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”宣传周

冬奥互联网严控的挑战及解决之道

赵宇辉 奇安信集团行为安全事业部 产品总监

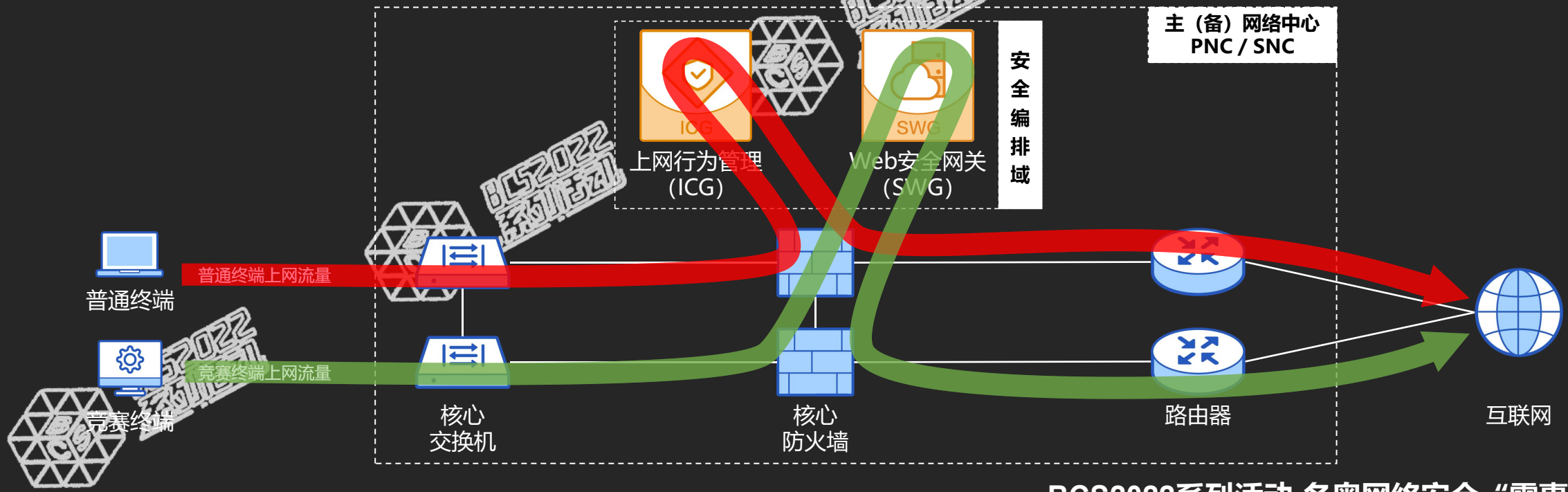
奇安信 | BEIJING 2022

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

冬奥网络纵深防御体系中的重要一环

在网络边界整合和网络分区分域的基础上，进行合理的安全策略设计。通过服务链编排的方式将**出向流量**通过**应用/域名白名单**和**代理**方式进行细粒度管控；在入向流量中通过WAF代理的方式进行源站隐藏，减少暴露面；整体纵深防御设计中除以上设计外还包含边界SDWAN/IPSec接入，同时部署蜜点诱捕及全包取证措施，溯源固证。

