奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

BCS2022系列活动-冬奥网络安全“零事故”[illegible]

边界组网优化与SSL解密在冬奥中的应用

戎泽麟 奇安信集团边界安全BG 高级产品经理

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

冬奥边界组网面临三大挑战

如何安全快速互联

冬奥涉及227个场馆、众多医院、车站等设施互联互通，跨越不同地域、快捷和安全的网络接入成为问题之一

如何保障业务连续性

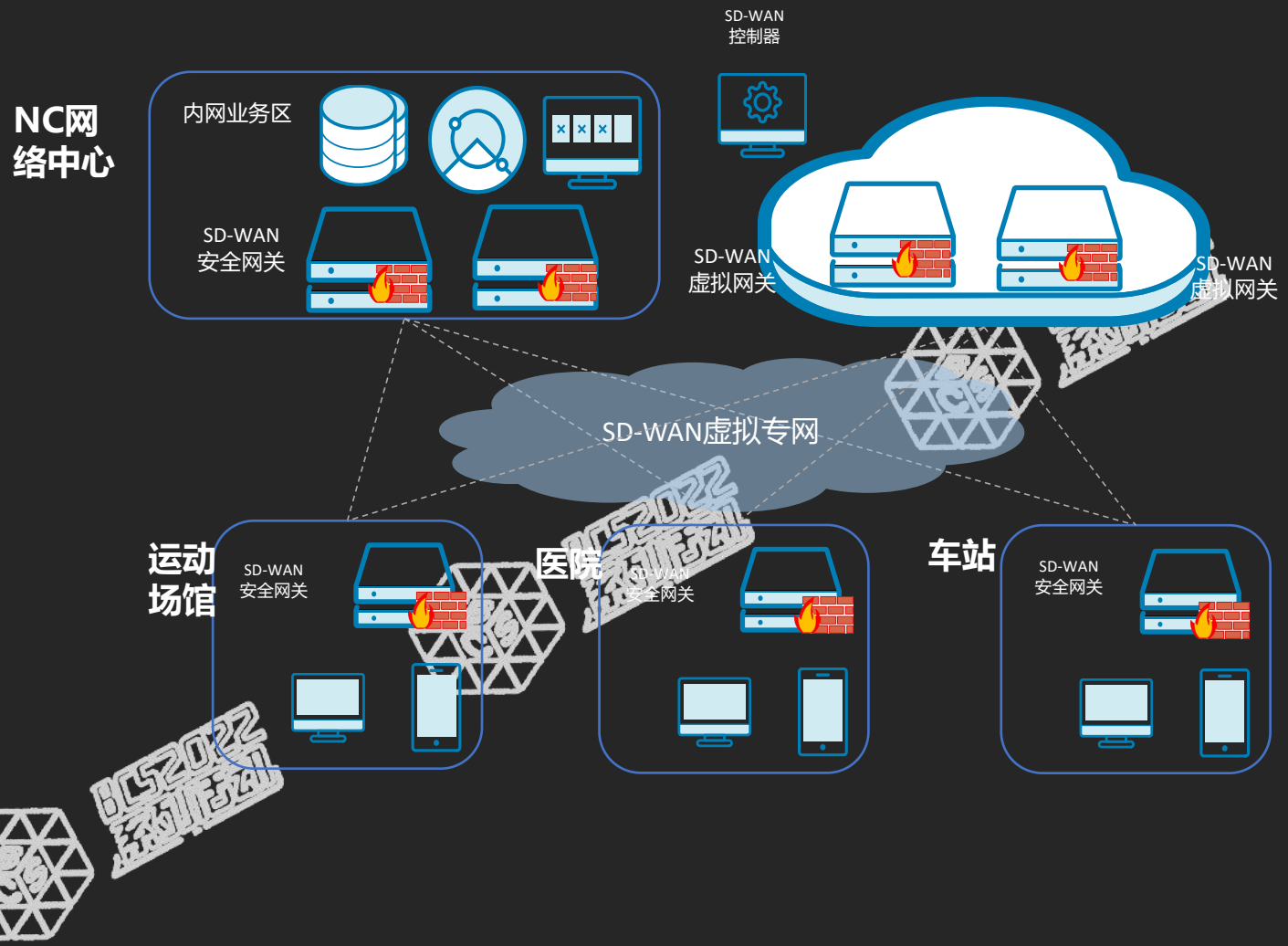
冬奥涉及60+核心业务系统，如何保证业务连续性是重中之重

如何让威胁看得见

