和勤网络信息审计系统
DD2000

技术白皮书

和勤软件技术有限公司

电话：010-58715366 传真：010-58715381
地址：北京市海淀区中关村大街 19 号新中关大厦 606-608 室 邮编 100080

一. 简介.....**错误！未定义书签。**

二. 功能规格.....3

2.1 信息记录与查询.....3

2.2 策略管理.....5

2.3 账号管理.....6

2.4 报表.....8

2.5 流量分析.....10

2.6 系统管理.....11

三. 环境建立与项目需求.....13

3.1 采用 Sniffer 模式下，选择使用 Hub 或交换机.....13

3.2 采用网关模式运作.....14

一. 概述

随着互联网技术的快速发展及信息数字化技术的日益普及，政府、企业、军队、院校的工作与日常活动对网络的依赖也日益深化。目前大多数的用户单位都已认识到信息安全管理的重要性，陆续建设完成了防火墙、防病毒系统等信息安全基础架构。但是目前的网络安全架构也只是对来自网络的攻击进行防御，但对于涉及与网络应用相应的内容安全与管理，还不具备更多的管理与防范。

和勤网络信息审计系统可详细记录与审计用户的上网行为，阻断 P2P 的非法应用，对 WEB_MAIL 的审计有独特的应用效果，系统可结合不同单位的管理制度，定制管理与过滤策略，通过详尽的分析报表让管理员快速而实时的掌握单位网络带宽的使用状况与流量趋势。

二. 功能规格

2.1 信息记录与查询

1. 完整记录 SMTP、POP3、IMAP 协议发送和接收的电子邮件。记录内容包括时间、源（目的）IP、寄件人、收件人、主题、邮件，并可查看邮件源文件的详细数据、本文及附件内容。

2. 完整记录经由下列网页电子邮件(webmail)服务器发送、接收的信息。记录的内容包括时间、源（目的）IP、寄件人、收件人、主题、邮件大小、邮件正文与附件。

Yahoo	Hotmail	Hinet	Url
PCHome	Sina	Yam	GiGa
Tom	Sohu	163	OpenWebMail
126	Eyou	21cn	China
Gmail	msn	263	

3. 提供根据时间、收/发信人、群组、邮件主题、源（目的）IP、邮件大小、协议类别(SMTP、POP3、IMAP、WebMail)等字段做关键词组合条件查询，并可依指定的查询条件做递增或递减的排序。

4. 完整记录 http 及 https 上网浏览的行为。记录内容包括时间、来源 IP、网址分类、网址等项目。可依时间、源 ip、目的 ip、网址关键词、协议类别、处理状态、查询使用者的上网记录。

5. 完整记录即时通讯软件(MSN、Yahoo Messenger、ICQ、AIM、QQ、GTALK)的使用状态及所接收与传送的信息。对 MSN、Yahoo Messenger、ICQ、AMI 可记录时间、即时通讯软件种类、使用者 IP、使用者账号、目的账号与完整的聊天内容。

6. 可记录通过 MSN 与 YMSG 所传送的文档内容。

7. 支持记录 Skype 的上下线状态。

8. 支持 WebIM 的信息记录。

9. 可依照时间、源 IP、目标 IP、使用者账号、目的账号、聊天内容关键词、即时通讯软件种类等条件，查询即时通讯软件(MSN、Yahoo Messager、ICQ、AIM、QQ)的使用记录。

10. 可组合查询条件，建立快速查询模式，方便快速查询。

11. 完整的 FTP 的操作记录与所传文件还原。

12. 完整的 Telnet 的操作记录与返回信息。

13.WebMail 寄信时附件名关键词过滤。

14.可在 AD 域账号管理模式下进行信息审计与管理。(使用者需登入 DC（域控制器)，且 DC 上需装 agent)。

2.2 策略管理

1. 针对上网行为与即时通讯软件的使用，采用排外名单的规则，来设定全部人员禁止使用而特例开放或全部人员开放使用而特例禁止这两种管理模式。
2. 可设定规则允许或拒绝指定群组,在一天中的特定时段或任何时间,通过 http 或 https 上网浏览。
3. 可针对网址设定阻断关键词，禁止特定网页浏览。
4. 可依据网址分类库，禁止特定类别网页的浏览。
5. 可按时间段、用户群组是否使用即时通讯工具进行策略管理。
6. 可依照即时通讯软件使用的账号设定允许或拒绝此帐号上网。
7. 可设定是否允许通过 MSN 与 YMSG 传送文档。

