UNIS iMC UBA 用户行为审计组件

产品简介

iMC UBA 用户行为审计组件通过与多种网络设备共同组网，用来对终端用户的上网行为进行事后审计，追查用户的非法网络行为，满足相关部门对用户网络访问日志进行审计的硬性要求。

UBA 用户行为审计组件提供 NAT 1.0、Flow 3.0、NetStream V5/V9、NetFlow V5/V9 和 DIG 日志的查询审计功能，网络管理员可以根据网络日志对上网用户的网络行为进行审计。

产品特点

UBA 具有以下特点：

◆ 全面的日志采集

UBA 用户行为审计组件可支持多种网络日志的采集（包括 NAT 1.0、Flow 3.0、NetStream V5/V9、NetFlow V5/V9 和 DIG 日志），对于不支持上述日志的设备，可以通过设备的镜像端口或 TAP 分流器采集网络流量生成 DIG 格式的日志。

◆ 分布式部署

UBA 用户行为审计组件采用分布式的体系结构，支持多点采集，统一 Web 界面审计分析，可以同时采集多个设备的日志信息，为网络管理员监控网络提供了灵活有效的支持。

◆ 强大的日志审计功能

UBA 用户行为审计组件可根据用户需要，通过接入用户名、上网时间、用户访问网页的 URL、ftp 操作文件及发送邮件的主题等各种条件的组合对网络日志进行快速审计，并对审计结果提供灵活的排序、分组、保存等功能。

网络管理员可以从海量的网络日志中精确审计终端用户的上网行为。终端用户何时访问了某网站、何时访问了某网页、发送了哪些 Email、向外发送了哪些文件等信息均可通过日志审计得出结果，日志审计包括：

通用日志审计：审计内容包括接入用户名、用户上网起止时间、来源/目的 IP 地址、来源/目的端口、使用的协议及应用名。

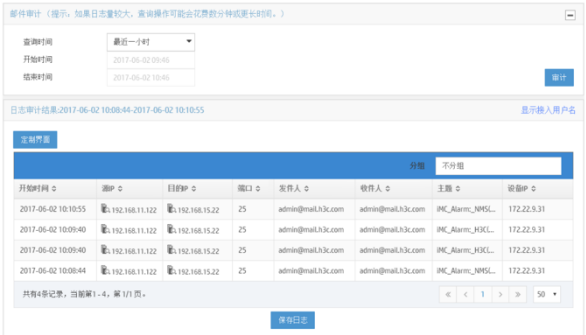
Web 访问审计：审计内容包括接入用户名、用户上网起止时间、来源/目的 IP 地址、端口、用户访问的站点、用户访问的网页等。

文件传输审计：审计内容包括接入用户名、用户传输文件起止时间、来源/目的 IP 地址、端口、ftp 用户名、传输文件名、传输方式（上传/下载）等。

邮件审计：审计内容包括接入用户名、邮件发送时间、来源/目的 IP 地址、发件人、收件人、邮件主题等。

地址转换审计：审计内容包括接入用户名、用户上网起止时间、来源/目的 IP 地址、来源/目的端口、使用的协议及应用名、NAT 转换后 IP 地址/端口等。

Telnet 审计：审计内容包括源 IP、目的 IP、端口、Telnet 用户名、执行命令等信息等。



◆ 基于用户的行为审计

结合 EAD 端点准入解决方案，UBA 用户行为审计组件可高效地管理网络用户，建立详细的用户访问互联网的日志，提供行之有效的网络管理和用户行为跟踪审计策略，帮助管理员分析用户的上网行为。

◆ 七层应用审计

端口不固定的应用，如 P2P 等应通过报文应用层数据的特征进行识别。基于七层应用的识别和分类，UBA 可基于用户全面审计网络中的七层应用使用信息。

组件已经将大部分常见的端口不固定的应用设定为组件预定义的应用，如：BT、DC、eDonkey、Gnutella、Kazaa、MSN、QQ、AIM 等。用户可根据需要，定义其它的应用识别。七层应用识别只对 DIG 日志有效，对其他类型的日志无效。

