



金融行业安全业务系统的优化与编排

陈玉奇 F5中国区资深安全架构师



网络安全创新大会
Cyber Security Innovation Summit

+ + > _ 加密——业务新常态

89%

- 页面调用通过SSL/TLS

SOURCE: F5.COM/LABS



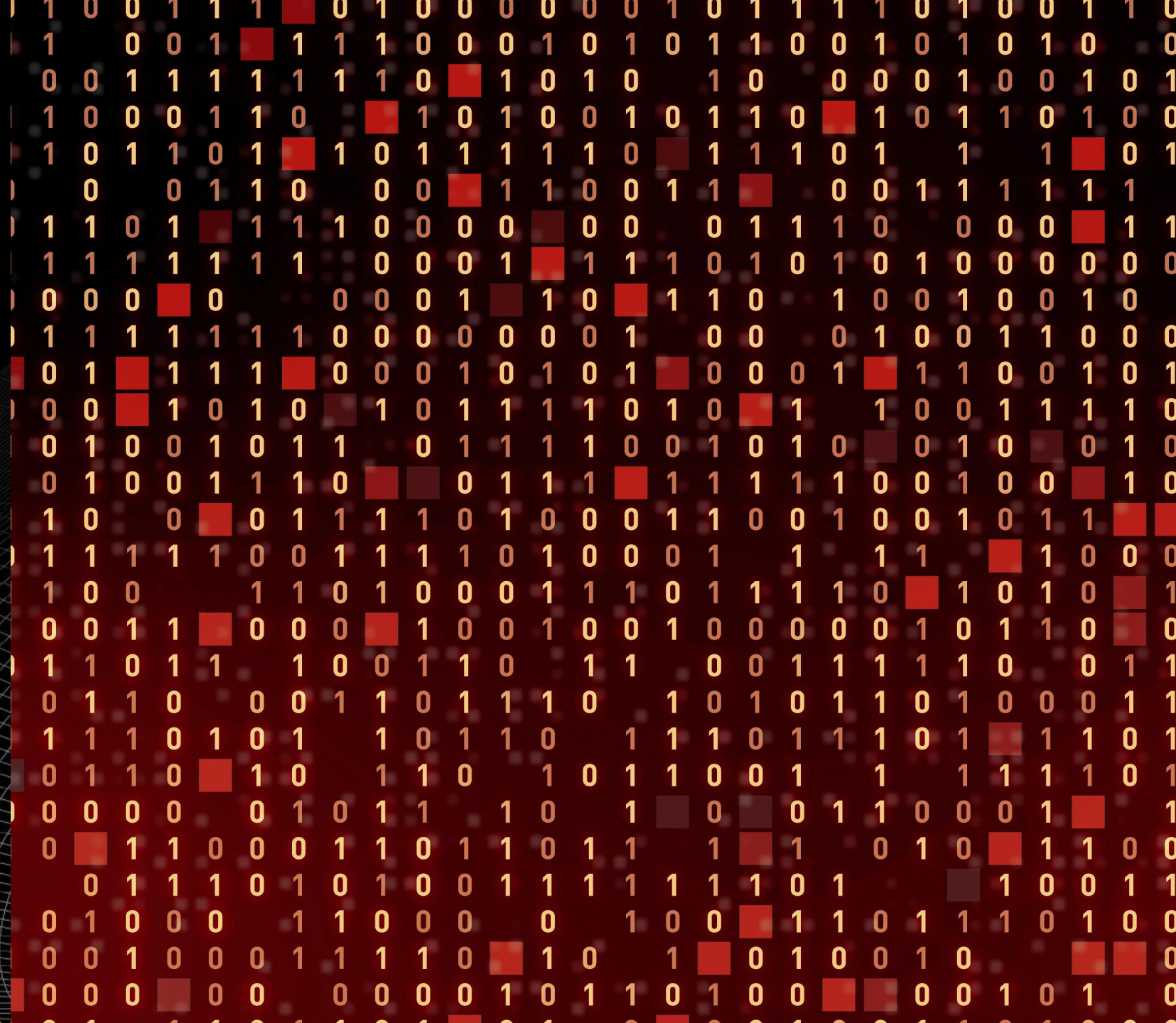
68%

恶意软件的站点引入了加密证书

93%

的钓鱼域名提供合法的安全连接

<https://www.f5.com/labs/articles/threat-intelligence/2018-phishing-and-fraud-report-attacks-peak-during-the-holidays>