8. 可设定是否允许 MSN 使用加密交谈。

9. 可设定是否允许 WebIM 的使用(MSN，YMSG)。

10. P2P 软件的使用记录与管制。

2.3 账号管理

1. 可依照 ip 网段设定群组，并可将成员信息与被审计用户的电子邮件账号、聊天账号等进行绑定管理。

2. 可针对群组设定是否记录该群组成员的网络使用行为。

3. 可开放一般使用者通过网页连上系统，自行注册其所属群组及个人的账号信息。

4. 对于使用者自行注册的群组信息，管理员可选择立即套用生效或需管理员审核后生效。

5. 系统提供自动分群功能，让系统通过电子邮件与 IP 信息自动把群组成员的数据补齐。

6. 支持通过 LDAP 同步电子邮件的账号与群组。

7. 支持计算机名称显示(NetBIOS Name)

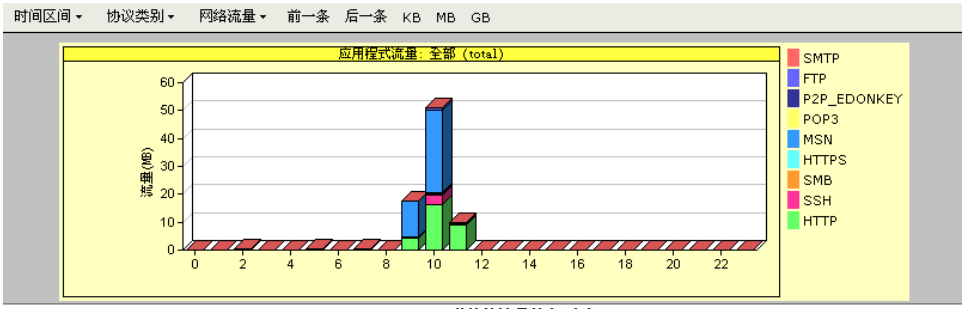
8. 系统自动记录未分群组的 IM 账号与 Mail 账号，方便管理员自行通过列表分群。

2.4 报表

1. 提供网络流量、上网行为统计、群组排名、人员排名等图表信息。

2. 所有报表可选择日报表、周报表、月报表、指定时段或时间，做出更弹性、更适宜的报表信息。

3. 所有报表可形成日、周、月报表自动发送到指定的管理邮箱帐号。



2007-03-26分协议流量信息(全部)

小时	0	1	2	3	4	5	6	7	8	9	10	11
流量(MB)	0.23	0.22	0.31	0.22	0.22	0.28	0.22	0.30	0.22	17.71	50.80	9.82

小时	12	13	14	15	16	17	18	19	20	21	22	23
流量(MB)	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

