创网智能流量镜像
医疗解决方案与用户案例

TRONET

方案概述

当前信息安全系统已成为医院各部门业务开展的必备工具，但传统流量镜像方式存在端口有限、配置有限、性能受损、功能单一等诸多限制，无法满足医院信息化安全建设的趋势，创网智能流量镜像系统汇聚全网镜像流量，将各设备以旁挂的方式接入，在统一平台中实现更为高效的精细化管理。

需求背景

随着近年国家监管层对于安全的持续重视，在网络安全法施行以后，医院由于其信息数据的敏感性，其作为关键信息基础设施必须按照“网络安全等级保护制度“进行合规建设。传统流量镜像存在诸多问题。

集中管理问题

安全设备多次部署后，流量数据采集、报文捕获变得零乱不堪，位置、来源、数据内容不清楚，无法集中管理

精细控制问题

不同安全审计设备对网络流量存在不同颗粒度要求，需要实现流量精准分配，避免全流量采集带来的粗放低效

泄密风险问题

流量数据无管控全量汇聚复制分流，敏感数据信息在多个分析工具存在数据拷贝，数据泄密风险很高

多院区之间流量调度问题

医院多个院区，如何将多院区流量分布式采集、集中汇聚、统一分析，成为一大挑战

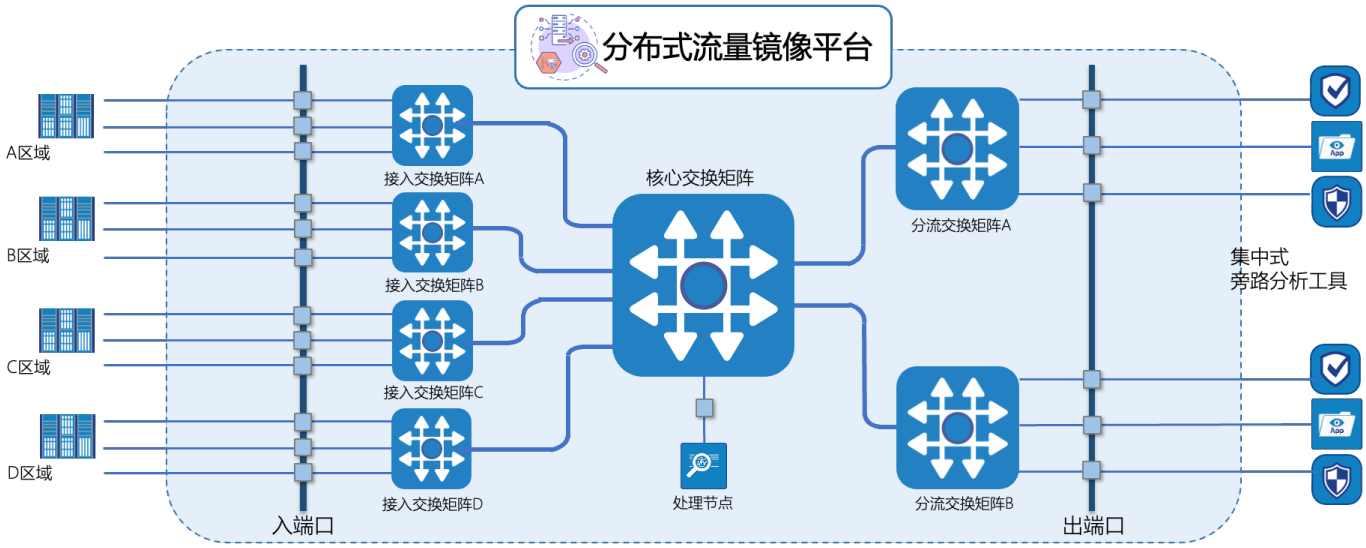
解决方案

创网智能流量镜像解决方案，将智能流量镜像系统部署于端口镜像或分光器与监测设备之间，汇聚全网镜像流量，分析设备以旁挂方式接入智能流量镜像系统，作为旁路监测设备的统一流量调度平台。

