流量探针技术在企业网络安全中的应用*

芦建文,乌 晨,丁 阳

(包头钢铁(集团)有限责任公司信息服务中心,内蒙古 包头 014010)

摘 要: 文章主要介绍流量探针技术原理以及在企业网络信息安全中的应用。阐述了流量探针技术在企业内的具体应用场景和发挥的作用。实际应用表明: 流量探针技术是保护网络安全稳定运行的重要工具之一。

关键词: 流量探针; 网络安全; 流量分析

中图分类号: TP393.08 **文献标识码**: B **文章编号**: 1009-5438(2021)04-0089-04

DOI:10.13647/j.cnki.btgkj.2021.04.023

Application of Flow Measuring Probe Technology in Enterprise Network Security

Lu Jian-wen, Wu Chen, Ding Yang

(*Information Service Center of Baotou Iron & Steel (Group) Co., Ltd., Baotou* 014010, *Inner Mongolia Autonomous Region, China*)

Abstract: In this paper, it is mainly introduced the principles of flow measuring probe technology and its applications in the information security of enterprise network as well as elaborated its specific application scenarios and functions in enterprises. The practical applications show that it is one of the important tools to ensure safe and stable operation of network.

Key words: flow measuring probe; network security; flow analysis

目前,各行各业均可见到网络的“身影”,在网络为工作带来便捷性的同时,网络中流量的数据、安全、业务、监控等连带性的问题也随之而来。如何保证网络使用通畅、出现问题及时预警、协助追查等工作是当今网络管理中的主要难题。包钢(集团)公司园区骨干网目前承载了丰富的数据业务,覆盖范围内有60余家二级单位的数据.主要包括ERP数据、协同办公平台数据、视频平台数据、因特网数据、集团公司云平台各业务系统的数据等。网络管理人员需要及时了解到网络中承载的业务,及时的掌握网络流量特征,使网络带宽配置最优化,这就需要及时洞察网络运行状况,及时了解网内应用情况,以解决网络性能问题,保障主要业务数据的正常传输。因此需要一种解决方案能够帮助网络管理人员了解详细的网络使用情形,解决网络、应用、用户使用网络的可视化问题。流量探针技术则可以帮助网络管理人员了解企业内部网络运行状况,了解各应用占用的网络带宽,各业务消耗的网络资源,帮助网络管理人员在网络规划、网络优化、故障诊断等方面做出及时、准确的决策。

1 流量探针原理

随着互联网的快速发展,越来越多研究机构开始致力于研究开发对网络流量实施监测和测量的技术。NIMI(National Internet Measurement Infrastructure)是由美国国家科学基金发起、美国国防部高级

* **收稿日期**: 2021-04-13

作者简介: 芦建文(1969-),男,山西省忻州市人,硕士,高级工程师,现从事计算机与自动化工作。

中国知网 https://www.cnki.net

计划局资助的一个研究项目，提出了一个分布式可扩展的(Scalable)动态的(Dynamic)网络测试基础构架。NIMI采用层次体系建构与主动测量技术，通过在网络中不同的测量点部署大量的测量探针(Probe)来实现对网络动态行为的测量。在国内，对网络测量的研究已经开始。清华大学提出了大规模互联网性能监控模型LIPM(Large scale Internet Performance Monitor model)，借鉴了ISO模型的层次结构思想，将整个模型分为数据采集、数据管理、数据分析、数据表示4个层次，易于实现和维护。

原始的网络流量以二进制方式呈现，无法直接读取和应用，因此需要通过工具和技术，把网络流量变成更加容易读取的数据信息，在这个过程中要对采集到的网络流量进行解码和分析，包括识别流量中的协议、业务、提取流量中的原始文件等。数据包解析还原的过程，就是对二进制比特流中各个位置的字段进行提取和解析重组的过程[1]。

提取和解析重组使用了多种技术，例如端口匹配、流量特征检测、自动连接关联和行为特征分析等。为了便于收集更全面的上下行流量数据，研究人员将流量探针主要部署在网络边界流量进出最大的位置、关键业务服务器区前端、核心交换机区等。利用端口流量镜像技术，把流量口的数据1:1全镜像复制1份出来接入流量探针，几乎不会对真实的网络环境造成影响，能让流量探针有充足的性能去分析和接收流量数据包。端口镜像(Spanning)的流量数据包包括数据链路层、网络层、传输层、会话层、应用层等各层会话信息，流量探针附带应用协议分析模块，把数据包解拆后得到数据包的头部信息，对其归属分类分析。流量探针内置威胁检测进程、IDS入侵检测库、Web应用防御库等，可识别现知的广泛应用层威胁，包括木马、Webshell、恶意广告、挖矿工具等，对疑似威胁打上标签产生告警；同时传感器还能对APT持续性攻击事件进行跟踪分析，并再次把分析数据加密传输给大数据分析平台汇总作进一步的关联性分析[2]，见图1。