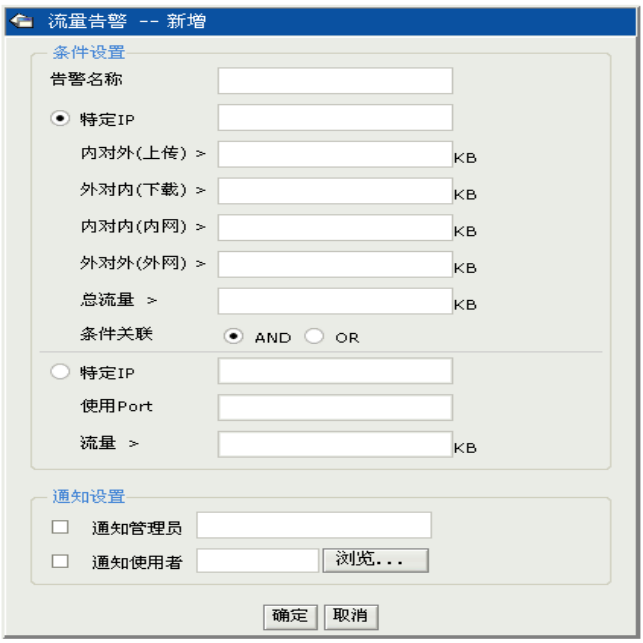
分协议流量信息

协议类别	流量(MB)
HTTP	29.559
SSH	6.157
SMB	0.587
HTTPS	0.633
MSN	42.691
POP3	0.142
P2P_EDONKEY	0.001
FTP	0.671
SMTP	0.098

4. 提供报表打印，或将报表数据导出另存成 csv 文档储存，利于做更进一步的数据处理。

5. 动态的系统操作记录查询功能，详细记录针对系统的各项操作记录。

6. 可设定流量报警阈值，并通过电子邮件提醒管理人员。



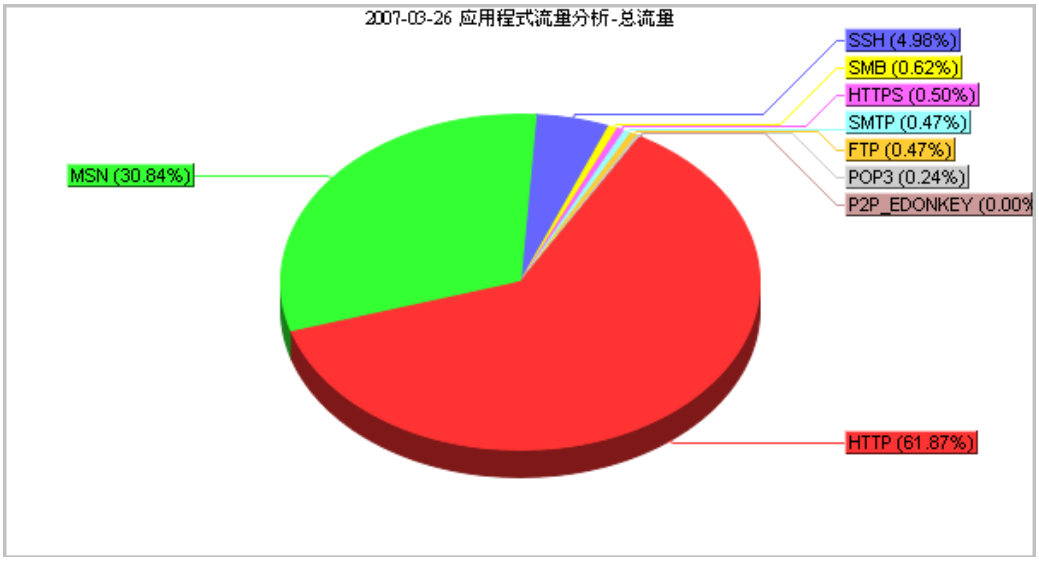
2.5 流量分析

1. 详细统计网络层流量使用状况，并可依据 IP、Port、流量交叉分析单个主机流量。
2. 可详细区分上传、下载与总流量，并分别依 IP 或 Port 进行流量 TOP 排名。
3. 可利用包特征码比对技术，针对应用程序的流量与使用者进行统计与追踪分析，包括 BT、eMule/eDonkey 等。

应用程式流量分析 2007-03-26 (排序方式:总流量(MB))

全部人员 | 时间区间 | 前一条 | 后一条 | 预览打印 | 导出报表 | KB | MB | GB

协议类别	内对外(上传)(MB)	外对内(下载)(MB)	内对内(内网)(MB)	总流量(MB)
HTTP	7.39	75.09	6.06	88.54
MSN	0.67	3.02	40.44	44.13
SSH	1.26	1.67	4.20	7.13
SMB	0.00	0.00	0.88	0.88
HTTPS	0.40	0.32	0.00	0.72
SMTP	0.61	0.07	0.00	0.68
FTP	0.02	0.51	0.14	0.67
POP3	0.07	0.28	0.00	0.35
P2P_EDONKEY	0.00	0.00	0.00	0
全部	10.42	80.96	51.73	143.11

