AnaTraf 网络流量分析仪

功能概览

功能	功能简介
基础	
系统部署	支持桥接、流量镜像、TAP 方式部署。支持分布式部署。
界面	全中文界面和资料文档，全中文的分析界面，全中文的文档资料。
架构	系统管理界面采用纯 B/S 架构，无需额外客户端支持。
数据安全传输	为保证数据在传输过程中的安全性，与服务器通信时使用 SSL 加密。
虚拟链路	支持 VLAN 虚拟链路分析，能够根据 VLAN ID 设定虚拟链路，实现对特定 VLAN 流量的独立流量分析。
	支持网口虚拟链路分析，能够根据物理网口设定虚拟链路，实现对特定网口流量的独立流量分析。
	支持 IP 网段虚链路分析，能够按 IP 地址范围设定虚链路，实现对特定 IP 网段的独立流量分析。
	链路聚合功能，将多网卡的流量聚合捕获分析。
数据存储	
循环存储	支持存储空间循环，以滚动存储方式不断更新数据，当数据达到本地存储容量上限时能够按照时间顺序从前至后自动更替。
报文截断存储	截断存储数据包以节约存储空间。支持数据包自定义长度截断存储，支持裁剪为64-65535之间的任意数值长度。
过滤捕获	捕获数据包时能够根据条件过滤捕获，包括根据 IP 地址、地址段、通讯协议、TCP/UDP 端口等条件过滤捕获。
数据包回放	支持数据包回放功能，能够将已捕获的数据包文件在系统上进行回放分析，实现与实时采集链路相同的分析功能。回放分析时不中断实时分析。
历史报文检索提取	可以将按特定时间、特定过滤条件过滤的流量提取并下载为PCAP文件。
协议解码识别	
在线解码	支持在 WEB 界面打开数据包解码页面，进行数据包分析。
IPv4 / IPv6 支持	支持识别 IPv4 和 IPv6 流量，同一界面分析 IPv4 / IPv6 流量。
应用定义	
自定义应用	可根据 IP 地址、地址组、地址范围自定义应用；可根据 IP 地址+端口自定义应用。
	能够灵活的自定义应用，针对自定义的应用进行流量监测分析； 可根据TCP/UDP 端口或端口范围、端口组自定义应用。
	可根据网段、网段组自定义应用。

功能	功能简介
统计分析	
TOP N 仪表板	全局流量概览，最活跃的MAC地址、IP地址、应用层协议流量的历史曲线图。
自定义仪表板	可以增加一个自定义面板，自由组合不同分析模块的图表。
MAC 分析	活跃IP、活跃时间、MAC Peers统计、网卡信息、OS、应用层协议等。
ARP 分析	ARP请求、响应信息，MAC地址、IP地址信息等。
VLAN 分析	支持IEEE 802.1Q VLAN。
QoS 分析	提供VLAN各优先级的流量统计。
数据包大小统计	统计全局、TCP / UDP 流量的数据包大小分布情况，以及数据包大小的历史变化趋势。
突发分析	测量每个网口的吞吐量和利用率。
IP 分析	观测到的所有IP地址的流量统计、活跃时间、地理位置、连接、应用层协议等。
IP Pairs 分析	能够统计分析所有IP主机间的通讯流量信息，包括接收发送流量，接收发送数据包，应用通讯信息，网络传输质量指标，包括双向的 TCP 重传，三次握手时延，TCP ACK时延等。
IP地理信息	国家、地区的IP流量统计。
QoS 分析	提供各差分服务编码点（DSCP）的流量统计。
连接分析	观测到的所有IP地址的连接统计，TCP、UDP各项指标，MTU等。 能够统计分析网络中所有TCP会话和UDP会话的通讯流量信息，包括接收发送流量，接收发送数据包等参数；
TCP 分析	TCP流量统计，TCP握手、响应时延、分配时间、重传、乱序、零窗口等。
TCP 时序图分析	能够图形化的显示TCP会话中的数据交互传输过程，能够图形化显示数据传输中的时间间隔。
TCP 流重组	提供 TCP 会话的流重组功能，将会话中的数据流重组显示。
端口分析	能够通过分析网络中的流量提供网络中每个IP主机提供的服务端口，并提供这些服务端口的流量统计数据，同时提供访问这些服务端口的所有客户端的流量信息。
L7 协议	提供所有识别出的应用层协议的流量统计，IP信息等。能够针对应用进行进一步的数据挖掘，分析某个应用中IP主机流量、IP会话、TCP会话和UDP会话详细列表。

