流量管理系统（FlowShaper）

技术白皮书

Version 3.0

关键词：流量分析、流量控制

摘要：本文重点介绍东华流量系统针对网络应用提出的 Flowshaper 系统的技术特点及功能。

术语：

术语	英文全名	中文解释
ASIC	Application Specific Integrated Circuit	专用集成电路
DPI	Deep Packet Inspection	深度数据包检验技术
DFI	Deep Flow Inspection	深度数据流检验技术
QoS	Quality of service	服务质量
Bypass	Bypass	旁路单元

目 录

前言

随着信息技术和互联网的深入发展，互联网已成为人们工作、学习和生活的一部分。在享受互联网带来巨大经济效益的时候，网络安全及带宽瓶颈等问题已日益凸显：管理员面对非透明网络，缺乏有效的分析手段，许多与工作无关的应用占用大量的带宽资源，致使信息传输滞留；用户终端上网行为无从得知，网络安全无法得到有效保障；流量认知模糊，无法定期呈现有效网络运维数据。

应对种种问题，东华软件股份公司推出了智能业务监控系统 FlowShaper，采用先进的特征识别技术，实时高效检测网络出口链路的各种业务和应用，拥有出色的网络协议和 URL 识别技术，提供精确智能的带宽管理能力和安全可靠的上网行为管理功能，采用丰富的数据展现以及便捷的操作界面，最大化的实现网络可视化管理，提高用户关键业务应用的响应时间，加强网络行为科学化管理，有效满足用户的网络应用和安全需求。

1. FlowShaper 产品概述

1.1 设计依据于执行标准

- IEEE 802.3 “Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications”，2002
- RFC 894 “A Standard for the Transmission of IP Datagrams over Ethernet Networks”，1984
- RFC 1662 “PPP in HDLC-like Framing”，1994
- RFC 2615，“Point to Point Protocol (PPP) over SONET/SDH Specification”，1994
- ITU-T G.707 “Network node interface for the synchronous digital hierarchy (SDH)”，1996
- ITU-T G.783 “Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks”，1997
- ITU-T G.813 “Timing characteristics of SDH equipment slace clocks (SEC)”，1996

- ITU-T G.823 “The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy”，1993
- ITU-T G.825 “The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)”，2000
- ITU-T G.957 “Optical interfaces for equipments and systems relating to the synchronous digital hierarchy”，1999
- ITU-T Q.922 “ISDN data link layer specification for frame mode bearer services”，1992

1.2 适应环境

运行环境温度	0℃~40℃
运行环境相对湿度	10%~90%，不结露
供电电源	电压允许变动范围为 220×(1±15%)V
接地阻抗	小于 5 欧姆
振动	加速度 5g，频率 50hz，三个方向
运输和储藏条件 （non-operating）	环境温度-25℃~55℃； +25℃ 时最大相对湿度小于 90%

2. FlowShaper 的技术特点

1.1 平台性能

东华流量管理系统采用纯硬件架构，满足 20M-10G 带宽链路下千兆以太网电口/光口双向线速条件下的全业务识别。

1.2 适用组网环境

支持固定分配 IP 地址、DHCP 或 Radius 动态分配 IP 地址、内网 NAT/NAPT 和防火墙等各种组网环境；可应用于多出口负载均衡链路或单向链路的业务识别和流量监控。

1.3 业务识别技术

- 逐报文进行协议识别、行为分析、业务统计、用户统计，支持 DPI 和 DFI；

-深度业务感知是以业务流的连接为对象，深入分析业务的高层协议内容，结合数据包的指纹特征检测和协议行为的分析，进行应用层协议的识别。

-深度流感知是以业务流的连接为对象，动态基于连接的统计行为特征，包括通信速率、连接时间、报文长度等指标，进行应用层协议的分类和识别。

1.4 精确的应用协议匹配

匹配 IP 网域、TCP/UDP 端口及 7 层包特征，内置庞大的应用协议库，划分 13 个大类若干个小类，应对不断更新的网络应用，有专业的协议库分析团队对网络实时监控抓包，保障最新最全的协议应用在设备中识别的准确率。支持用户自定义应用，解决用户内部应用分析的识别问题。

1.5 URL 识别及网络内容字节匹配

系统具有全面的 URL 分类库，并不断更新。针对 web、邮件、论坛等提供内容审计，自动获取器内部传输字节文本，提供自定义敏感词告警机制，采用字节匹配方式确保网络安全。

1.6 可靠性和安全性

- 设备具备 BYPASS 旁路功能，软件宕机、设备掉电、Bypass 设备掉电均可实现 Bypass，切换时间≤3ms；
- 具备完整的 Bypass 解决方案：百兆、千兆电口内置 Bypass，千兆光口与外置 Bypass 设备联动；
- SSH 可设置访问控制策略限制对设备的访问及操作；
- 配置双电源提供冗余功能（可选配）。