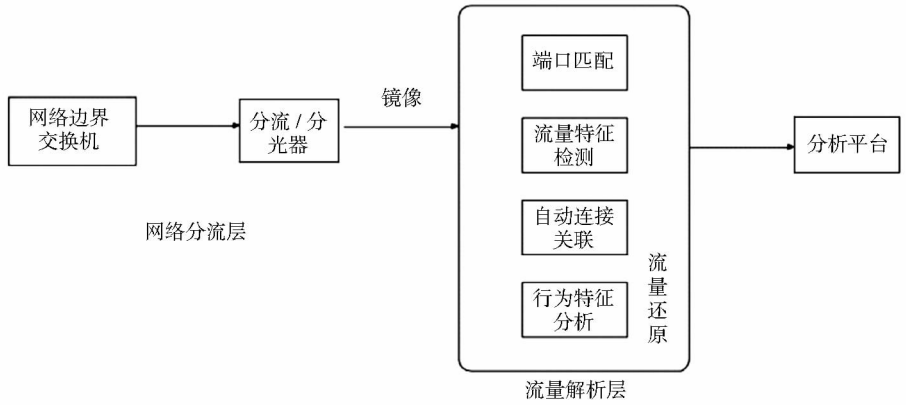


图1 流量还原流程

2 流量探针优势

(1)丰富的应用识别：流量探针技术是基于三层协议号、端口号，可识别例如Notes应用、FTP应用、HTTP应用等几百种已知应用。

(2)可提供各类实用组合报表：通过简易图形界面。提供从用户主观分析角度的分析内容，并整合为组合报表，使用户更快速的得到所需要的分析结果。

(3)实时流量监控：流量探针支持对流量进行实时的分析，当网络流量日志产生之后，在很短的时间内即可得到分析结果，方便使用报表进行网络异常问题的定位。

(4)通用性强：可以与不同层次网络安全设备配合，对广域网核心层、广域网出口、局域网核心层、局域网汇聚层流量的监控与分析，实现整网流量多点的可视化。

(5)成本低：基于现有的网络安全设备，通过增加板卡的方式，或者开启端口镜像功能，在不改变网络拓扑的情况下就能在所需要的各处网络节点上布放流量探针。

中国知网 https://www.cnki.net

3　流量探针硬件配置

该系统部署在普通 x86 架构服务器上，有良好的通用性与扩展性，支持网络最大流量吞吐可达到 40 Gbps，全天持续运行，实时接收、上报、分析不同信息和数据。服务器可内置多网卡，采用一个快速以太网接口用作管理口，一个 10 G 光口接入镜像交换机直接获取镜像流量，操作系统采用 LINUX centos7.6版本，稳定高效。系统具体硬件配置清单见表 1。

表 1　硬件配置表

设备	配置
CPU	1×4110(2.1 GHz、8 核、11 MB、85 W)
内存	32 G，共 24 个插槽，可扩展
硬盘	1 T 3.5 寸硬盘，可扩展至 7 T
RAID 卡	板载 RAID 卡，支持 RAID 0、1、5、10
接口	1 个 mLOM 4×GE 电口，2 个 2×10 G 光口
USB	3 个 USB3.0 接口
电源	2×550 W 冗余电源

4　流量探针的实际应用

利用流量探针的应用协议解析功能，能准确识别公司内网上全时段运行的应用，洞悉整个网络的运行情况，而且可针对具体需求做用户行为的准确管控，这在一定程度上既可保证业务流的高效运行也可预防由于内网机器受到攻击而生产的威胁，同时识别应用类型也是应用审计与应用流量控制的基础。通过一段时间业务流量抓取，发现集团公司内外部网络流量峰值规律如下：早上 7:30 后，内外部网络流量逐渐增大，公司视频早调会视频流量在 7:40左右达到一个高峰，几乎占据整个早间时段带宽。对全天内网业务系统分析，我们发现 ERP 系统与生产环保相关的业务系统 24 h 都呈现一个平稳的访问水平，早 8:30 至下午 6:30，公司协同办公数据流量与外网带宽使用保持在一个相对较高的水平，夜间外网流量急剧减少，内网流量平稳下降，符合钢铁行业全流程连续的生产特点。

