2026

跨境通信检测解决方案

目录

CONTENTS

01 跨境通信基础原理

02 政策及监管态势

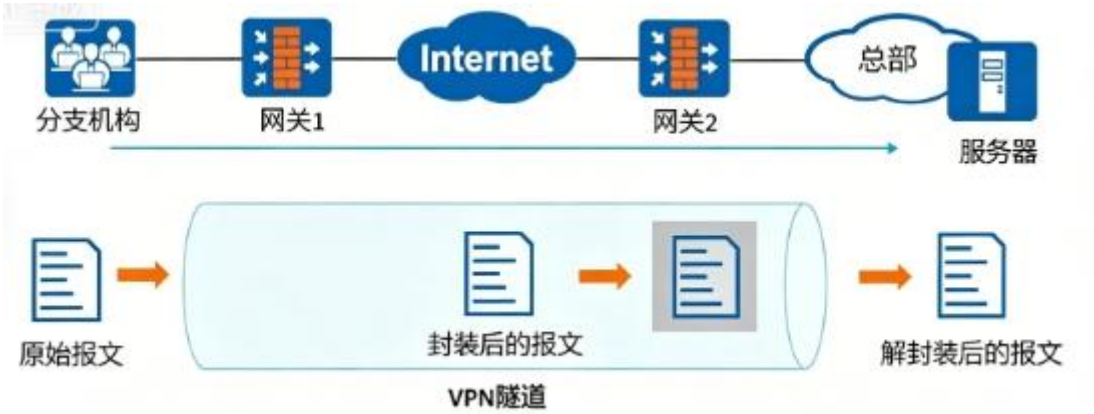
03 解决方案及优势

跨境通信基础原理

PART ONE

VPN技术原理

VPN（虚拟专用网络）是一种在公共网络（如互联网）上建立加密通信通道的专有网络技术，其标准用途在于安全地扩展企业内部网络，实现跨地域分支机构互联或员工远程安全接入。传统VPN协议主要包括IPSec、L2TP、PPTP、GRE等。



VPN原理

在中国网络管理语境下，通常所称的“翻墙”即“突破网络封锁”，特指绕过国家公共网络监控系统（GFW，中国国家防火墙）的行为。该行为通常指：未经批准，擅自使用VPN等技术手段，规避IP封锁、内容过滤、域名劫持等监管措施，访问国家禁止的境外网站或服务。 此类行为属于违规跨境联网，是国家法律法规所明令禁止的。

常见跨境通信方式

01

VPS 直连方式

原理：用户直接连接境外VPS上的代理服务，没有中间节点转发。

特点：配置步骤最简单，时间与资金成本最低；但出口IP极易被封锁，整体网络稳定性较差。

02

VPS 普通中转

原理：用户流量经过一个或多个中间服务器进行转发，以此隐藏最终落地VPS的真实IP地址。

特点：有效提高了抗封锁能力，规避IP被封风险；但因增加转发节点，会带来一定的网络延迟。

03

VPS 建立BGP隧道中转

原理：利用BGP（边界网关协议）自动计算并获取互联网中最优的网络传输路径，建立稳定的通信隧道。

特点：连接速度快，稳定性显著提升，体验接近专线；但技术门槛较高，相应的运维和租用成本也更高。

04

VPS 搭建IPLC专线中转

原理：租用运营商提供的IPLC（国际专用租用电路）服务，实现两点之间的专属、私密网络连接。

特点：物理隔离于公共互联网，拥有最快的传输速度、最低的延迟和最高的稳定性；缺点是成本非常高昂。

从简单到复杂的演进

常见跨境通信方式

技术演进：更隐蔽、更易用

私自搭建

当前，部分中小机构或个人通过租用国内BGP/多线云主机，结合IPLC/IEPL等跨境专线，私自搭建并提供跨境代理服务。此类服务以境内主机中转流量，以套餐形式非法向用户提供跨境联网接入。

高隐蔽性协议

为规避监管跨境服务普遍采用SSR、Vmess、Trojan等协议通过伪装流量特征，模拟正常HTTP/HTTPS流量，规避检测难度大。

一体化客户端

Clash、V2RayN等工具提供图形化操作界面，集成多种协议与规则，大幅降低了普通用户的使用门槛。

应用生态：违规平台与专用客户端

违规VPN服务平台（“机场”）

服务商在境外搭建大量网络节点，将多条线路打包整合为服务出售。用户通常通过微信、TG等渠道联系，按月、按季度或按年购买流量套餐，形成了完整的地下灰色产业链。

专用VPN客户端

主流“机场”均开发了适用于Windows、macOS、iOS及Android的专用客户端，一站式集成账号登录、节点自动更新、线路测速及支付功能，用户体验已接近商业级软件。

