# 聚生网管 2008 使用说明

## 目 录

<i>—</i> ,	配置篇	2
	配置说明	2
二,	使用篇	4
	1、启动网络控制服务	4
	2、网络主机扫描	5
	3、修改主机说明	6
	4、带宽管理(流速管理)	7
	5、流量管理:	8
	6、P2P 下载限制	.10
	7、普通下载限制	.12
	8、网址控制	.13
	9、门户邮箱控制功能	.15
	10、聊天控制	.16
	11、ACL 访问规则	.17
	12、股票控制	. 19
	13、控制时间设置	.21
	14、应用策略	.22
	15、指派策略	.23
	16、控制策略设置	.26
	17、网络安全管理	.26
	18、网内其他主机运行聚生网管的纪录	.28
	19、局域网攻击工具检测	. 29
	20、如何注册软件	.32
	21、其他说明	.33

## 一、配置篇

配置说明

 第一次启动软件,系统会提示让你新建监控网段,请点击"新建监控网段",按照向导提示进行 操作。如配置1、配置2、配置3、配置4所示。

监控网段配置	
	新建监控网段
	编辑监控网段
	删除监控网段
	开始监控

配置 1-新建网段

段名称		
	监控网段配置	
書輸入新网段名称:		
VLARI		
		2月 一部助

配置 2-输入网段名称

网络无限 从此有序

	监控网段配置
网段选择对应的网卡:	
Realtek RTL8139 Fam	ily PCI Fast Ethernet NIC - 数据包计划程
IP地址:	192. 168. 0. 24
MAC地址:	00:0B:2F:03:DC:9C
子网掩码:	255. 255. 255. 0
网关地址:	192. 168. 0. 10
网关MAC地址:	00:11:95:CD:73:D6

配置 3-选择待监控网段网卡

监控	网段配置		-
、带宽:	自动检测		
	监控	监控网段配置	监控网段配置 带宽: <u>自动检测</u>

配置 4-选择监控网段出口带宽(自动检测)

## NetSense<sup>™</sup> 网络无限 从此有序

然后您可以选中刚刚建立的监控网段,双击或者点击"开始监控"按钮,进入 NetSense 主界面, 如配置5所示。

监控网段配置	
VLAN1 [Realtek RT18139 Femily PCT Fast Fthernet NTC]	新建监控网段
[192, 168, 0, 103-255, 255, 255, 0]	编辑监控网段
	删除监控网段
	开始监控

#### 配置 5-选择网段开始监控

依照上述方法,你可以建立多个网段。如果想监控第二个网段,请再次打开一个聚生网管的窗口, 从中选择你建立的第二个网段,然后点击"开始监控"。依次类推。

## 二、使用篇

#### 1、启动网络控制服务

点击软件左上角的"网络控制台",选择"启动网络控制服务"。

如果你想控制查看单个/全部主机的流速(带宽),请在"网络主机扫描"那里选择"控制全部主机", 然后点击"应用控制设置",这时所有的主机对应的上、下行带宽就可以显示了。

注意:这里虽然你控制了全部主机,但是只是让你查看带宽,并没有对主机进行其它的控制,如果 你想启用各种控制(如下载、聊天等),你需要为主机建立一个策略,并且指派给你想控制的主机或 者全部主机,只有指派策略的主机才能够真正被控制;此外,在选择"全部控制"时,确保你的局 域网没有在路由器或者防火墙进行 IP-MAC 绑定,否则可能影响到局域网电脑的公网访问。

网络无限 从此有序

🥻 聚生阿管2008专业版[68	3用户][网段名称:VLAN1]	- <b>D</b> ×
Welcom	e to Grabsun NetSense Control Center	<b>Grabsunsoft</b> 网络无限 从此有序
🗑 网络控制台	<ul> <li>● 主动引导模式</li> <li>○ 网关模式</li> <li>○ 网桥模式</li> <li>○ 旁路模式</li> </ul>	C 监视模式
🗾 网络主机扫描	启动网络控制服务 📉 查看网络流量实时图	控制日志查询
於 控制策略设置	限制 [bogon   192.168.0.30   00:30:18:A0:20:FC] P2P下载 (eMule (电骡 限制 [bogon   192.168.0.30   00:30:18:A0:20:FC] P2P下载 (eMule (电骡 限制 [bogon   192.168.0.178   00:30:18:AF:06:73] HTTP下载 (logo.mp3	))流量【策略:测试策略】20 ))流量【策略:测试策略】20 )流量【策略:测试策略】200
网络安全管理	限制【bogon   192.168.0.178   00:30:18:AF:06:73】WWW访问(voteview. 限制【bogon   192.168.0.178   00:30:18:AF:06:73】WWW访问(voteview. 限制【bogon   192.168.0.30   00:30:18:AO:20:FC】WWW访问(blog.sina.	auto, sina, com, cn/gi-bin/v sina, com, cn/gi-bin/votevi com, cn/inning11cn?action=
🕟 网络实用工具	限制 [bogon   192.168.0.30   00:30:18:A0:20:FC] WWW访问 (blog.sina. 限制 [bogon   192.168.0.178   00:30:18:AF:06:73] HTTF 下载 (forum/po 限制 [bogon   192.168.0.30   00:30:18:AO:20:FC] WWW访问 (blog.sina.	com.cn/hohcn?action=apply st.asp?forum_id=11method= com.cn/hohcn?action=apply
💝 软件配置		
🥥 软件激活		

