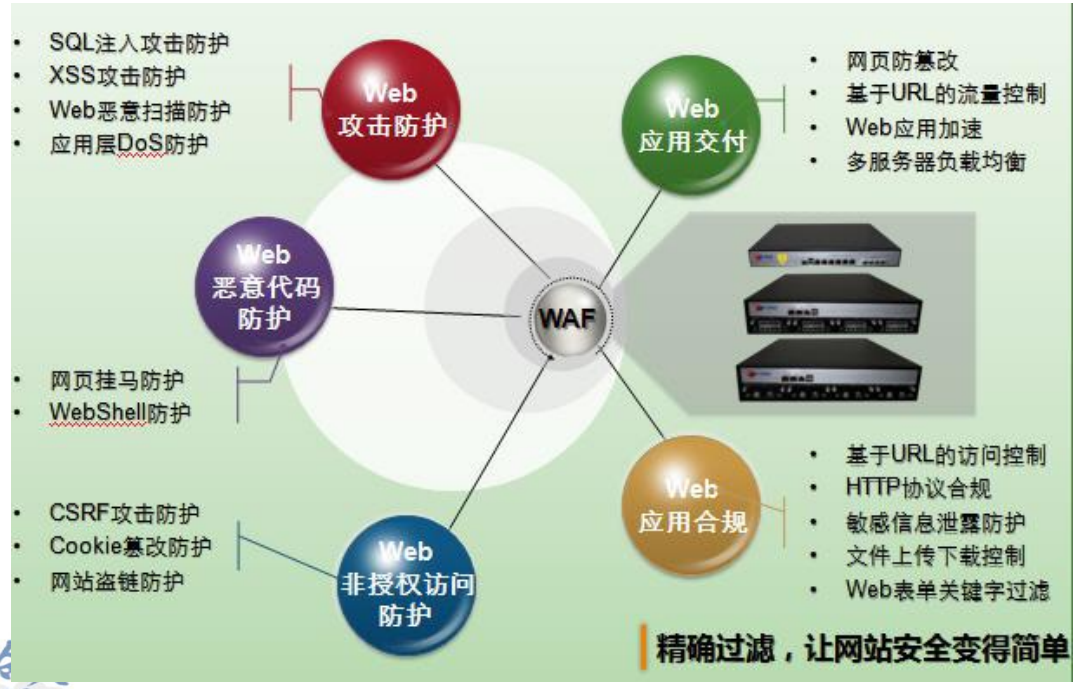
访问控制也是安全防护的基线，应该在每个边界区域进行访问控制策略。通过五元组、角色授权等手段，对访问进行允许或禁止。该功能通常以下一代防火墙实现，用于坚守访问的第一道防线。

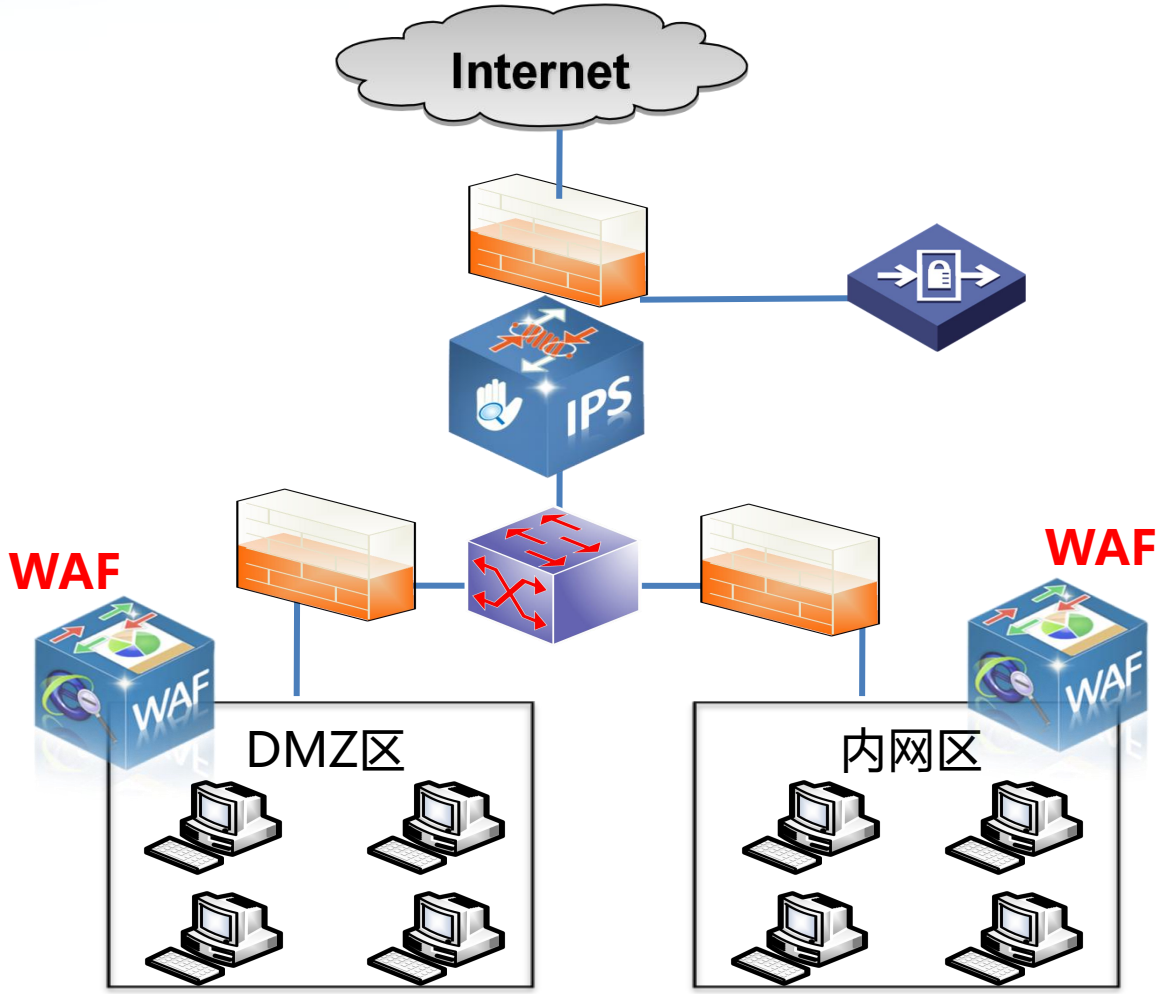
此外，还需要对流量中的恶意流量进行阻断。通常通过IPS（开启防病毒）实现。需要注意的是，由于远程接入是加密流量，因此IPS需要部署在加密机下一级，用于检测远程接入的流量中是否包含恶意流量。



