中神通
TrustComputing

UTMWALL 网关
管理员手册

武汉中神通信息技术有限公司

版权说明

第三方信息

本文档中所涉及到的产品名称和商标，属于各自公司或组织所有。

武汉中神通信息技术有限公司
Wuhan TrustComputing Information Technology Ltd.， Co.
湖北省武汉市武昌区民主二路 22 号
No.22 Minzhuer Road， Wuchang District， Wuhan， Hubei， P.R.China
电话（TEL）：+86(027)87737510
传真（FAX）：+86(027)87737512
电子信箱（Email）：support@trustcomputing.com
网站（WebSite）：www.trustcomputing.com.cn

架构安全网络—武汉中神通

目录

概述

A 功能简介

UTMWALL®网关的功能按菜单布局分为系统管理、访问控制、应用过滤、入侵检测与防御、远程接入等 5 个模块；按目的属性分为功能设置和状态统计等 2 大系列。

功能设置的过程一般是先确定网卡接入方式（NAT、网桥、路由等），再进行具体安全策略的设置，可以从“初始设置”功能起步，之后再进行细化调整。图 1 所示为 UTMWALL® 数据包处理流程中各功能设置所处的逻辑位置。

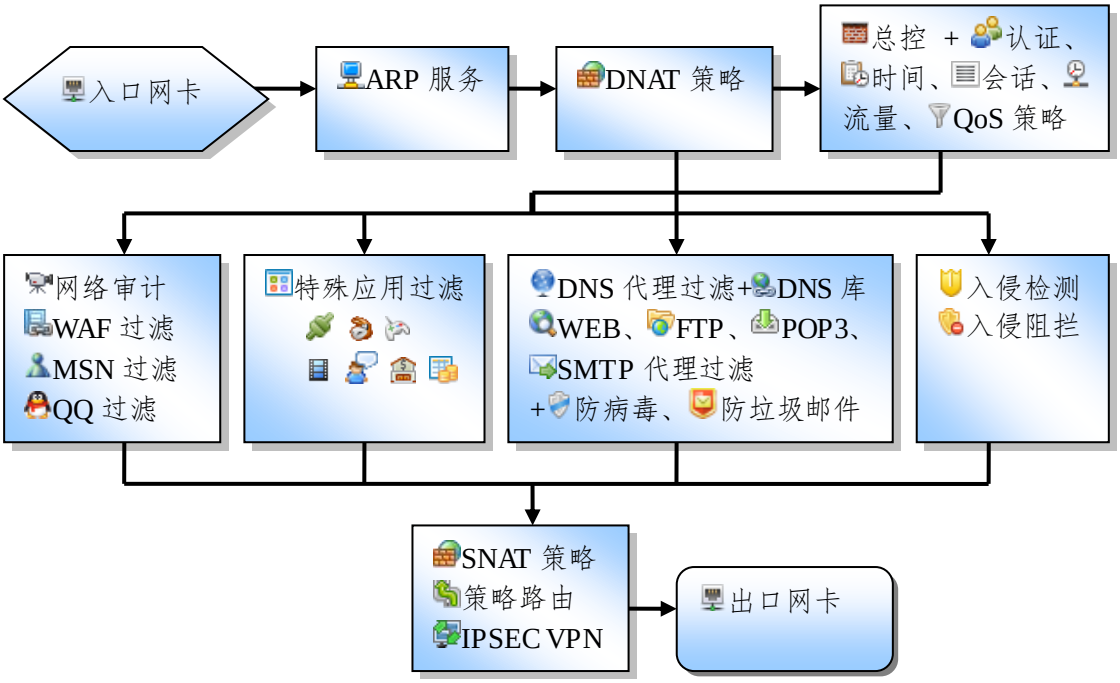


图 1 UTMWALL®数据包处理流程示意图

状态统计功能可以查看当前系统及用户的使用情况，从而了解功能设置的运行情况。状态统计功能按时间点可以分为当前状态统计和历史状态统计 2 大类，“在线主机”、“会话状态”、“实时监控”等属于当前状态统计，“状态趋势图”、“流量统计”、“日志查询与统计”等属于历史状态统计，“应用状态”等既包含当前状态统计也包含历史状态统计。每一个功能设置都至少有一个当前状态统计和一个历史状态统计功能与之相配套。

在 WEB 管理界面中，点击右侧主界面标题位置的三角图标获得当前功能的帮助及向导提示。绝大多数功能链接均可以用鼠标左键或右键点击，左键点击将在主界面中显示，右键点击将在新的选项卡 TAB 中打开一个或多个相关页面，从而保持现有主界面的显示内容，进而构成多页面操作模式，极大地提高管理员的工作效率。

B 快速安装指南

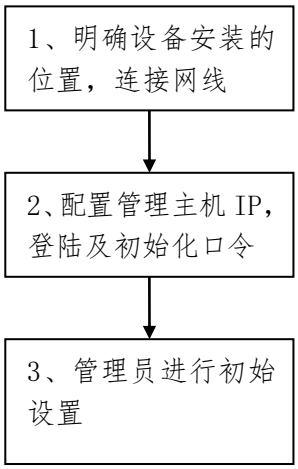


图 2　UTMWALL 网关快速安装流程图

1、明确安装位置并连接网线

- NAT 方式：一般 WAN 口直接接上级 ISP 网线，不需要路由器，LAN 口接交换机
- 网桥方式：一般 WAN 口接上级路由器，LAN 口接交换机，见图 3 所示；设置时，WAN 网卡无 IP，LAN 网卡有 IP 且需要设置网关 IP
- 单臂路由/旁路方式：LAN 口接交换机，网关为上级路由器的 IP，不需要 WAN 口
- 内网路由/三层交换机方式：一般 LAN 口接交换机，WAN 口可选接上级路由器

图 3　网桥接入拓扑图

按照网络与网卡的对应关系连接网线，例如，WAN 区网线连接至 WAN 口，LAN 区网线连接至 LAN 口等。其中，连接至交换机的网线用普通交叉线，连接至 PC、服务器的网线用直通线。见图 4 所示。

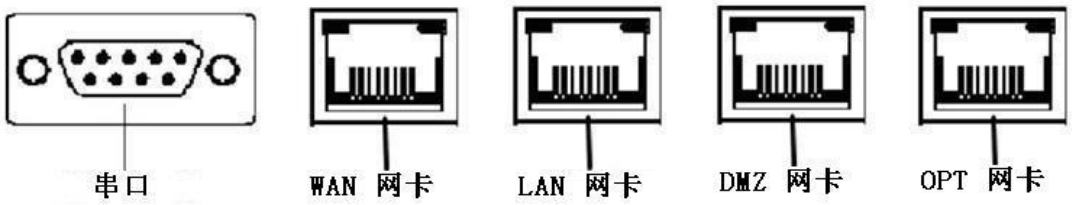


图 4 UTMWALL®网关接口示意图

当接通第 2 块网卡（LAN 口）时，系统会发出“嘀”的一声高音，由此可以判断网卡顺序。另外，系统启动完毕也会发出“嘀”的一声，只不过音频不同。

2、准备管理主机并登陆初始化口令

将一台 PC 或笔记本作为管理主机，设置其 IP 地址:192.168.10.2，掩码：255.255.255.0，同时也删除其它 IP，连接至 LAN 区交换机，或直接与 LAN 口相连。

打开 UTMWALL®网关设备电源，等待设备启动完毕，第一声高音“嘀”表示 LAN 网卡连通，第 2 声低音“嘀”表示设备启动完毕。在管理主机上启动 Internet Explorer（IE），在地址栏处输入 https://192.168.10.1:8443，回车后出现证书错误窗口，如图 5 所示。