政策及监管态势

PART TWO

政策法规约束

网络安全法

- **关键信息基础设施保护**
  重要数据需在境内存储，严防数据流失。
- **数据出境安全评估**
  关键信息基础设施运营者数据出境必须经过严格的安全评估。
- **禁止非法跨境联网**
  严禁擅自建立或使用非法定信道进行国际联网。

数据安全法

- **数据分类分级保护**
  国家建立数据分类分级保护制度，对核心、重要数据实施重点保护。
- **重要数据出境管理**
  重要数据出境原则上需进行安全评估，严格管控。
- **向境外提供数据限制**
  非经主管机关批准，不得向外国司法或执法机构提供境内数据。

个人信息保护法

- **个人信息出境合规路径**
  明确了三条合规路径：通过安全评估、订立标准合同或通过个人信息保护认证。
- **告知与单独同意**
  向境外提供个人信息前，必须充分告知接收方情况并取得个人的单独同意。
- **敏感个人信息特殊保护**
  对敏感个人信息的处理设置了更严格的条件和限制。

法律责任与执法实践警示

擅自建立非法定信道

法律依据：

《中华人民共和国网络安全法》第79条

法律责任：

责令停止联网，给予警告，并处**15000元以下**罚款；有违法所得的，没收违法所得

违法向境外提供重要数据

法律依据：

《中华人民共和国数据安全法》第46条

法律责任：

由相关部门没收违法所得，最高可处**1000万元**罚款；并可责令暂停相关业务、停业整顿、吊销许可证。

违法处理/提供个人信息

法律依据：

《中华人民共和国个人信息保护法》第66条

法律责任：

没收违法所得，最高可处**1000万元**罚款；并可责令暂停或终止服务、吊销相关业务许可。

跨境访问中面临的网络安全问题

01. APT攻击与知识产权窃取

案例：西北工业大学遭国家级APT攻击

美国NSA利用“酸狐狸”平台等多种武器，长期窃取学校核心网络设备配置、管理人员账号口令等关键敏感数据，严重威胁我国顶尖学府的科研安全。

02. 数据泄露与个人信息滥用

案例：企业因安全配置不当导致数据泄露

某物流科技企业ES数据库端口直接向公网开放，未采取加密、访问控制等措施，导致包含敏感个人信息的大量业务数据疑似被境外可疑IP窃取。

03. 供应链攻击与钓鱼陷阱

案例：利用软件升级功能进行供应链攻击

某先进材料设计研究院的电子文件系统被入侵，攻击者篡改客户端分发程序，利用升级功能向276台科研人员主机批量投递特种木马，针对性窃取知识产权文件。

跨境行为监管行动

国家网信办

统筹协调与执法监督

核心行动：

发布执法典型案例，强化合规意识

对多家企业因数据违规出境、未经评估擅自出境等行为进行处罚，明确了数据出境必须遵循“合法、正当、必要”原则，为企业合规提供了清晰指引。

公安机关

刑事打击与立案侦查

核心行动：

对重大网络攻击事件立案调查

针对“西北工业大学遭美国NSA网络攻击案”正式立案调查，彰显捍卫国家网络主权的决心；严厉打击为境外刺探、非法提供情报等危害国家安全的犯罪行为。

工信部

技术监测与预警通报

核心行动：

发布网络攻击技术调查报告

依托国家互联网应急中心（CNCERT）发布多份技术调查报告，详细披露境外网络攻击的具体手段与特征，为国内关键信息基础设施运营单位提供重要的防御预警和技术指引。

当前跨境监测面临的六大难点

01 政策要求复杂多变

- 法规体系复合框架复杂
- 百万级信息需安全评估
- “重要数据”界定模糊
- 跟踪动态调整的政策

02 监管考核压力巨大

- 等保2.0涉及211个考点
- 重大风险可“一票否决”
- 指标不符扣3倍基准分
- 重点行业常态化通报

03 大流量监测瓶颈

- DPI致吞吐量降30%
- 83%加密流量可见性低
- 境外SaaS识别率仅78.5%
- 协议混淆规避传统监测

04 多厂商设备整合难

- 日志碎片化溯源超8h
- 告警风暴淹没真实威胁
- API兼容差联动响应难
- 缺统一视图难发现攻击链

05 原始数据预处理

- 日均产生上百TB数据
- 碎片化数据包重组会话
- 特征提取制约AI模型
- 敏感信息严格脱敏合规

06 管理决策维度

- 安全投入ROI难量化
- 风险评估与决策脱节
- 管理层认知支持不足
- 安全策略执行落地难

解决方案及优势

PART THREE

全方位跨境监测解决方案

01 多维度跨境应用精准识别

•**全流量采集解析**：无干扰、全量采集出口网络流量。
•**DPI引擎**：深入载荷，精准识别数千种应用协议，涵盖VPN协议、代理、远程控制及特定敏感应用等，有效识别如Freegate、V2ray、Clash、SSR、OpenVPN等主流与隐蔽的跨境应用。
•**隐蔽隧道识别**：还原加密流量中的违规跨境通道。