冬奥为保证业务安全可靠，采用加密流量居多，如何在加密流量中识别出潜在的安全风险，成为新的挑战

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

SD-WAN安全组网



安全SD-WAN组网价值

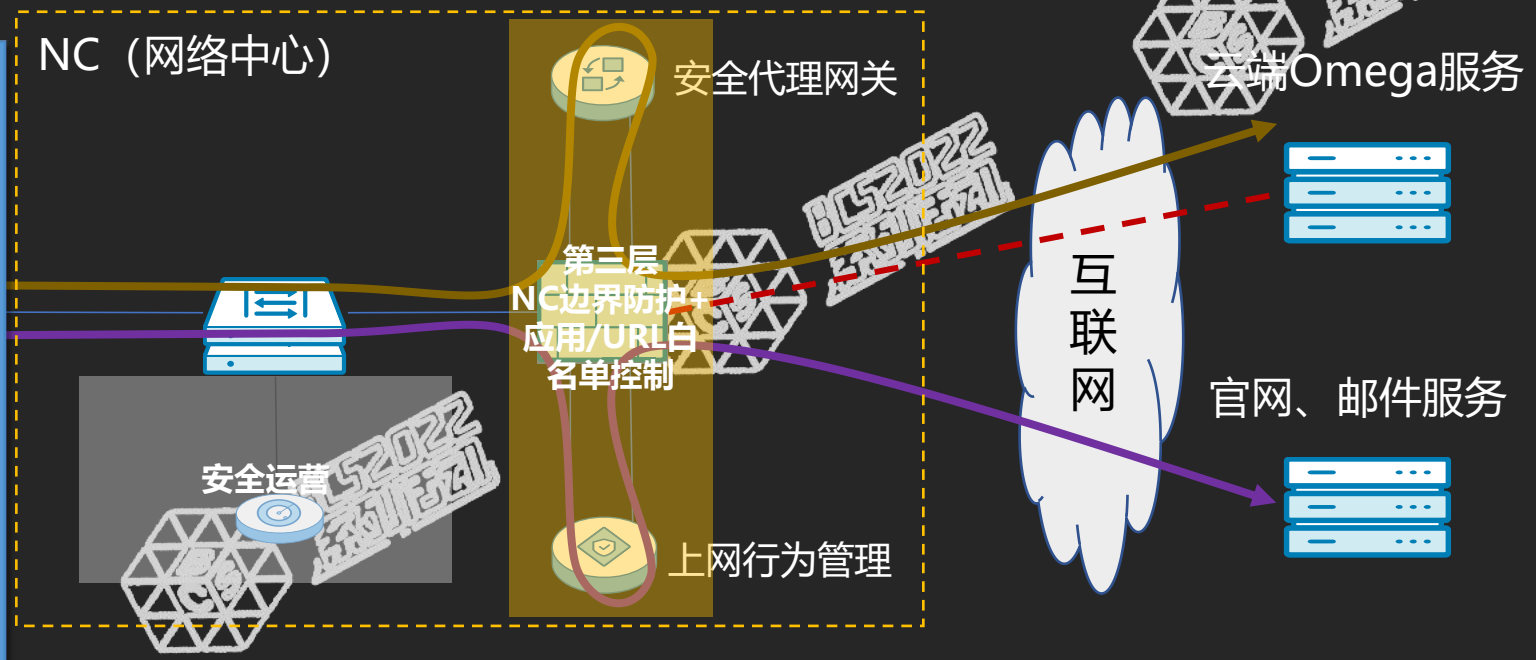
- ✓ **零配置上线：**SD-WAN组网方案加速了业务发放，简化了系统运维，一键式编排，自动配置部署，简化网络复杂度，即插即用。
- ✓ **全网集中管控：**通过管控平台集中管理以及监控全网，实时监控组网链路情况。
- ✓ **数据加密传输：**IPSec加密来保护传输中的数据，保障数据安全。
- ✓ **接入安全：**接入认证授权，降低网络风险采集设备的安全边界防护

