社会科学研究中信息防护模式的探究

李福强
中国社会科学院网络中心

主要内容

01 科研人员工作特点分析

02 解决办法

03 小结

科研人员工作特点分析

1、信息需求量大、范围广

2、对外交流比较频繁

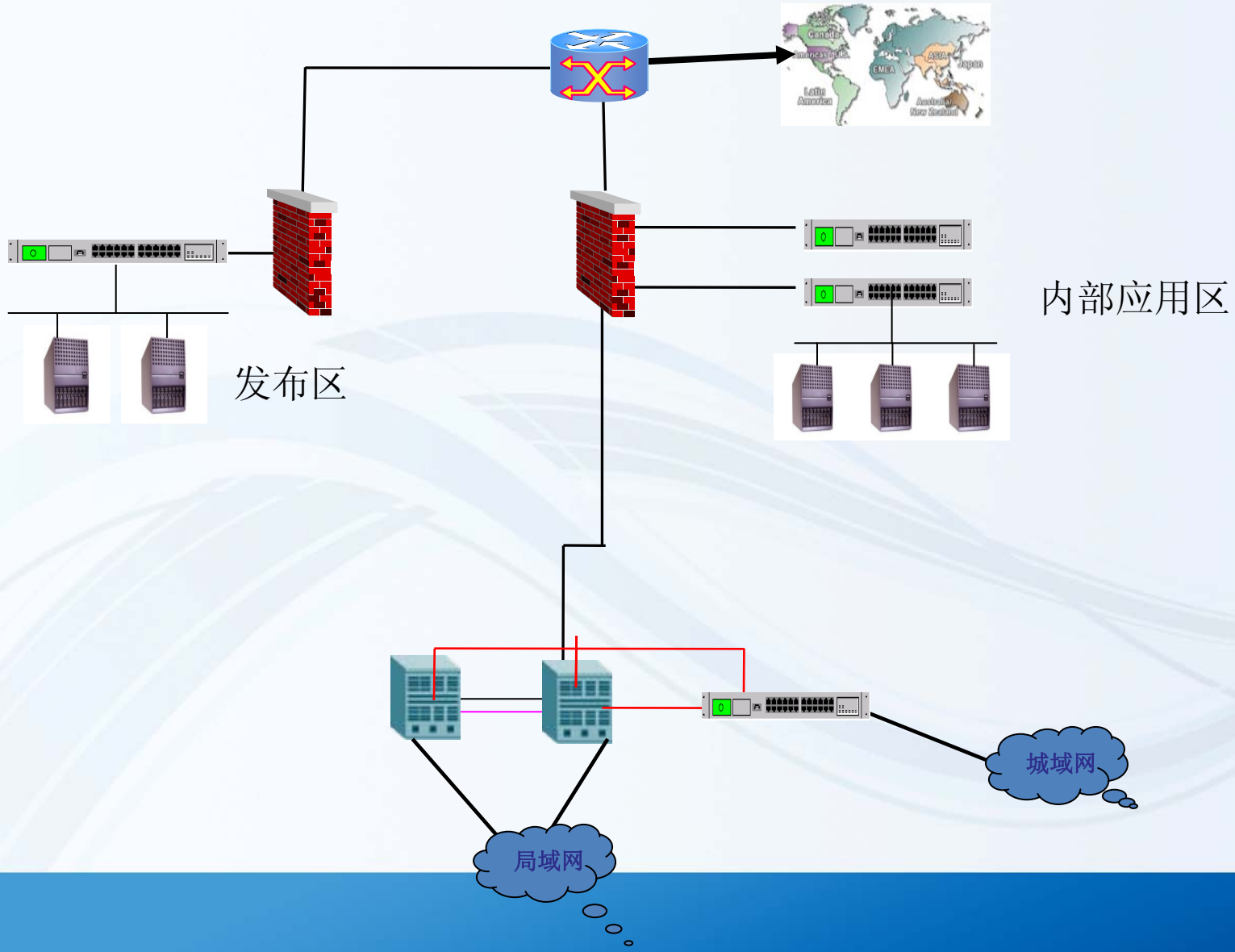
3、好奇心较重

4、外出调研多

5、查杀病毒类工具软件使用水平不够

6、防护意识薄弱

网络基础建设



网络设置

1、固定IP地址