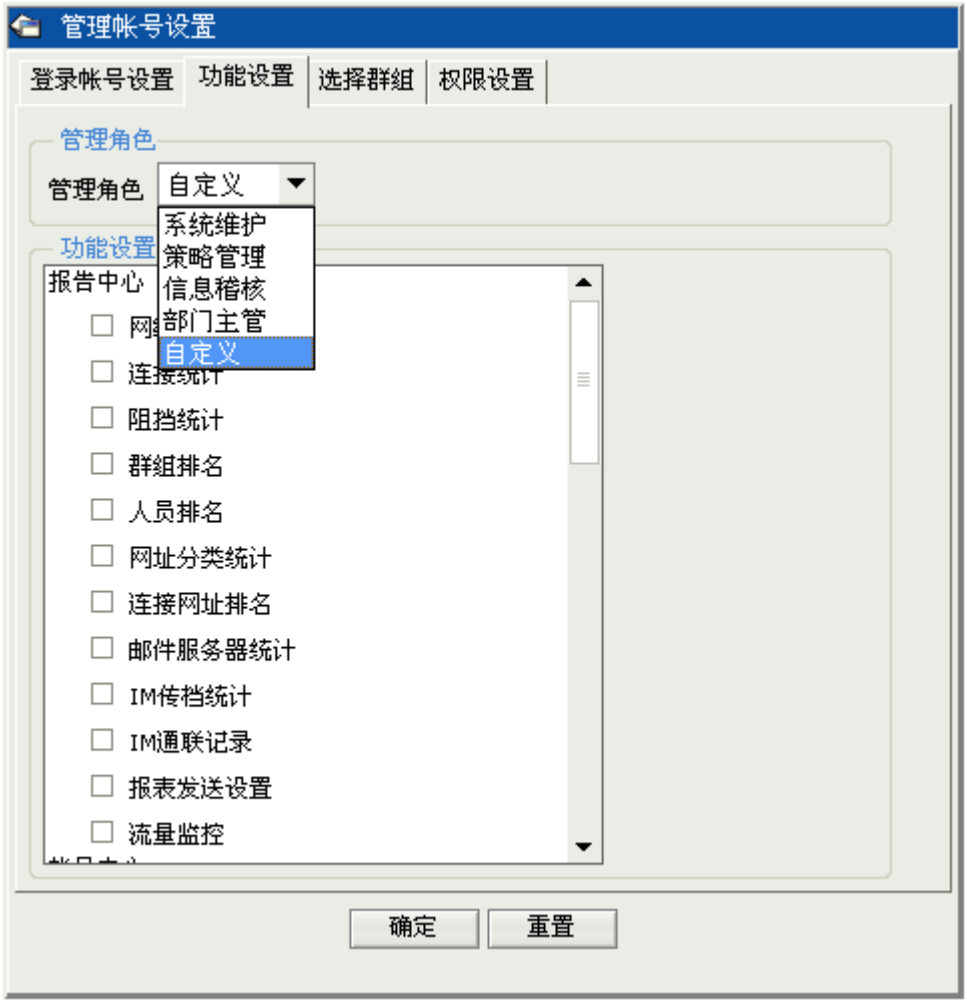


4. 可针对特定主机的流量大小与方向设定异常流量监控条件，并通过电子邮件实时通知系统管理员。
5. 可对个别主机所使用的特定 Port 设定异常流量监控条件，并通过电子邮件