2.3 边界安全防护——应用防护

Web架构的办公系统，还需要进行应用防护，通常是在应用服务器集群前部署WAF防火墙，用以阻挡包括SQL注入攻击、跨站脚本、恶意代码、脆弱性攻击等，WAF防火墙为Web应用的贴身保镖！





二、建设方案

2.1 安全远程接入

2.2 身份识别准入

2.3 边界安全防护

2.4 内外安全检测

2.5 安全管理响应

2.4 内外安全检测——网站应用安全检测

网站应用的持续可用性检测，是一项基础的工作，可以通过远程服务或者部署硬件的方式，对办公网站应用进行风险全面监测。
可检测网站挂马、DNS篡改。
可用性异常等异常行为。

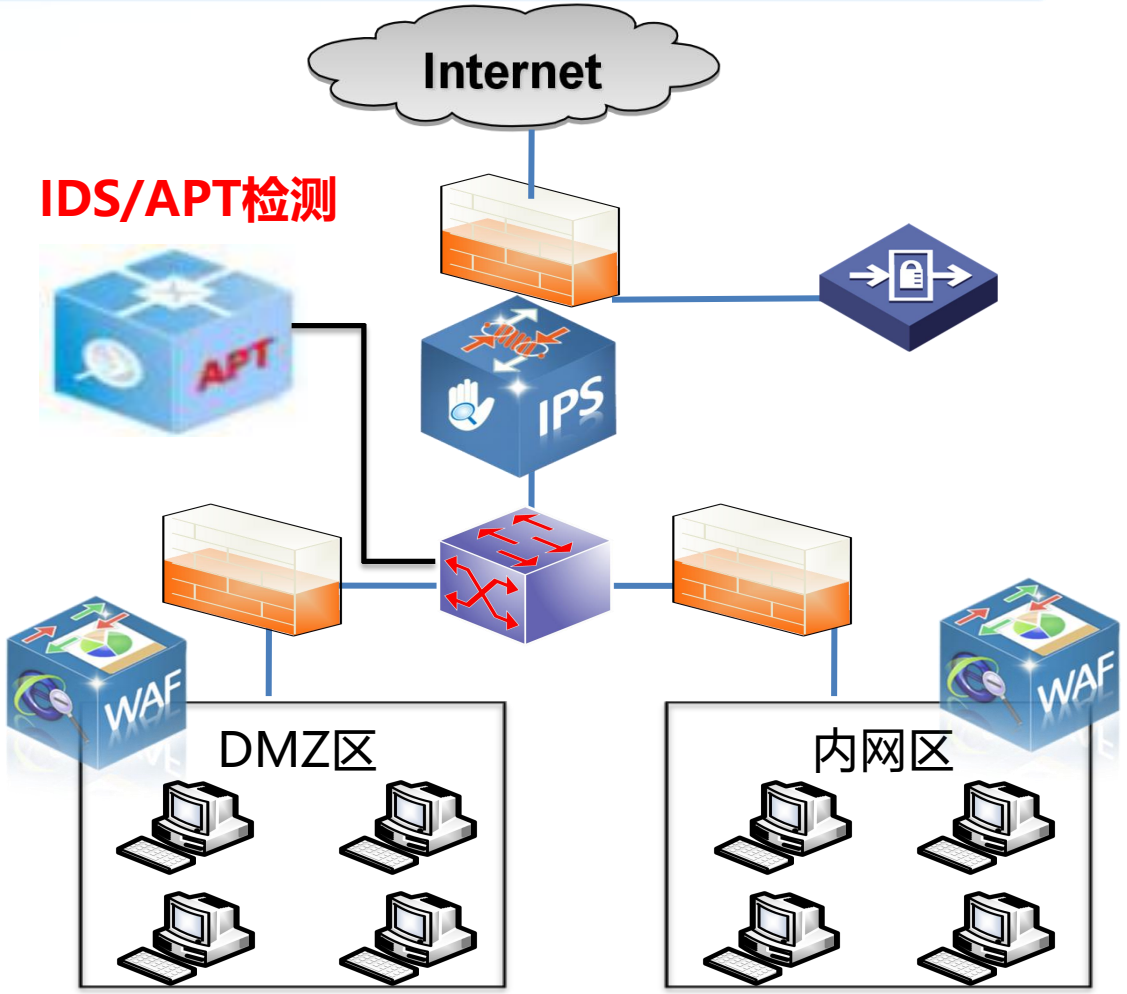
2.4 内外安全检测——已知/未知威胁检测

通过内网部署APT设备，检测外网或全网镜像流，并实时更新最新特征库，实现对已知/未知威胁的检测。

已知威胁检测：（1）IDS特征库识别
（2）已检出威胁样本特征

未知威胁检测：（1）沙箱检测