2、固定单位编号

3、分段NAT地址

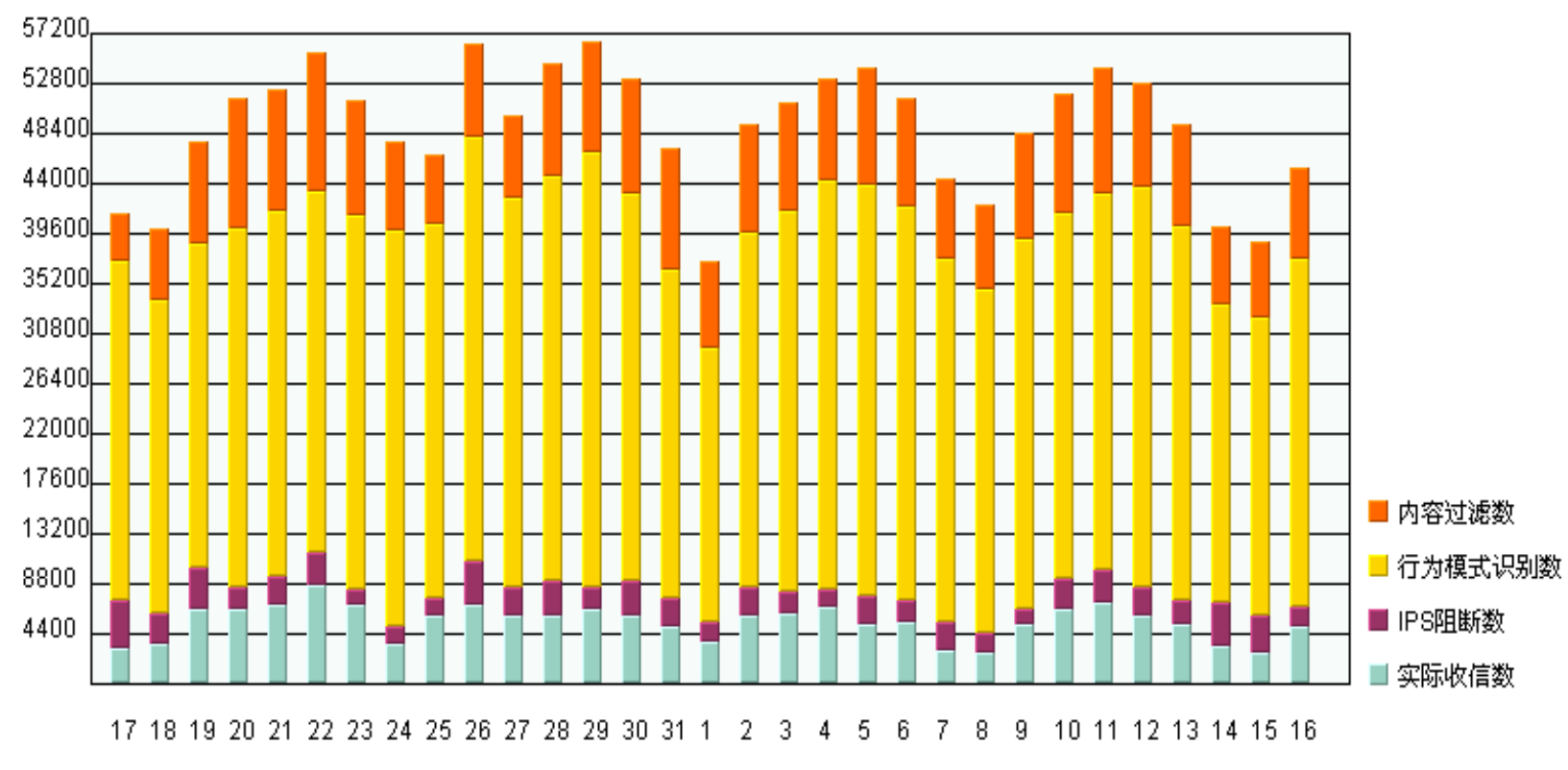
网络畅通保障

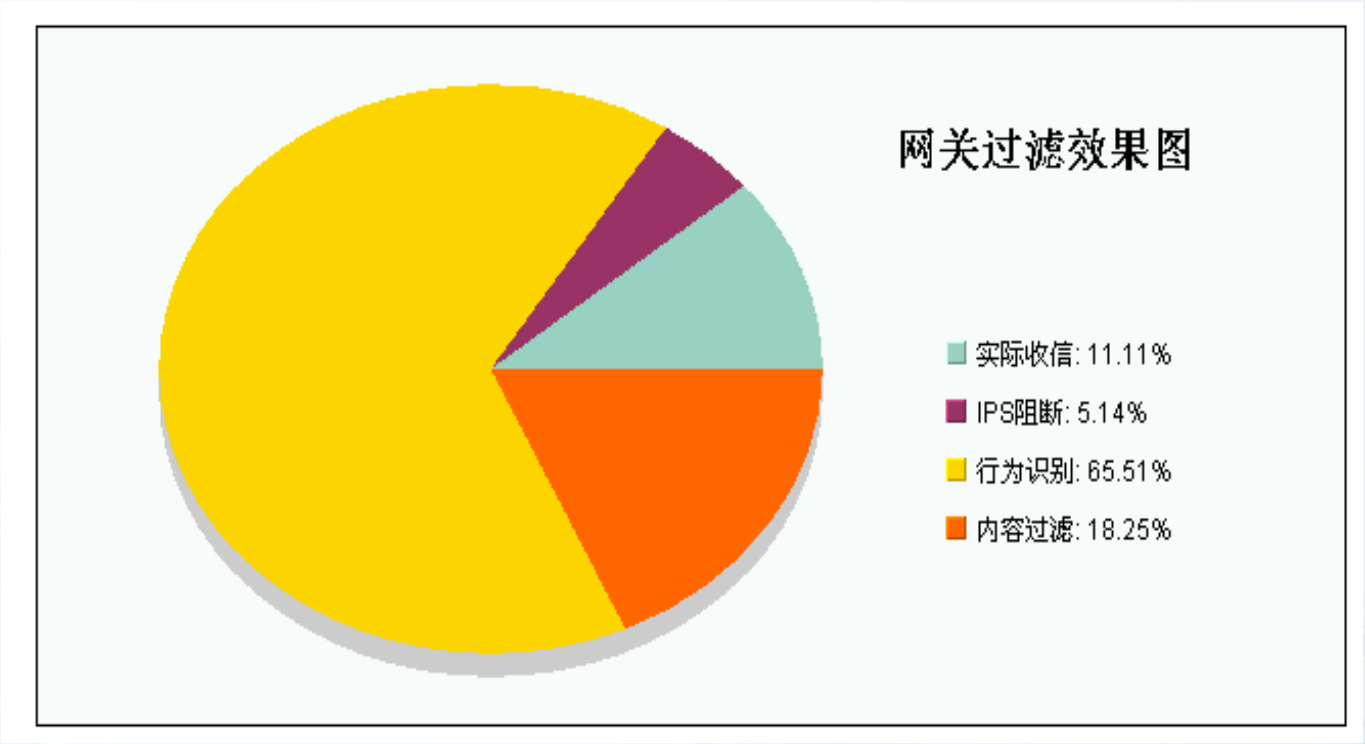