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

流量灵活编排保障业务连续性

冬奥Omega的云端服务需要收集汇总竞赛场馆的**计时计分系统的原始数据**，所有比赛的数据必须确保万无一失的传输到云端Omega服务系统中；

两类不同的业务数据通过防火墙，基于自研的**无路由服务链引擎**做流量编排，实现精细化的业务流量走向控制，使得两类设备只处理各自相关业务流量即可。



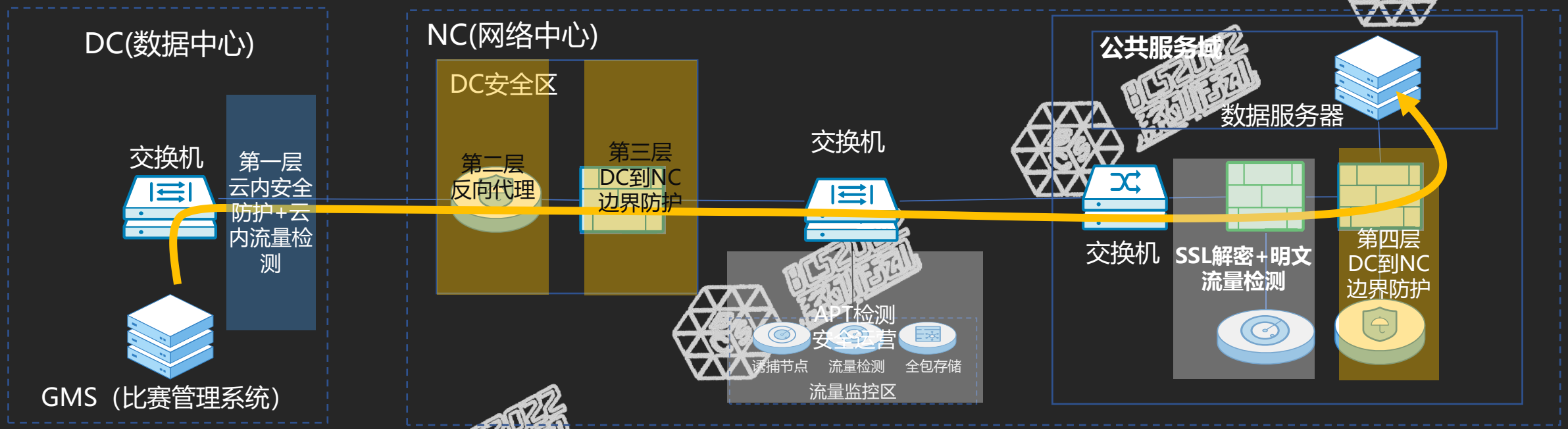
白名单+安全编排

为了减少边界防护设备的故障点、运维简约化及强管控的需求，防火墙采用**域名及地址白名单**进行管控，通过白名单的流量使用服务链编排方式进行办公终端的应用/URL白名单管控，将竞赛终端通过代理上网及URL白名单进行管控；