该警告可以忽略，因为此处安全证书只是作为加密通讯用，不是作为公开的网站在互联网上使用。

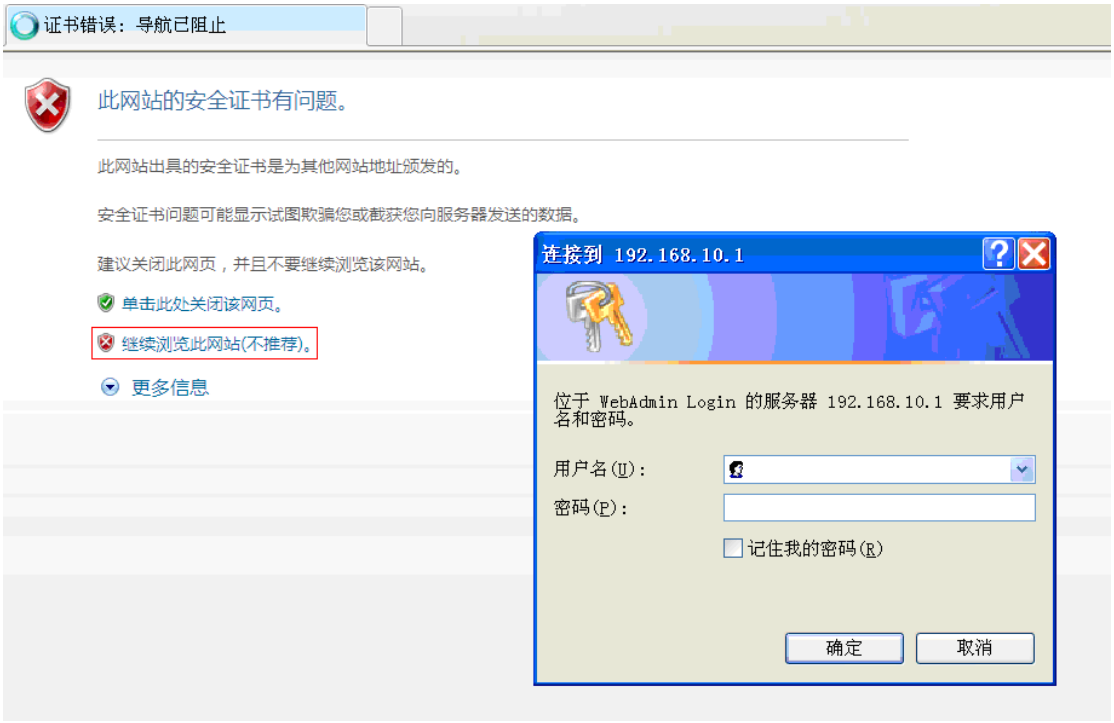


图 5 安全警告窗口

选择“继续浏览此网站（不推荐）”链接继续。出现管理员登录窗口，如图 5 右侧所示。

输入缺省用户名“ppp”，缺省口令“welcome”，点击“确定”按钮，出现修改口令界面，如图 6 所示。当管理员用户第一次登录 WEBAdmin 界面时，必须修改缺省口令。

图 6 第一次登录时强制性修改口令界面

输入原口令并按要求输入两遍新口令，修改成功后，点击“返回”按钮，又出现管理员登录窗口，输入新口令，登录后进入正常 WEBAdmin 管理界面。

为了以后登录方便，在确保安全的前提下，可以选择“记住我的密码”；并打开 IE 的“查看>工具栏>收藏夹栏”选项，再将 WEBAdmin 地址拖入到收藏夹栏中，方便以后直接点击。

3、策略初始化

管理员修改口令后，第一次进入管理界面时，提示进行初始设置，如图 7 所示；点击“确定”按钮进入初始设置界面，如图 8 所示。以后也可以从“系统管理>初始设置”处再次设置。

图 7 初次登录“初始设置”提示对话框

图 8 初始设置界面

在此可以对 WAN、LAN 网卡参数，运行方式，总控策略，DMZ 对外服务器（可选），网络审计（可选），特殊应用，DNS&URL 库（可选）等进行设置，此页面以调查问卷的方式采集最基本的信息，对用户隐藏了相关的技术细节，因此高中文化程度的人士即可进行设置；对于专家而言，还可以在此基础上继续进行深入的、细致的策略调整和设置。至此，UTMWALL® 网关快速安装完毕，系统已可上线试运行。

C 缺省配置

WAN 网卡 IP：10.10.10.10，掩码：255.255.255.0，有“服务”、“管理”选项

LAN 网卡 IP：192.168.10.1，掩码：255.255.255.0，有“服务”、“管理”选项

DMZ 网卡 IP：192.168.20.1，掩码：255.255.255.0，有“服务”、“管理”选项

OPT 网卡 IP：192.168.30.1，掩码：255.255.255.0，有“服务”、“管理”选项

网卡缺省工作方式是全双工，自动协商网卡传输速率，MTU 为 1500

缺省网关 IP：10.10.10.254

管理主机 IP：192.168.10.2

WEBAdmin 管理 URL：https://192.168.10.1:8443

管理员用户名及口令：ppp/welcome

无线网卡密码：ABCDE

总控策略：除了 192.168.10.2->192.168.10.1:8443/TCP，

192.168.10.0/24->192.168.10.1:ICMP 外，其它通讯均阻拦

总控策略匹配规则：待处理的数据包和总控策略比对，相同的五元组（源 IP、源端口、协议、目的 IP、目的端口），最后匹配的总控策略起作用

NAT 策略匹配规则：待处理的数据包和 NAT 策略比对，相同的五元组（源 IP、源端口、协议、目的 IP、目的端口），最先匹配的 NAT 策略起作用

主机名：gateway.company.com

DNS 服务器 IP：114.114.114.114

用户 Portal 认证 URL：https://192.168.10.1:3443 或 http://192.168.10.1:380

流量统计间隔时间：5 分钟

打包备份日志时间：凌晨 0 点 0 分以及系统启动时

Email 发送日志备份时间：凌晨 1 点 30 分

其它缺省设置参见界面输入框右侧小括号中的内容。

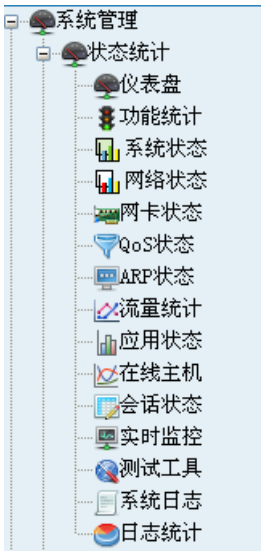
配置项名称要求：小写字母[a-z]、大写字母[A-Z]、数字[0-9]、下划线_、破折号-、小数点.

备注要求：可以是中英文，但不包括 13 个特殊字符\'"`$%^&*|<>;

口令要求：长度 8～18 位，口令复杂度至少为字母和数字的组合，新口令不能与用户名或原口令相同

一、系统管理篇

1 状态统计


系统管理
状态统计
仪表盘
功能统计
系统状态
网络状态
网卡状态
QoS状态
ARP状态
流量统计
应用状态
在线主机
会话状态
实时监控
测试工具
系统日志
日志统计

1.1 系统概要/仪表盘

1.1.1 功能简介

功能代码：infoshow，在此可以全面了解设备运行状态、策略状态和在线主机状态。

1.1.2 操作说明

1、按"F5"键可以刷新整个框架页面，模拟第一次登录
2、点击主界面并按"F1"键，系统显示该界面的帮助窗口
3、蓝色字体均是超链接，可以左键点进去查看相关信息，右键点击会在新选项卡中打开

1.1.3 视频演示

1、第一次登陆:
http://www.trustcomputing.com.cn/help/cn/system/firstlogin/webadmin_first_login.html
2、安装根证书:
http://www.trustcomputing.com.cn/help/cn/system/firstlogin/install_root_cert.html
3、加入收藏栏:
http://www.trustcomputing.com.cn/help/cn/system/firstlogin/add_to_favorite.html
4、在线帮助介绍:
http://www.trustcomputing.com.cn/help/cn/system/webgui/help_intro.html
5、任务向导介绍:
http://www.trustcomputing.com.cn/help/cn/system/guide/guide.html
---
官方讨论区:
http://www.trustcomputing.com.cn/help/cn/status/bbs.html