1、按应用分配带宽

2、分时段进行带宽限制

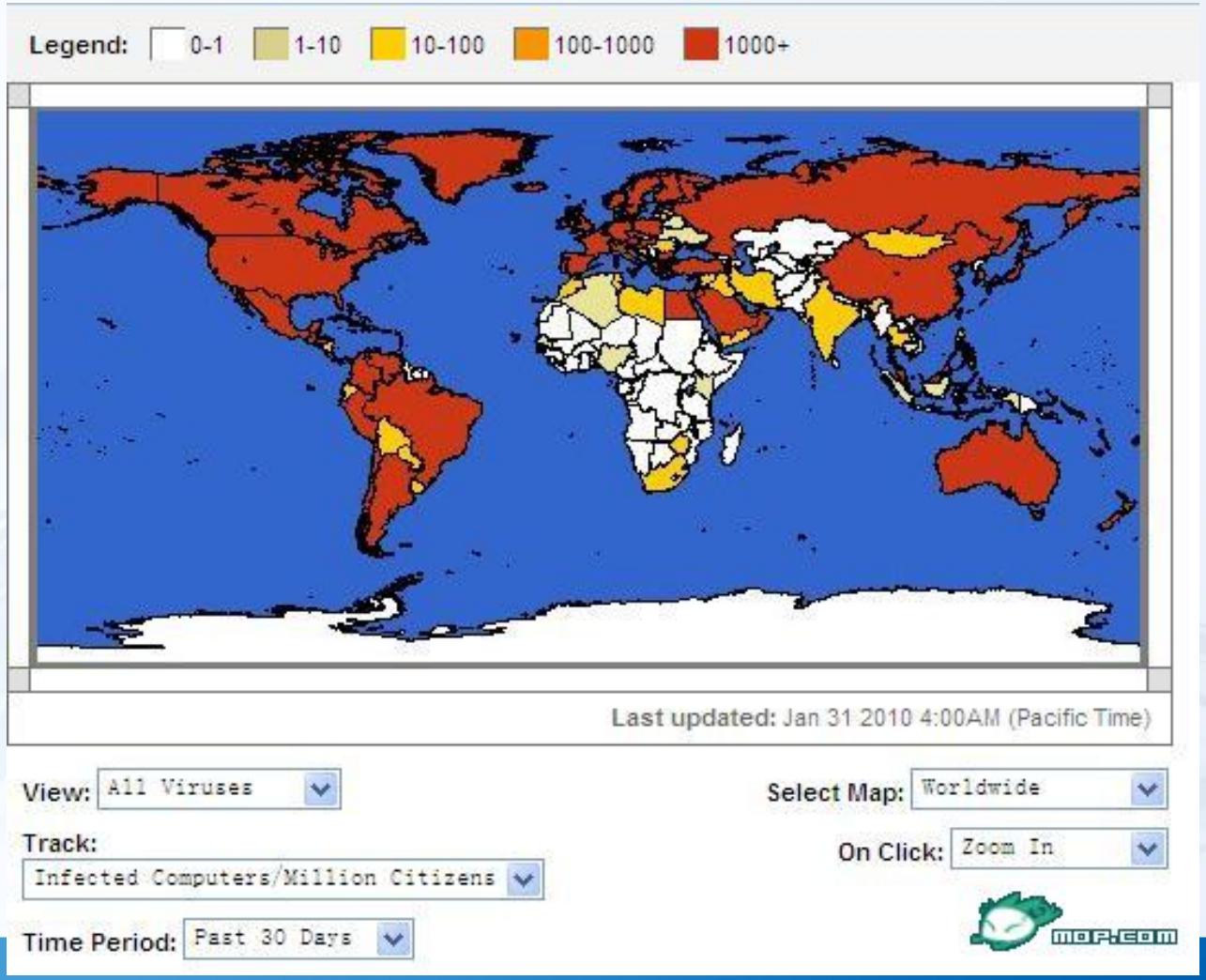
3、有针对性收费

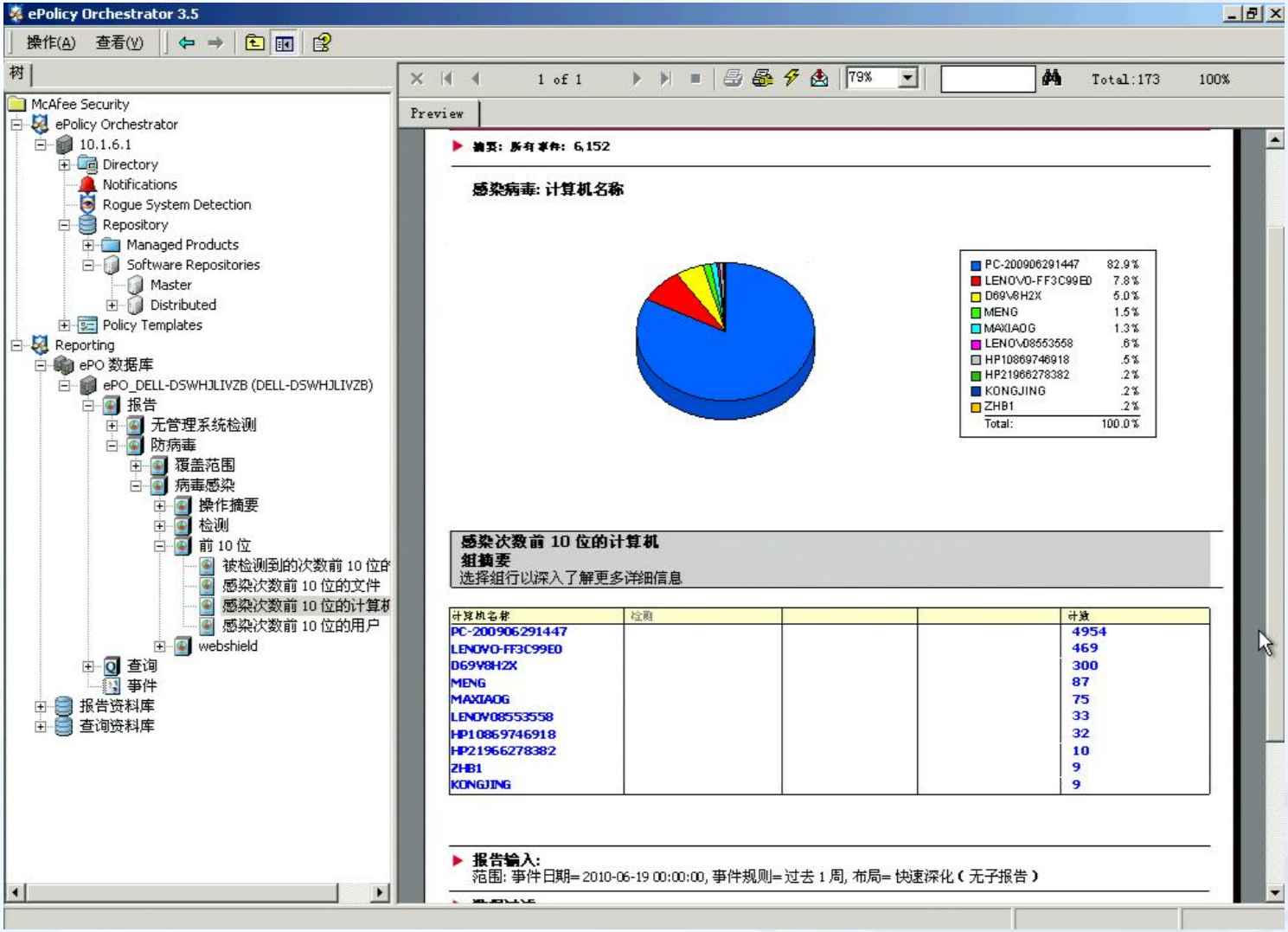