02 智能跨境行为建模与分析

•**UEBA技术**：建立用户、账号、设备的动态行为基线。
•**多维度基线**：从时空、设备、数据访问模式等维度构建。
•**异常检测**：实时识别“首访敏感区”、“非工作时间大量上传”等异常。
•**风险评分**：对异常行为量化评分，优先处理高危事件。

03 动态威胁情报节点监测

•**情报整合**：实时对接全球主流情报源，获取最新IoC。
•**节点探针**：持续监测网络节点的外联连接行为。
•**关联分析**：实时比对外联行为与情报库，发现恶意外联。
•**快速定位**：精准定位黑客控制的失陷主机，防止横向移动。

04 全景可视与溯源

•提供场景化监测分析大屏
•实现跨境安全态势一屏总览
•一键关联全维度溯源，支持定制自动化报告，助力运维分析，提升响应效率。

05 自动化联动处置与阻断

•内置编排、自动发送跨境监测告警
•支持“发现恶意外联自动阻断IP”等响应动作。
•**设备联动**：无缝对接路由设备协同响应，对跨境流量的阻断。
•**灵活配置**：支持用户自定义和修改自动化响应流程。

06 主动预警与合规风险管控

•**资产梳理**：自动发现企业内涉及跨境的数据资产。
•**风险评估**：按法规要求，自动化评估数据出境风险。
•**持续监控**：7x24小时监控并实时告警违规行为。
•**合规报告**：自动生成符合监管要求的审计与合规证明。

跨境监测模型

01
VPN流量监测模型

- **核心技术**：基于机器学习的加密流量指纹识别，无需解密即可精准识别。
- **模型优势**：采用随机森林模型，F1分数高达99%，精准捕捉VPN特有传输模式。
- **核心价值**：高准确率、强隐蔽性、抗混淆性，实现对加密流量的无死角覆盖。

02
VPN应用识别模型

- **精准识别**：覆盖Clash、V2Ray、Trojan、Shadowsocks等主流客户端与协议。
- **技术融合**：结合TLS指纹识别与行为建模引擎，快速识别新型变种协议。
- **核心价值**：实现从“是什么”到“用什么”的穿透，为差异化安全策略提供依据。

03
境外IP监测模型

- **动态评分**：超越简单的地理位置查询，构建包含威胁情报的动态风险评分体系。
- **情报支撑**：内置持续更新的威胁情报库，精准标记高风险境外节点。
- **核心价值**：实现从被动响应到主动预警的转变，赋能跨境行为智能决策。

跨境监测趋势图

跨境监测

节点

模型
全部

2026-04-26 16:14:41

2026-04-28 16:14:41

查询

跨境检测趋势图

跨境检测识别能力-基于DPI的协议和应用识别

跨境监测方案，通过对海量VPN应用与协议样本的深度分析，构建了精准的多维度特征识别模型。结合持续更新的威胁情报库，该方案能够对互联网出口双向流量进行实时深度检测，精准识别并溯源**小火箭（Shadowrocket）、V2rayN、Clash**等主流VPN客户端，以及**Vmess、Vless、Trojan、SS**等多种加密通信协议，为网络安全与合规提供坚实保障。

小火箭 (Shadowrocket)

iOS 平台主流代理工具

支持多种协议配置

V2rayN

Windows 端功能强大的代理客户端

支持丰富协议

Clash

基于规则的多协议代理工具

广泛适配各类操作系统

跨境检测识别能力-多维智能识别体系

01 VPN流量特征与跨境威胁联动

根据**四元组信息、最大包长度、最小包长度、包首字节等统计特征**，利用上下报文的关联属性，构造多角度统计特征模型算法，并持续更行跨境威胁情报，形成跨境VPN流量特征库和跨境威胁情报库，实现隐蔽VPN的精准识别。

02 敏感网站识别：语义与特征的精准分类

- **多维识别技术**：综合运用URL特征分析、网页内容语义分析及深度学习文本分类模型。
- **指纹与更新**：建立内容指纹有效识别域名变更网站，每日更新并精细化分类数据库。

场景化跨境监测分析能力

跨境监测工作台：洞察流量，高效运维

一站式仪表盘

集中展示VPN流量、VPN应用、跨境IP等核心数据，比例构成一目了然。

多维下钻分析

支持源IP、目的IP、域名多维度统计，点击即可深入细节，挖掘数据价值。

快速态势感知

帮助您迅速掌握全网跨境行为，洞悉业务动态，及时捕捉潜在风险。

敏捷问题排查

完美适配现网演进，支持分场景快速定位与解决问题，大幅提升运维效率。

场景化跨境监测分析能力

“**跨境监测场景视图**”，跨境分析专属工作台，统计用户的源IP地址、目的IP地址、应用协议、伪装域名等关键信息，可逐级下钻每个跨境用户的详细会话信息，进一步调查溯源