（2）外部威胁情报比对

联动协同防御：（1）与防护网关联动协同
（2）与防病毒软件联动协同

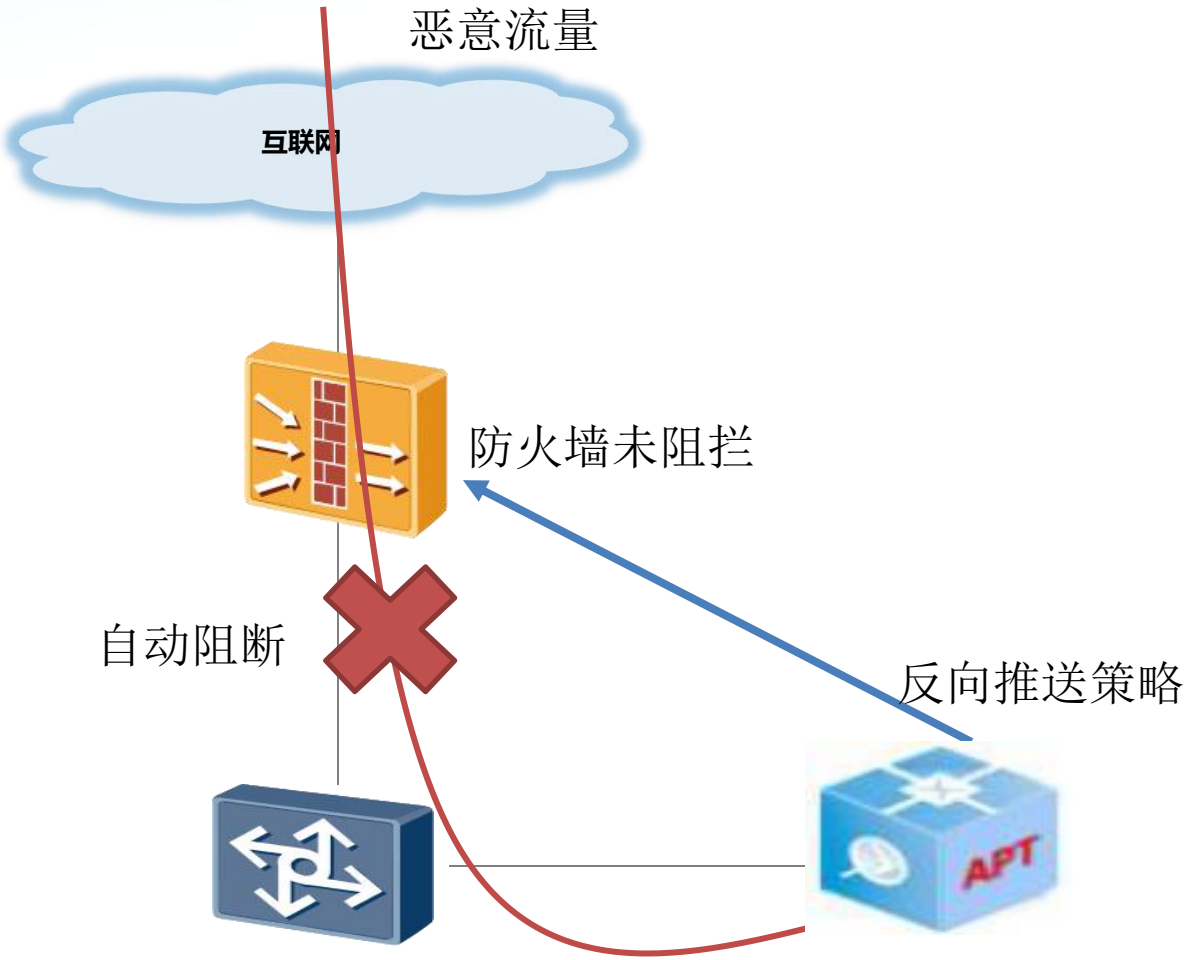


2.4 内外安全检测——已知/未知威胁检测与联动防御示意图

可以将旁路检测设备与串行防护设备进行智能协同防御。

当检测设备检测到攻击行为，但是防护设备未阻断，那么检测设备会反向推送策略给边界网关自动阻断，从而能够在第一时间对攻击行为做出响应。

将需要大量人员分析流量与日志的沉重工作中解脱出来，只需要对智能联动防御后的网关处策略，人工排查是否有白名单应用或IP的误拦截，进行放行或督促整改即可。



IDS/APT检测设备感知

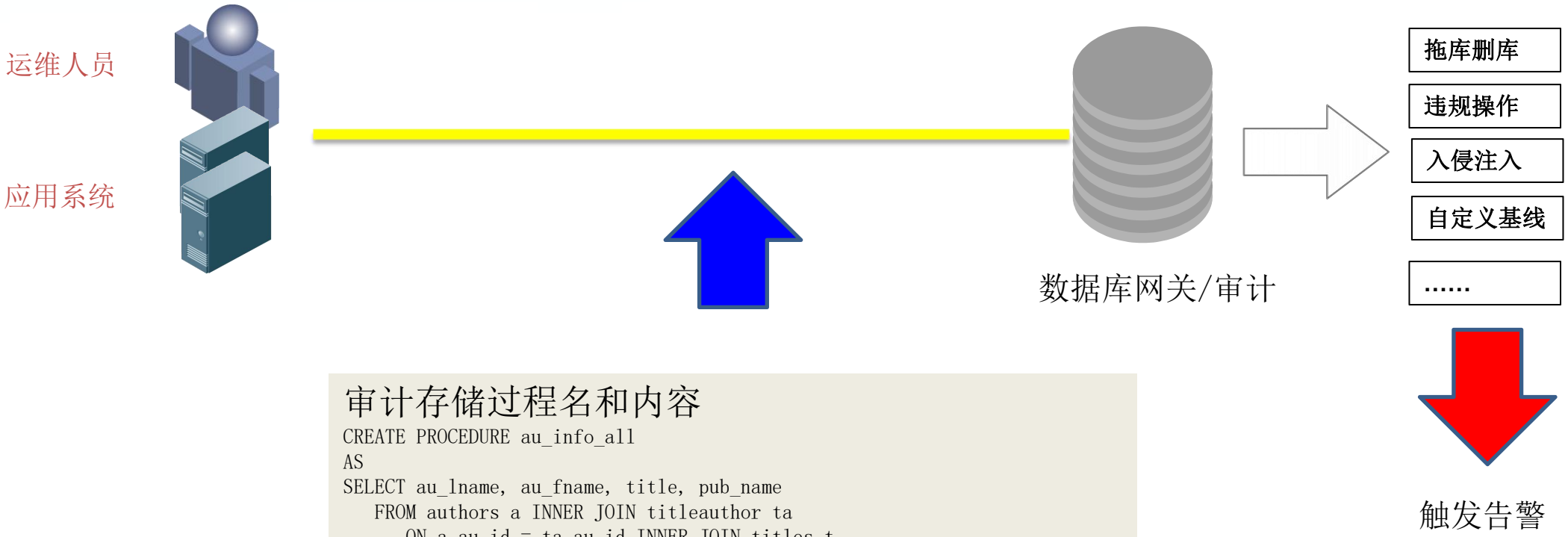
2.4 内外安全检测——漏洞检测

漏洞检测手段，识别内网应用存在的漏洞，掌控资产风险。漏洞检测可以是硬件产品，也可以是服务形式。硬件产品还可集成web应用安全检测，以及配置核查功能。

漏洞的评估、扫描、
监控与修复模型，