垃圾邮件过滤

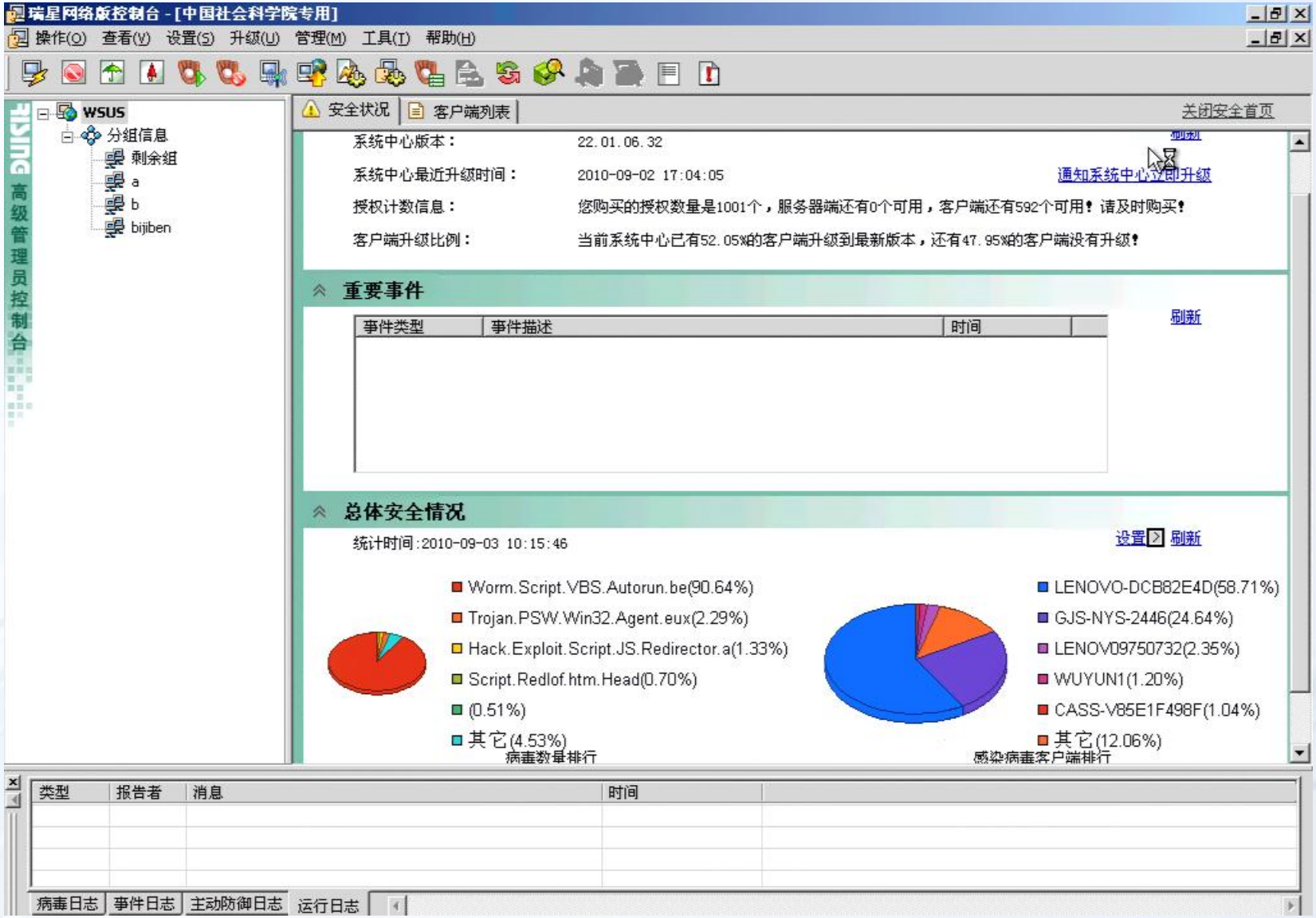

57200
52800
48400
44000
39600
35200
30800
26400
22000
17600
13200
8800
4400
17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
内容过滤数
行为模式识别数
IPS阻断数
实际收信数