源IP地址：172.20.250.91 会话详情

列筛选 导出Excel 打印

序号	节点	用户账号	用户地址	目标地址	NAT地址	协议	应用协议	HOST	归属地	运营商	上/下行包数	时延app/c/s	会话开始时间	会话结束时间
1	同迅科技		172.20.250.91:60014	4.4.4.4:6789	0.0.0.0:0	UDP	UDP垃圾包		美国	未知	3647 / 777	0ms / 0ms /0.11ms	2026-04-28 20:38:26	2026-04-29 11:33:58
2	同迅科技		172.20.250.91:60014	3.3.3.3:6789	0.0.0.0:0	UDP	UDP垃圾包		美国	未知	3581 / 777	0ms / 0ms /0.16ms	2026-04-28 20:38:26	2026-04-29 11:34:28
3	同迅科技		172.20.250.91:60018	4.4.4.4:6789	0.0.0.0:0	UDP	UDP垃圾包		美国	未知	444 / 77	0ms / 0ms /0.03ms	2026-04-29 09:36:58	2026-04-29 11:34:46
4	同迅科技		172.20.250.91:60018	3.3.3.3:6789	0.0.0.0:0	UDP	UDP垃圾包		美国	未知	427 / 77	0ms / 0ms /0.03ms	2026-04-29 09:37:34	2026-04-29 11:35:00
5	同迅科技		172.20.250.91:2307	4.145.79.80:443	10.64.250.2:2307	TCP	SharePoint/OneDrive	client.wns.windows.com	美国	未知	52 / 47	3.38ms / 2.80ms /67.37ms	2026-04-29 09:42:22	2026-04-29 11:29:52
6	同迅科技		172.20.250.91:60018	2.2.2.2:6789	10.64.250.2:60018	UDP	Unknown		瑞典	未知	77 / 0	0ms / 0ms /0ms	2026-04-29 10:08:14	2026-04-29 11:34:42
7	同迅科技		172.20.250.91:60004	1.1.1.111:6789	211.142.218.74:60004	UDP	UDP垃圾包		澳大利亚	未知	77 / 0	0ms / 0ms /0ms	2026-04-29 10:08:14	2026-04-29 11:35:26
8	同迅科技		172.20.250.91:60004	2.2.2.2:6789	10.64.250.2:60004	UDP	Unknown		瑞典	未知	77 / 0	0ms / 0ms /0ms	2026-04-29 10:08:14	2026-04-29 11:35:26
9	同迅科技		172.20.250.91:60004	5.5.5.5:6789	10.64.250.2:60004	UDP	UDP垃圾包		德国	未知	77 / 0	0ms / 0ms /0ms	2026-04-29 10:08:14	2026-04-29 11:35:28
10	同迅科技		172.20.250.91:60018	5.5.5.5:6789	10.64.250.2:60018	UDP	UDP垃圾包		德国	未知	77 / 0	0ms / 0ms /0ms	2026-04-29 10:08:16	2026-04-29 11:34:44
11	同迅科技		172.20.250.91:60018	1.1.1.111:6789	211.142.218.74:60018	UDP	UDP垃圾包		澳大利亚	未知	77 / 0	0ms / 0ms /0ms	2026-04-29 10:08:16	2026-04-29 11:34:44
12	同迅科技		172.20.250.91:60014	2.2.2.2:6789	10.64.250.2:60014	UDP	Unknown		瑞典	未知	71 / 0	0ms / 0ms /0ms	2026-04-29 10:08:58	2026-04-29 11:34:00
13	同迅科技		172.20.250.91:60014	5.5.5.5:6789	10.64.250.2:60014	UDP	UDP垃圾包		德国	未知	71 / 0	0ms / 0ms /0ms	2026-04-29 10:09:00	2026-04-29 11:33:56
14	同迅科技		172.20.250.91:60014	1.1.1.111:6789	211.142.218.74:60014	UDP	UDP垃圾包		澳大利亚	未知	71 / 0	0ms / 0ms /0ms	2026-04-29 10:09:02	2026-04-29 11:33:58
15	同迅科技		172.20.250.91:10779	17.57.145.25:5223	10.64.250.2:10779	TCP	Unknown		中国台湾	未知	94 / 68	0ms / 7.11ms /86.21ms	2026-04-29 11:00:10	2026-04-29 11:17:34