边界整合 | 分区分域 | **纵深防御** | 威胁防护



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

问题与挑战

北京冬奥会、冬残奥会涉及业务环境及需求异常复杂

信息系统多
60+

- 住宿信息管理系统（ACM）
- 抵离信息管理系统（ADS）
- 文档管理系统（DMS）
- 工单管理系统（ITSM）
- ……

+

区域分布广
227+

- 竞赛场馆12个
- 非竞赛场馆26个
- 服务场站188个
- 公有云平台1个
- ……

+

人员单位多
10000+

- 涉奥关基成员单位47个
- 国内外开发商10个
- 涉奥终端10,000+
- 参赛运动员2,892人
- ……

=

外联需求极其复杂

- 在互联网边界，除终端正常的互联网访问外，还涉及**赛事、外事、管理等多个业务系统的数据报送**互联网外联需求

采用白名单机制精准管控出向流量，杜绝未知外联

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

解决之道

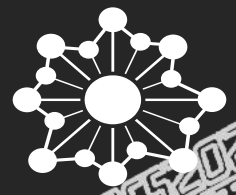
业界领先、覆盖广泛应用/URL数据库

应用协议库 **12,000+**

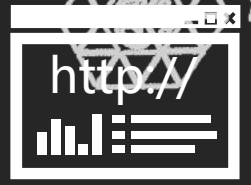
URL库 **2.8亿+**

- 可识别超过99%的已知网站
- 可精确识别各种业务访问及其具体操作

灵活多样的自定义应用



端口规则

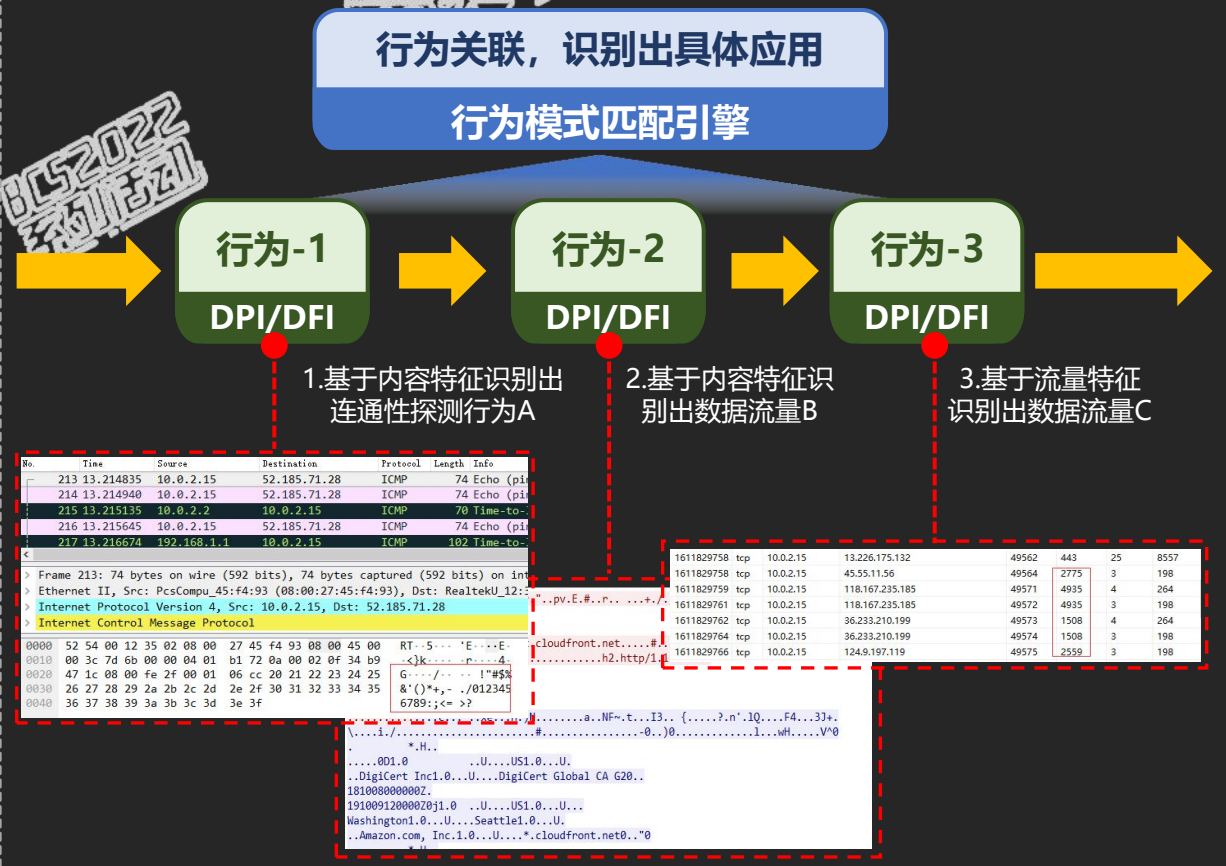


HTTP规则

域名/IP

基于行为的应用识别技术

- 基于内容特征或流量特征识别出具体行为，再对多个行为进行关联
- 快速、精准识别如 P2P、翻墙软件等弱特征应用



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

针对普通终端的白名单策略

高优先级
针对不同用户、指定应用的"显式放行"策略

优先级	状态	名称	描述	时间	用户	应用	动作
↓0	启用	联通TOC监控电脑探测NC核心路...		所有时间	[未共享] /根/联通TOC监...	基础协议/ICMP	
↑↓1	启用	各场馆成绩用户访问Beijing2022....		所有时间	[未共享] /根/TOC-Atos...	DNS/DNS, 用户自定义/Beijing2022官网	
↑↓2	启用	OMEGA-Ix		所有时间	[未共享] /根/OMEGA-A...	DNS/DNS, 用户自定义/OMEGA_ALL, 用户自定...	
↑↓3	启用	BHQ-交通指挥中心-高德地图		所有时间	[未共享] /根/BHQ-交通...	用户自定义/交通-高德地图	
↑↓4	启用	TOC-Atos终端访问Beijing2022...		所有时间	[未共享] /根/TOC场馆-...	用户自定义/Beijing2022官网	
↑↓5	启用	TOC-Atos工作终端访问策略		所有时间	[未共享] /根/TOC-Atos...	DNS/DNS, 用户自定义/TOC-Atos仅工作终端使...	
↑↓6	启用	各场馆成绩用户访问策略		所有时间	[未共享] /根/TOC-Atos...	DNS/HttpDNS, DNS/DNS, DNS/MDNS, 用户自...	