网关过滤效果图
实际收信: 11.11%
IPS阻断: 5.14%
行为识别: 65.51%
内容过滤: 18.25%

终端防护
现状分析


Legend: 0-1 1-10 10-100 100-1000 1000+
Last updated: Jan 31 2010 4:00AM (Pacific Time)
View: All Viruses
Select Map: Worldwide
Track:
Infected Computers/Million Citizens
On Click: Zoom In
Time Period: Past 30 Days
MCAFEE


ePolicy Orchestrator 3.5
操作(A) 查看(V)
树
McAfee Security
ePolicy Orchestrator
10.1.6.1
Directory
Notifications
Rogue System Detection
Repository
Managed Products
Software Repositories
Master
Distributed
Policy Templates
Reporting
ePO 数据库
ePO_DELL-DSWHJLIVZB (DELL-DSWHJLIVZB)
报告
无管理系统检测
防病毒
覆盖范围
病毒感染
操作摘要
检测
前 10 位
被检测到的次数前 10 位的
感染次数前 10 位的文件
感染次数前 10 位的计算机
感染次数前 10 位的用户
webshield
查询
事件
报告资料库
查询资料库
1 of 1
79%
Total:173
100%
Preview
摘要: 所有事件: 6,152
感染病毒: 计算机名称
PC-200906291447 82.9%
LENOVO-FF3C99E0 7.8%
D69V8H2X 5.0%
MENG 1.5%
MAXIAOG 1.3%
LENOV08553558 .6%
HP10869746918 .5%
HP21966278382 .2%
KONGJING .2%
ZHB1 .2%
Total: 100.0%
感染次数前 10 位的计算机
组摘要
选择组行以深入了解更多详细信息
计算机名称 检测 计数
PC-200906291447 4954
LENOVO-FF3C99E0 469
D69V8H2X 300
MENG 87
MAXIAOG 75
LENOV08553558 33
HP10869746918 32
HP21966278382 10
ZHB1 9
KONGJING 9
报告输入:
范围: 事件日期= 2010-06-19 00:00:00, 事件规则= 过去 1 周, 布局= 快速深化 (无子报告)


瑞星网络版控制台 - [中国社会科学院专用]
操作(O) 查看(V) 设置(S) 升级(U) 管理(M) 工具(T) 帮助(H)
RISING 高级管理员控制台
WSUS
分组信息
剩余组
a
b
bijiben
安全状况
客户端列表
关闭安全首页
系统中心版本：
22.01.06.32
系统中心最近升级时间：
2010-09-02 17:04:05
通知系统中心立即升级
授权计数信息：
您购买的授权数量是1001个，服务器端还有0个可用，客户端还有592个可用！请及时购买！
客户端升级比例：
当前系统中心已有52.05%的客户端升级到最新版本，还有47.95%的客户端没有升级！
重要事件
刷新
事件类型
事件描述
时间
总体安全情况
统计时间:2010-09-03 10:15:46
设置
刷新
Worm.Script.VBS.Autorun.be(90.64%)
Trojan.PSW.Win32.Agent.eux(2.29%)
Hack.Exploit.Script.JS.Redirector.a(1.33%)
Script.Redlof.htm.Head(0.70%)
(0.51%)
其它(4.53%)
病毒数量排行
LENOVO-DCB82E4D(58.71%)
GJS-NYS-2446(24.64%)
LENOV09750732(2.35%)
WUYUN1(1.20%)
CASS-V85E1F498F(1.04%)
其它(12.06%)
感染病毒客户端排行
类型
报告者
消息
时间
病毒日志
事件日志
主动防御日志
运行日志

解决办法

1、杀毒软件统一管理

2、内部补丁分发

宣传教育

1、多渠道多样型宣传

2、常态化的教育

3、专业教育与基础教育相结合

规章制度建设

小结

THANKS