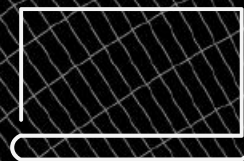


RSA



- 密钥可以被截取

DHE



- 密钥无法被截取

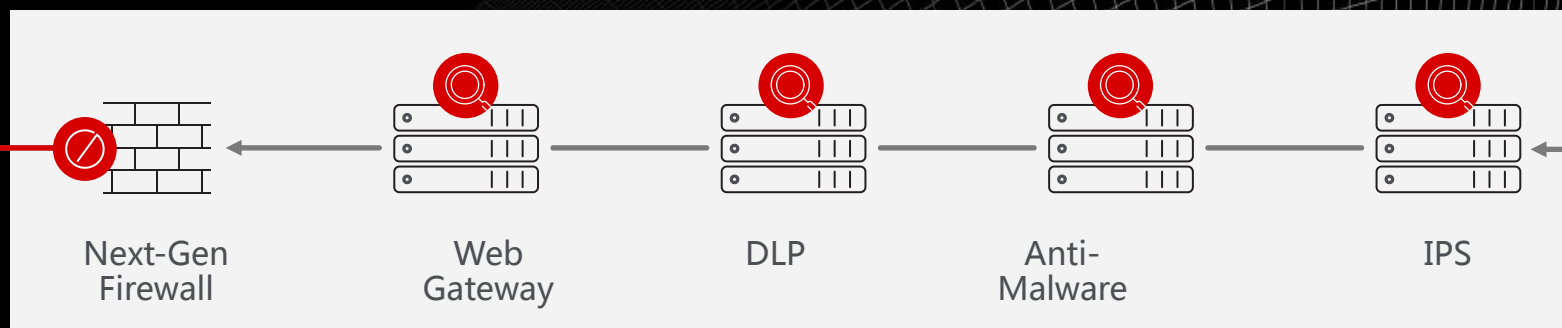
不受信网络



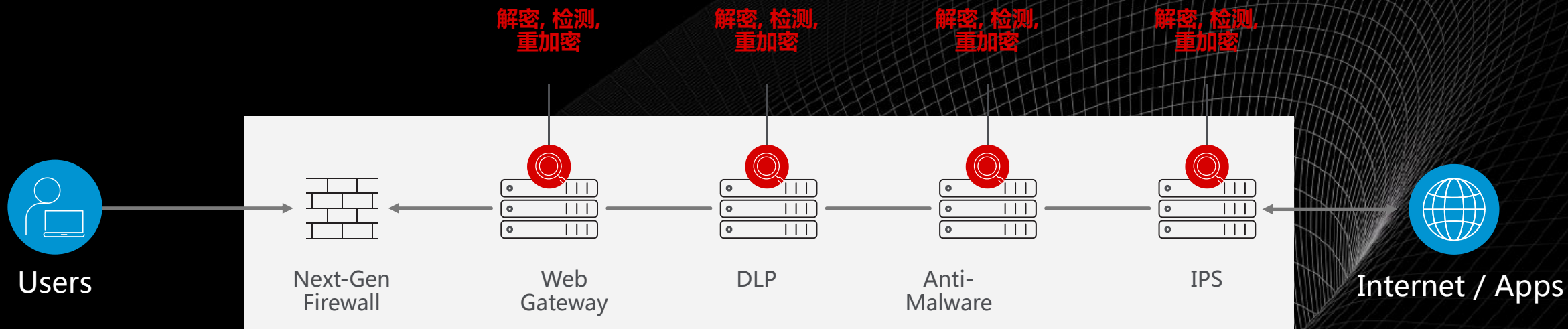
未加密威胁



加密威胁



Internet / Apps



加解密能力?

业务延时?

管理难度?