功能	功能简介
统计分析	
HTTP 分析	HTTP服务器流量统计，请求和响应信息，响应时间、响应代码等。
HTTP 交易分析	图形化显示指定HTTP应用的交易处理数量变化趋势，交易处理数量包括：交易次数、请求数量、响应数量等。交易处理时间变化趋势，包括平均交易处理时间、最大交易处理时间、最小交易处理时间等。
WEB 应用分析	提供WEB应用详情分析，内容包括访问时间、应用名称、源地址、目的地址、URL、响应时间及返回码。
TLS 分析	提供TLS服务器、证书、响应时延等信息。
DHCP 分析	网络中动态分配IP的统计，响应时延、分配时间、租期等。
DNS 分析	提供DNS服务器流量统计，域名解析统计，服务器响应时间、回复代码统计等。
服务端口统计	能够通过分析网络中的流量提供网络中每个IP主机提供的服务端口，并提供这些服务端口的流量统计数据，同时提供访问这些服务端口的所有客户端的流量信息。
IP 主机数据挖掘分析	能够针对IP主机进行进一步数据挖掘分析，分析某个IP主机的应用、IP 会话、TCP 会话和 UDP 会话。
多点关联分析	多节点数据关联分析，监控网络多节点带宽、延迟、丢包。
WiFi 分析	
信道分析	分析所有可见的 WiFi 信道，包括频率、流量统计、重传字节、BSS 数量等。
BSS 统计分析	统计分析所有的基本服务集，包括BSS ID、名称、信道、频率、流量统计、重传字节、信号质量等。
告警推送	
流量告警	支持针对 IP 地址、IP 网段、端口等对象进行流量字段的阈值设定进行告警。
推送通知	能够通过邮件、Syslog将报警信息发给指定接收者。
主机流量监控告警	警报流量参数：能够针对关键主机或全局主机的每秒字节数、收发每秒字节数、数据包数、收发每秒数据包数、平均包长、收发平均包长、数据包发收比、每秒发送 TCP SYN 包数、每秒接收 TCP SYN 包数、每秒发送 TCP SYN-ACK 包数、每秒接收 TCP SYN-ACK 数据包数等参数设定阀值，产生警报。
告警配置	告警触发的时间间隔可以设置：1秒，10秒，1分钟，10分钟，1小时； 支持警报触发时间范围设置，能够为每条警报设置不同的触发时间。例如：工作日8:00~18:00可触发，其他时段不可触发。
可疑域名解析告警	对可疑域名解析行为进行监测产生警报，可以定义域名列表、域名地址列表进行监测，发现可疑的域名解析，产生警报。

功能	功能简介
网络安全	
威胁情报检测	支持基于威胁情报的威胁检测，检测类型包含APT事件、僵尸网络、勒索软件、流氓推广、窃密木马、网络蠕虫、远控木马、黑市工具、其他恶意软件。
情报特征库	内置各类特征库、威胁情报库，支持在线自动升级和手动升级。
威胁溯源	支持对任意威胁事件进行按通讯源端口、源IP、目标端口、目标IP、IP会话等维度进行快速流量回溯分析，能够展示出该威胁事件一段时间内的原始通讯流量趋势图； 能够对通讯内容进行原始数据包级别的取证分析，显示威胁上下文内容。
系统管理	
用户管理	支持用户按角色管理，不同角色具有不同等级的配置权限。可以设定用户访问权限，权限包括是否能下载数据包，是否允许更改系统设置等。
访问控制	支持对访问分析服务器的IP地址做限制，只允许特定的客户端IP访问服务器对访问服务器的用户。