跨境会话溯源及取证能力

全链路精细溯源，**报文级**深度取证，为客户运维提供全面的技术服务

序号	节点	用户账号	用户地址	目标地址	NAT地址	协议	应用协议	HOST	归属地	运营商	上/下行包数	时延app
1	镜像流量		111.45.25.137:8443	172.20.254.22:57454	0.0.0.0:0	TCP	Unknown		内网地址	未知	34 / 40	0ms / 0r
2	镜像流量		43.139.73.88:80	172.20.255.37:19814	0.0.0.0:0	TCP	HTTP/超文本传输协议	open.zhuzher.com	内网地址	未知	40 / 46	0ms / 0r
3	镜像流量		172.20.247.92:52162	183.214.183.149:19883	0.0.0.0:0	TCP	Unknown		中国湖南省长沙市	未知	46 / 45	0ms / 0r
4	镜像流量		172.20.247.92:36429	183.214.183.149:19883	0.0.0.0:0	TCP	Unknown		中国湖南省长沙市	未知	30 / 34	0ms / 0r
5	镜像流量		142.251.46.74:443	172.20.254.90:62568	0.0.0.0:0	TCP	Unknown		内网地址	未知	33 / 47	0ms / 0r
6	镜像流量		172.20.253.10:1883	172.20.254.67:7			Unknown		内网地址	未知	40 / 39	0ms / 0r
7	镜像流量		172.20.247.92:44445	183.214.183.149:19883	0.0.0.0:0	TCP	MQTT/MQTT物联网消息协议		中国湖南省长沙市	未知	41 / 64	0ms / 0r
8	镜像流量		172.20.249.40:50364	223.109.215.124:80	0.0.0.0:0	TCP	Unknown		中国江苏省南京市	移动运营商	38 / 50	0ms / 0r
9	镜像流量		172.20.247.92:51087	183.214.183.149:19883	0.0.0.0:0	TCP	Unknown		中国湖南省长沙市	未知	28 / 38	0ms / 0r

会话日志

2	镜像流量	172.20.255.37:37110	203.195.195.174:80	TCP		0.0.0.0:0	54:89:98:f5:a3:b7	中国广东省广州市	未知	Unknown	OFFLINE	0 / 0 /30	0
3	镜像流量	103.167.60.188:56887	172.20.249.190:6444	TCP		0.0.0.0:0	54:89:98:f5:a3:b7	内网地址	未知	Unknown	ONLINE	0 / 0 /0	0
4	镜像流量	103.167.60.188:56887	172.20.249.190:6444	TCP		0.0.0.0:0	54:89:98:f5:a3:b7	内网地址	未知	Unknown	OFFLINE	0 / 0 /30	0
5	镜像流量	172.20.254.22:57278	194.146.86.250:443	TCP		0.0.0.0:0	e4:3a:a3:c6:0f:f7	中国香港	未知	Unknown	ONLINE	0 / 0 /0	0
6	镜像流量	172.20.254.22:57278	194.146.86.250:443	TCP		0.0.0.0:0	e4:3a:a3:c6:0f:f7	中国香港	未知	Unknown	OFFLINE	0 / 0 /24	0
7	镜像流量	43.139.73.88:80	172.20.255.37:19814	TCP	open.zhuzher.com	0.0.0.0:0	54:89:98:f5:a3:b7	内网地址	未知	HTTP/超文本传输协议	ONLINE	0 / 0 /0	0
8	镜像流量	116.205.40.114:443	172.20.254.22:57297	TCP		0.0.0.0:0	e4:3a:a3:c6:0f:f7	内网地址	未知	Unknown	ONLINE	0 / 0 /0	0 / 0