#### 图 3: 启动网络控制服务

注:聚生网管 2008 版较之聚生网管 2.2 版,首次支持高达 5 种监控模式:主动引导模式、网关模式、 网桥模式、旁路模式、监视模式等。常规情况下,一般选择主动引导模式,也就是聚生网管传统的 "虚拟路由技术"。有关其它监控模式的说明,请向我公司索取技术白皮书。

#### 2、网络主机扫描

点击软件左侧功能栏的"网络主机扫描",你可以双击某个主机(如图 4,双击: 192.168.0.105)为 这个主机建立一个控制策略(也即上网权限),输入策略名字,然后系统会弹出一个对话框,你可以 按照控制需要点击各个控制项目(如流量控制、网址控制、聊天控制、网络游戏、带宽控制、时间 控制等等)进行控制,对每一个控制项目设置后,必须保存。如图 4、图 5

网络无限 从此有序

	目户][网段名称:vLAN1] e to Grabsun NetS	ense C	ontrol Cer	iter	<u>_</u> ロメ <i>Grabsunsoft</i> 网络无限 从此有序
😡 网络控制台	1 月描网络主机	90]	全部控制	全部取消控制	间 👔 应用控制设置
🔝 网络主机扫描	IP地址	主机说明	主机	上行帯宽(	108/S)   下行帯宽(108/S)   !
0		控制机		0.00	0.02 (
🔨 控制策略设置			CHEN	0.00	0.00 (
<ul> <li>网络实用工具</li> <li>软件配置</li> </ul>					
欽件激活					
		<b>• - - -</b>		Autor	Þ
	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	📕 不活动	王祝L 🙎	』 彼断附王机	
		峞	と行帯宽: 0.	00 KB/S ,분	3下行带宽: 0.02 KB/S

图 4: 双击某个主机建立一个控制策略

## 3、修改主机说明

注: 有时候主机名字无法显示,你查看常见问题进行设置; 也可以右键单击主机选择"修改主机说明"为他们指定一个名字。

网络无限 从此有序



图 5: 设定要各个控制项目

## 4、带宽管理(流速管理)

首先选择"启用主机带宽管理",然后分别设定上行、下行带宽,可以控制这台主机的公网带宽(也即公网数据流速);选择"主机带宽智能控制",然后分别设定上行、下行带宽,可以对这台主机的带宽进行智能控制,即发现其进行"BT、电驴"时,系统就会自动限制这台主机的带宽到你设定的上行、下行带宽范围内,从而有效地避免了因为 P2P 下载对网络带宽的过分占用。如图 6

网络无限 从此有序

编辑策略[员工策略]的内容	X
NAN AN	│ 💞 ACL 规则 │ 🔯 时间设置 │ ↓↓ 流量限制   😋 普通下载限制
── 启用主机公网带宽限制 ─────	
请设定被控主机上行带宽限制	不限制 <15K
请设定被控主机下行带宽限制	(20K (25K (30K
主机带宽智能抑制	<40K <50K ≪60K
□ 启用发现P2P下载时自动限制该主机带宽功能	<70K <80K <90K
请设定发现P2P下载时该主机上行带宽限制:	<100K <150K <200K
请设定发现P2P下载时该主机下行带宽限制:	く300K 11992前3
帯宽精确控制	
▶ 精确控制带宽(此项对上述两项均有控制)	
-	确定 取消

图 6: 设定带宽管理

注:

1.如果"请设定被控主机上行带宽"和"请设定被控主机下行带宽"设置的数值过小,就会 影响 电脑基本的上网速度,因为网站访问的原理也是将一个网站下载到本地。建议设置:上行不低于 50KB,下行不低于 100KB。

2. "精确控制带宽",此设置的完全生效,需要进行其他简单设置,具体方法联系本公司技术支持, 单独勾选此项也能一定程度上提升带宽控制的精确性。

#### 5、流量管理:

系统不仅可以控制局域网任意主机的带宽,即流速,还可以控制局域网任意主机的流量。如上图 6, 打开"流量限制"对话框,你可以为这个主机设定一个公网日流量或上行、下行日流量,超过此流

**NetSense<sup>™</sup>** 网络无限 从此有序

量,系统就会自动切断这台主机的公网连接,即禁止其上网;同时,你也可以指定每日的某个时间, 自动清空流量,这样次日就会从零开始,重新计算流量了。如图 7:

编辑策略[员工策略]的内容
🏾 🌇 游戏限制 📗 🎆 股票限制 📗 🔧 聊天限制 📗 🛷 ACL 规则 📗 🔯 时间设置 🗋 🧀 网络限制 🔤 带宽限制 💐 P2P下载限制 🚺 流量限制 🚺 普通下载限制
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
④ 总流量限制 ○ 上下行流量分别限制
总流量限制 ————————————————————————————————————
请设定毎日总流量限制: 0 (M)
上下行流量限制
诸设定毎日上传流量限制: 0 (M)
请设定毎日下载流量限制: 0 (M)
流量自动清空时间
毎天 0:00:00 🕂
主机公网流量限制仅在本策略所设定的时间范围内生效,如果在策略所设定的 时间范围内流量超标,系统将会自动断开该主机的公网连接。而对于被控主机 在本策略所设定的时间范围外所产生的流量仅进行统计,不再进行自动阻断。
确定