竞赛终端上传数据

办公终端上网

SSL解密实现威胁可见



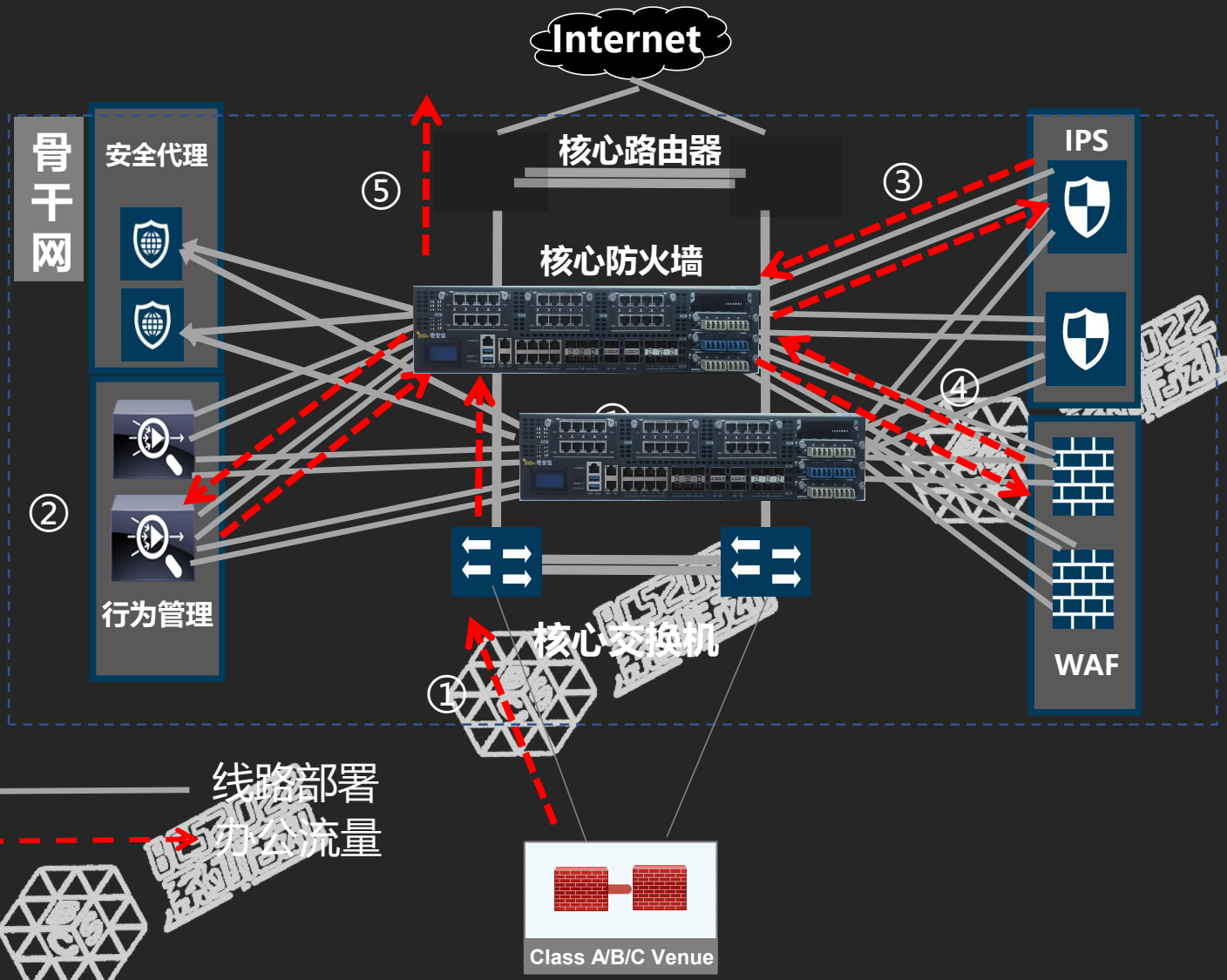
NC中的流量绝大部分是**HTTPS加密流量**，包括从OIN网络通过专线去往DC的业务系统，通过流量检测探针抓取的流量均为加密流量，导致损失了大部分流量分析手段。

部署**防火墙作为流量解密设备**，让其作为流量转发的中间人，将流入防火墙的加密流量进行解密，然后将**解密后的流量直接转发至流量检测探针**，使得分析平台能够获取NC场馆的明文流量；