镜像流量统一规划，按需精准转发，旁路设备无限延展。让流量采集和分发告别复杂的操作、捉襟见肘的资源限制和功能制约，在统一平台中实现更为高效的精细化管理。

创网智能流量镜像系统还支持分布式结构部署，对多跨区域流量做统一调度，转发平台与调度平台解耦，可以跨地域、区域实现流量复制、汇聚、映射、负载均衡等功能，实现多地域、多区域的一体化采集和分发，消除跨广域网和多区域之间流量调度的诸多限制，在单一用户界面实现多区域流量调度的集中化管理。

利用报文截断技术，进一步降低流量大小，减轻分点机构出口带宽压力。支持多台同类型旁路设备负载均衡，智能流量策略，实现精准分流。将多个智能分流器部署多个接入数据中心及分流数据中心之间，作为旁路监测设备的统一流量调度平台，在统一平台中实现多个数据中心流量调度的精细化管理。



流量复制

支持“一对多”端口的流量复制。定义一个入口对应多个出口，将一个入口的流量同时复制给多个出口；

流量汇聚

支持“多到一”端口的流量汇聚。定义多个入口对应一个出口，将多个入口流量汇聚后发送给一个出口；

流量复制加汇聚

支持“多对多”端口的流量采集需求，定义多个入口对应多个出口，按需将流量先汇聚再复制；

负载均衡

支持“一对多”端口的负载均衡采集需求。实现入口大流量分拆为多个出口小流量，降低监控设备的负载；

流量映射

提供基于2至4层信息的流量映射，按需配置策略，将网络流量灵活分发到一个或多个监控设备，降低监控设备的资源负载；

分流可视化

提供丰富的可视化功能，包括分流器架构的逻辑拓扑、全局吞吐量、入口及出口的吞吐量、端口包速率等可视化报表。

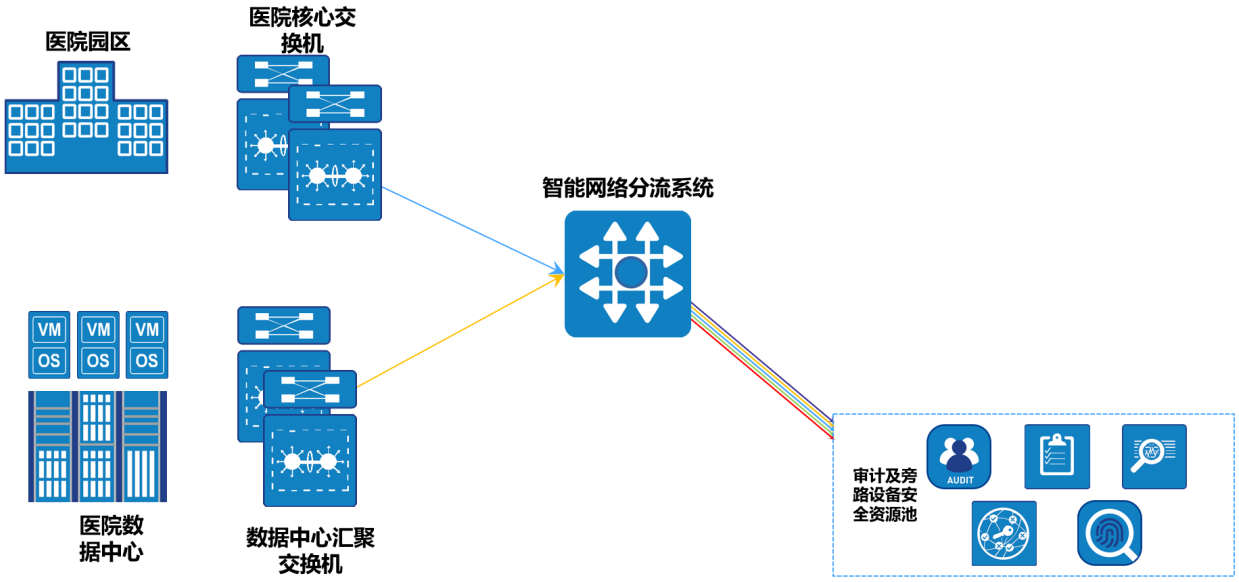
北京某三甲医院审计分流

背景与问题