针对加密流量的网络安全分析与恶意软件检测

-- PRS-NTA --

斗象PRS-NTA以大数据、AI作为基础技术能力，深度分析数据包内容，智能化分析，高效率检测，在网络流量安全分析与恶意文件检测方面具备出众能力。

-- F5-SSLO --

F5-SSLO对流量进行统一加/解密，优化安全设备部署，智能调度业务服务流量，为安全分析引擎提供最有力的数据支持能力。



X

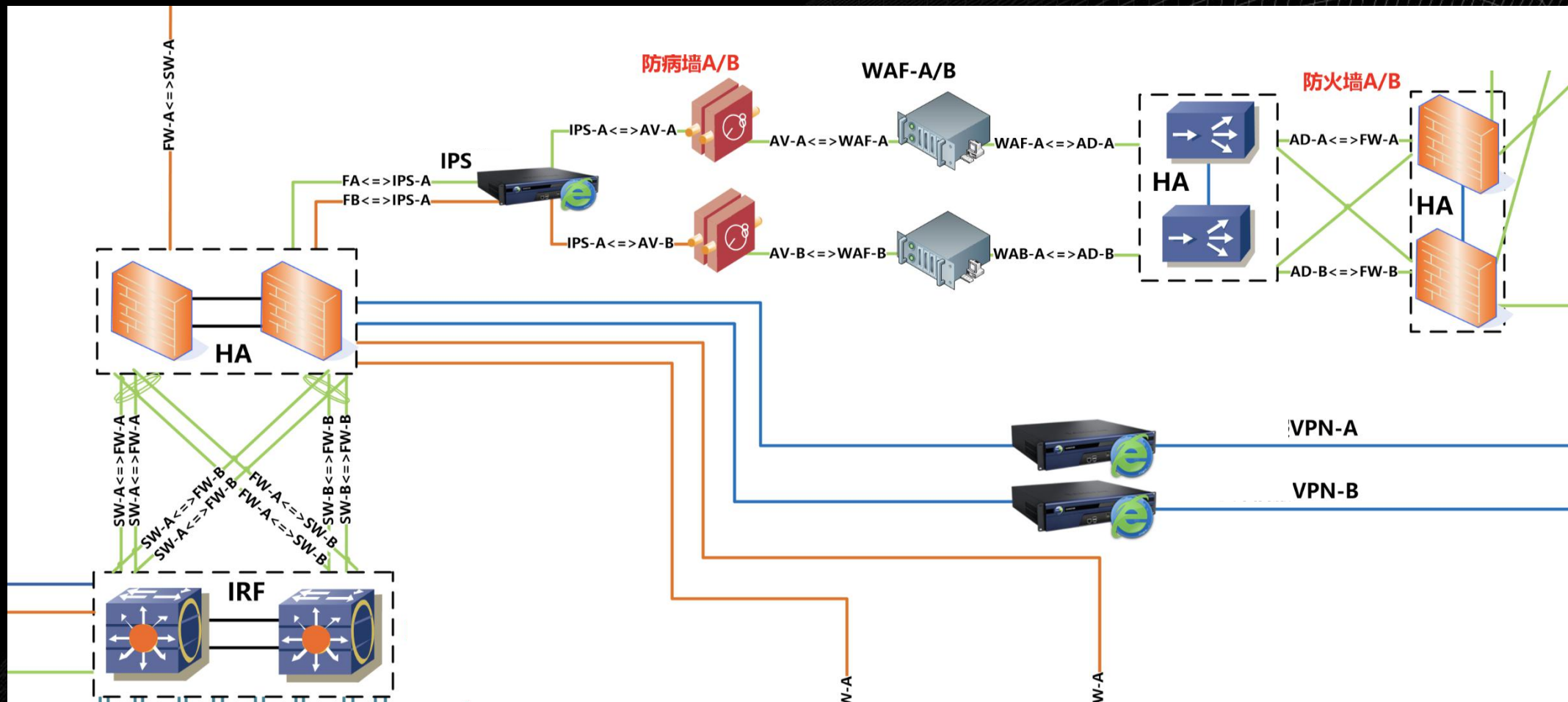




只是可见性？

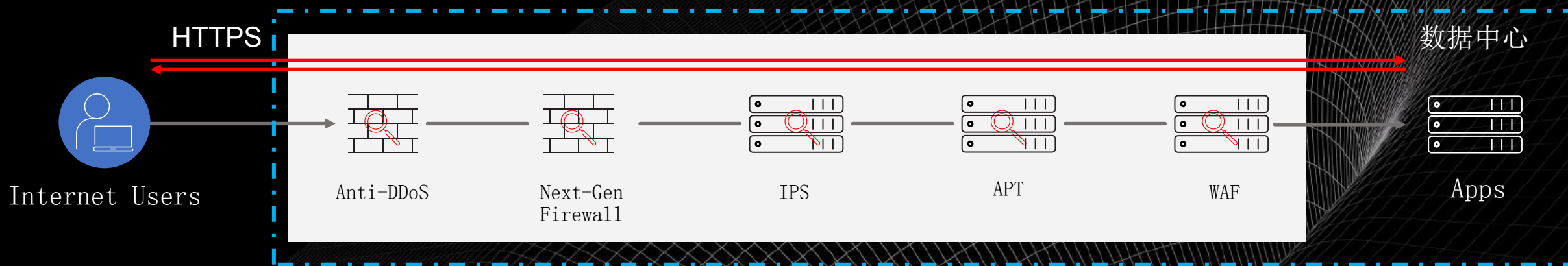


网络安全创新大会
Cyber Security Innovation Summit



安全能力的束缚

L7安全检查设备



- 安全设备与网络紧耦合
- 所有流量流过所有设备导致噪音
- 设备难以增删
- 策略不敢轻易调整