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

冬奥能力-流量编排



精细化流量编排

■ **业务连续性保障**

核心出口防火墙两台HA主备部署，实施同步会话信息，任意防火墙切换不会导致业务中断，物理接口采用bypass网卡，保障业务连续性；

■ **安全资源池旁挂部署影响小**

在出口核心防火墙旁挂入侵检测、WAF、行为管理安全资源池，通过二层接入方式部署，旁路设备资源池单臂部署；

■ **安全编排高灵活**

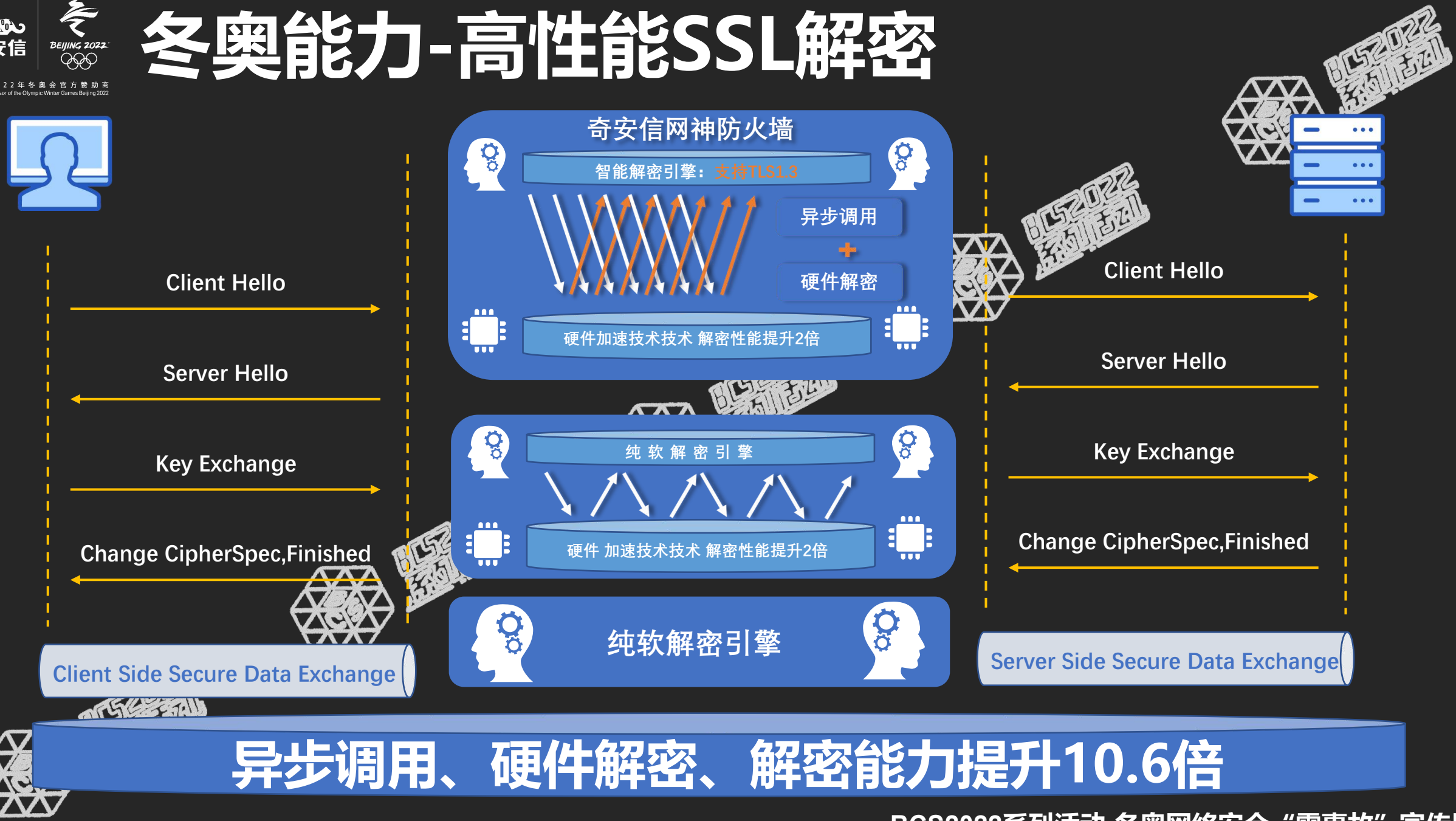
服务链匹配办公上网从的流量流经ICG实现上网行为管理，解决安全审计问题；通过IPS进行威胁发现与阻断，解决漏洞利用等风险；