北京某三甲医院由于其信息数据的敏感性，涉及大量安全设备，同时也会有各类针对医疗大数据的业务分析系统，不同的分析系统所需要的流量不同，设备负载也不同；另外核心交换机等类网络设备一般只能提供少量的镜像会话，一旦镜像会话超限，将会极大推高设备的负载，产生性能瓶颈。

解决方案

院方采用了创网NPB系列智能分流解决方案，部署于网络交换机与监控设备之间，将院方数据中心和院区内网的旁路镜像数据作了汇总集中，作为网络流量的一体化采集和分发平台，提供网络流量的报文复制、流量汇聚、流量映射、报文截断、负载均衡等功能，借助精准的流量映射技术，实现针对2-4层级别信息（Vlan ID、IP、TCP/UDP、网段等）的精确分流。



方案价值

平台化集中管理 全Web页面，告别复杂操作，降低难度，简化运维；

流量复制与汇聚 对流量报文进行复制及汇聚，实现流量的任意分发；

流量映射 基于2至4层信息，进行流量映射，按需分发，降低旁路设备性能负载；

流量负载分担 针对旁路设备性能不足问题，将流量报文拆分给多台旁路设备协同处理，可顺应流量带宽的发展便捷的横向扩展；

南京某三甲医院分布式分流

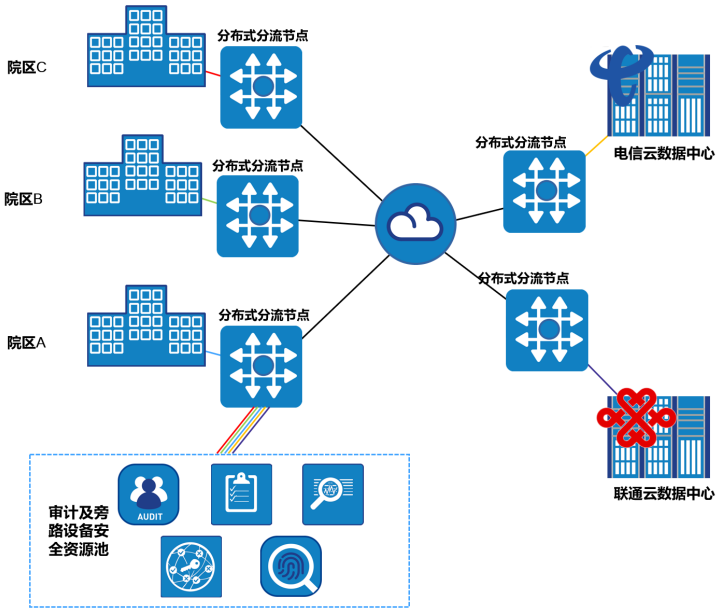
背景与问题

南京某三甲医院，3个院区分布在南京多个区域，多院区和数据中心均有专线或通道互联。院方在部署安全审计系统和业务分析系统时，需要从多个院区，多个数据中心抽调流量。从单一院区获取的旁路审计流量是很难展现去多院区的流量视图，需要能够将审计流量跨越院区进行集中处理，为院方提供更加全面的视角和着力点：

解决方案

院方采用了创网NPB系列分布式智能分流解决方案，部署情况如下：

- 三个院区，两个运营商数据中心机房；
- 审计类安全设备，安全态势感知均部署于医院本部；
- 分布式分流架构，每个院区和数据中心各部署一套分布式分流节点每个分布式分流节点均抓取本地镜像流量，并通过隧道统一集中到医院本部；
- 所有节点均在本地进行脱敏，过滤，去重，减轻隧道的压力；