实时通知系统管理员。

2.6 系统管理

1. 系统管理员权限分级管理。通过细致的划分功能、所能管理的群组以及浏览权限设定，可设定个性独立的管理账号，达到分级管理的目的。



2. 管理账号的浏览权限可根据不同的需要赋予其是否具有查看系统所记录的邮件内容、网页内容、IM 聊天信息的功能。

3. 提供不同管理员登入系统的时间、登入 IP 及详细的操作记录。

4. 提供系统运行状态的记录。

5. 提供系统信息以及系统状态（CPU、Memory、Swap）的图表，以了解系统的效率及负载状况。

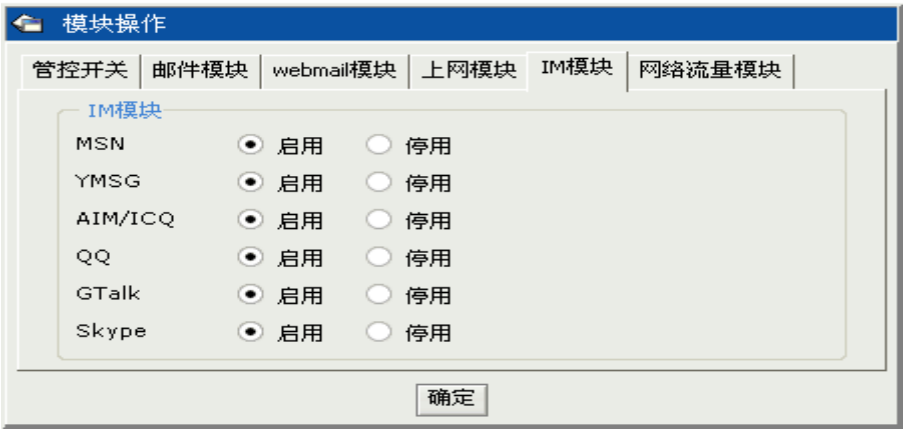
6. 管理员可启用系统在线更新（升级）机制，以同步产品的新功能。

7. 提供磁盘空间容量报警机制。可选择停止备份、删除旧备份数据、及通知指定的管理员。

8. 每日定时备份数据库与系统设定文件至远程服务器(SMB)。

9. 管理员可手动或自动，分别针对信息记录与统计数据进行数据库维护的工作。

10. 模块化功能机制，管理员可针对邮件、WebMail、网页浏览、即时通讯软件，设定启用或停用。



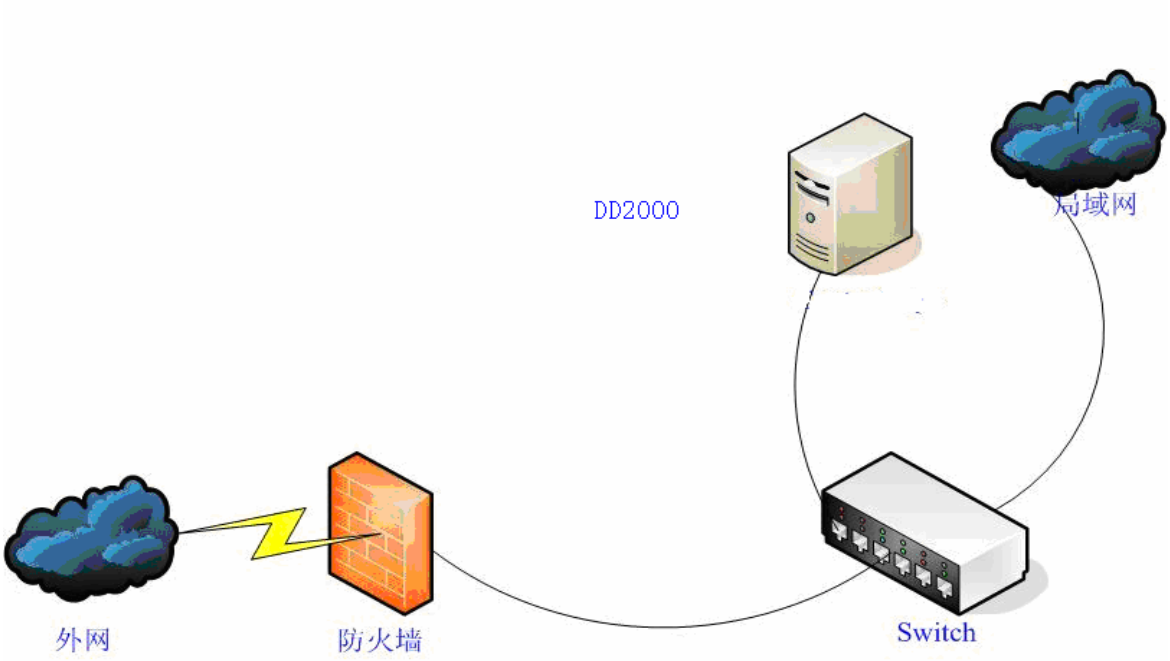
11. 管理员可自行新增网址分类类别，或新增网址至预设的网址分类数据库，更丰富网址数据库以做更有效的分类管理。

三.　环境建立与项目需求

本产品支持 Sniffer（旁路监听模式）与 Inline（网关模式）两种运作模式，可在对现有网络架构影响最小的状况下快速部署。

3.1 采用 Sniffer 模式下，选择使用 Hub 或交换机

使用 Hub 是最简单方便的选择。不用任何额外设定，只要将 DD2000 和希望管理的网段通过 Hub 链接起来，DD2000 即可进行内容记录与策略管理的工作。如果使用交换机则需要设定交换机上镜像端口的功能。



图表 1：网络信息审计系统架构示意图

3.2 采用网关模式运作

DD2000 支持以透明的方式与现有的网络结构整合，此时需要使用两张网卡以一进一出的连线方式与现有的网络设备串联。同样需要考虑哪些网段或服务需要被管理，来决定实际布署位置。通常会放置在企事业单位的网络边界防火墙与内部网路之间，如下图所示：