全流量日志记录

对所有流量进行无抽样、无过滤的完整记录，防篡改

保存完整历史流量

提供大容量、高可靠的海量存储架构

精细化逐级溯源

从网络边界到应用内部，实现“从IP到行为”的精准画像

满足相关部门法规要求

符合网络安全法及等保要求，提供开箱即用的合规保障。

跨境会话溯源及取证能力

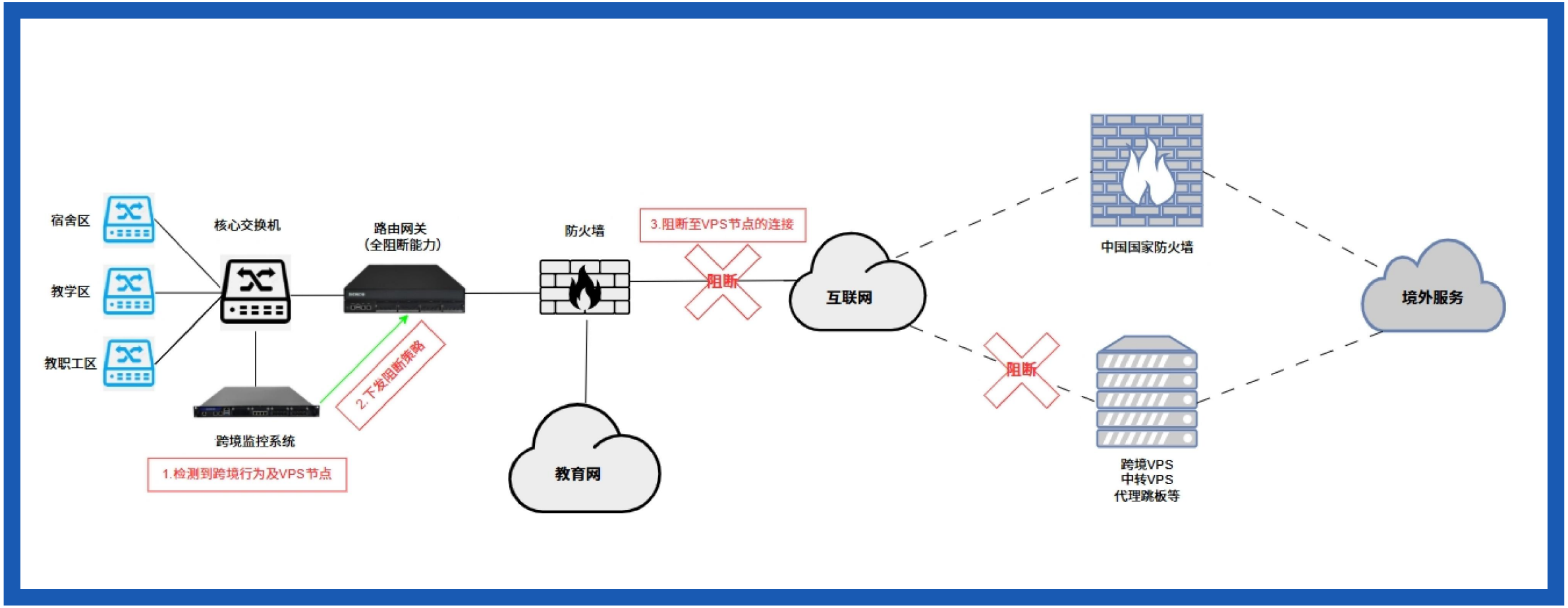
全流量1:1记录行为日志及对应行为数据包，并基于用户账号，将IP、行为精准关联至具体个人。由此明确“什么人、什么时间、做了什么”，让责任划分有据可依，确保全程可溯，全面满足安全合规要求。

跨境实时告警-微信、邮箱等实时告警通知

支持配置跨境行为触发告警，可对接企业微信、钉钉、邮箱等方式实时通知网络运维人员

联动阻断跨境流量

路由可以针对检测出的跨境节点或跨境用户，一键下发阻断策略，完成对跨境流量的阻断，减少被通报风险



联动阻断跨境流量

策略化自动阻断、限流与隔离，无缝联动防火墙、IDS、SOC等现有安全设施，实现威胁阻断率**≥99%**。支持链路故障时自动切换至备用线路，对违规流量进行毫秒级自动阻断，全方位保障业务连续性。