方案价值

平台化集中管理 全Web页面，告别复杂操作，降低难度，简化运维；

流量复制与汇聚 对流量报文进行复制及汇聚，实现流量的任意分发；

流量映射 基于2至4层信息，进行流量映射，按需分发，降低旁路设备性能负载；

流量负载分担 针对旁路设备性能不足问题，将流量报文拆分给多台旁路设备协同处理，可顺应流量带宽的发展便捷的横向扩展；

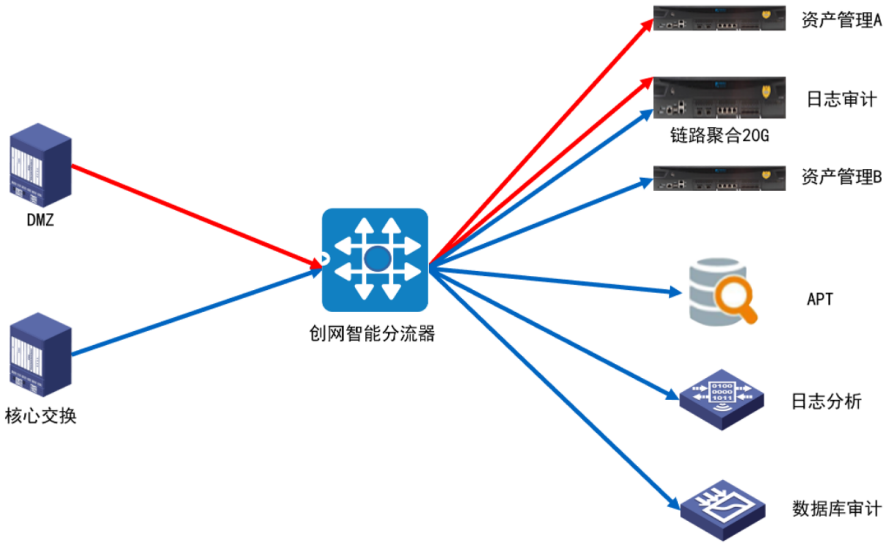
上海某医院审计分析分流

背景与问题

上海某三甲医院，是全国建立健全现代医院管理制度试点医院。为应对网络安全审计，院区网络中多处部署了流量分析系统、数据库审计等设备。但长久下来流量数据采集、报文捕获变得零乱不堪。网络的逐步扩容导致多类数据分析系统疲于处理无关背景数据，性能降低。另外各个系统需要的流量不同，设备负载能力也都不同。

解决方案

院方采用了创网NPB系列智能分流解决方案，旁路部署在核心交换机与监控设备之间，将院方院区内网和DMZ区的旁路镜像数据作了汇总集中，作为网络流量的一体化采集和分发平台，提供网络流量的报文复制、流量汇聚、流量映射、报文截断、负载均衡等功能，借助精准的流量映射技术，实现针对2-4层级别信息（Vlan ID、IP、TCP/UDP、网段等）的精确分流。