1.1.4 注意事项

1、第一次登录时显示“流量状态图表”页面
2、“网卡设置状态”中，带*号的是缺省路由网卡，灰色字体表示该网卡网线未连接
3、必须保证“系统及网络状态”监控功能状态为有效，否则 CPU、网卡状态功能无效
4、可以在任何界面处点击主界面并按“F1”键，获得所在界面的功能帮助
5、为了在浏览器状态栏处显示帮助信息，需要更改浏览器设置，具体操作是点击“工具>Internet 选项>安全(TAB)>自定义级别”，在打开的“安全设置”窗口中，找到“脚本”大类，将“允许状态栏通过脚本更新”项设置成“启用”

1.1.5 相关功能

1、上游功能：

初始设置

任务向导
路由流控功能控制
2、相关功能：
系统日志
3、下游功能：<无>
4、任务向导
A1 查看运行状态
B1 初始化本机数据
C3 网络流量控制

1.2 功能统计

1.2.1 功能简介

功能代码：funcshow，在此可以查看各功能启用、停用状态，以及来源地址与功能状态的二维统计透视表。

1.2.2 操作说明

1、功能划分为三类，点击右边的三个 TAB，显示不同类别的功能状态
2、点击最左边的 TAB 显示来源功能统计表

3、点击下方的按钮，重启或关闭系统

1.2.3 视频演示

功能统计示例:http://www.trustcomputing.com.cn/help/cn/status/funcstat/funcstat.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/status/funcstat/bbs.html

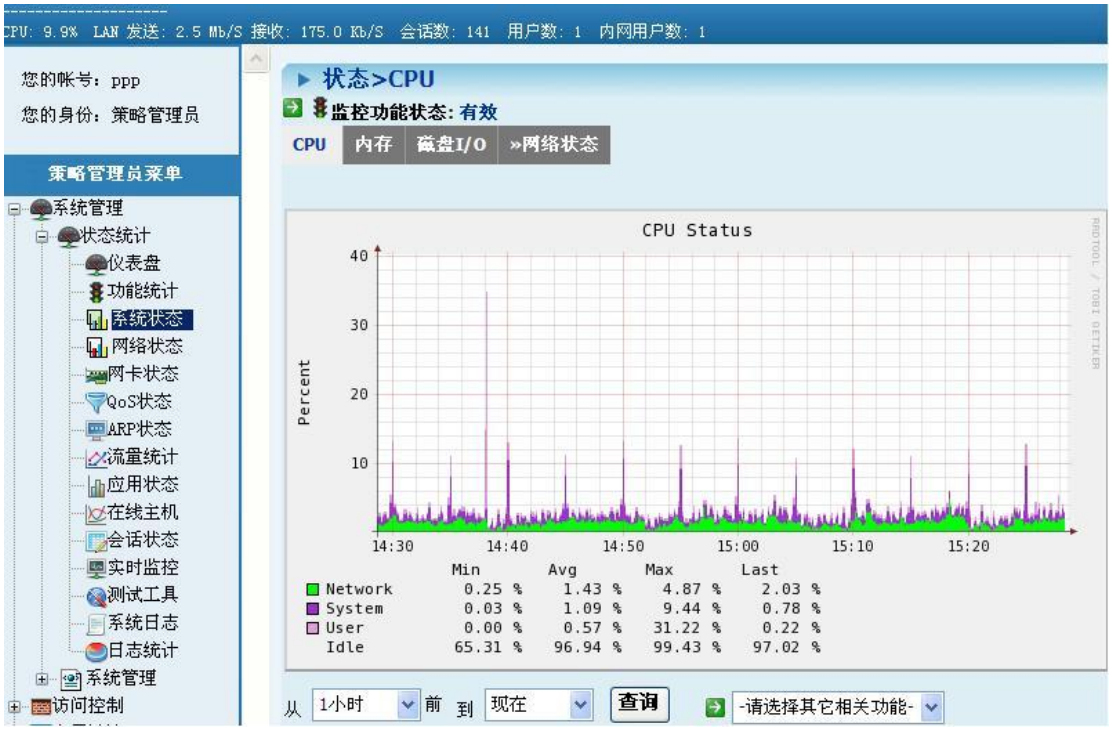
1.2.4 注意事项

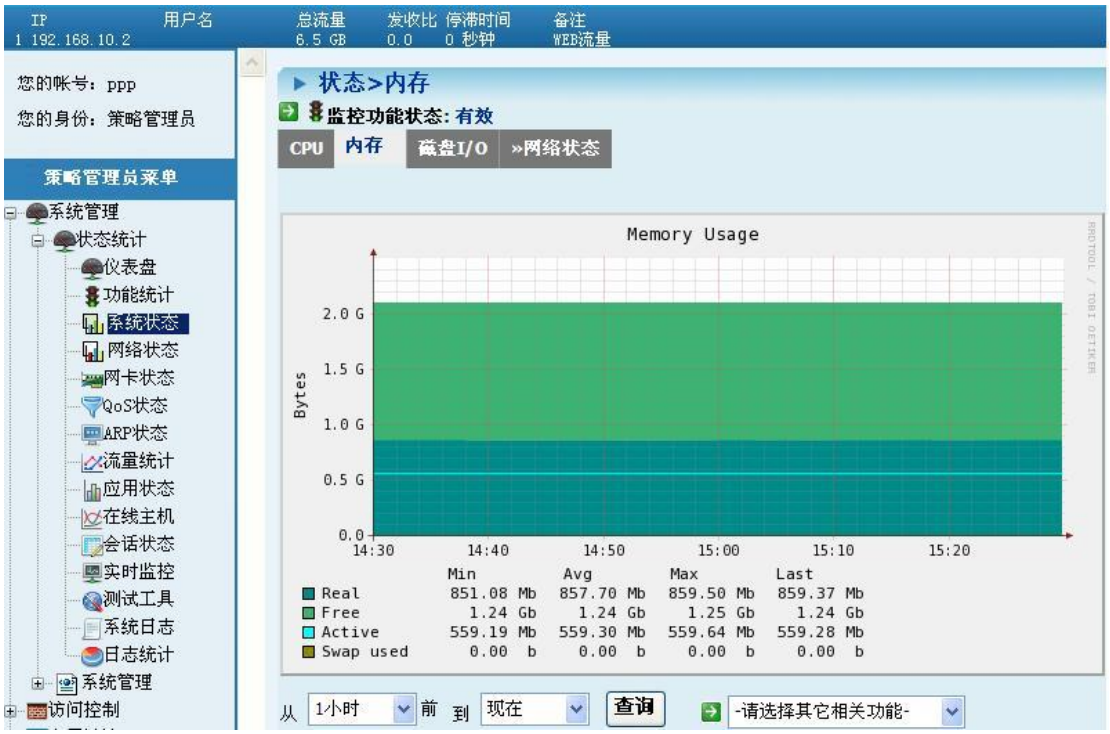
1、功能动作列:“仅启用服务”的，需要手工设置 NAT 或总控策略;“启用服务+自动策略”的，则系统自动设置了相关 NAT、总控策略
2、点击各功能设置列表页面的导航标题的第一项，会最终转至本功能列表，并高亮显示该项功能

1.2.5 相关功能

1、上游功能:
初始设置
任务向导
2、相关功能:
终端工具
3、下游功能:
各具体功能
4、任务向导
A1 查看运行状态
B1 初始化本机数据
C1 上网行为管理
D2 SSL 接入
E2 WEB 门户认证
F1 PPTP、PPPOE 用户接入