图 7: 设定主机总流量(如: 150M)

此外,你也可以在左侧"网络主机扫描"里面,实时查看这台主机(192.168.0.105)当日的某一时 刻累计用了多少流量,如图 8

网络无限 从此有序

📓 聚生网管政府专用版[20用户	][网段名称:VLAN1]			_ <b>_</b> X
Welcome to	o Grabsun NetS	Sense Control	Center	<b>Grabsunsoft</b> 网络无限 从此有序
	🤍 扫描网络主机		🐑 全部取消控制	🔊 应用控制设置
📕 网络主机扫描	上行帯宽(KB/S) 1 0.00 0	下行带宽(KB/S)   MAC地 0.00 00:0E	址 指派策略 :2F:03:DC:9C 未指派策略	日流量(M) ↓ 0,00
<u> 控制策略设置</u>	0.00	0.00 00:16 0.00 00:30	:36:3C:C9:79 员工策略 :18:AF:06:73 未指派策略	0.00
网络安全管理				
💦 网络实用工具				
💝 软件配置				
🙆 软件激活				
	▲ 活动主机	📕 不活动主机	📕 被断网主机	•
	网络主机数: 3	■■ 1,11-30上01 总上行带宽	: 0.00 KB/S 总1	「行带宽: 0.00 KB/S

图 8: 查看主机日流量实时累加

注:你可以单击右键,可以清空当前或者全部主机的流量。

## 6、P2P 下载限制

打开 "P2P 下载限制"对话框,在这里,你可以选择要禁止的各种 P2P 工具,如 BT、电驴、PP 点 点通、卡盟等等,你可以单独选择控制某个 P2P 工具的下载,又可以选择控制全部;但是现在由于 很多 P2P 工具交叉采用其他工具的传输方式,所以为了更有效的封堵,系统默认将会控制所有的 P2P 下载;本系统目前可以控制几乎所有流行的 P2P 下载工具和 P2P 视频工具。 如图 9:

NetSense<sup>™</sup>

网络无限 从此有序

编辑策略[测试策略]的内容	X
<ul> <li></li></ul>	
☑ 启用P2P下载限制	
▶ P2P下載主动防御 □ P2P站点智能拦截	
☑ P2P下载协议拦截 □ P2P下载链接控制	□ P2P下载常规控制
eMule(电骡) eDonkey(电驴) Poco/PP点点通 Kamun(卡盟) 迅雷多点(本选项限制迅雷多点下载) Vagaa(哇嘎画时代) Kugoo(酷狗) Baidu下吧 BitSprit(比特精灵) #Torrent 百宝	
PPVOD (PP点播) PFStream (PPS网络电视) QQLive (QQ直播) ViviPlay (TVKoo网络电视) UUSee (悠视网网络电视) CoolStreaming	
□ P2P强制抑制技术(请慎用!)	
	确定 取消

图 9: 控制 P2P 下载

注 1: 聚生网管 2008 较之于聚生网管 2.2,首创了对 P2P 工具的"六层分层过滤"技术,这样管理员可以根据自己的需要,选择过滤的强度;一般选择"P2P 下载主动防御"和"P2P 下载协议拦截"就可以封堵 P2P 下载工具和 P2P 视频工具 80%以上的流量;如果你想对各种 P2P 工具进行更严格的封堵,你可以选择全部过滤层;但是由于过滤层的增加,在封堵力度加大的情况下,也可能对网速有一定的影响。"P2P 强制抑制技术"是在六层过滤之外,进行的智能强化识别并拦截的技术,但又可能误封一些正常的网络应用,故此审用。

注 2: 因为"迅雷"是一种多点 HTTP 下载,应用 HTTP 协议而不是 P2P 协议。这里限制"迅雷"下载,是禁止它从多个服务器进行多点下载,但不能禁止"迅雷"从单个服务器下载。但是因为即使从单点下载速度也可能很快。所以,如果想完全禁止"迅雷"下载,你还需要在"普通下载限制"中禁止相应文件类型的 HTTP 下载;或者启用"严格禁止 HTTP 下载"。除迅雷外的所有其它 P2P 工具,系统都可以完全拦截。

## 7、普通下载限制

打开"普通下载限制"对话框,在这里,你可以限制所有的 HTTP 下载和 FTP 下载。限制 HTTP 下载可以输入文件后缀名限制相应格式的文件下载,也可以选择"严格禁止 HTTP 下载"从而禁止一切 HTTP 下载;而限制 FTP 下载,你既可以输入文件后缀名来进行限制,又可以直接输入通配符"\*",来禁止所有的 FTP 下载。如图 10:

编辑策略[员工策略]的内容
💽 游戏限制 📗 🎆 股票限制 📗 🖄 聊天限制 🛛 🤣 ACL 规则 📗 🔯 时间设置 🗋 🧽 网络限制 🔤 带宽限制 🗳 P2P下载限制 🚺 流量限制 🙆 普通下载限制
HTTP下载
☑ 追用普通HTTP下载限制 编辑限制文件后缀名
选中后将拦截HTTP下载文件,你可以指定需要拦截的文件后缀名
□ 严格禁止HTTP下载
选中后将拦截所有HTTP下载,此功能会部分增加系统负担,请根 据系统性能决定是否使用
FTP下载 ————————————————————————————————————
□ 启用FTP下载限制 编辑限制文件后缀名
□ 启用FTP上传限制 选中后将拦截FTP下载文件