↑↓7	启用	TOC-Atos-logicmtr.page.link		所有时间	[未共享] /根/TOC-Atos/...	用户自定义/Atos-logicmtr.page.link	
↑↓8	启用	TOC-IAM运维终端访问IAM测试环...		所有时间	[未共享] /根/TOC-IAM...	DNS/DNS, 用户自定义/IAM测试环境协议, 用户...	
↑↓9	启用	TOC-应用控制策略		所有时间	[未共享] /根/TOC-Atos...	DNS/DNS, 用户自定义/瞩目会议域名, 用户自定...	
↑↓10	启用	MMC INFO访问策略		所有时间	[未共享] /根/MMC INFO...	DNS/DNS, 用户自定义/冬奥组委邮箱域名, 用户...	
↑↓11	启用	TOC-域控运维终端		所有时间	[未共享] /根/TOC-域控...	DNS/DNS, 电子邮件/SMTP/SMTP, 用户自定义/...	
↑↓12	启用	TOC		所有时间	[未共享] /根/TOC/	DNS/DNS, 电子邮件/SMTP, 用户自定义/冬奥组...	
↑↓13	启用	TOC场馆-Atos允许访问白名单应用		所有时间	[未共享] /根/TOC-Atos/,...	DNS/DNS, 用户自定义/冬奥组委邮箱域名, 用户...	
↑↓14	启用	OIN场馆-BON区域允许访问白名...		所有时间	[未共享] /根/ATC场馆-B...	DNS/DNS, 用户自定义/冬奥组委邮箱域名, 用户...	
↑↓15	启用	残奥会期间访问策略	有效...	残奥会期...	[未共享] /根/BAS场馆-B...	DNS/DNS, 用户自定义/残奥会期间访问域名	
↑↓16	启用	TCC用户访问在线翻译系统	TCC...	所有时间	[未共享] /根/TCC场馆-B...	DNS/DNS, 用户自定义/在线翻译系统	
↑↓17	启用	OIN场馆-BON区域拒绝所有		所有时间	[未共享] /根/ATC场馆-B...	所有应用	

最低优先级
默认"阻塞所有"策略

自定义应用

名称	描述	域名/IP
残奥会期间访问域名	有效...	beijing2022-para.medalpresenter.ome...
NC核心路由器		10.134.1.1,10.134.1.2,10.135.1.1,10....
在线翻译系统	TCC...	iciba.com
OMEGA_ALL		update.microsoft.com,windowsupdate....
交通-高德地图		restapi.amap.com,a.amap.com,webapi....
新华社-新闻网		www.news.cn,news.cn,xinhuanet.com
Beijing2022官网		beijing2022.cn,btrace.qq.com,btrace.vi...
TOC-Atos仅工作终端使用域名		adfs.myatos.net
Atos-logicmtr.page.link		logicmtr.page.link,142.251.43.14,logic...
IAM测试环境地址		39.107.180.230
TOC可访问白名单		bif-btf.beijing2022.cn,bif.beijing2022.c...
共享文档系统		dmsmev.sharepoint.com,svc.ms

为冬奥会、冬残奥会所涉及的各类URL自定义的"Web应用"，共计**50余个对象**，涉及**URL近千条**

针对竞赛终端的代理上网策略

每条代理上网策略，都明确定义了具体的“目的域名”