进行长期监测与修复。
最终对漏洞管理实现闭环。

2.4 内外安全检测——数据库审计

利用数据库审计系统，对远程访问数据库的行为进行审计，洞察一切针对数据库的操作，发现恶意违规的数据访问行为，保护企业数据资产。该系统既可以旁路检测审计，也可以作为数据库网关进行防护阻断。

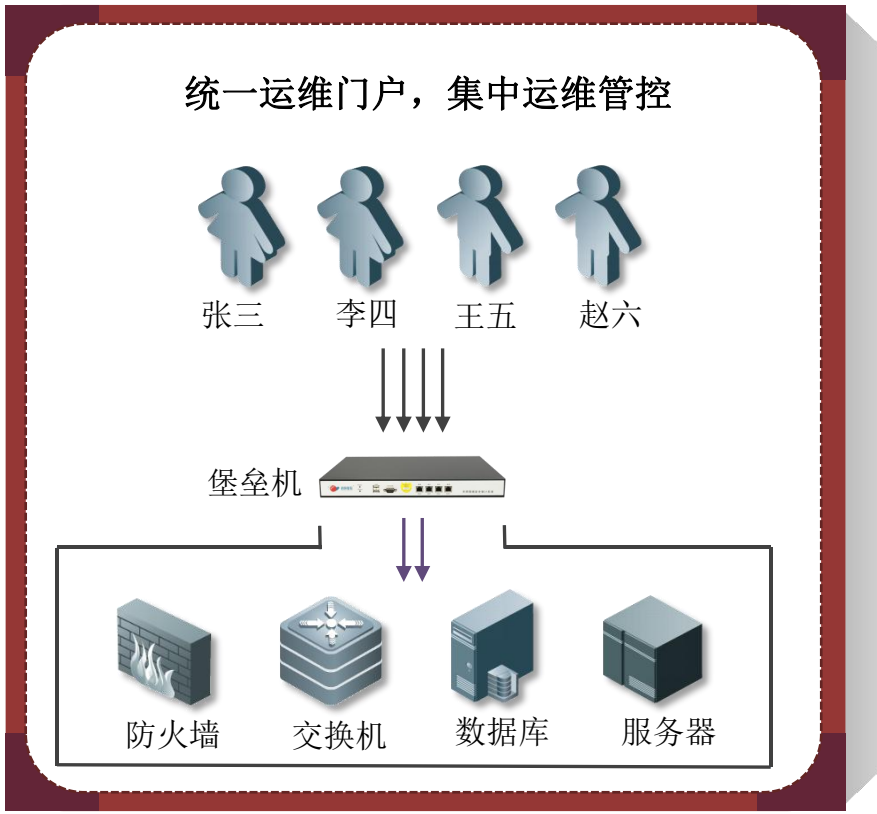


审计存储过程名和内容

```
CREATE PROCEDURE au_info_all
AS
SELECT au_lname, au_fname, title, pub_name
   FROM authors a INNER JOIN titleauthor ta
      ON a.au_id = ta.au_id INNER JOIN titles t
      ON t.title_id = ta.title_id INNER JOIN publishers p
      ON t.pub_id = p.pub_id
GO
```