◆ 任务式审计

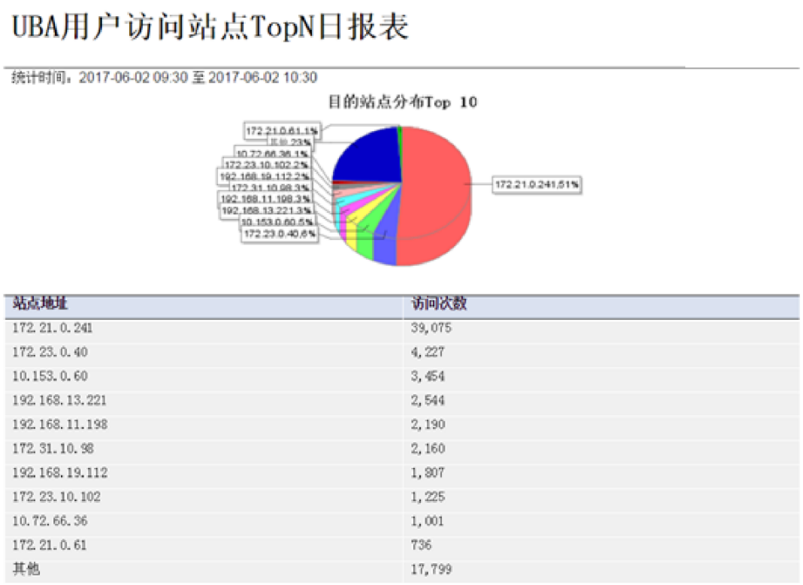
UBA 用户行为审计组件提供基于任务的自动跟踪审计功能，可以根据接入用户名、用户访问网页的 URL 等各种查询审计条件灵活制定审计任务。任务一旦制定，组件将自动跟踪审计当前时间段内满足查询条件的所有用户及日志信息。审计任务包括：地址转换、Web 访问、文件传输、邮件、通用等多种类型。

◆ 日志转储

UBA 用户行为审计组件支持对海量日志进行转储。用户可以将敏感日志和由于数据库空间限制无法存储的日志定时导出到数据文件中进行异地保存，同时组件提供转储日志查询工具，用户可直接对转储日志进行查询操作。

◆ 审计报表

UBA 系统提供专业的报表，包括访问站点、会话数、应用分布、未知应用的 TopN 报表，SMTP、HTTP、FTP 的应用分析报表，每种报表都可以按照天、周等周期和图形、列表等形式输出。通过使用这些自带的报表，管理员可以非常清楚的了解当前用户对网络的使用情况。



UBA用户访问站点TopN日报表

统计时间：2017-06-02 09:30 至 2017-06-02 10:30

目的站点分布Top 10

站点地址	访问次数
172.21.0.241	39,075
172.23.0.40	4,227
10.153.0.60	3,454
192.168.13.221	2,544
192.168.11.198	2,190
172.31.10.98	2,160
192.168.19.112	1,807
172.23.10.102	1,225
10.72.66.36	1,001
172.21.0.61	736
其他	17,799

运行环境

属性	参数
硬件平台	服务器端：PC 服务器：CPU 主频≥3GHz、内存≥4G、硬盘≥10G、至少 1 块 10/100/1000Mb 自适应以太网卡、Windows 32 位或 64 位，Linux 32 位或 64 位环境 客户端：PC：主频 1.8G（及以上）、内存 512MB（及以上）、硬盘 20GB（及以上）、48 倍速光驱、100M 网卡、显卡支持分辨率 1024×768、声卡
操作系统	服务器端：Windows Server 2003/Windows Server 200 32 位或 64 位或者 Windows Server2012 64 位、Red Hat Enterprise Linux Server 5/5.5/5.9/6.1/6.4 32 位或 64 位 客户端：Windows、MAC OS、Redhat Linux 等 浏览器：IE9/IE10、Firefox20 及以上版本、Chrome 26 及以上版本
数据库	SQL Server 2005/SQL Server 2008/SQL Server 2012（Windows） Oracle 11g Release 1 or Oracle 11g Release 2（Linux）

北京紫光恒越网络科技有限公司

北京基地
北京市海淀区中关村东路 1 号院 2 号楼 402 室
邮编：100084
电话：010-62166890
传真：010-51652020-116
版本：

http://www.unishy.com

客户服务热线
400-910-9998