优先级	状态	名称	描述	用户	源IP	目的域名	动作
↓0	启用	EDC-S2SWMCG_to_lenovo		所有用户	EDC-...	lenovo	
↑↓1	启用	ATOS-TOC-A1AGENCW_to_g...		所有用户	ATOS...	grafana-apps-monitoring.apps-mev...	
↑↓2	启用	ATA-SCOM上网代理策略		/根/ATA-SCOM访问域名/	任意	ATA-SCOM访问域名	
↑↓3	启用	PNC-SF-NGSOC代理		/根/PNC-SF-SOC001	任意	阿里云资产,Aliyun-OpenAPI,aliyun-l...	
↑↓4	启用	PNC-威胁运营平台升级代理		/根/PNC-威胁运营平台	任意	天眼升级域名	
↑↓5	启用	CPN-ALL-D1-VLAN上网代理...		/根/CPN-ALL-D1-VLAN/	任意	sftp-ow22-int.mev.atos.net,D1-VLA...	
↑↓6	启用	CPN-ALL-Cx-VLAN上网代理策...		/根/CPN-ALL-Cx-VLAN/	任意	sftp-ow22-int.mev.atos.net,Cx-VLAN	
↑↓7	启用	CPN-ALL-Ox-VLAN上网代理策...		/根/CPN-ALL-Ox-VLAN/	任意	ATC访问域名,sftp-ow22-int.mev.ato...	
↑↓8	启用	CPN-ALL-Ix-VLNA上网代理策略		/根/CPN-ALL-Ix-VLAN/	任意	Atos-wrs-e2e,sftp-ow22-int.mev.at...	
↑↓9	启用	SMAC升级库代理		未指定	SMAC	ngfwup.sg.qianxin.com	
↑↓10	启用	监控系统访问短信网关		/根/PNC可用性监控	任意	SMS平台	
↑↓11	启用	ZSP-CPN代理上网策略		未指定	任意	CPN-ALL域名访问清单,Atos-wrs-e2...	

名称	描述	域名信息
lenovo		download.lenovo.com, support...
adobe		*.adobe.io
grafana-apps-monitoring.apps-...		grafana-apps-monitoring.apps...
ngfwup.sg.qianxin.com		ngfwup.sg.qianxin.com
ADOBE		*.licensing.adobe.com, *.adobe...
sftp-ow22-int.mev.atos.net		*.sftp-ow22-int.mev.atos.net, s...
ATA-SCOM访问域名		210.73.66.103, *.mail.beijing2...
Omega_Specific_Web		*.Beijing2022.omegatiming.co...
OME_All_SWT		*.swtservice.com, *.storage.sp...
OME_ALL_PcMgmt		*.crl.microsoft.com, *.delivery....
aliyun-logservice		100.49.133, 100.100.49....