2.4 内外安全检测——运维审计

如有远程运维场景，则需要运维堡垒机进行运维审计，将运维记录归档录屏，并且阻断高危命令，保障运维可靠。



事前 统一身份标识 —— 你是谁

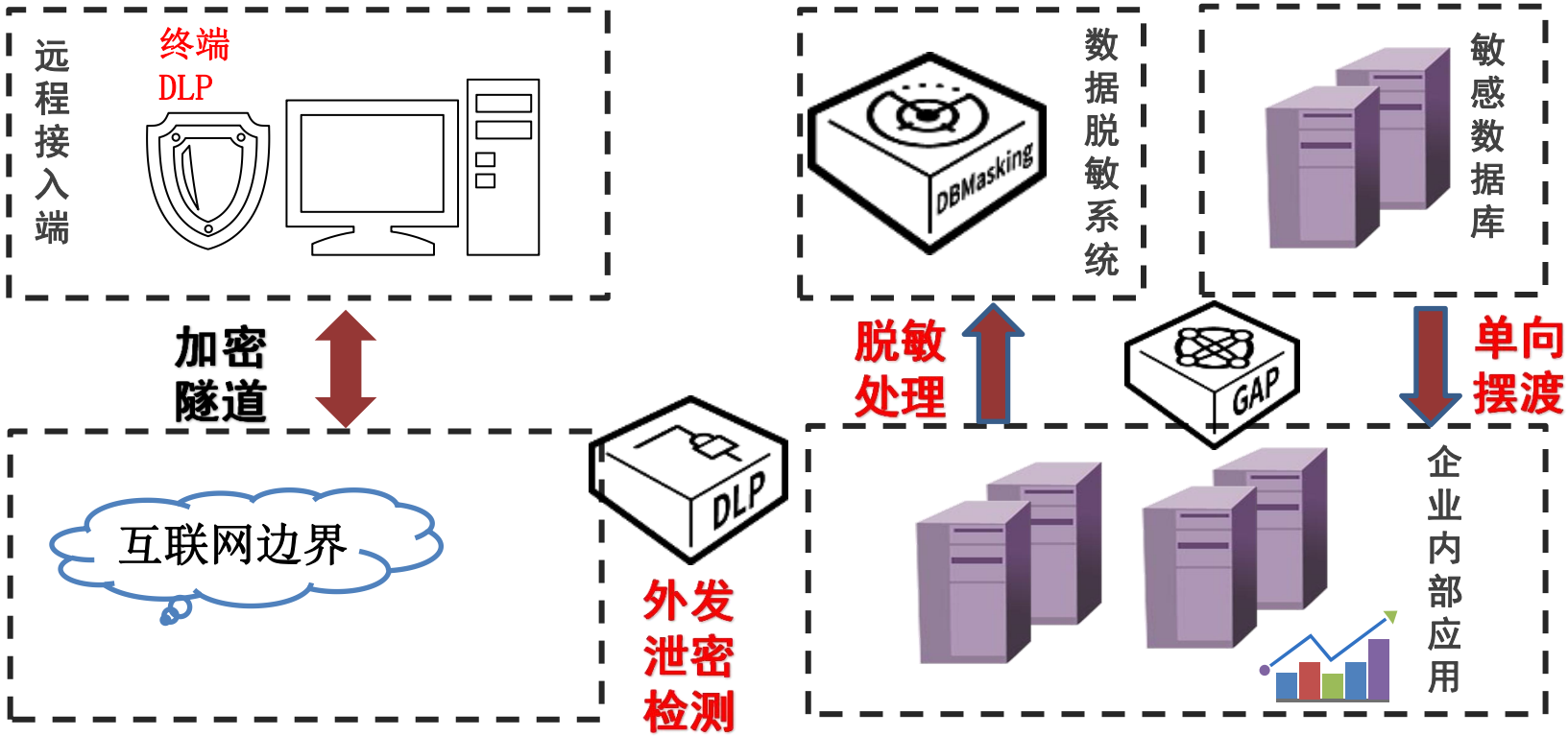
事中 细致权限控制 —— 能做什么操作

事后 完整的审计记录 ——追溯与定责

2.4 内外安全检测——DLP防泄密

在远程接入办公场景下，如果有敏感数据、隐私数据、涉密数据的场合，还需要进行DLP防泄密的检测。DLP防泄密是一种组合手段，无法通过单一设备来实现。通过多个场景下的套件组合，为数据提供“额温枪”，敏感数据逃不脱。