1.7 液晶面板控制台

液晶面板控制台方便用户直观了解设备的一些基本信息并对设备进行一些基本操作，包括显示数据流入、流出的总流量，基本的网络配置和恢复设置等。

1.8 完善的视图呈现

利用 flash 技术展现网络链路视图，提供横纵坐标详解，支持实时、历史模式，每张视图提供多层关联，支持多视图种呈现方式包括区域图、饼状图、柱状图、线形图，每张视图支持多种模式导出，包括 word、excel、pdf。

3 部署方式

FlowShaper 采用的是网桥的透明接入模式，把 FS 接入到网络出口中时，不需要改变现有网络的拓扑结构，直接将设备接入到交换机和网关之间即可使用，FS 的内-外网链路端口不需要分配地址，内部或外部用户也将不会感知 FS 的接入，使得 FS 的使用更为快捷方便。

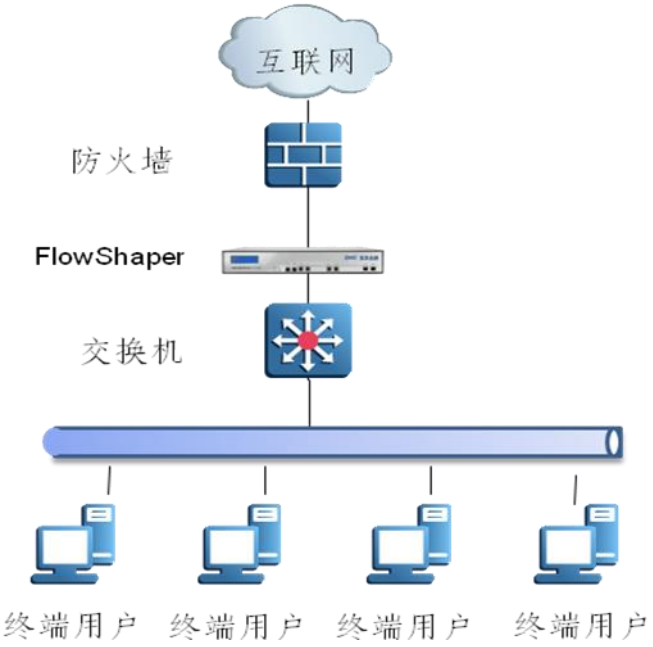

图 4 部署方式

4 产品功能

4.1 丰富的自定义功能

- 支持自定义管理员账户及权限分配，方便不同职能用户管理各自网络及业务；
- 支持自定义用户、用户组及黑白名单功能，提供 IP、IP+MAC、IP 网段、IP 地址段等多种用户定义方式；

- 支持自定义应用及应用组功能，提供 IP 网域、TCP/UDP 端口及 7 层包特征等多种协议匹配方式；
- 支持自定义监控对象，提供用户、端口及应用匹配的方式；
- 支持自定义 URL，提供 URL 模糊匹配；
- 支持自定义审计内容告警词；

4.2 流量分析功能

FlowShaper 系统的流量分析与其他同类产品相比较，有着以下两个“全面”和一个“深度”的优势：第一个“全面”是指全面的深度数据分析功能；第二个“全面”是指全面的数据视图展示方式；一个“深度”则是指支持用户进行“用户----应用”相关联数据的二级深度查看。

4.2.1 全面数据深度分析功能

FlowShaper 系统中包括十分全面的深度流量分析功能，其主要对应的视图包括以下几种：

◆ 网络带宽使用概要视图（首页）

FS 系统的页面在首页展示出用户相对比较关注的 4 个视图，分别是：带宽趋势图、应用流量分布图、总流量、用户流量排名。让用户在以进入系统后，便对最近一个小时内的 FS 系统运行的整体状态以及网络行为构成有个大致的了解。为后续的用户或应用的深度分析提供一个快速的、全面的数据依据。

◆ 总带宽（进、出）统计视图

让用户便对最近一个小时内的 FS 系统运行的整体带宽状态有个大致的了解。为后续的用户或应用的深度分析提供一个快速的、全面的数据依据。

◆ 网站点击率分析

分析最近一小时用户点击的网站次数并统计各网站占点击总量的百分比，让用户对全网网站访问提供全面数据依据。

◆ 用户活跃度分布统计视图

用户活跃度是指单位时间内用户同时并发的连接的数量，一个用户的并发连接数越多，用户越活跃。该视图可以清楚的为用户展现最近一个小时内，内网中每台机器的活跃程

度，给网管对内网用户进行策略的制定提供数据依据。而用户组活跃度分析则是将多个用户组合为一个组进行的活跃度分析。

◆ 用户带宽分布统计视图

用户带宽分布统计视图为用户提供最近一个小时内，每个内网用户带宽的变化曲线。十分直观的为网管提供用户的带宽大小的排名，为网管对内网用户进行策略的制定提供数据依据。用户组带宽分析则是将多个用户组合为一个组进行的带宽分析。