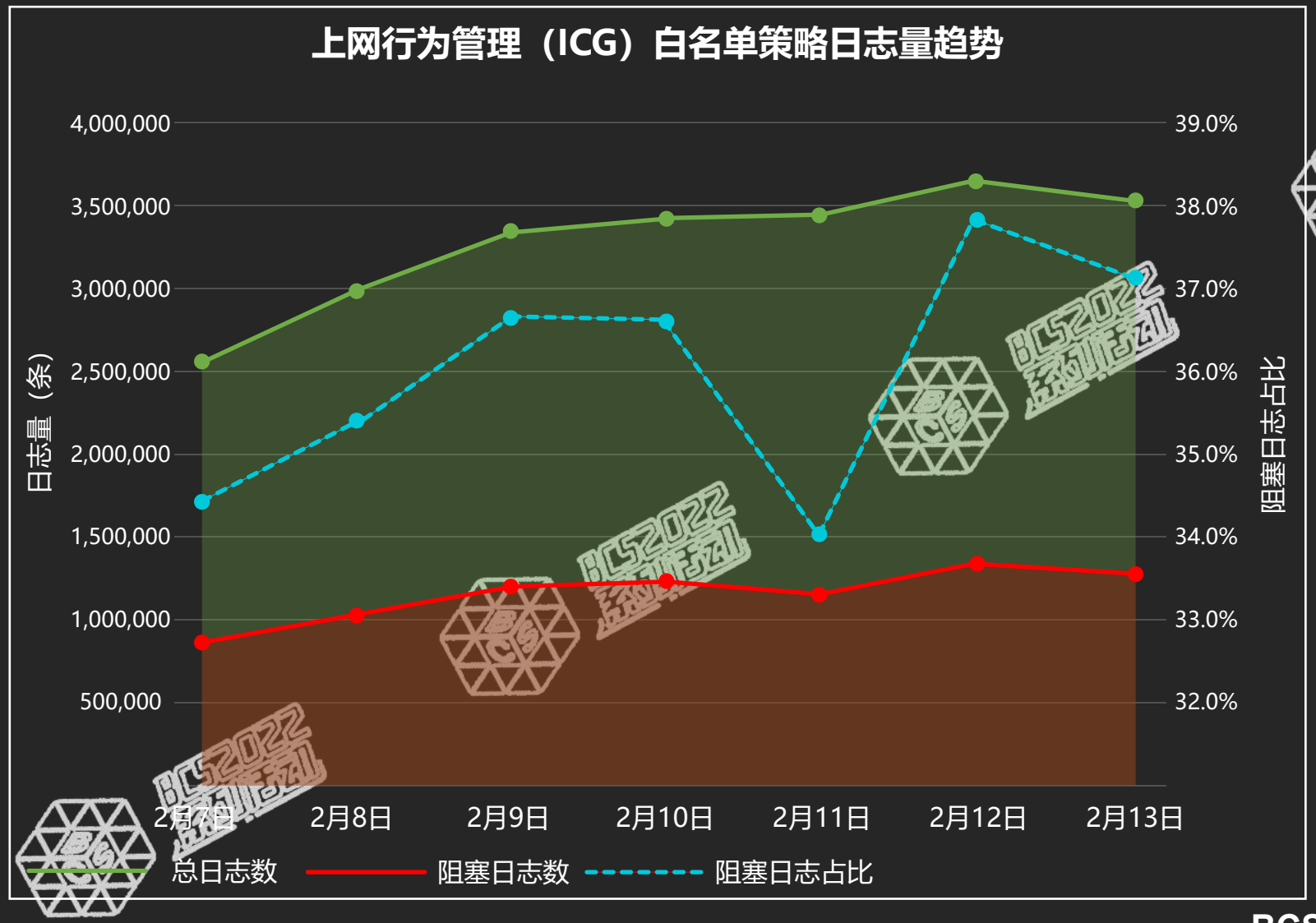
为冬奥会、冬残奥会所涉及的代理目的域名，共计**130余个**

针对不同竞赛终端（IP）的代理上网策略；不在策略定义范围内的代理上网行为，都被“默认阻塞”

奇安信

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

运行效果



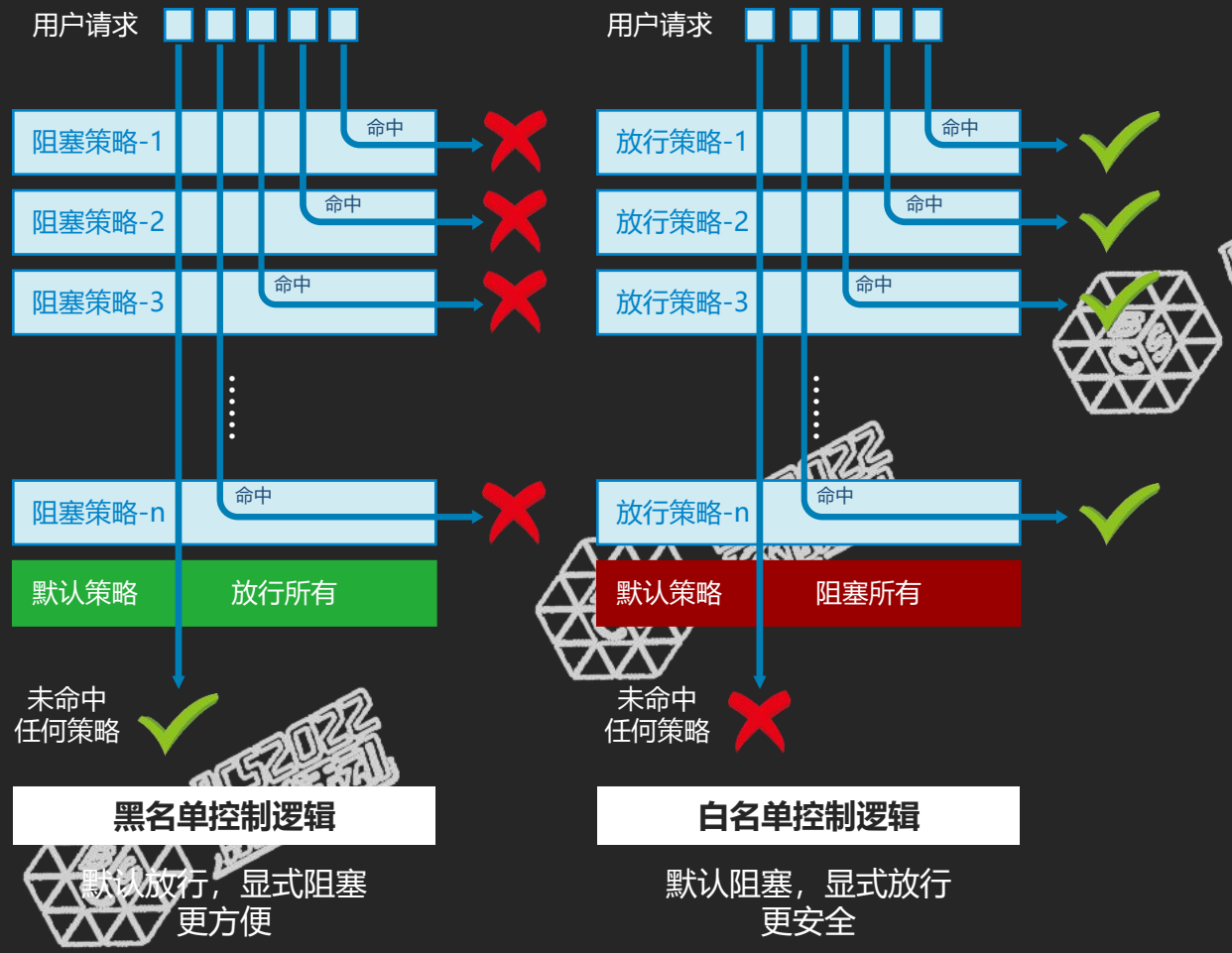
- 赛时期间，应用管控总日志 **300～350万**/天
- 默认阻塞日志量 **100～150万**/天
- 约**1/3**的用户请求被阻塞管控