■ **旁挂逃生机制**

服务链具备**负载均衡**和**业务探测**功能，能够根据业务情况及时调整流量走向，当检测到旁挂硬件设备故障时，会自动bypass该设备。

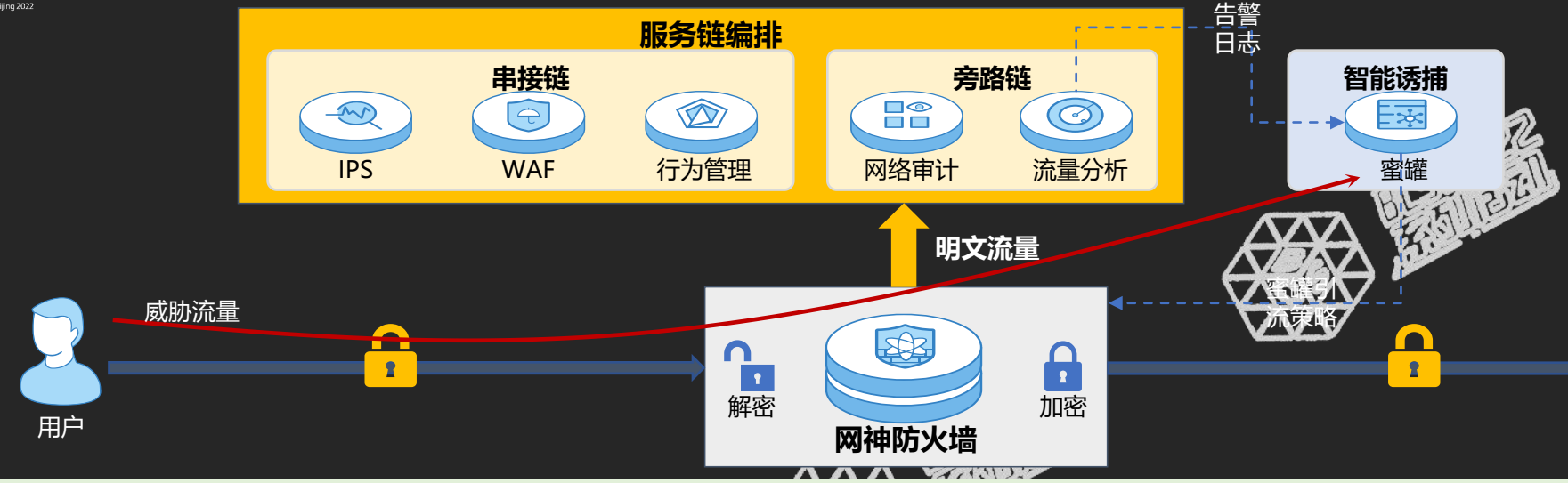
奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

冬奥能力-高性能SSL解密



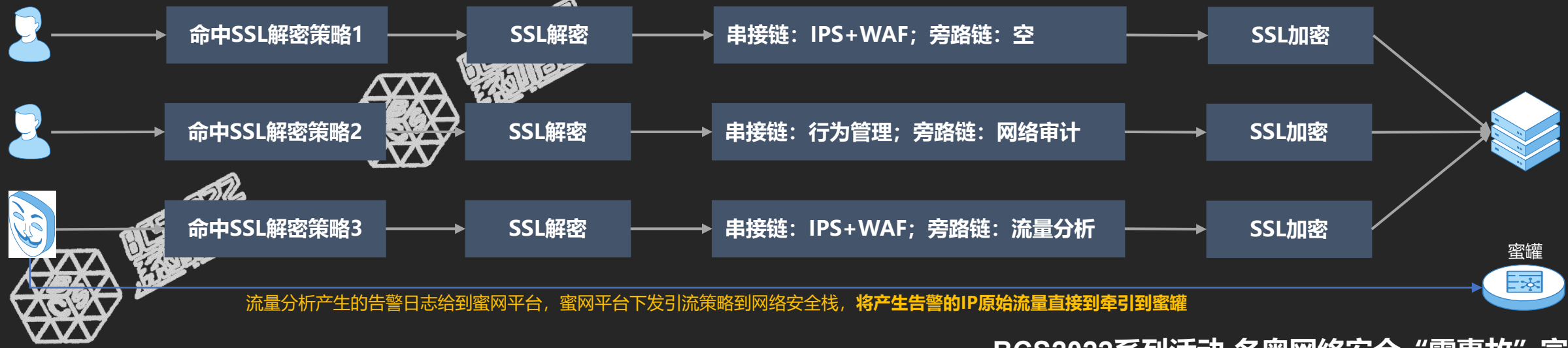
异步调用、硬件解密、解密能力提升10.6倍

展望：解密与编排融合，防火墙与蜜罐协同



流程： 1、命中SSL解密策略； 2、SSL解密； 3、命中引流策略，根据定义的服务链进行转发； 4、SSL加密；

智能诱捕： 部分流量触发蜜罐引流策略，流量通过防火墙直接牵引到蜜罐



奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

冬奥边界安全零事故

227个比赛场馆

- 竞赛场馆
- 非竞赛场馆

60套业务系统

- ODR系统
- OVS系统
- OMS系统
- GMS系统
- …

280台SD-WAN

- 车站
- 医院
- 飞机场
- …

78台防火墙

- 流量编排
- SSL解密
- 开通并维护5760条防火墙策略（优化前6543条）
- …

654天稳定运行

- 安全运行无中断
- …

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

改变传统边界安全架构，重塑边界安全防护体系

为用户提供更加智能、动态的安全防护

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

BCS2022系列活动-冬奥网络安全“零事故”[illegible]

THANKS