◆ 7 层应用活跃度分布统计试图

应用活跃度是指单位时间内应用同时并发的连接的数量，一个应用的并发连接数越多，该应用越活跃。7 层应用活跃度分布统计视图为用户提供最近一个小时内，每个识别出来的 7 层应用活跃度的变化曲线。十分直观的为网管提供应用的活跃度大小的排名，为网管对 7 层应用进行策略的制定提供数据依据。

◆ 7 层应用带宽分布统计视图

7 层应用带宽分布统计视图为用户提供最近一个小时内，每个 7 层应用带宽的变化曲线。十分直观的为网管提供 7 层应用的带宽大小的排名，为网管对 7 层应用进行策略的制定提供数据依据。

◆ 7 层应用组带宽分布统计视图

7 层应用组带宽分布统计视图为用户提供最近一个小时内，每个识别出来的 7 层应用组带宽的变化曲线。十分直观的为网管提供应用组的带宽大小的排名，为网管对 7 层应用组进行策略的制定提供数据依据。

4.2.2 全面的数据视图展示方式

FlowShaper 流控系统中包括十分全面的数据视图展示方式，其对应的视图包括以下几种：

◆ 鼠标选取任意时间段数据变化曲线图

在最近一小时的数据变化曲线图的基础上，用户可以用鼠标框选其关心的任意时段的数据曲线图，并且可以多次鼠标进一步的框选。

◆ 数据组成柱图

数据组成柱图主要是侧重于在单位时间内观测主题中各个组成部分占总体的变化趋势图，让用户可以直观的了解整体的组成，以及单位时间内的各个组成的变化趋势。

◆ 数据组成饼图

数据组成饼图主要是侧重于一个观测主体中各个组成部分所占比例的一个视图，让用户可以直观的了解整体的组成，以及异常个体组成的情况。

◆ 数据实时刷新曲线图

数据实时刷新曲线图给用户展示观测主体实时的变化趋势，让用户快速、直观了解当前所观测的用户或应用的实时变化。

4.2.3 关联数据的二级深度查看

◆ 用户及用户组深度分析

用户可以通过“用户深度分析----带宽分析”视图来了解所有用户最近一小时内的带宽变化趋势。而用户除了对整体的变化有个大致的了解，往往对某一个用户有过什么样的应用更感兴趣。这时，只需继续点击关心的用户，出现的视图便罗列出该用户最近一小时内的应用，以及应用的变化趋势。

◆ 应用及应用组深度分析

用户可以通过“深度应用分析——带宽分析”视图了解最近一小时网内所有应用带宽情况。而用户除了对全网应用有个整体了解外，会对个别应用的使用用户更感兴趣。这时。只需继续点击关心的应用，出现的视图便罗列出该应用最近一小时的使用用户，以及用户所占带宽变化趋势。

4.3 QoS 流量控制功能

FlowShaper 实时管控功能可以对被管理用户进行实时的精细化的带宽管理和控制，其中带宽管理的精度为 1kbps。

◆ 三大组成元素配合策略管理

一条管控策略由被管用户、应用对象和服务目标 3 大元素组成，其中被管用户是系统所配置的用户，可以是内网被管用户、外网被管用户，用户同时支持多种表达方式，如 IP 地址，IP 网段、IP 地址段、MAC、IP+MAC、Vlan-id 等；应用对象是系统所支持的所有应用/应用组，或用户的自定义应用/应用组，或以上两种的任意组合；服务目标则是被管用户的应用所分配的管控带宽以及此策略的生效时间段，管控带宽具有两种类型，保障和限制，其中保障性带宽能保障数据流的带宽，用于需要保障的重点业务，限制则将相应的数据流的带宽占有限制在配置的限额以下。

◆ 多级分层次策略

管控策略在逻辑上支持两级策略，即一级策略和二级策略，其中二级策略从属于某条一级策略，是其父策略(一级策略)的具体和细化，如被管用户的细分，应用对象的细分和服务目标相应的微调。另外，从属于同一父策略的所有二级策略可以显示指定 5 种不同的优先级，优先级数值越小，优先级别越高，从而能优先通过网络转发出去。

◆ 时间策略实现监管全自动

另外提供时间策略设定，系统时间将自动与时间服务器进行时钟同步，当策略到达时间阀值时，策略智能的停止或生效，真正实现了策略部署的多维实现方式，只需进行一次配置组合，系统就可以完全自动的开启或停止符合时间阀值的策略。

◆ 黑白名单策略实现特殊用户部署

管控策略支持黑白名单功能，白名单将不受管控策略控制，黑名单的数据包则将被完全禁止。除了正常的黑白名单配置外，同时还支持黑白名单的快捷操作，在实时查看用户的流量信息时，可以直接将用户实时加入黑白名单，从而高效的完成网络突发情况的实时处理。

管控策略一旦下发给系统后，将立即生效，配合其灵活多变的配置方式，能充分满足企业网络中的各种需求。