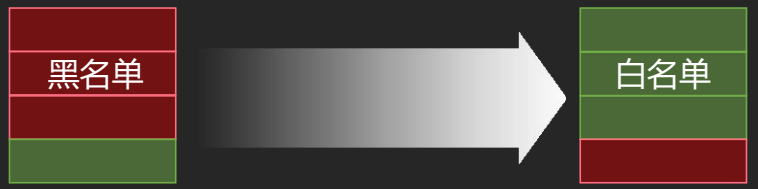
奇安信 | BEIJING 2022

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

总结与启示

启示-1：为什么采用“白名单”的控制逻辑？





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

总结与启示

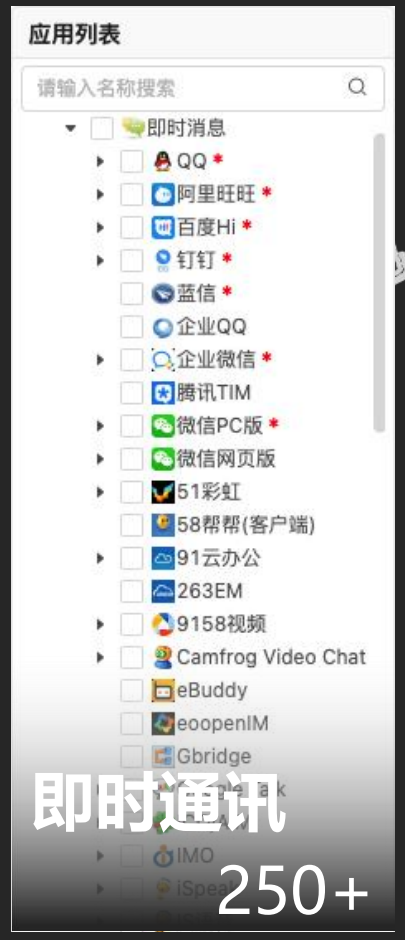
启示-1：为什么采用“白名单”的控制逻辑?