图 10-1 选择"启用普通 HTTP 下载限制"

网络无限 从此有序

rm	添加
прЗ	
ar 	
exe crh	

图 10-2: 添加文件后缀名

注: 文件后缀名的添加,一定是".EXE"的形式,就是"点 exe",不能直接添加"exe";另外,添加完成后,一定点"确定",否则可能无法保存。

#### 8、网址控制

打开左上角的"网络限制"对话框。在这里你既可以完全禁止局域网主机的公网访问,又可以为局 域网主机设定黑、白名单以及股票、色情等网址。系统还可以防止局域网主机启用代理上网或充当 代理,同时还可以记录局域网主机的网址浏览。如图:11

网络无限 从此有序



图 11: 网址控制

**注**1: "启用高级网络控制"以及"启用主机强制隔离功能"这两个功能可能会对系统造成一定的负荷,非紧急情况,请慎用。

注 2: 系统提供了精确的网址控制功能,通过通配符,你可以控制局域网主机只可以访问某一个网站及其所有的二级页面,也可以只把某个网站的某一个频道设置为白名单,你也可以把一个单一的网页设置为白名单。局域网主机只能访问设置为白名单的网址。同理,你也可以设置为黑名单来控制局域网主机的公网访问。如图 12: www.sina.com.cn 表示只可以访问新浪网的首页;\*.sina.com.cn\*,表示整个新浪网都可以被访问; tech.sina.com.cn\*则表示局域网主机只可以访问新浪网站的"科技频道"的所有页面。此外,系统支持对网址的导入、导出功能,可以方便地让你增加大量的网址进行

网络无限 从此有序



图 12: 网址精确控制功能

## 9、门户邮箱控制功能

鉴于许多中小企业没有自己独立的企业邮箱,系统提供了对门户网站邮箱的特殊许可功能。即你进行了网址控制设置,但是可以允许员工进行使用门户网站的邮箱。比如,你禁止了局域网主机访问 新浪网址(可以把新浪网站作为黑名单或者完全禁止局域网主机访问公网),只要在这里选择许可使 用新浪网的邮箱(普通邮箱、企业邮箱、VIP邮箱等),则员工仍然可以访问新浪网的首页,并且登 陆邮箱进行收信、发信等等对邮箱的所有操作,但是不可以点击新浪网站的其他任意连接,包括信 箱里面的所有连接。如图 12:



网络无限 从此有序

编辑[员工策略]内容	ş			X
🔜 带宽限制 🔰	↓流量限制 门户邮箱	🤤 P2P下载限制 聊天限制	」 ) <mark>〇</mark> 普通 《 <b>3</b> ACL规则	下载限制   <mark>②</mark> 时间
在您对₩₩₩访问进 了常用门户网站邮箱 新浪邮箱,请对应说 任何其他的新浪链热 下面列表中为系统 包括在内,那么请然 □雅虎中国门户邮 163门户邮箱 □163门户邮箱	行了限制的同时, 值的特殊设置,例如 也中新浪邮箱即可 度。 统默认提供的常见 强购买正式版,我们	为了方便企业说 回您限制了主机系 ,则被控制主机系 门户网站邮箱, 门将会为您定制的	5 何门户网站邮箱 时新浪的访问但是 只能访问新浪邮箱 如果您需要使用的 您所需要使用的	着,系统提供 是仍然想使用 首而不能打开 的邮箱尚未 顺箱。
			确定	取消

图 13: 门户邮箱控制

10、聊天控制

打开"聊天限制"对话框,系统可以控制局域网内的任意主机登录使用各种聊天工具,系统可以完 全封堵 QQ、MSN、新浪 UC、网易泡泡等。如图 13:

网络无限 从此有序

编辑策略[员工策略]的内容	×
网络限制 〒 電 帯宽限制 学 P2P下载限制 游戏限制 〒 服 股票限制 3 聊天限制	│ 👍 流量限制 🛛 💍 普通下载限制 🗎 │ 💞 ACL 规则 📔 🔯 时间设置 🗋
☑ 禁止♀♀聊天	件
☑ 禁止MSX聊天	文件
☑ 禁止阿里旺旺聊天	
☑ 禁止网易泡泡聊天	
☑ 禁止新浪uc聊天	
☑ 禁止Yahoo聊天	
☑ 禁止Skype聊天	
☑ 禁止AIM (ICQ)聊天	
☑ 禁止搜Q聊天	
☑ 禁止IRC聊天	
	确定

图 14: 禁止聊天工具

11、ACL 访问规则

ACL 访问规则、股票软件控制、游戏软件控制(因为三者原理类似,故在此一并阐述)