- 安全设备扩容只能做整体替换



针对双向SSL/TLS加密流量的安全业务优化调度

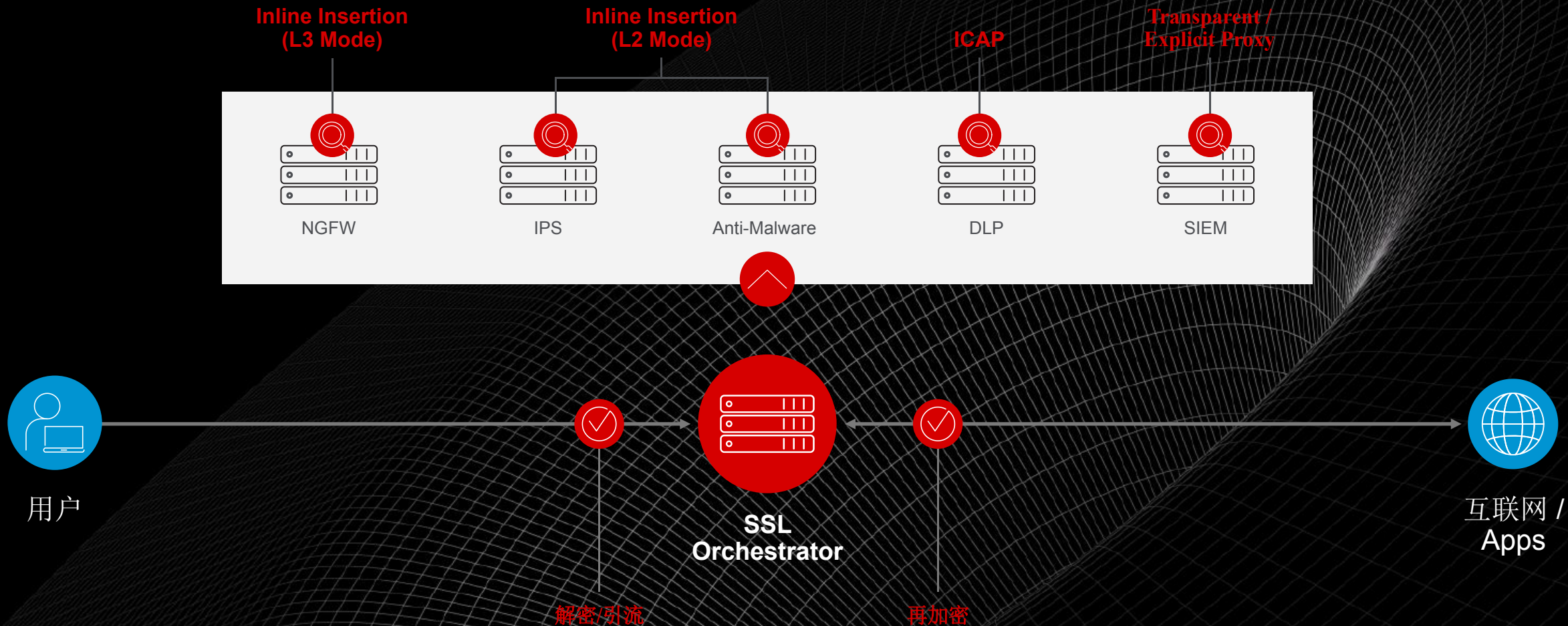




全类型设备接入

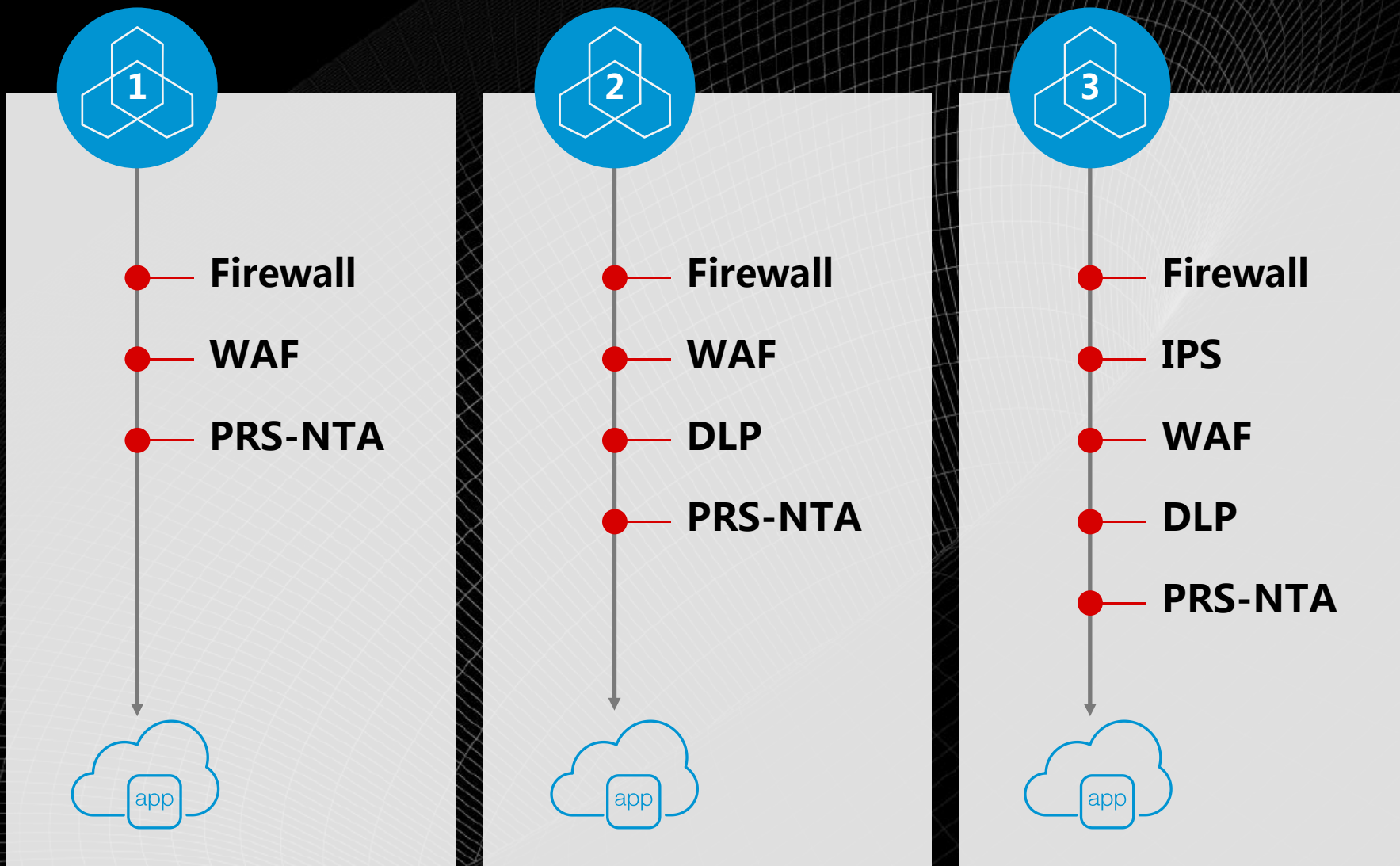


网络安全创新大会
Cyber Security Innovation Summit



设备无关性

- ✓ 安全设备动态分组