应用总数

12,000+

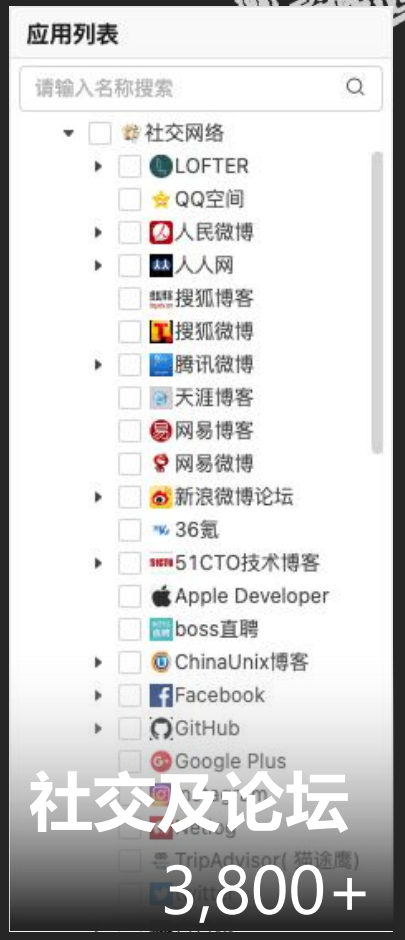
移动应用

5,000+



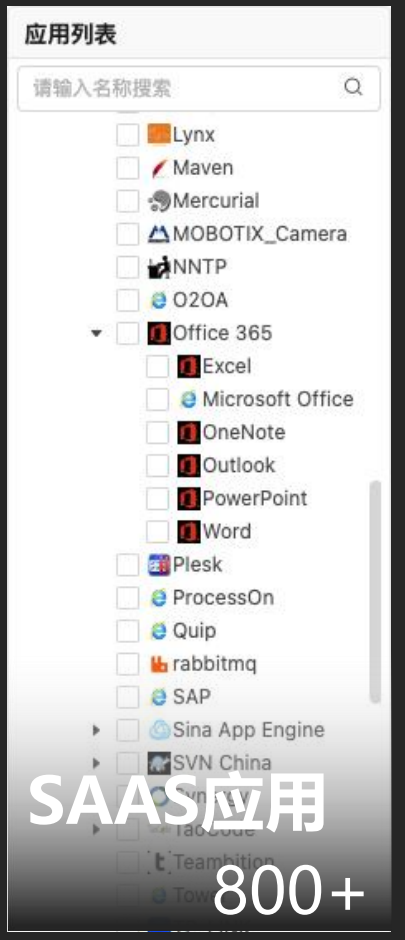
即时通讯

250+



社交及论坛

3,800+



SAAS应用

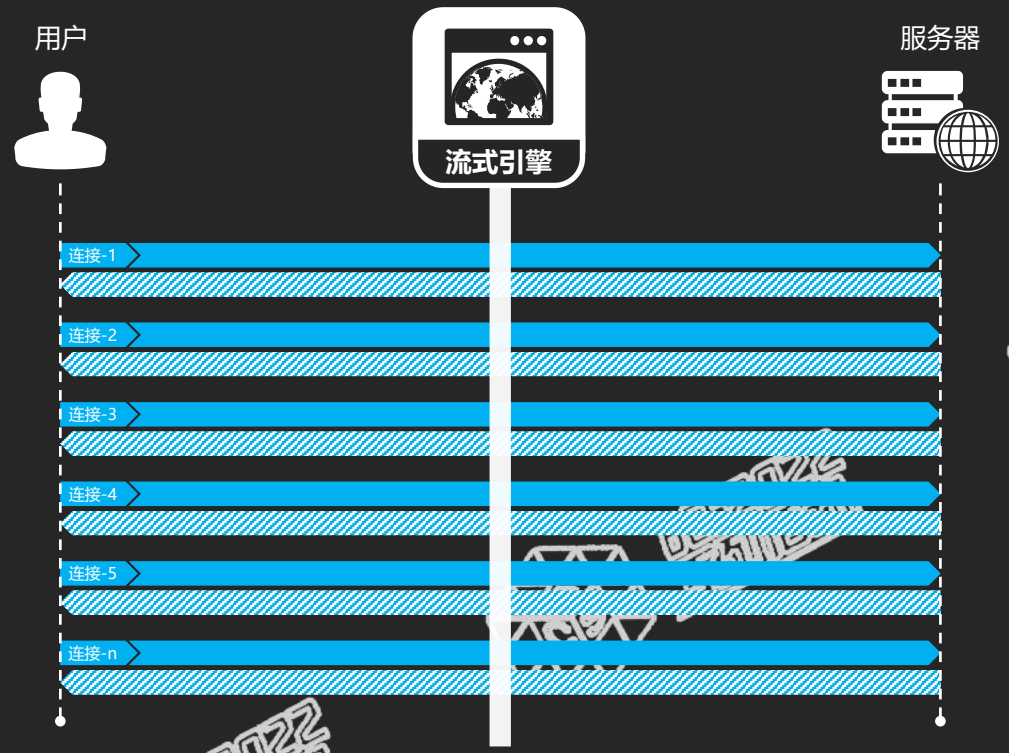
800+

奇安信 | BEIJING 2022

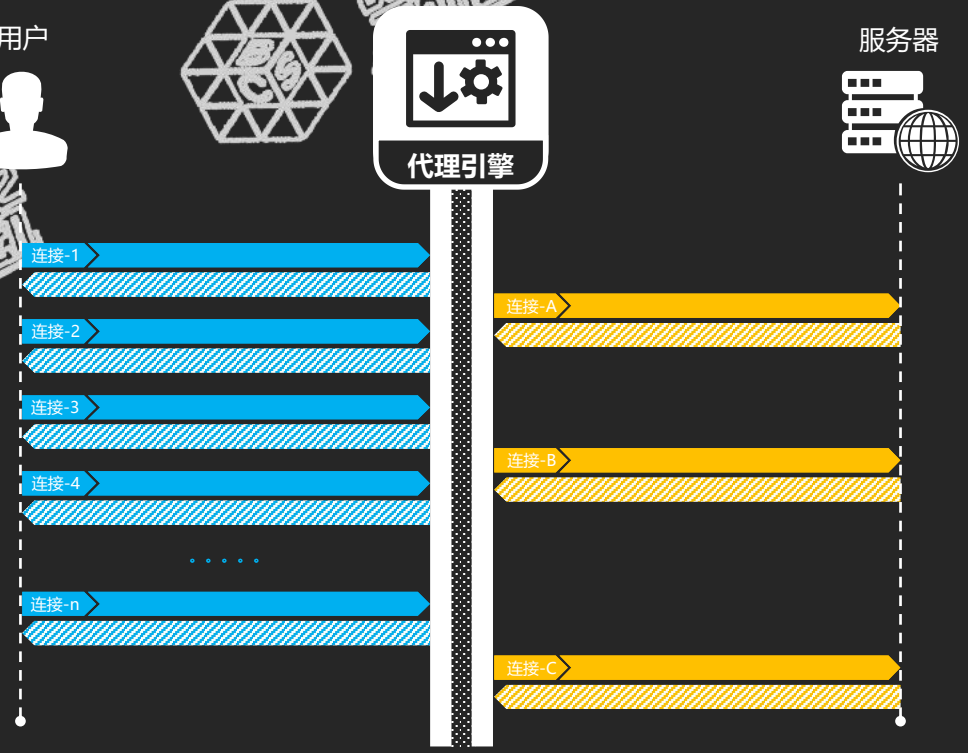
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

总结与启示

启示-2：为什么采用代理架构?



- 高转发、低延迟的转发架构，实时的流量透传转发
- 基于DPI、DFI机制的流式（一体化）检测引擎，基于规则的包检测
- 在低延迟的刚性要求下，会妥协检测能力，超出后放通



- 基于全代理架构的终结式引擎，重新构建外发流量，按需发送
- 基于完整内容层深度还原后，完整内容层检测扫描
- 在保证应用可用的前提下，做到内容检测无遗漏