1.3 系统状态


CPU: 9.9% LAN 发送: 2.5 Mb/S 接收: 175.0 Kb/S 会话数: 141 用户数: 1 内网用户数: 1
您的帐号: ppp
您的身份: 策略管理员
策略管理员菜单
系统管理
状态统计
仪表盘
功能统计
系统状态
网络状态
网卡状态
QoS状态
ARP状态
流量统计
应用状态
在线主机
会话状态
实时监控
测试工具
系统日志
日志统计
系统管理
访问控制
状态>CPU
监控功能状态: 有效
CPU
内存
磁盘I/O
»网络状态
CPU Status
Percent
40
30
20
10
14:30
14:40
14:50
15:00
15:10
15:20
Min Avg Max Last
Network 0.25 % 1.43 % 4.87 % 2.03 %
System 0.03 % 1.09 % 9.44 % 0.78 %
User 0.00 % 0.57 % 31.22 % 0.22 %
Idle 65.31 % 96.94 % 99.43 % 97.02 %
从 1小时 前 到 现在 查询
-请选择其它相关功能-


IP 用户名 总流量 发收比 停滞时间 备注
1 192.168.10.2 6.5 GB 0.0 0 秒钟 WEB流量
您的帐号: ppp
您的身份: 策略管理员
策略管理员菜单
系统管理
状态统计
仪表盘
功能统计
系统状态
网络状态
网卡状态
QoS状态
ARP状态
流量统计
应用状态
在线主机
会话状态
实时监控
测试工具
系统日志
日志统计
系统管理
访问控制
状态>内存
监控功能状态: 有效
CPU
内存
磁盘I/O
»网络状态
Memory Usage
Bytes
2.0 G
1.5 G
1.0 G
0.5 G
0.0
14:30
14:40
14:50
15:00
15:10
15:20
Min Avg Max Last
Real 851.08 Mb 857.70 Mb 859.50 Mb 859.37 Mb
Free 1.24 Gb 1.24 Gb 1.25 Gb 1.24 Gb
Active 559.19 Mb 559.30 Mb 559.64 Mb 559.28 Mb
Swap used 0.00 b 0.00 b 0.00 b 0.00 b
从 1小时 前 到 现在 查询
-请选择其它相关功能-

1.3.1 功能简介

功能代码：monitorsystem，在此可以查看系统运行状态参数的 24 小时趋势图，发现系统运行的日常规律及异常现象出现的时间点。

1.3.2 操作说明

1、点击上方各参数 TAB，查看相应的状态
2、选择下方时间框，查看相应时间段的状态
3、选择“本机状态日志”查看历史记录

1.3.3 视频演示

系统趋势状态:http://www.trustcomputing.com.cn/help/cn/status/monitor/system_monitor.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/status/monitor/bbs.html

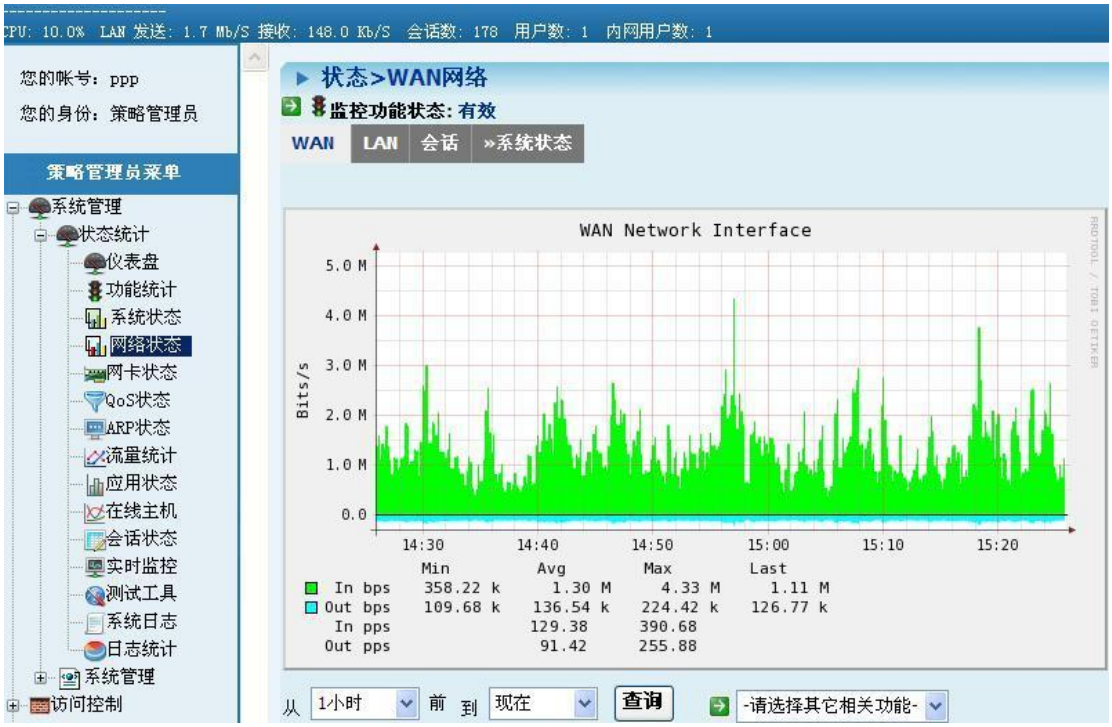
1.3.4 注意事项

1、必须保证“系统及网络状态”监控功能为有效，否则本功能无效
2、如果第一次启动时，系统时间不正确，则没有状态图形显示，需要等到第二天才有状态图形

1.3.5 相关功能

1、上游功能：
路由流控功能控制
系统时间
2、相关功能：
本机状态日志
系统日志
网络状态趋势
仪表盘
3、下游功能：<无>
4、任务向导
A1 查看运行状态
B1 初始化本机数据

1.4 网络状态



1.4.1 功能简介

功能代码：monitornic，在此可以查看网络吞吐量的 24 小时趋势图，发现其日常规律及异常流量出现的时间点。

1.4.2 操作说明

1、点击上方各网卡 TAB，查看相应网络的状态，in 代表流入网卡的流量，out 代表流出网卡的流量
2、选择下方时间框，查看相应时间段的吞吐量数值
3、选择“本机状态日志”查看历史记录

1.4.3 视频演示

网络趋势状态:http://www.trustcomputing.com.cn/help/cn/status/monitor/network_monitor.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/status/monitor/bbs.html

1.4.4 注意事项

1、必须保证“系统及网络状态”监控功能为有效，否则本功能无效
2、如果第一次启动时，系统时间不正确，则没有状态图形显示，需要等到第二天才有状态图形

1.4.5 相关功能

1、上游功能：
网卡设置
系统及网络状态监控
系统时间
2、相关功能：
本机状态日志
流量日志
流量统计日志
在线主机
流量统计
流量策略
QoS 策略
QoS 状态
网卡状态
会话状态管理
会话状态趋势
CPU 状态趋势
仪表盘
Netflow 探针
3、下游功能：<无>
4、任务向导
A1 查看运行状态
B1 初始化本机数据
C3 网络流量控制

1.5 网卡状态

1.5.1 功能简介

功能代码：nicstate，在此可以查看各网卡的运行状态，查看是否有错误、碰撞、丢弃数据包出现。

1.5.2 操作说明

1、点击蓝色字体，进一步查看相关信息

1.5.3 视频演示

网卡设置:http://www.trustcomputing.com.cn/help/cn/network/nic/nic_setting.html
WAN 网卡设置:http://www.trustcomputing.com.cn/help/cn/network/nic/update_wan.html
LAN 网卡设置:http://www.trustcomputing.com.cn/help/cn/network/nic/update_lan.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/network/nic/bbs.html