打开 "ACL 规则"对话框,在这里你可以设定要拦截的局域网主机发出的公网报文。 借助 ACL 规则,你可以禁止局域网任意主机通过任意协议、任意端口、访问任意 IP。这样你可以拦 截局域网主机如:网络游戏在内的任意公网报文。添加 ACL 规则:如入规则名字:"边锋网络游戏 世界",本地 IP 选择"任意",目标 IP 选择"任意",协议选择"TCP",端口选择"4000"。这样就 可以禁止局域网所有主机连接"边锋游戏"。如图 14:

网络无限 从此有序

新规则信息输入—————		
请输入规则名称:		边锋网络游戏世界
<b>请指定源地址类别:</b>		任意
0 1 0 1 0 1 0	到	0 . 0 . 0 . 0
请指定目标地址类别 <b>:</b>		任意
0 4 0 4 0 4 0	到	
请指定协议类型 <b>:</b>		TCP

图 15-1: 添加 ACL 访问规则

注: 正式版会提供当前所有流行的网络游戏 ACL 规则列表。通过 ACL 规则列表,你可以禁止局域 网主机玩当前几乎所有流行的网络游戏,并且 ACL 规则列表实时更新。

## 12、股票控制

首先点"股票控制"

编辑策略[员工策略]的内容	×
🧀 网络限制 🔤 带宽限制 🗐 🧐 P2P下载限制 🚺 流量限 🌉 游戏限制 🛛 🚮 股票限制 🛛 🖄 聊天限制 🛛 🤣 ACL	制 🛛 🖄 普通下载限制 🗍 规则 📗 🔯 时间设置 🛔
	]
股票软件名称	-
	增加股票软件
	修改股票软件
	删除股票软件
	清空列表
	导入股票规则
	导出股票规则
确定	取消

图 15-2 启用股票控制

然后点"增加股票软件",在"软件名称"那里输入名字:

网络无限 从此有序

			×
软件么称:	1		 确定
-2011-011-011-0	ŀ		取消
┌IP/端口列表-			 
IPt地址		端口	
		1997	
			増加
			修改
			删除

图 15-3 增加股票控制

然后点下面的"增加",在 IP 那里输入股票软件的服务器 IP,在 port 那里输入相应的端口,然后点"确定"关闭此对话框。然后再点上图的"确定"按钮,至此我们就增加了一个股票软件的控制。

IP/Port						×
					确	定
IP:	0	. 0	. 0	. 0	取	消
Port:	0					

#### 图 15-4 增加 IP 和端口

注 1: 股票软件的控制,不需要指定被控电脑,凡是应用此策略的局域网电脑都将被禁止访问股票 服务器的 IP 和端口;游戏软件的控制方法与原理与此相同。

注 2: 正式版我们会提供当前所有的股票、游戏软件列表,你可以应用导入功能,全部实施控制;

同时,建议客户不要导入过多,否则将会影响电脑的网络访问速度和系统的负荷。

#### 13、控制时间设置

打开"时间"对话框,你可以设置控制时间。你既可以设定控制全部时间(以蓝色表示),又可以设定控制工作时间(早9:00-17:00)。系统默认控制全部时间,你可以右键点击取消,然后选择"工作时间",也可以不设定控制时间。但是如果希望所有的控制项目生效,则必须选择控制时间。如图 16:



图 16: 控制时间设置

注:选择控制时间时,必须根据星期几和时刻来确定。比如你想控制星期一的10点~10点半;如果 是星期三的下午1点-2点之前。你应该这样选择,如下图所示:

网络无限 从此有序



所有控制项目设置后,必须选择保存或确定。至此,我们建立了一个完整的控制策略。

#### 14、应用策略

建立好策略后,你可以在"网络主机扫描"里面,双击其他"未指派策略"的主机指派已经建好的 策略,也可以再建一个新的策略。如图 17,双击: 192.168.0.104 系统会提示你已经建立了一个策 略,你可以选择继续新建一个策略,又可以选择选择否,而直接指派你刚才建立的策略,或者仍旧 保持"未指派策略"状态。如果你选择否,则系统就会弹出一个新的对话框。如图 17、18:

网络无限 从此有序

🚺 聚生阿管政府专用版[123用]	户][网段名称:VLAN1]	<u> </u>
Welcome to	o Grabsun NetSense Control Center	<b>Grabsunsoft</b> 网络无限 从此有序
🚱 网络控制台	🤍 扫描网络主机 👻 全部控制 👻 全部取消控制	应用控制设置
🗾 网络主机扫描	□ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	下行带宽 (KB/S)   MAC±
0	192.168.0.101 控制税 grabsun 0.00	0.00 00:0
🤨 控制策略设置	□ 192.168.0.112 E8A7BA54 0.00	0.00 00:3
网络安全管理		
💦 网络实用工具	<u>兼生</u> 网管	
🍚 软件配置	《2》 您已经定义过策略,现在继续新建一个策略吗?	
🧼 软件激活	<u> </u>	
	📙 活动主机 📰 不活动主机 関 被断网主机	
	│ 网络主机数: 3 总上行带宽: 0.00 KB/S 总下	「行帯宽: 0.00 KB/S