1、敏感数据摆渡：如果有权限访问敏感数据，则需要通过单向网闸进行摆渡（谨慎，会导致敏感数据降级，只针对一般机密）
2、在终端处应当安装DLP防泄密终端，记录并同步敏感数据访问行为，用于后期审计。并且限制U口与刻录，限制录屏与打印
3、在办公出口部署DLP防泄密网关，用于网络/邮件的外发防泄密的检测（旁路模式）或阻断（网关模式）
4、在第三方开发、运维、数据分析人员提取数据的场景下，需要进行匿名化/假名化处理（通过数据库脱敏系统实现）



2.4 内外安全检测——用户行为画像检测

结合UEBA的大数据用户画像分析系统，对远程接入用户的行为进行画像。从而根据用户的习惯基线判断是否为用户本人，或者有无异常操作。

可以基于用户会话、访问习惯、账号、访问资源频次基线等发现异常。洞察用户行为，护航企业安全

二、建设方案

2.1 安全远程接入

2.2 身份识别准入

2.3 边界安全防护

2.4 内外安全检测

2.5 安全管理响应

2.5 安管管理响应——基于安全管理平台

安全管理与响应，首先是要对办公系统等关键设备进行持续的监控。

可以利用安全管理平台，对关键系统的CPU占用率、内存占用率、磁盘占用率、网卡流量进行监控。以及利用ping包检测设备存活等。

此外，基于大数据的告警日志收集与分析，是持续监控、持续运营、及时安全响应的重点。

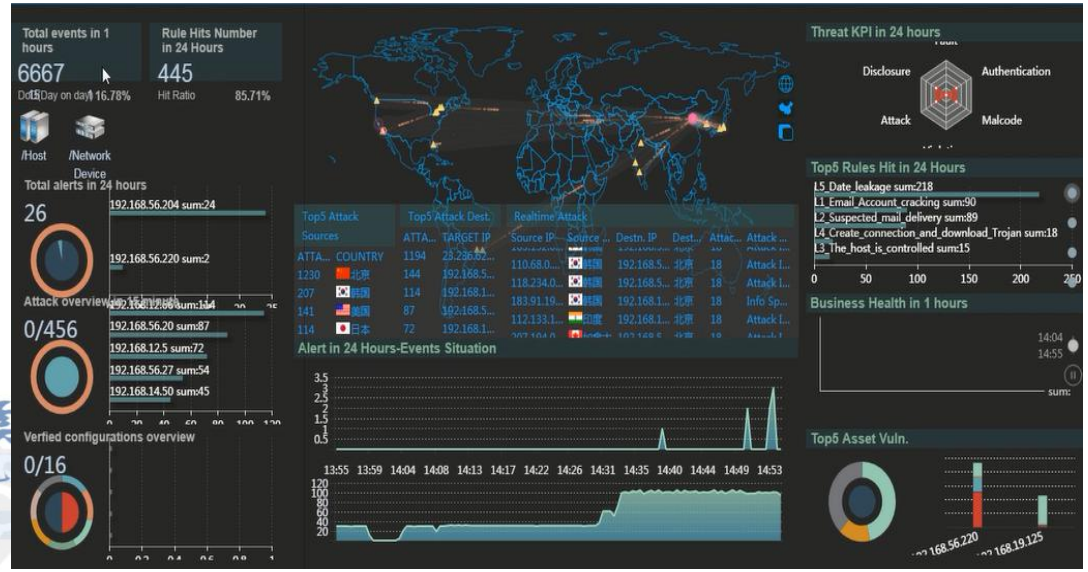
性能监控与安全日志收集告警两不误。

2.5 安管管理响应——管理界面展示

资产性能监控

脆弱性展示

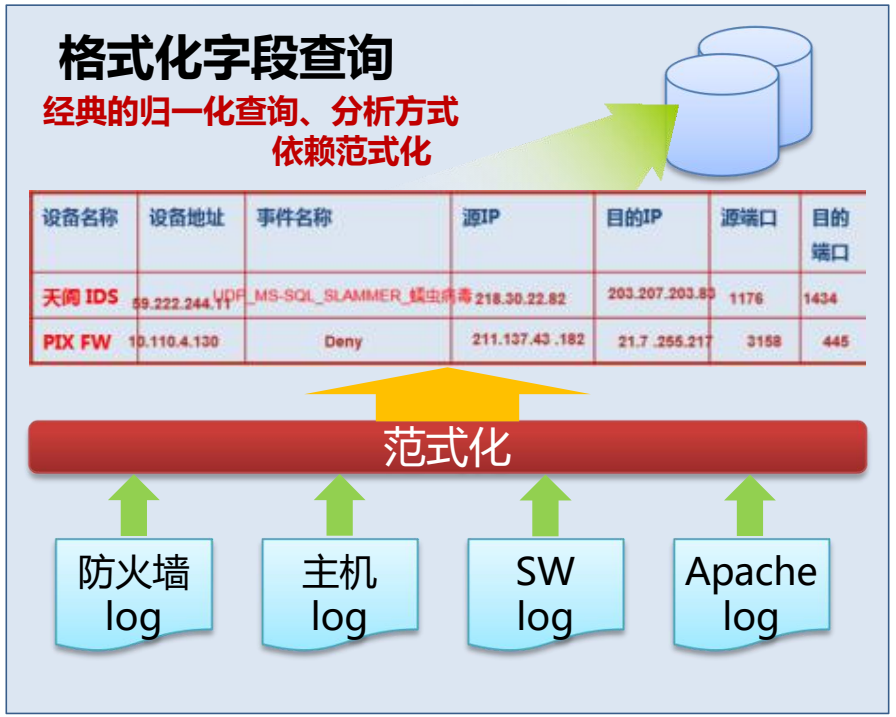
攻击事件展示



终端管理界面

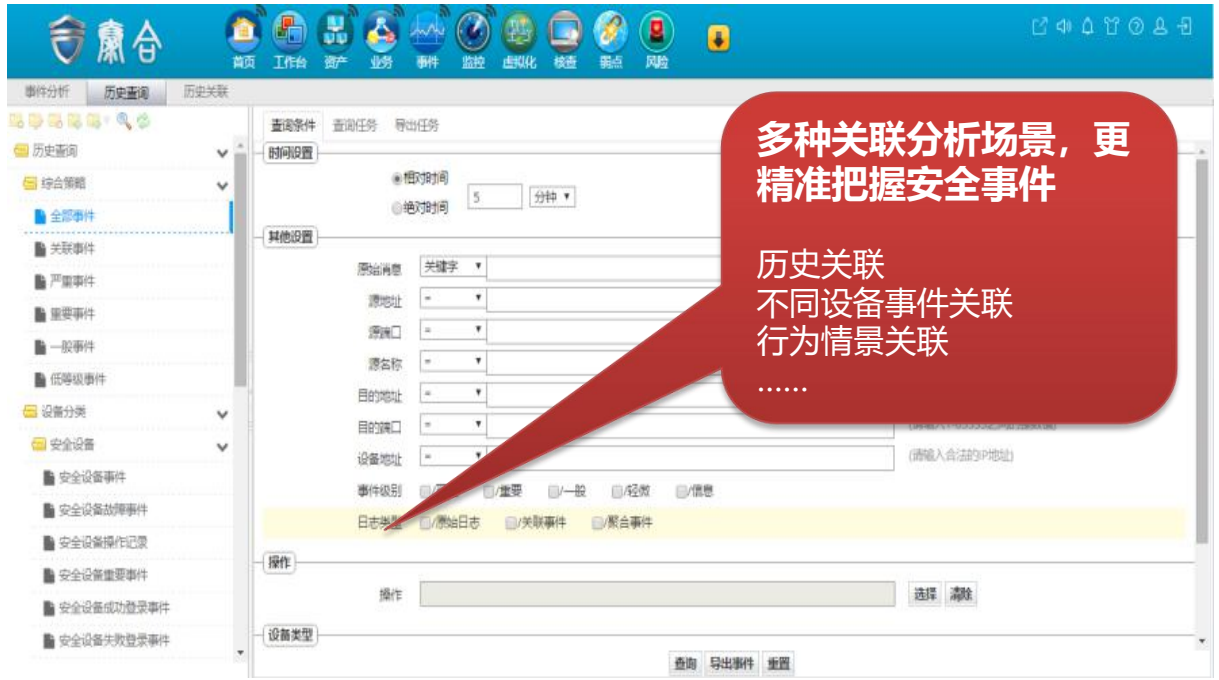
2.5 安管管理响应——安全告警日志处理

日志采集与范式化



范式化的日志统一了各种安全日志的格式，降低了解读难度

日志关联分析



多场景的日志关联分析，有助于发现潜在深藏的安全事件与隐患。