1.5.4 注意事项

1、必须保证“系统及网络状态”监控功能为有效，否则实时带宽功能无效

1.5.5 相关功能

1、上游功能：
网卡设置
链路聚合
VLAN 设置
网桥设置
双机热备
系统及网络状态监控
2、相关功能：

 路由状态
 网络状态
 ARP 状态
 仪表盘

3、下游功能：<无>

4、任务向导

A1 查看运行状态

B2 NAT 模式接入

B3 透明网桥模式接入

B4 路由模式接入

D1 服务器接入

1.6 QoS 状态

序号	名称	带宽(比特/秒)	优先级	封包个数	字节大小	丢弃封包	丢弃字节	排队长度	借用封包	延缓封包	封包/秒	字节
1	WAN_root	100M	0	579	98250	0	0	0	0	0	96	13K
2	LAN_root	100M	0	539	467K	0	0	0	0	0	95	95K
3	P2P_qos	1M	3	0	0	0	0	0	0	0	0	0
4	TCP_qos	800K	3	1	66	0	0	0	0	0	0	0
5	UDP_qos	800K	3	19	1839	0	0	0	0	0	5	611
6	FAKE80_qos	800K	3	0	0	0	0	0	0	0	0	0
7	WEB_qos	2M	6	0	0	0	0	0	0	0	0	0

1.6.1 功能简介

功能代码：qosstatus，在此显示 QoS 策略应用情况，各 QoS 对象按树状排列显示。

1.6.2 操作说明

1、点击蓝色字体，进一步查看相关信息

1.6.3 视频演示

QOS 策略应用:http://www.trustcomputing.com.cn/help/cn/policy/qos/qos_policy.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/policy/qos/bbs.html

1.6.4 注意事项

1、必须保证总控策略、QoS 功能为有效，否则本功能无效

1.6.5 相关功能

1、上游功能：
QoS 对象
总控策略
路由流控功能控制
2、相关功能：<无>
3、下游功能：<无>
4、任务向导
A1 查看运行状态
C3 网络流量控制

1.7 ARP 状态

1.7.1 功能简介

功能代码：arpstatus，在此可以查看设备自身的 ARP 缓存状态，绑定及代理的 MAC 地址为确定的 MAC 地址。

1.7.2 操作说明

1、选择右上方的网络选择框，查看单一网络内的 ARP 状态
2、点击“更新”按钮进入自动查找 IP、MAC 界面
3、点击“日志”按钮查看 ARP 日志
4、选择最右边三列的“查看”链接，查看该 IP 的流量、日志信息
5、点击“+*”链接，进入 IP、用户名绑定界面
6、点击表头蓝色字体进行排序

1.7.3 视频演示

1、ARP 状态示例:http://www.trustcomputing.com.cn/help/cn/services/ipmac/mac_status.html
2、手工单个绑定:http://www.trustcomputing.com.cn/help/cn/services/ipmac/mac_binding.html
3、自动扫描绑定:http://www.trustcomputing.com.cn/help/cn/services/ipmac/mac_update.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/services/ipmac/bbs.html

1.7.4 注意事项

1、ARP 流量为 0，表示该 IP 没有开机或联网
2、ARP 流量异常大的 IP，表示内网网络操作多，可能有 ARP 病毒

1.7.5 相关功能

1、上游功能：

ARP 服务

链路聚合设置

VLAN 设置

2、相关功能：

用户定义

ARP 日志

DHCP 服务状态

Netbios 查询工具

NAT 策略

网卡状态

在线主机

流量统计

流量日志

流量统计日志

应用状态

日志统计

系统概要

3、下游功能：<无>

4、任务向导

A1 查看运行状态

C1 上网行为管理

D1 服务器接入

E1 实名制查看用户状态

1.8 流量统计

1.8.1 功能简介

功能代码：trafficstat，分为“源 IP 流量汇总”、“规则流量汇总”和“流量明细”三种透视图，前两种视图对源 IP、总控规则进行历史累计流量汇总统计，“流量明细”视图可以查看各源 IP 的历史累计流量统计，及对应的总控规则号、应用层日志等。

1.8.2 操作说明

1、点击“统计范围”链接，重置为全部
2、点击“源 IP”列链接，只统计该源 IP；点击“规则”列链接，只统计该规则
3、点击“总流量”“总计”链接，或鼠标右键，进入在线主机界面
4、点击“修改”列链接，进入修改总控规则界面
5、点击“备注”列链接，查看应用层日志
6、选择“显示内容”框，单独显示活动流量统计，或其他状态统计
7、点击“+*”链接，进入 IP、用户名绑定界面
8、点击表头蓝色字体进行排序
9、点击“更新”按钮，强制进行流量数据更新统计

1.8.3 视频演示

1、流量统计示例:
http://www.trustcomputing.com.cn/help/cn/status/traffic_statistics/traffic_statistics.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/status/traffic_statistics/bbs.html

1.8.4 注意事项

1、流量统计间隔时间由第一条流量对象 Normal_tc 设置
2、两次流量统计结果一样的，是停滞状态不是活动流量
3、系统每隔 1 小时自动生成流量统计日志，再发送到管理员 Email，方便其快速了解网络流量情况

1.8.5 相关功能

1、上游功能：
 总控策略
 流量对象
 IP 地址对象
2、相关功能：
 用户定义
 流量状态仪表盘
 网络状态
 IPS 状态
 在线主机
 流量日志
 流量统计日志
 用户流量统计
 应用状态
 日志统计
3、下游功能：<无>
4、任务向导
A1 查看运行状态
B2 NAT 模式接入
B3 透明网桥模式接入
B4 路由模式接入
C1 上网行为管理
C3 网络流量控制
C4 网络流量计费
D1 服务器接入
E1 实名制查看用户状态

1.9 应用状态

1.9.1 功能简介

功能代码：specappstatus，显示特殊应用的流量统计状态，通过的或阻拦的，可以查看各 IP 的不同应用的流量，流量统计值既可以是通过的，也可以是阻拦的。

1.9.2 操作说明

1、选择上方下拉框，查询各应用大类及具体应用的流量统计
2、点击“源 IP”列链接，只统计该源 IP；或在右上方直接输入源 IP 查询
3、点击“开始统计时间”列链接，进入该应用的设置界面
4、选择“显示内容”框，单独显示一定包数限制的应用统计，或其他状态统计
5、点击“+*”链接，进入 IP、用户名绑定界面
6、点击表头蓝色字体进行排序
7、点击“日志”按钮，进入特殊应用日志列表界面

1.9.3 视频演示

1、策略设置示例:
http://www.trustcomputing.com.cn/help/cn/appfilter/specapp/policy_setting.html
2、状态统计示例:
http://www.trustcomputing.com.cn/help/cn/appfilter/specapp/specappstatus.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/specapp/bbs.html

1.9.4 注意事项

1、当具体特殊应用策略是“通过”时，本功能可以起到应用审计的作用，即哪些人运行了哪些应用
2、PC 客户端后台可能有服务程序，进而产生微小流量，这种流量不是用户交互式上网产生

的流量，可以选择不显示，方法是选择“显示内容”下拉框中合适的封包数下限选项
3、此处显示的封包数、字节数不代表该应用的全部流量，只是定性分析的结果，在多个 IP 之间做相对比较有意义
4、对通过的封包数和通过的字节数进行排序，实际上是对接收的封包数和字节数进行排序，不包括发送的封包数和字节数

1.9.5 相关功能

1、上游功能：
特殊应用
IP 地址对象
用户定义
上网管理功能控制
2、相关功能：
来源功能统计
DNS 及 URL 库
WEB 审计过滤（WAF）
应用日志
在线主机
流量统计
流量日志
流量统计日志
会话状态
日志统计
ARP 状态
系统概要
3、下游功能：<无>
4、任务向导
A1 查看运行状态
C1 上网行为管理
C12 抓包分析并阻拦特定应用
E1 实名制查看用户状态

1.10 在线主机

1.10.1 功能简介

功能代码：onlinehoststatus，分为“源 IP 流量汇总”、“规则流量汇总”和“流量明细”三种透视图，前两种视图对源 IP、总控规则进行实时流量汇总统计，“流量明细”视图可以查看当前活动的各源 IP 的会话、流量、带宽统计，及对应的总控规则号、应用层日志等。