图 17: 新建或指派策略

<b>长指派策略</b>	▼ 确定
5工策略 2指派策略	取消

图 18: 指派已建策略

## 15、指派策略

如果你想对所有的主机或者一部分主机都应用同一个策略,请在软件左侧功能栏的"控制策略设置" 里面选择"指派策略"。如图 19

网络无限 从此有序

📓 聚生阿管政府专用版[20用户]	[网段名称:VLAN1]	
Welcome to	Grabsun NetSense Control Center	<b>Grabsunsoft</b> 网络无限 从此有序
<ul> <li>网络控制台</li> </ul>	<b>《</b> 员工策略	新建策略           编辑策略
网络主机扫描 经制策略设置		重命名策略           删除策略
网络安全管理		指派策略
💦 网络实用工具		
♀ 软件配置		
🥥 软件激活		

图 19: 指派策略

点击后会弹出一个窗口,左右两侧分别为已经指派策略的主机和未指派策略的主机,你可以把其中的一个已经建立好策略的组或未建立策略的组里面的所有主机,全部指派到右侧的某个策略组里面或未指派的策略组里面;你也可以选择某一个或几个(按住 shift 选择)已经指派策略的组或者未指派的组里面的主机,指派到右侧的某一个已经建立的组或未建立的组里面;右侧的同样也可以指派到左侧的组里面。这样的转换是为了让管理员可以根据情况对不同的主机灵活分配上网权限。转换后可以立即生效。如图 20、21、22



网络无限 从此有序

选定策略:		<b>诘选定策略</b> :		
员工策略 《经被指派为选定策略的主机:	•	经理策略 已经被指派为选定第	5略的主机:	
IP地址   主机名		IP地址		
92.168.0.101 GRABSUN1	选中>	192.168.0.103	GRABSUN3	
	《选中	Ī		
	(公会部)			

图 20: 将员工策略组里面的主机指派到经理策略组里面

略指派设置					
<b>唐选定策略:</b>			<b>诘选定策略</b> :		
经理策略		•	员工策略		•
已经被指派为选定第	<b>策略的主机:</b>		已经被指派为选定第	<b>策略的主机:</b>	
IP地址	主机名		IP地址	主机名	
192, 168, 0, 103	GRABSUN3	选中>	192. 168. 0. 101	GRABSUN1	
		《选中			
		全部>>	1		
		(《全部			
			L		

图 21: 将经理策略里面的主机指派到员工策略组里面

网络无限 从此有序

选定策略 <b>:</b>			<b>语选定策略</b> :		
卡指派策略			员工策略		
经被指派为选定第	5略的主机:		已经被指派为选定第	6略的主机:	
IP地址	主机名		IP地址	主机名	
	GRABSUN4 加速計	选中>	192.168.0.101	GRABSUN1	
192. 168. 0. 106	GRABSUNG	《选中	1		
			1		
			-		
			1		

图 22: 将全部未指派策略的主机添加到员工策略组里面(如果选择部分,可用 shift 选中)

注 1: 当对已经建立好的策略进行更改时,则所有应用此策略的主机都将自动会相应更改,无需一一设置。比如,你可以双击某个已经应用"员工策略"的主机,对策略重新进行设置,则"网络主机扫描"里面所有应用"员工策略"的主机将会全部自动更新为最新的策略配置,不需要全部重新指派或者一一修改。

注 2: 系统默认不控制"控制机"本身,所以无论是新建策略还是指派策略,都不需要对控制机本 身进行设定;如果强行设定,还可能增加系统自身的负荷。

#### 16、控制策略设置

点击软件左侧功能栏的"控制策略设置",点击"新建策略",输入策略名字,然后系统会弹出一个 对话框,你可以按照控制需要点击各个控制项目进行控制。设置完毕后,选择保存。你也可以选中 编辑好的策略进行更改配置。操作如上述所示。

#### 17、网络安全管理

在这里,你可以设置 IP-MAC 绑定。首先点击"启用 IP-MAC 绑定",然后你可以点击"获取 IP-MAC 列表"。你也可以进行:主机名、IP、网卡的三重绑定。你也可以单机 IP、网卡进行更改,也可以手 工添加、删除等操作。另外,绑定 IP 之后,你也可以选择下面的两个控制措施,如:"发现非法 IP-MAC 绑定时,发送禁止消息"以及"发现非法 IP-MAC 绑定时,断开改主机公网连接"等等。如下图 23:

网络无限 从此有序

🥻 聚生阿管政府专用版[20用户	][网段名称:VLA 🖁	i 🛛 🛼 😰 👯			
Welcome to	Grabsun Ne	etSense Cont	rol Center		<b>Grabsunsoft</b> 网络无限 从此有序
	□ 启用IP-MAC地	址绑定			
	主机名	IP地址	MAC地址	主机	获取IP-MAC关系
🗾 网络主机扫描		192. 168. 0. 101 192. 168. 0. 100	00:0B:2F:03:DC:9C 00:16:36:3C:C9:79		手工添加绑定
校制策略设置		192. 168. 0. 159	00:30:18:AF:06:73		删除选中绑定
<u> </u>					<u>清空全部</u> 绑定
● 网络安全管理					
📝 IP-MAC绑定					
📔 网内其他运行记录					
💦 网络实用工具					
♀♀ 软件配置					
🙆 软件激活	•			Þ	
	🗌 🗌 自动发现新主机	机并进行绑定			
	│□ 发现非法IP-M/	AC绑定时,发送禁止消	息: 为了系统安全,请不要	随意修改	QIP,你的默认IP为%s
	□ 发现非法IP-M/	AC绑定时,断开该主机	这网连接		
					保存配置