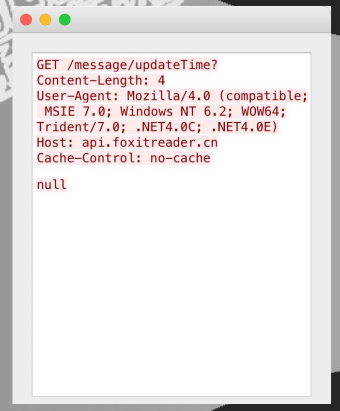
奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

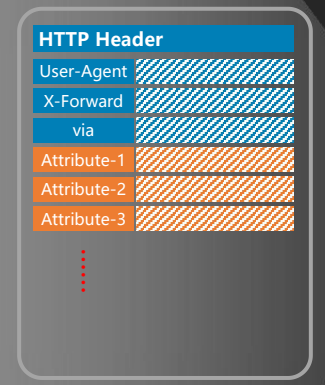
总结与启示

启示-2：为什么采用代理架构?

协议修改、隐藏和增加

- 可定义添加，修改，删除协议头中的各种信息，比如Via，X-Forwarded-For等
- 验证是否符合协议标准，并防止不符合要求的流量
- 重写和重定向URL
- 协议的转换





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

总结与启示

启示-2：为什么采用代理架构?

内容检测、控制和替换

- 分析和处理Web页面上的脚本内容，进行检测、控制和替换
- Web上传下载内容检查，去除恶意或敏感信息
- 文件内容检测，替换掉敏感文件或去除文件中的恶意内容
- 场景：恶意内容检测，替换、去除恶意内容；敏感信息控制等

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”宣传周

THANKS