1.10.2 操作说明

1、点击“统计范围”链接，重置为全部
2、点击“源 IP”列链接，只统计该源 IP；点击“规则”列链接，只统计该规则
3、点击“会话数”“总计”链接，进入会话状态界面；点击除“总计”行的链接，进入该源 IP 对应规则的会话状态界面
4、点击“总流量”“总计”链接，或鼠标右键，进入流量统计界面
5、点击“修改”列链接，进入修改总控规则界面
6、点击“备注”列链接，查看应用层日志
7、选择“显示内容”框，单独显示各异常流量统计，或其他状态统计
8、点击“+*”链接，进入 IP、用户名绑定界面
9、点击表头蓝色字体进行排序

1.10.3 视频演示

1、在线主机示例:http://www.trustcomputing.com.cn/help/cn/status/active_host/active_host.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/status/active_host/bbs.html

1.10.4 注意事项

1、异常流量分为突发、持续、上传三类，用不同颜色表示，由该流量对应的总控策略的流量对象所定义，可通过选择“显示内容”框单独或一起显示
2、源 IP 可以是内网 IP，也可以是外网 IP
3、带宽是平均值，是流量值除以在线时间得到的，不是实时带宽

1.10.5 相关功能

1、上游功能：
 总控策略
 流量对象
2、相关功能：
 用户定义
流量状态仪表盘
 网络状态
 IPS 状态
 QoS 状态
 流量统计
 流量日志
 流量统计日志
 会话状态
 应用状态
 日志统计
 ARP 状态
3、下游功能：<无>
4、任务向导
A1 查看运行状态
B2 NAT 模式接入
B3 透明网桥模式接入
B4 路由模式接入
C1 上网行为管理
C3 网络流量控制
C4 网络流量计费
D1 服务器接入
D2 SSL 接入
E1 实名制查看用户状态
E2 WEB 门户认证

1.11 会话状态

1.11.1 功能简介

功能代码：sessionstatus，在此可以查看当前发生的会话，还可以通过查询显示满足特定条件的会话，并终止这些会话。

1.11.2 操作说明

1、在下方选择、输入查询条件，点击“查询”按钮查询
2、点击“终止”按钮，终止目前显示的会话
3、点击“统计”按钮，对当前显示的会话进行统计

1.11.3 视频演示

1、会话状态管理示例:
http://www.trustcomputing.com.cn/help/cn/status/session_status/session_status.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/status/session_status/bbs.html

1.11.4 注意事项

1、“方向”一般选择“流入网卡”,以反映总控策略的实施情况
2、如果在具体总控策略中会话选项是第一项“No Session”，则不会产生会话，也就不会在

此查看到相应的会话

3、如果总控策略发生变化，之前已有的会话所对应的总控策略号就变成了*号，为保持一一对应关系，需要终止这些会话

1.11.5 相关功能

1、上游功能：

总控策略

会话对象

2、相关功能：

流量状态仪表盘

在线主机

WEB 审计日志

非标准 80 端口服务器 IP

网络状态

QoS 状态

IPS 状态

3、下游功能：<无>

4、任务向导

A1 查看运行状态

B2 NAT 模式接入

B3 透明网桥模式接入

B4 路由模式接入

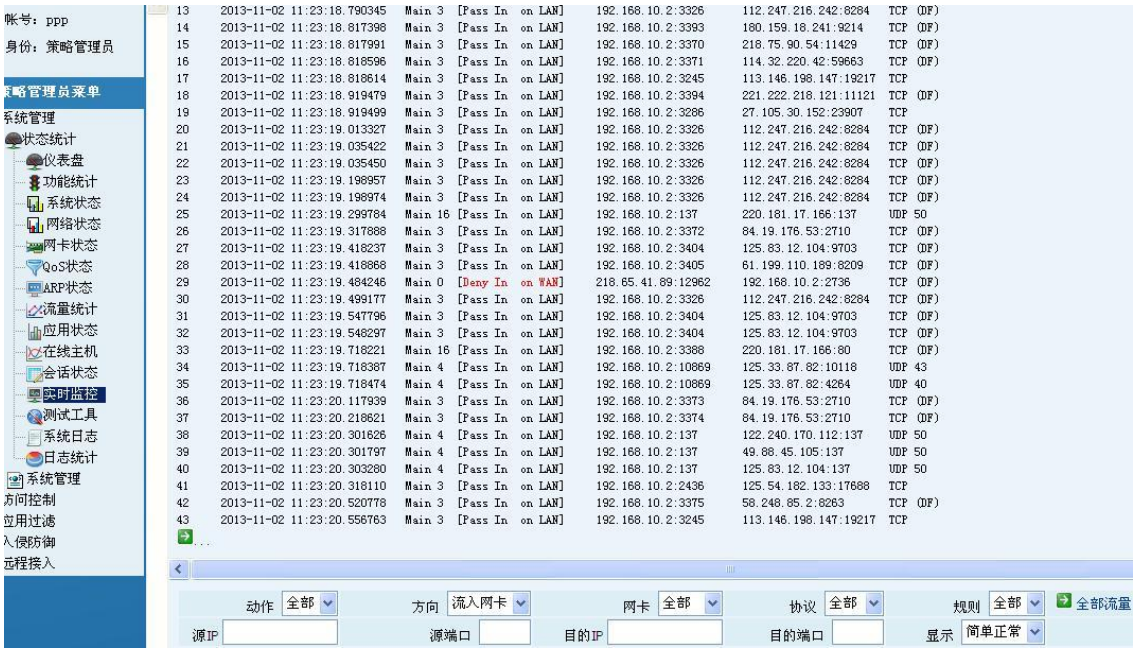
C3 网络流量控制

C12 抓包分析并阻拦特定应用

D1 服务器接入

F2 IPSEC VPN 接入

1.12 实时监控



1.12.1 功能简介

功能代码：realtimemonitor，在此可以对数据包进行实施抓包分析，还可以通过查询显示满足特定条件的数据包。

1.12.2 操作说明

1、在下方选择、输入查询条件，点击“确定”按钮查询
2、点击“停止”按钮，停止抓包
3、点击“停止卷屏”按钮，使显示内容由手工拖拉确定

1.12.3 视频演示

1、实时监控示例:
http://www.trustcomputing.com.cn/help/cn/status/realtime_monitor/realtime_monitor.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/status/realtime_monitor/bbs.html

1.12.4 注意事项

1、“方向”一般选择“流入网卡”,以反映总控策略的实施情况
2、如果已发生的"允许"的流量没有显示，请在会话状态中查找。总控策略中日志项为"简单"或"无"的策略，只显示第一个数据包或不显示

3、如果总控策略发生变化，之前已"允许"的流量所对应的总控策略号就变成了*号，为保持一一对应关系，需要终止这些会话

1.12.5 相关功能

1、上游功能：
总控策略
2、相关功能：
在线主机
会话状态
包过滤日志
3、下游功能：<无>
4、任务向导
A1 查看运行状态
B2 NAT 模式接入
B3 透明网桥模式接入
B4 路由模式接入
C12 抓包分析并阻拦特定应用
D1 服务器接入
F2 IPSEC VPN 接入

1.13 测试工具

1.13.1 功能简介

功能代码：nettool，在此可以以本机为客户端进行各项网络测试，以确定网络连通性等问题。

1.13.2 操作说明

1、在下方选择、输入测试条件，点击“确定”按钮测试
2、点击“停止”按钮，停止测试

1.13.3 视频演示

测试工具示例:http://www.trustcomputing.com.cn/help/cn/status/nettool/nettool.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/status/nettool/bbs.html

1.13.4 注意事项

1、可以在此测试网关自身的连通性，以排除因网关网络设置而导致的连通性故障

1.13.5 相关功能

1、上游功能：

网卡设置
路由设置

2、相关功能：

IP 地址对象
DNS 解析
DNS 库
域名规则
DDNS 服务
实时监控

3、下游功能：<无>

4、任务向导

A1 查看运行状态
B1 初始化本机数据
B2 NAT 模式接入
B3 透明网桥模式接入
B4 路由模式接入
D1 服务器接入
F2 IPSEC VPN 接入

1.14 日志操作

1.14.1 功能简介

功能代码：logshow，在此显示当天日志创建时间、文件大小以及历史日志文件大小、数目等信息。基本上所有的功能都产生日志，以方便了解策略实施的情况，并为日后查询提供信息来源。