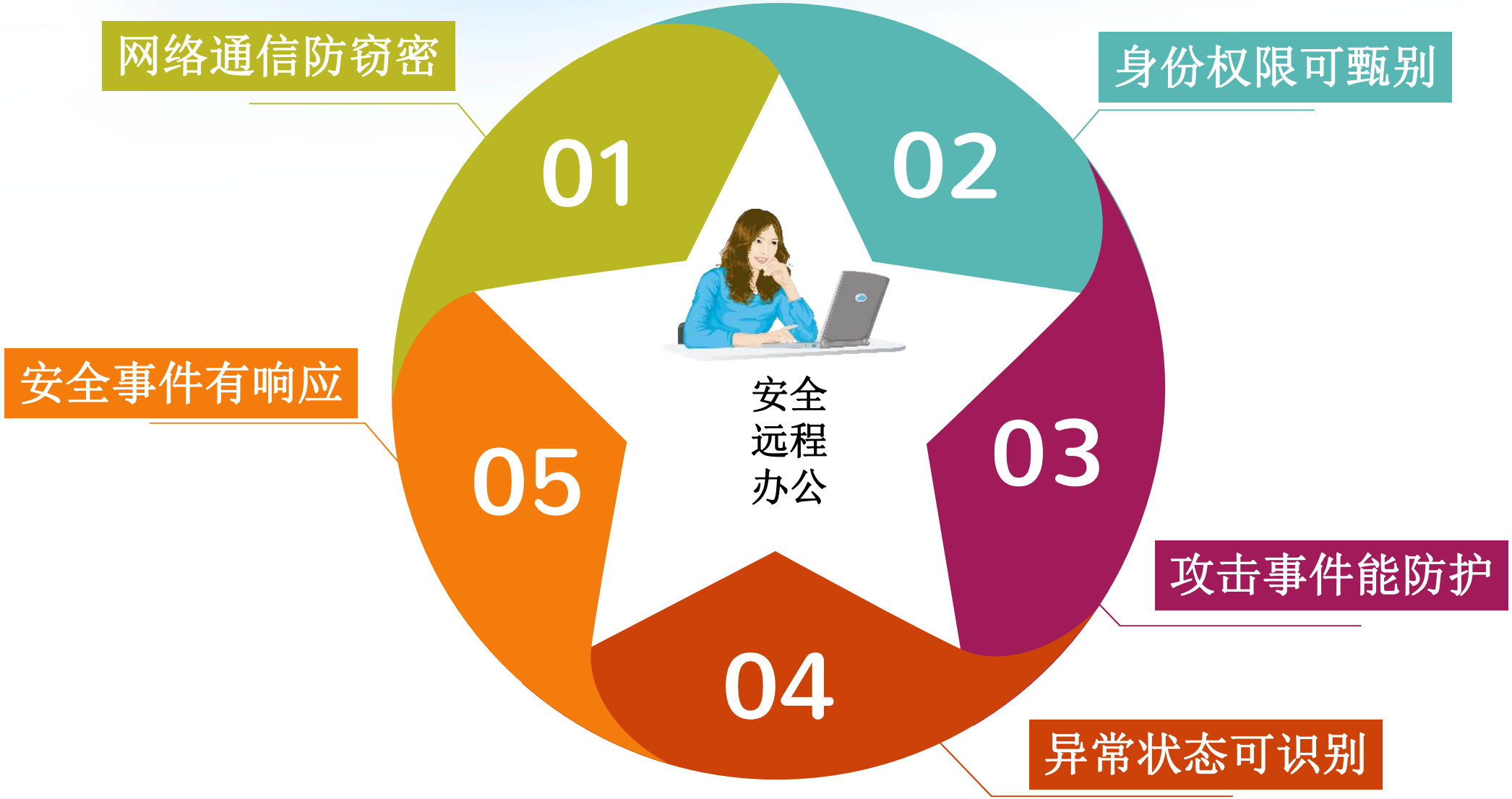
三、方案效果

3.1 方案效果总结

3.2 产品清单一栏

3.3 需求场景分析

3.1 方案效果总结——五大能力



3.1 方案效果总结——六重防护

保护账户	多因素认证加固账户；用户画像识别账户风险
保护网络	访问控制、授信准入与威胁识别防御组合，全面保护网络
保护应用	Web应用系统可用性保障与恶意攻击防护、运维操作保护
保护数据	加密传输与重要敏感数据摆渡、外发及拷贝泄密监控
持续监控	持续的性能监控与安全日志监控响应
安全审计	访问与操作记录归档，随时溯源审计追责

三、方案效果

3.1 方案效果总结

3.2 产品清单一栏

3.3 需求场景分析

3.2 产品清单一览

序号	设备类型	功能																		形态
		网络通信加密	VPN应用加速	身份识别鉴权	账号准入控制	终端准入控制	抗DDoS	五元组访问控制	入侵防御	防病毒	应用防护	网站应用检测	已知威胁检测	未知威胁检测	漏洞检测	数据库审计	运维审计	防泄密	用户行为检测	安全管理平台	
1	VPN	√		√	√			○													硬件
2	云子可信			√		√		√		√											服务
3	应用安全网关	√		√	√											√	√	√	√		软件
4	天珣内网审计					√		√		○								○	√		软件
5	NAC					√		√													硬件
6	Anti-DDoS						√	√			○										硬件/服务
7	NGFW	○	○	○	○		○	√	○	○	○										硬件
8	UTM	○					○	√	○	○											硬件
9	IPS							√	√	○											硬件
10	WAF										√										硬件
11	网站远程监控											√			√						服务