- ✓ 物理拓扑无关性
- ✓ 最大化安全投资
- ✓ 高度灵活的安全服务的插入、监控和扩展





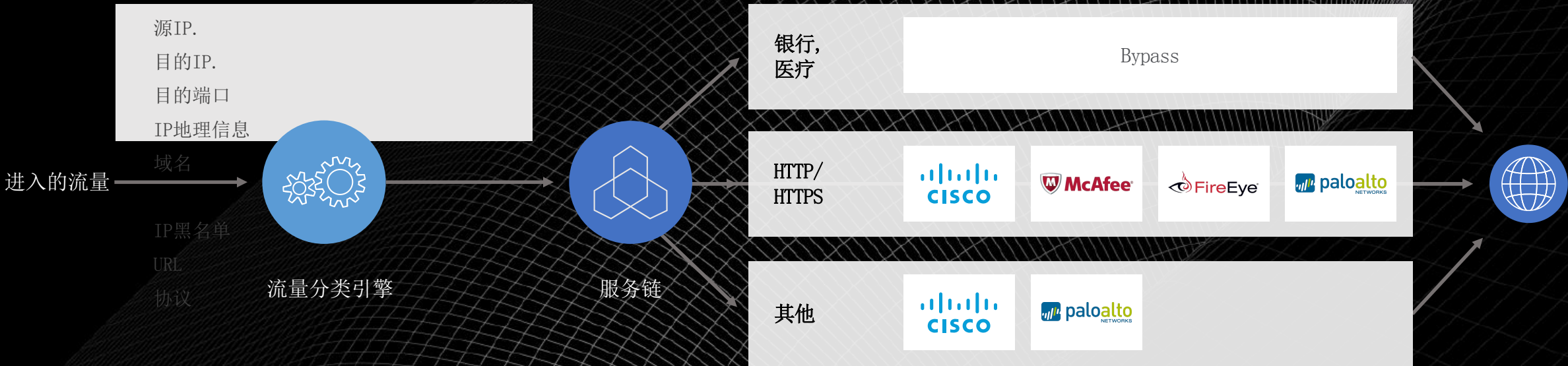
上下文分类引擎

丰富的流量选择

基于策略的解密和流
量调度

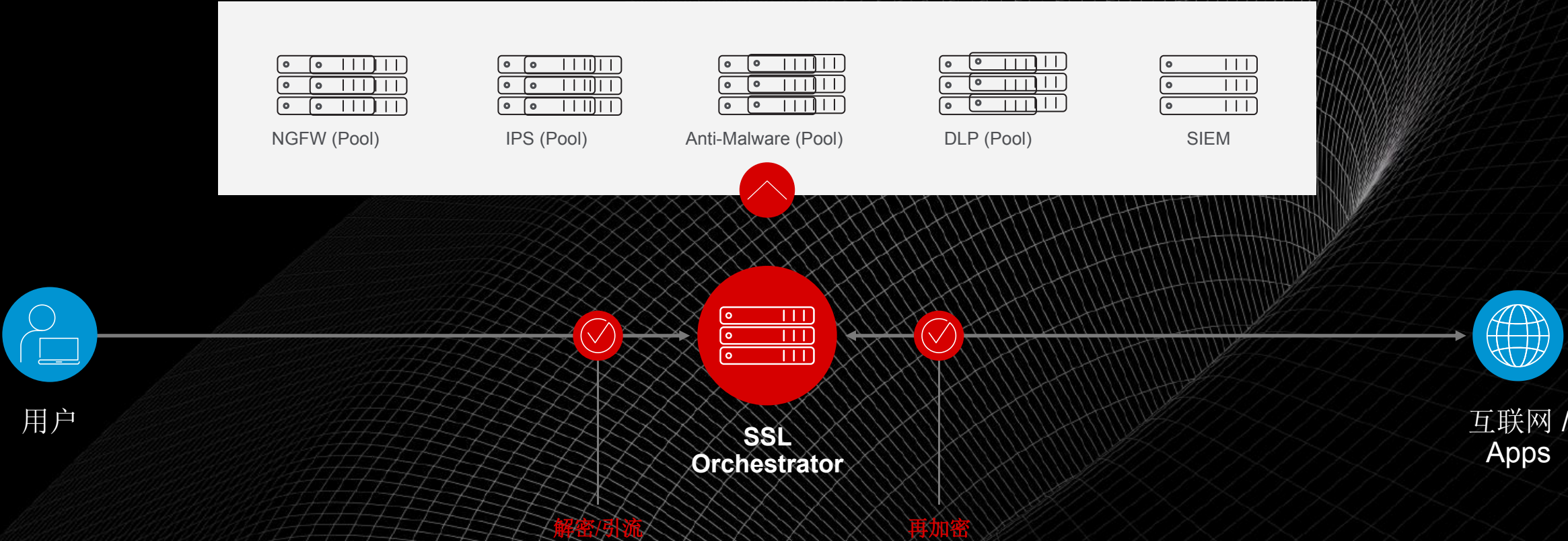
Bypass, 阻断, 检测等
多种行为

高级业务监控和可扩
展