方案价值

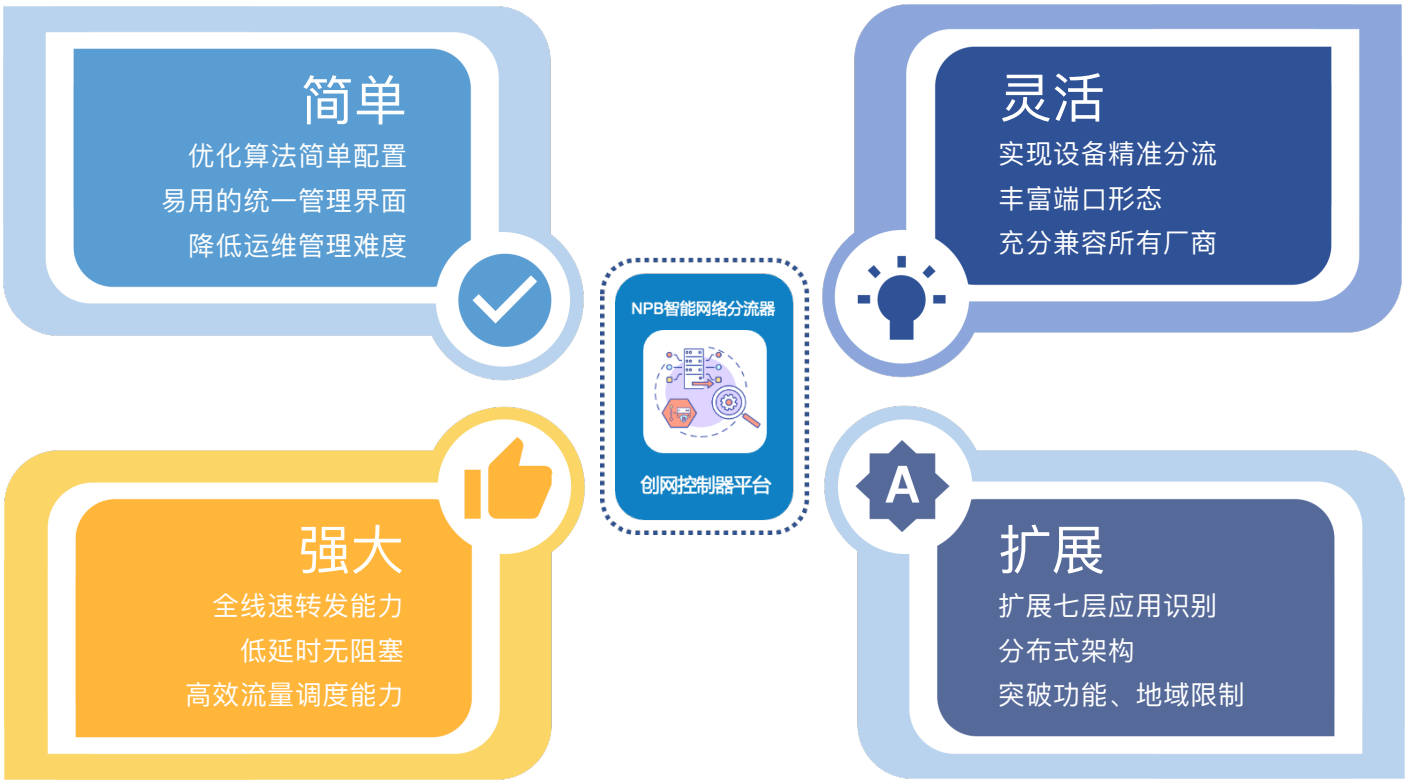
流量复制与汇聚 对流量报文进行复制及汇聚，实现流量的任意分发；

流量映射 基于2至4层信息，进行流量映射，按需分发，降低旁路设备性能负载；

流量负载分担 针对旁路设备性能不足问题，将流量报文拆分给多台旁路设备协同处理，可顺应流量带宽的发展便捷的横向扩展；

灵活扩容 端口丰富，扩展方便，线速转发，灵活调度;

产品价值



关于创网

南京创网网络技术有限公司成立于2013年，坐落于“创新名城·美丽古都”－南京，是国家高新技术企业。

自成立以来，南京创网网络技术有限公司坚持以专注的精神提供专业化服务，努力成为网络边界解决方案产品提供商的领导者。至今，创网的客户已涵盖医疗、教育、企业、金融、政府、电力等重要行业以及互联网服务提供商（ISP）。创网提供的智能服务链（流量编排）解决方案和智能流量镜像解决方案已成为众多业务领域不可或缺的信息技术基础架构并发挥日益重要的作用。

南京创网网络技术有限公司
地址：南京市雨花台区宁双路云密城L栋8层801
电话：4008055017
网址：www.tronet.com.cn
邮箱：admin@tronet.com.cn