联动阻断跨境流量

自动化响应

基于预设的安全策略，对潜在风险自动执行精准的阻断、限流或隔离操作，无需人工干预。

跨设备联动

打破安全孤岛，与企业现有的防火墙、SOC及各类检测设备无缝集成，形成全域防御合力。

业务连续性保障

当网络链路出现故障或遭遇大规模攻击时，自动切换至备用链路，确保核心业务稳定运行。

应用场景

高校学术访问

•保障国际学术交流
• 规范境外学术资源访问
• 兼顾安全与科研合规

金融风控

实时监控跨境资金流动，识别异常交易模式，防范金融欺诈和洗钱风险。通过全局数据视图，满足反洗钱（AML）和合规审计要求。

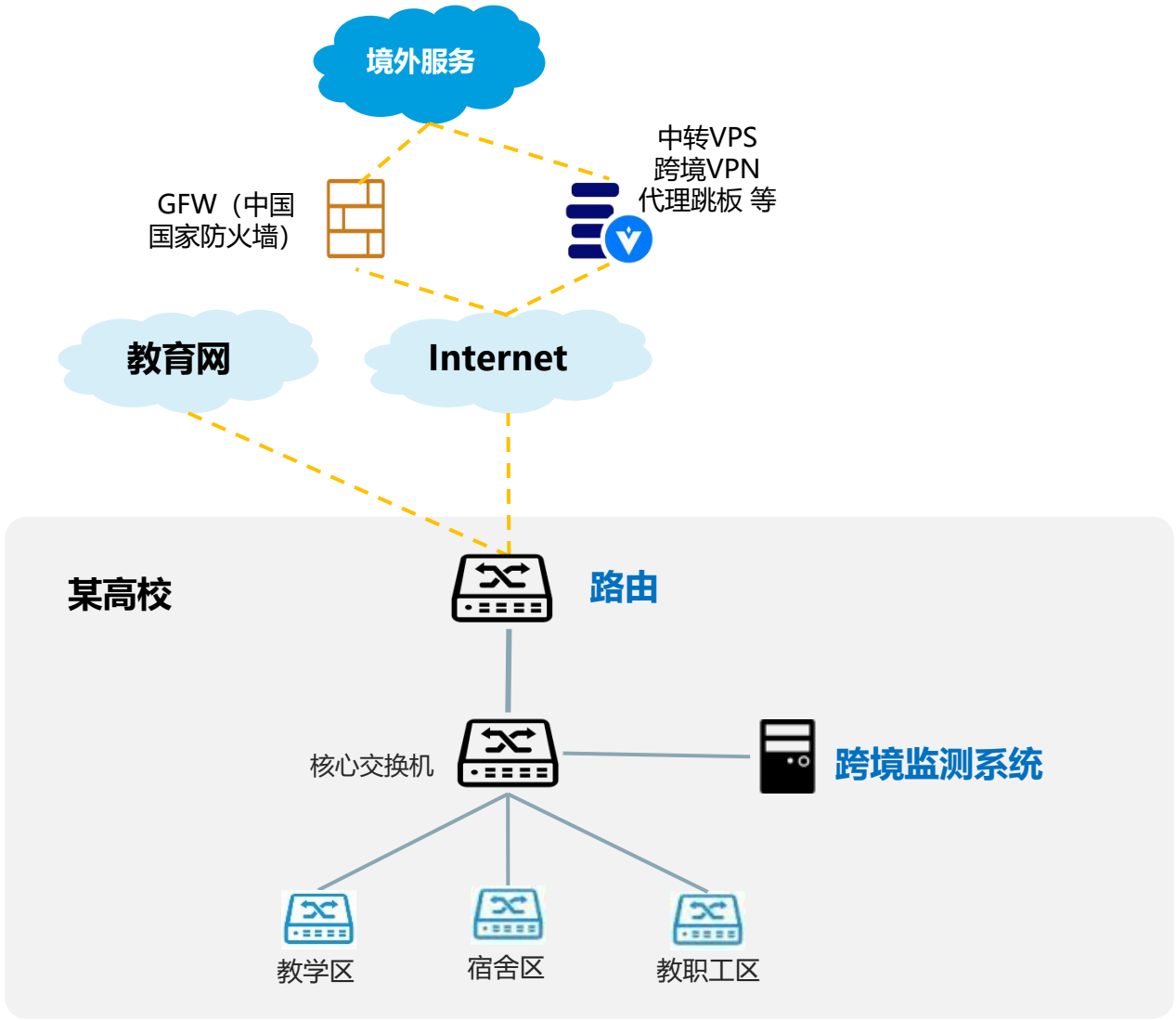
电商运营

分析全球用户行为和销售数据，优化营销策略和供应链管理。实时监控网站性能和支付链路，提升用户体验和转化率。

跨国协作

保障跨国团队的安全通信和数据共享。监控员工的跨境访问行为，防止敏感信息泄露，确保远程办公的安全性和合规性。

监测溯源方案



■ 方案说明

在路由器旁路部署跨境监测系统采集镜像流量，通过跨境分析模型对流量中的跨境流量进行识别与解析，并全量留存相关会话日志和原始报文，以便于溯源分析。

■ 方案组成

① 跨境监测系统

② 路由系统

■ 方案能力

① 进行场景化跨境监测分析

② 对跨境行为进行溯源取证

方案亮点及优势

01 超大流量处理能力

•**核心能力**：支持100Gbps全流量深度分析，从容应对海量数据洪流。

•**价值**：保障业务连续性，实现100%流量可见性，保护客户投资。

02 DPI深度识别

•**核心能力**：内置1300余种应用特征库。

•**价值**：精细化应用管控，精准威胁检测，满足合规审计要求。

03 支持联动阻断

•**核心能力**：从“发现威胁”到“自动阻断”的秒级闭环响应。

•**价值**：提升威胁响应效率，减轻运维压力，构建主动防御体系。

04 自动报表与告警

•**能力**：提供多维度报表和实时告警，告警对接企业微信、钉钉、邮箱等方式实时通知运维人员迅速处置。

•**价值**：实现智能化的运维与决策支持，主动风险预警，数据驱动业务决策。

05 跨境IP库每日更新

•**能力**：多源数据融合与清洗，每日自动更新全球IP库，精准识别动态边界。

•**价值**：确保合规保障，具备高抗规避能力，精准识别各类网络行为。

从“看见”到“预见”