1.14.2 操作说明

1、点击“日志”列链接，浏览日志内容，当天日志请点击“查看日志”，历史日志请点击“查看”；点击左边主菜单的“XX 日志”链接，可以直接进入到查看当前日志内容的界面
2、点击“统计”列链接，查看日志统计列表，“源 IP 统计”显示最活跃用户统计及日志内容，“内容统计”显示最热门内容统计及日志内容
3、点击最上方当前菜单位置提示中的前半部分链接，显示与日志相关联的功能设置界面
4、查询更多历史日志，请选择上方的“第 X/Y 页”下拉框；查询其它日志，请选择上方的日志类型下拉框
5、跨天数查询日志，请点击下方的“查询”按钮；查看日志统计，请点击下方的“统计”按钮

1.14.3 视频演示

1、日志示例:http://www.trustcomputing.com.cn/help/cn/log/_LOG_.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/log/log/bbs.html

1.14.4 注意事项

1、可以通过查看创建时间判断当前日志内容是否有更新；可以通过查看文件大小判断日志内容的多少

2、系统启动时或每晚 12 点系统会自动打包压缩所有日志，但一天只做一次，故开机第一天当晚 12 点不会打包日志

3、只有日志审计员才能下载、删除历史日志，只有日志审计员才能查看管理员日志记录，日志审计员可以设置每种日志的最大日志留存天数，系统会根据最大日志数的设置删除最老历史日志，为新日志流出空间

4、日志查询中，除序号外所有内容都可以查询，输入"AAA BBB"将查询一行日志中前部分有"AAA"，后部分有"BBB"的内容

5、查看当前日志时，如果内容不是最新的，需要点击“确定”按钮刷新

1.14.5 相关功能

1、上游功能：

网络审计>总体设置

总控策略

上网管理功能控制

2、相关功能：<无>

3、下游功能：

日志统计

4、任务向导

A1 查看运行状态

A2 查看当前日志内容

A3 查看当前日志统计

B2 NAT 模式接入

B3 透明网桥模式接入

B4 路由模式接入

C2 防控 ARP 病毒

1.15 日志统计

1.15.1 功能简介

功能代码：logstat，分为"日期统计表"、"小时统计表(源 IP 明细)"和日志查询三部分，"小时统计表(源 IP 明细)"可以查看 1~24 小时内，每小时各个日志的条数统计及源 IP 个数统计，或者可以查看一个源 IP 当天相关日志条数的统计及每种日志最近发生的日志内容。在此列出的日志是与上网有关的日志，还有部分日志，例如 IDP 等没有在此显示。

1.15.2 操作说明

1、红色字体列表示最近一个小时的统计值
2、在下方输入 IP 或用户名，查询单个 IP 的日志统计
3、左/右键点击左边主菜单的“日志统计”链接，直接进入当前管理主机的源 IP 明细界面

1.15.3 视频演示

1、日志统计示例: http://www.trustcomputing.com.cn/help/cn/log/log_statistics/log_statistics.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/log/log_statistics/bbs.html

1.15.4 注意事项

1、只有做了用户名与 IP 地址的绑定，才能按登陆账号或用户姓名查询
2、源 IP 明细是按各日志最新记录时间的新老程度进行排序显示
3、源 IP 明细统计时间比较长，请耐心等待

1.15.5 相关功能

1、上游功能：

 用户定义

2、相关功能：

 日志统计仪表盘

 在线主机

 流量统计

 应用状态

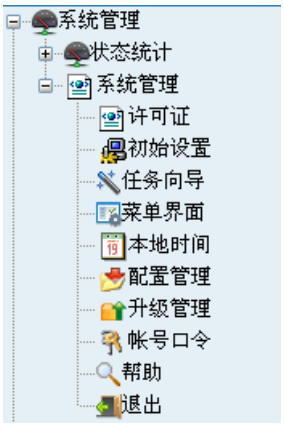
3、下游功能：<无>

4、任务向导

A2 查看当前日志内容

A3 查看当前日志统计

2 系统管理



2.1 许可证

2.1.1 功能简介

功能代码：licshow，在此可以查看当前已具备的许可证类型、时间期限和生效状态，以及购买、升级信息。

2.1.2 操作说明

1、点击当前菜单位置提示中的“系统”，显示系统概要
2、点击当前菜单位置提示中的“许可证”，刷新本页面

2.1.3 视频演示

许可证示例:http://www.trustcomputing.com.cn/help/cn/system/license/license.html
---

官方讨论区:http://www.trustcomputing.com.cn/help/cn/system/license/bbs.html

2.1.4 注意事项

1、在许可证过期前 1~30 天，系统每天均会产生系统日志提示做好备份并马上升级许可证

2.1.5 相关功能

1、上游功能：<无>
2、相关功能：<无>
3、下游功能：
 特殊应用>总体设置
 网络审计>总体设置
 DNS 及 URL 库
 防病毒引擎>数据库
 IDP 规则>特征值
4、任务向导
A1 查看运行状态
B1 初始化本机数据

2.2 初始设置

2.2.1 功能简介

功能代码：quicksetshow，在此可以对设备的接入方式、运行方式、总控策略、上网管理、SSLVPN 等进行初始化设置，适用于初次设置或新手进行一站式设置。其它未列出的策略，需要另外做设置。

2.2.2 操作说明

1、根据提示分别选择或输入相关的参数
2、外网网卡的方式有静态、DHCP、PPPoE 三种，内网网卡的方式只有静态一种；当运行方式是透明网桥时，外网方式重置为静态，且无 IP、掩码、路由
3、DNS 服务器 IP 按本地 ISP 提供的 DNS 服务器填写，可以参考“常用 DNS 服务器地址”页面的信息
4、“DMZ 区服务器 IP 地址及端口”中填写有 IP 地址(LAN 区/G2 或 DMZ 区/G3 IP 地址)端口值，系统自动创建相应的 DNAT、总控策略
5、“运行方式”和“总控策略”中，如果策略已发生改变，又希望保留，则选择“保持现状不变”
6、“特殊应用”中，选中的将被阻拦，没选中的通过且做审计
7、“DNS 及 URL 库”中，选中的将被阻拦，如果全部都没选中，则停用 DNS 代理过滤

2.2.3 视频演示

1、初始设置示例:
http://www.trustcomputing.com.cn/help/cn/system/quickset/quickset_demo.doc
2、初始设置指南:
http://www.trustcomputing.com.cn/help/cn/system/quickset/quickset_intro.doc

3、来源 NAT 接入:
http://www.trustcomputing.com.cn/help/cn/system/quickset/quickset_snat_demo.html
4、透明网桥接入:
http://www.trustcomputing.com.cn/help/cn/system/quickset/quickset_bridge_demo.html
5、任务向导介绍:
http://www.trustcomputing.com.cn/help/cn/system/guide/guide.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/system/quickset/bbs.html

2.2.4 注意事项

1、本功能假设的外、内网卡分别是设备的第一、二块网卡，连接网线时要注意相对应；连接上第二块网卡时，系统会鸣响一声；也可以不用本功能，自行定义内外网卡
2、涉及到的功能有网卡设置、DHCP 服务、DNS 解析、网桥设置、NAT 策略、总控策略、网络审计、WEB 审计过滤（WAF）、MSN 审计过滤、QQ 审计过滤、特殊应用、DNS 代理过滤、DNS 及 URL 库、SSLVPN 等，各项还可以进行进一步的细化设置，其它未涉及到的功能需要另外做设置
3、PPPoE 方式只能获得 IP 地址及网络掩码，不能自动设置 DNS 服务器，所以需要另外设置 DNS 服务器 IP
4、最右边一列显示当前各项的值，红色表示与初始设置内容不一致