全设备扩展





SSL Orchestration: 智能流量调度与编排



广泛的拓扑和设备支持



基于策略的动态服务链引导业务流量



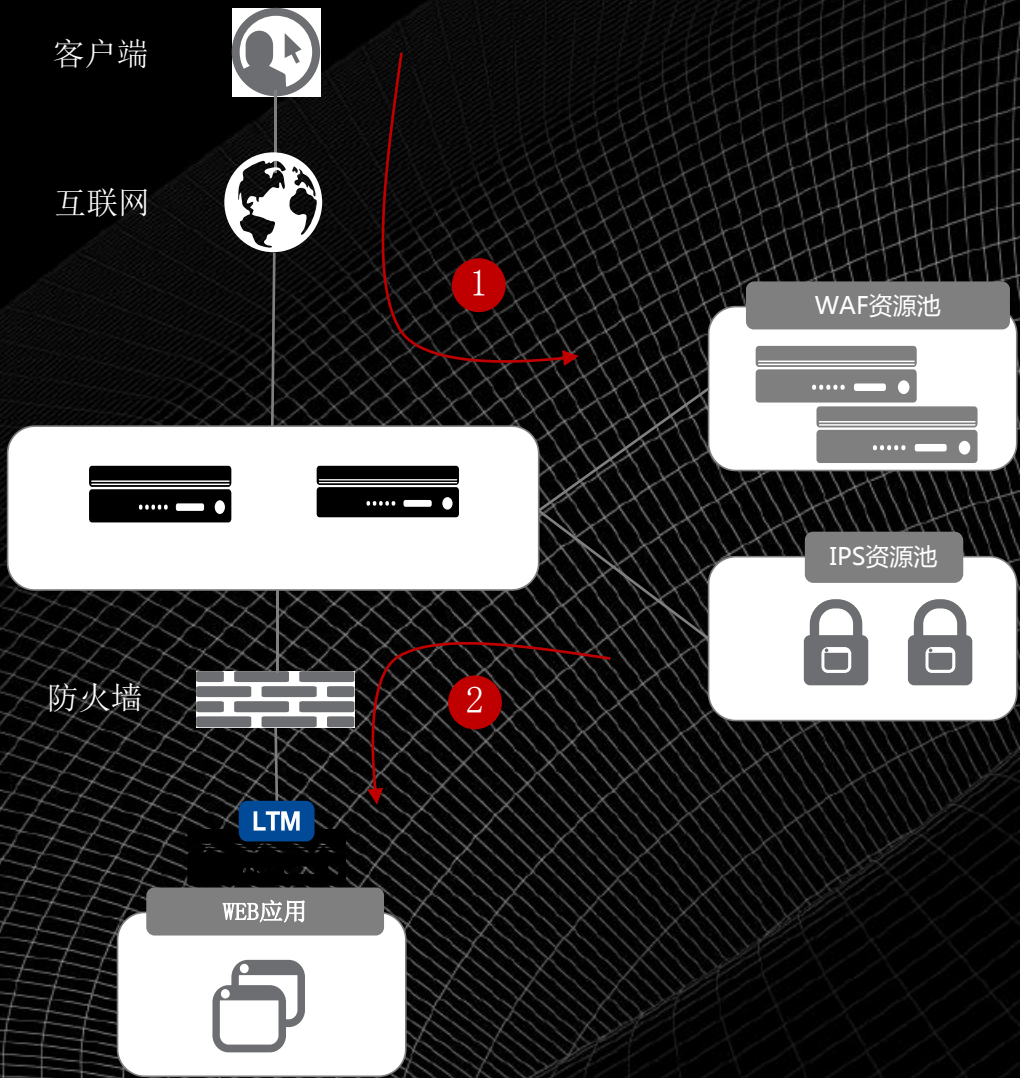
高级健康检查，负载均衡和弹性扩展



集中并简化证书和密钥的管理



灵活策略调度和故障排除





姓名 陈玉奇

公司 F5

联系方式 18930807668