看见

打破信息壁垒，实时掌握全球业务的每一个细节，让业务运行状态一目了然。

洞见

深入挖掘海量监测数据价值，从复杂的信息中发现潜在的商业规律与增长机会。

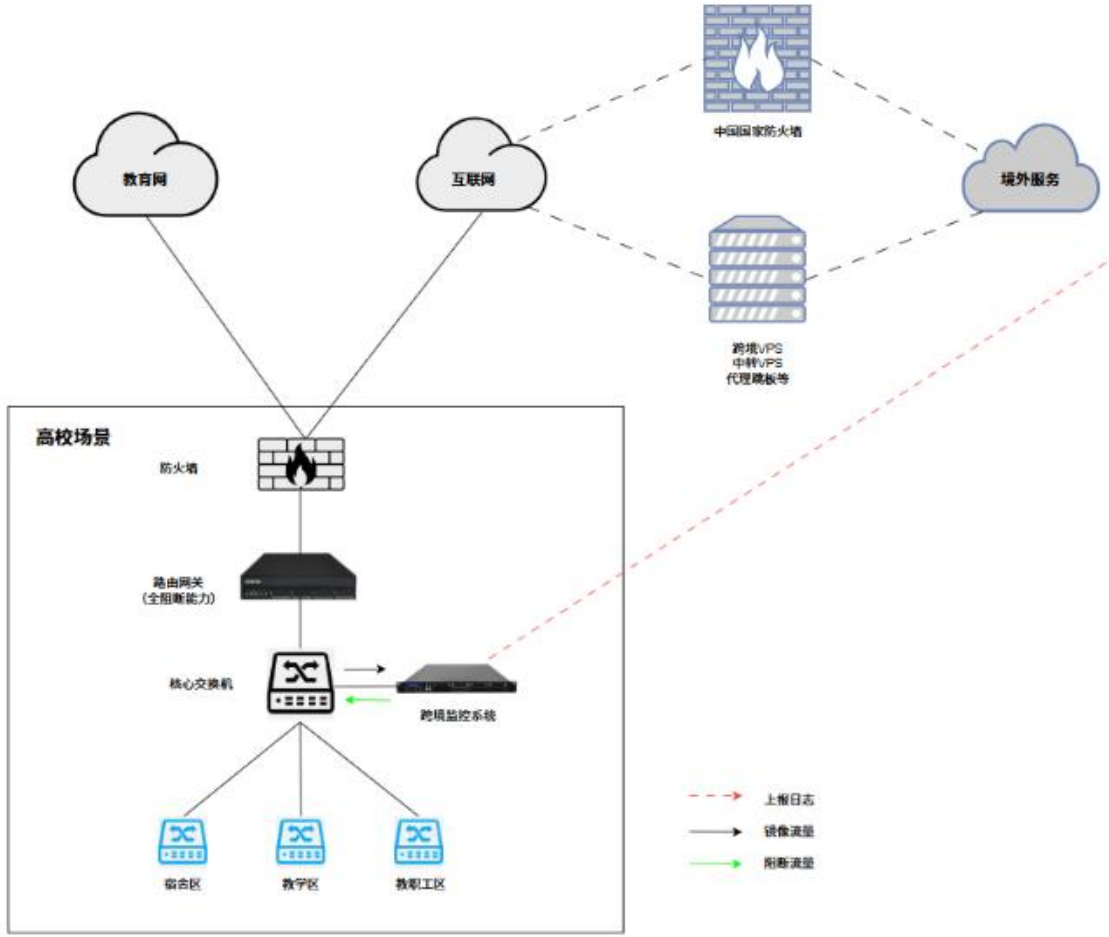
预见

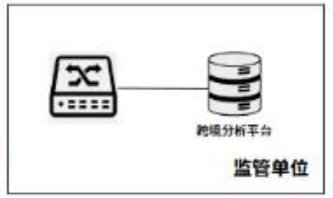
基于强大的数据模型科学预测风险，提前战略布局，从容应对挑战，引领行业未来。

“不仅仅是一个监测工具，更是一个战略决策平台”

— 更 智 能 、 更 安 全 、 更 高 效 —

某高校-跨境检测溯源+阻断部署实施方案





解决方案

- 跨境监测系统旁路部署在学校核心，进行跨境监测
- 跨境监测系统系统接收会话日志和认证日志并进行关联处理后，按照要求格式上报给监管单位。
- 路由提供阻断能力

价值

- 完成对校内跨境行为的监测和溯源（根据关联的认证日志，落实到人）
- 上报日志满足分中心对高校的跨境检测合规要求
- 对检测出的跨境行为及时阻断，减少被通报风险

谢　谢　！