#### 图 23: 进行 IP-MAC 绑定

注:如果你的局域网已经进行了 IP-MAC 绑定,请首先取消,否则可能导致局域网暂时掉线,并可能导致软件的一些功能失效;如果你的局域网没有进行 IP-MAC 绑定,你可以选择上述各项,以增强网络安全;如果你的局域网对安全要求不高,也可以不选。

关于 IP-MAC 绑定的使用说明:

1、如果选择了"自动发现新主机并自动绑定",那么在这种情况下,软件一旦扫描到新主机,就可 以将它们加入到 IP-MAC 表里面,并且自动进行了绑定,这样当局域网初次部署本软件的时候,在 局域网的电脑陆续开机的情况下,软件会陆续将局域网的电脑自动加入进来并自动进行绑定,最终 实现全部绑定;当然你也可以选择手工添加的方式,增加绑定关系,点"手工添加绑定",输入 IP 和 MAC 地址即可;此外,你也可以点"获取 IP-MAC 关系"这样软件就会获取当前所有主机的 IP-MAC 对应关系,但是局域网的电脑一般不会同时全部开机,所以你需要在全部开机的情况下,再次点此 按钮,这样陆续最终会全部加入进来,但是你还要点右下角的"保存配置"才能生效,而在"自动 发现新主机并自动进行绑定"的情况下,软件会自动保存并生效。

2、在通过软件将局域网电脑的 IP-MAC 绑定的情况下,局域网主机私自更改 IP 或者 MAC 后,软件 就会通过浏览器向其发送禁止消息,迫使其改回;如果你想绑定其修改后的 IP 或者 MAC,则可以 通过点"获取 IP-MAC 关系"来更新数据,直接覆盖即可;如果不覆盖,则维持以前的绑定关系, 被控电脑必须改回原来的 IP 才可以上网。



图 24: IP-MAC 绑定

## 18、网内其他主机运行聚生网管的纪录

系统为了保证局域网的安全,防止局域网内其他用户用聚生网管扰乱局域网,特别提供了防护功能: 即聚生网管的正式版可以强制测试版、新版本聚生网管将会强制以前版本退出,并且纪录运行聚生 网管的主机的机器名、运行时间、网卡、IP、以及系统对其处理结果情况。如下图 24:

网络无限 从此有序

Welcome to	Grabsun NetS	ense Contro	ol Center	网络	无限 从此有
网络控制台	局域网内其他主机运行	<b>う本软件发现记录</b>		强制试用版退出!	
	时间	IP地址	主机名	网卡地址	处理结果
网络主机扫描	2008-3-18 23:08:42	192.168.0.104	XU	00-30-18-A0-20-FC	系统已经强
)	2008-3-18 23:10:46	192.168.0.30	XU	00-30-18-A0-20-FC	系统已经强
控制策略设置	2008-3-18 23:28:01	192.168.0.30	XU	00-30-18-A0-20-FC	系统已经了
网络安全管理					
📝 IP-MAC绑定					
🚺 网内其他运行记录					
网络实用工具					
软件配置					
软件激活					

图 25: 强制局域网内试用版退出

注:强制试用版退出功能默认是生效的;但是你也可以不勾选此功能,则就不会强制试用版退出了。 此功能不会强制以前的正式版退出,但是会纪录是那台电脑在运行以前的正式版,并且可以详细记 录相关信息。

## 19、局域网攻击工具检测

系统可以检测当前对局域网危害最为严重的三大工具:局域网终结者、网络剪刀手和网络执法官,因为这三种工具采用 windows 的底层协议,所以,无法被防火墙和各个杀毒软件检测到。而聚生网管可以分析其报文,可以检测出其所在的主机名、IP、网卡、运行时间等信息,以便于管理员迅速采取措施应对,降低危害;同时,系统集成了"增强性主动管理工具",可以将局域网内危险电脑进行完全的隔离,被隔离后的电脑既不能访问公网,又不能访问局域网,也不能被局域网内的其他电脑所访问,从而最大限度地保证内网的安全。如图 26:

网络无限 从此有序



## 图 26-1: 检测局域网三大攻击工具

网络无限 从此有序

🎇 聚生网管増强	生主动管理工具		×
┌ 请输入被控申	脑的相关参数		
IP地址:		强制隔离	
用户名:	admin	取消隔离	
密码:		获取主机信息	
- 主机信息 -			
		<b>_</b>	

图 26-2 聚生网管增强性主动管理工具

注:"聚生网管增强性主动管理工具"此功能过于强大,极容易被黑客和不法分子用来恶意破坏局域 网,故而此功能在试用版和标准版均不提供,同时我们也不公布此工具的使用方法,购买集团公司 专用版和政府专用版的客户,可以向我们公司索要使用方法。

## 20、软件配置

在软件配置里面,聚生网管 2008 增加了很多极富创意的功能:

网络无限 从此有序

		Grabsunsof
Welcom	e to Grabsun NetSense Control Center	网络无限 从此有所
<u>)</u>	系统设置	
网络控制台		
9 网络主机扫描	\$X1年启初设直 Language Select: English ▼	
2 控制策略设置	<ul> <li>□ 电脑启动时自动运行</li> <li>选中后电脑重新启动</li> <li>□ 软件运行即转为控制状态</li> <li>选中后软件启动将自</li> </ul>	时软件会自动运行 动转为控制状态
网络安全管理	<ul> <li>□ 监控意外中断时自动重新加载选中后软件实现不间</li> <li>□ 软件运行一段时间后自动释放内存</li> <li>4 ➡ 小时(</li> </ul>	断全自动监控(下次启动软( 例如:4小时)(下次启录
9 网络实用工具	<ul> <li>□ 定时自动关机 18 → 点 0 → 分下次启动4</li> <li>托盘图标设置</li> </ul>	次件将在此时停止监控并自动 
软件配置	▶ 最小化到任务栏图标不勾选此项软件最小化时隐藏到	创后台,需热键唤出(默认热镜
文字 软件 激活	请您在右侧框中按下热键 无	
	空時保护 「 哈出时変码保护 法输入家码・	面次輪λ 家码:
	□ 程序关闭时密码保护 (注:哈出密码输入窗口与呼出:	
	软件CPU占用设置	
	软件运行CPU占用设定 效率高(CPU占用高) ▼	]
	监控定时更新时间 1 秒 隔离强度:	50 (建议不要超过50)
	· · · · · · · · · · · · · · · · · · ·	1.2 International Activity (ACAS) (ACAS)

图 27: 聚生网管 2008 软件配置

在这里你可以勾选:

1、"电脑启动时自动运行":勾选此项后聚生网管系统会随电脑一起启动;如果你同时选择"软件运行即转为控制状态"则聚生网管系统则自动转入控制状态,并且自动监控第一个网段,如果你有两个或者以上网段,则你需要手工选择其他网段。

2、监控意外中断时自动重新加载:当聚生网管系统因为自身或者操作系统等原因而意外停止监控时,则通过系统的"进程守护",就会自动重新启动软件,并且可以自动转入控制状态(需勾选"软件运行即转为控制状态")。从而可以实现软件在无人值守情况下的不间断、全自动监控。

3、"软件运行一段时间后自动释放内存":勾选此项后,则聚生网管系统则在你设定的时间后,自动 释放占用的内存,从而可以防止软件在长期运行的情况下对内存的过量占用,从而可以保证系统的 长期、高速运行,防止由于内存占用过多导致的软件运行效率的降低。

4、定时自动关机功能:勾选此项后,软件就会在指定的时间自动停止监控并且自动关闭 windows 操 作系统,从而可以实现软件的智能工作;同时,我们还提供客户定时开机,并且自动转入控制状态 的功能,从而可以极大地降低网管人员的手工操作,提升网络管理的效率和自动化程度。

## 21、如何注册软件

A、针对聚生网管 2.10 版本(注,此版本无法支持 SCSI 硬盘)

点击软件左侧右下角的"软件购买"里面的"软件购买",然后点击"我要购买,享受更多功能", 系统就会弹出注册框,将机器码发送到聚生科技,确认并汇款完毕后,聚生科技提供注册码。如下 图 26

网络无限 从此有序

【紫生网官专业版[256用户	'[[ 内段名称:VLAN1]	
	te Oerteen NetOeree Oerteel Oertee	Grabsunsoft 网络王明 川北方南
Welcome	e to Grabsun NetSense Control Center	№47℃胶 从此有序
	版本信息	
<b>一</b> 网络控制台	版本号: 聚生阿管2008版 Build20080315	
🛃 网络主机扫描	版本类别: 专业版[256用户]	
🄀 控制策略设置	联系方式	
网络安全管理	北京聚生科技有限公司	
💦 网络实用工具	公司主页: http://www.grabsun.com	
💡 软件配置	联系邮箱: grabsun@vip.163.com	
🙆 软件激活	● 联系电话: 010-85411818	
	点 工 做 酒	
	D41D8CD98F00B204E9800998ECF8427E	获取注册号
	请在下面的输入框内输入软件激活序列号	
		一元成微活
	注:如果你用的是2.1及其以前的版本,则购买后需要将此机器码发送 的序列号(试用版无需注册);如果是2.2及其以后的版本,则通过加	送至我公司信箱,索取正式 吅密狗激活,无须激活了。

图 26: 软件激活

B、针对聚生网管 2.2 及其以后的新版本

聚生网管 2.2 及其以后新版本将采用国际顶级的加密狗进行加密,从而方便了用户的激活和随时使用,也保证正式版的安全。

## 22、其他说明

聚生网管 2.2 集成了很多非常使用的功能,如:右键强制断网功能、自动清空所有或全部主机流量 的功能、软件唤出或退出的密码保护功能、控制频率设置、隔离强度设置、多语言设置等等功能, 由于非常简单,在此不再一一阐述。

如仍有其他未尽事宜,请联系本公司。

## 联系我们

#### 北京聚生科技有限公司

- 地址:北京市海淀区东北旺西路8号中关村软件园3号楼201-203室
- 邮编: 100085
- 网址: http://www.grabsun.com

http://www.grabsun.com.cn(备用站点)

http://www.grabsun.cn(备用站点)

- 电话: 010-85411818 010-86630101 010-86630058
- 传真: 010-58874140
- Email: grabsun@vip.163.com
- MSN: <u>sale@grabsun.com</u>