根据网络流量按照业务类型分析，研究人员发现公司内网用户每天早 7:00 至早 11:00 在集团公司信息资源访问平台业务流量最大，总字节数达到了 483.09 GB。其次是对公司协同管理平台手机端的访问，这一时段总字节数达到了 301 GB。而 ERP 数据库在这一时段流量的进出也达到了近300 GB。针对这样的访问特点，网络管理人员配合各系统管理人员对重要的访问量大的业务系统进行了针对性的优化和调整。

5　流量探针应用效果

通过近一段时间对流量探针的系统报表分析，了解到公司网络流量的分布情况、网络流量的历史发展趋势、网络应用的流量分布以及网络流量的异常信息等。帮助网络管理人员进行了网络的合理规划，调整了网络带宽分布，保障了关键业务数据的传输，并及时发现了包钢(集团) 公司内网部分用户感染永恒之蓝病毒信息，及时采取措施，锁定被感染计算机的 IP，第一时间进行了处理，最大限度挽回了损失。实现了“数据可视、行为可分、威胁可知、动作可记”的目标。

2020 年内蒙古自治区东西部网络攻防演练中，包钢(集团) 公司作为防守方通过流量探针及时完整的发现了进攻方通过集团公网 IP 地址攻击的痕迹和线路。攻防演练前，作为防守方首先调整流量探针监控策略，将其部署在集团公司互联网出口侧以及公司 DMZ 区汇聚交换机一侧，实时监控互联网进出流量。在演练开始的第三天，开始发现有数个源自阿里云的 IP 地址开始对上报参与演练的电子采购系统进行大量的 port－scan 扫描，流量探针及时的发送威胁警报，通知防守方将进攻方 IP 地址加入黑名单进行封堵，第一时间将恶意攻击挡在业务系统之外，并向自治区攻防演练指挥部汇报，夜间指挥部确认拦截准确。事实证明，在以往没有流量探针的情况下，往往攻击方都已经入侵到业务系统时才能发现，启用流量探针后，基本可以做到对网络进攻的及时发现。

6　结束语

随着未来包钢(集团) 公司 IDC 中心、工业互联网、云平台的建设，依托在信息化基础设施上的数据流量的安全越来越重要。流量探针这种可靠、便利的技术方案，可以帮助网络管理人员了解企业内部网络运行状况，了解各种类型网络流量占用的比重，帮助网络管理人员在网络规划、网络优化、故障诊断等方面做出更加准确的判断。为实现更好的企业网络信息安全，通过更高等级保护信息安全标准打下

中国知网　https://www.cnki.net

坚实基础。

参 考 文 献

[1] 孙瑜. 网络流量探针的关键技术探析[J]. 信息记录材料,2020,21(11):153-154.

[2] 张祖茂. 基于网络探针的电力综合数据网监测方案的研究[J]. 中国新通信,2017,19(8):107-108.

中文名称	英文	含义
厘		“市厘”的异名。
里		“市里”的异名。
哩		“英里”的异名。
立方码	cubic yard; yd^3	体积的英制单位,为0.764 555立方米。
立方英尺	cubic foot; ft^3	体积的英制单位,为28.316 9立方米。
立方英尺每磅	cubic foot per pound; ft^3/lb	质量体积的英制单位,为0.062 428立方米每千克。
立方英寸	cubic inch; in^3	体积的英制单位,为16.387 1立方厘米。
两		“市两”的异名。
流每平方英尺		“流明每平方英尺”的异名。
流明每平方英尺	lumen per square foot; lm/ft^2	光照度的英制单位,为10.764勒克斯。
卢瑟福	futherford; Rd	放射性活度的旧单位,为1 000 000贝可勒尔。
马力		“米制马力”的异名。
码	yard; yd	长度的英制单位,为0.914 4米。
米制克拉	metric carat	质量的非国际单位制计量单位,为200毫克。
米制马力	metric horsepower	功率的工程单位制单位,为753.499瓦特。
密耳		“密位”“毫英寸”的异名。
密位	mil	平面角的非国际单位制计量单位,为圆周的1/6 400(英美)或1/6 000(俄)。

中国知网 https://www.cnki.net