12	APT												○	√							硬件
13	IDS/CS												√								硬件
14	漏洞检测														√						硬件/服务
15	数据库审计															√					硬件
16	运维审计																√				硬件/软件
17	DLP网关																	√			硬件
18	网闸																	√			硬件
19	数据库脱敏																	√			硬件/软件
20	UEBA																		√		硬件/软件
21	BSM/SOC																			√	软件

注：√为产品主打功能，○为可选功能，产品间功能重合部分，需要根据成本预算以及客户现网环境进行组合筛选。

三、方案效果

3.1 方案效果总结

3.2 产品清单一栏

3.3 需求场景分析

3.4 需求场景分析

序号	场景描述	推荐
1	无涉密敏感数据、无需OA系统、疫情期间临时性的文档与信息分发	云子可信
2	有OA相关系统、无涉密数据、简单的远程接入需求、无远程手段	VPN系列
3	有OA相关系统、无远程手段、有敏感数据	VPN系列/数据安全系列/身份认证准入系列
4	外包人员远程开发测试运维	VPN系列/数据安全系列/身份认证准入系列
5	分子公司协同，跨国或对远程速度有要求	T墙
6	小规模(50人以内)最低成本要求	T墙/UTM
7	外包人员远程开发测试运维	VPN系列/数据安全系列/身份认证准入系列/审计/安管
8	有远程手段。有涉密网内秘密级别数据访问	身份认证准入系列、网闸、审计、安管
9	仅仅为PC端远程接入的场景	身份认证与准入选择天珣内网审计
10	既有PC端也有移动端远程接入，且有敏感数据	天珣内网审计与NAC结合
11	既有PC端也有移动端远程接入，无敏感内容	NAC即可

谢　　谢

Thank you