2.2.5 相关功能

1、上游功能：<无>
2、相关功能：
网卡设置
DHCP 服务
DNS 解析
网桥设置
NAT 策略
总控策略
网络审计
WEB 审计过滤（WAF）
MSN 审计过滤
QQ 审计过滤
特殊应用
DNS 代理总体设置
DNS 及 URL 库
SSLVPN>总体设置
任务向导
3、下游功能：
功能统计
4、任务向导

B1 初始化本机数据
B2 NAT 模式接入
B3 透明网桥模式接入
B4 路由模式接入
C1 上网行为管理
D1 服务器接入

2.3 任务向导

2.3.1 功能简介

为了展示实现某一特定任务所需的系列功能，系统提供任务向导窗口，在此管理员可以依次点击各步骤中的功能链接进行操作，最终完成该任务。

2.3.2 操作说明

1、用鼠标右键点击主界面左上角的图符，系统弹出包含当前功能的任务向导窗口；如果需要查找其它任务向导，可以点击“全部任务”链接，再从下拉框中选择
2、在步骤等各列中，用鼠标右键点击功能链接，显示包含该功能的任务向导内容；用鼠标左键点击功能链接，在主界面中显示该功能的设置界面

2.3.3 视频演示

2.3.4 注意事项

进入任务向导时的功能链接用红色表示，鼠标左键点击的当前功能链接用蓝色表示

2.3.5 相关功能

1、上游功能： <无>

2、相关功能：

帮助功能

3、下游功能：

2.4 菜单界面

2.4.1 功能简介

功能代码：guishow，在此可以设置显示语言、主菜单、快捷菜单、标题等的内容。

2.4.2 操作说明

1、根据提示分别选择或输入相关的参数，提交后系统自动刷新整个框架页面
2、任何时候均可以点击快捷图标最左边的一个，调用本功能

2.4.3 视频演示

1、图形界面介绍:http://www.trustcomputing.com.cn/help/cn/system/webgui/gui_intro.html
2、菜单界面设置:http://www.trustcomputing.com.cn/help/cn/system/webgui/gui_setup.html
3、在线帮助介绍:http://www.trustcomputing.com.cn/help/cn/system/webgui/help_intro.html
4、任务向导介绍:http://www.trustcomputing.com.cn/help/cn/system/guide/guide.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/system/webgui/bbs.html

2.4.4 注意事项

1、右上角快捷菜单分为文字和图表两部分，快捷文字可以在此调整，快捷图标是固定的
2、改变语言后，以原来语言记录的配置、日志等，可能会显示乱码，例如原来是中文，现

在是英文

2.4.5 相关功能

1、上游功能：<无>
2、相关功能：<无>
3、下游功能：
 系统概要
4、任务向导
B1 初始化本机数据

2.5 本地时间

2.5.1 功能简介

功能代码：systimeshow，在此可以设置本机当地时间及是否启用 NTP 自动更新本机时间。

2.5.2 操作说明

1、根据提示分别选择或输入相关的参数

2.5.3 视频演示

官方讨论区:http://www.trustcomputing.com.cn/help/cn/system/bbs.html

2.5.4 注意事项

1、时间不能往前设置超过 1 小时
2、时间对象是以本机时间为对照
3、各项日志也是以本机时间进行记录

2.5.5 相关功能

1、上游功能：<无>
2、相关功能：<无>
3、下游功能：
许可证

 系统状态
 网络状态
 时间对象
 总控策略
 特殊应用
 DNS 及 URL 库

4、任务向导

B1 初始化本机数据

2.6 配置管理

2.6.1 功能简介

功能代码：backupshow，在此可以保存一部分或全部当前系统的配置，或恢复原来保存的配置。

2.6.2 操作说明

1、点击“新建”按钮用于保存配置，点击“还原”链接用于还原配置
2、点击“文件下载”列的链接用于下载保存配置文件
3、选择“序号”列的多选框，再点击“删除”按钮用于删除配置文件
4、点击“上传”按钮，用于上传 PC 里的配置文件到设备中

2.6.3 视频演示

1、新建配置示例: http://www.trustcomputing.com.cn/help/cn/system/backup/create_backup.html
2、恢复配置示例:http://www.trustcomputing.com.cn/help/cn/system/backup/apply_backup.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/system/backup/bbs.html

2.6.4 注意事项

1、第一行是设备出厂时的配置文件，可用于恢复出厂设置，不可删除；系统每天自动生成最新的配置，并邮寄给管理员邮箱
2、还原配置时，如果不立即生效，则需要重启系统才能真正使配置生效
3、配置取得阶段性进展后，要记得新建配置文件，并下载到 PC 中保存，以备后用

2.6.5 相关功能

1、上游功能：<无>
2、相关功能：

各模块功能

3、下游功能：

 功能统计

2.7 升级管理

2.7.1 功能简介

功能代码：updateshow，在此可以上传升级文件，升级系统，以解决问题或扩充功能。

2.7.2 操作说明

1、点击“上传”按钮，用于上传 PC 里的升级文件到设备中
2、点击“升级”链接用于升级系统
3、选择“序号”列的多选框，再点击“删除”按钮用于删除升级文件
4、点击“文件下载”列的链接用于下载保存升级文件

2.7.3 视频演示

升级管理示例:http://www.trustcomputing.com.cn/help/cn/system/upgrade/upgrade.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/system/upgrade/bbs.html

2.7.4 注意事项

1、大部分升级过程不需要重启系统，只需要刷新相关页面即可，有专门的提示的，要重启系统才能生效
2、如果是向中神通公司申请许可证或增值 APP，则先要打开仪表盘>系统概要，点击设备序列号，下载设备信息包文件，文件名形如 xxxxxx_devinfo.zst，并发给中神通公司负责升级的人员，中神通公司就此才能做出相应的.gpk 升级文件

2.7.5 相关功能

1、上游功能：<无>
2、相关功能：<无>

3、下游功能：

 系统概要

2.8 帐号口令

2.8.1 功能简介

功能代码：adminshow，在此可以修改当前管理员的口令，下载证书登陆用的数字证书。

2.8.2 操作说明

1、根据提示分别输入相关的内容
2、如果需要证书认证登陆，则点击下方的下载按钮，下载证书并保存到 PC 中，点击下载的证书文件，根据提示安装到 IE 浏览器中

2.8.3 视频演示

账号口令设置:http://www.trustcomputing.com.cn/help/cn/system/password/password.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/system/bbs.html

2.8.4 注意事项

1、新口令长度有提示，口令复杂度应至少为字母和数字的组合
2、新旧口令不得一样，新口令与用户名不得一样
3、如果口令错误次数达到系统设置的上限，则系统会阻止登陆 IP 一段时间，同时显示在"系统概要"页面中，但前提是必须把"系统实时报警"的功能启用

2.8.5 相关功能

1、上游功能：
系统实时报警功能
2、相关功能：<无>

3、下游功能：

 系统概要

4、任务向导

B1 初始化本机数据

2.9 帮助功能

2.9.1 功能简介

系统为每个功能提供在线帮助功能，并且可以通过功能代码查找相应功能的帮助信息，帮助信息包括功能简介、操作说明、视频演示、注意事项、相关功能等 5 个方面的内容。

2.9.2 操作说明

1、用鼠标左键点击主界面左上角的图符，系统弹出帮助窗口；用鼠标左键点击主界面，使之成为当前窗口，再按 F1 键，系统弹出帮助窗口

2、在帮助窗口的查询输入框中，输入功能编号，例如：5.6，或者功能代码，例如：natshow，或者功能名称，例如：NAT 策略，就可以查询到相应的功能

3、在“相关功能”列中，用鼠标右键点击功能链接，显示该功能的帮助内容；用鼠标左键点击功能链接，在主界面中显示该功能的设置界面

2.9.3 视频演示

2.9.4 注意事项

如果没有弹出帮助窗口，可以按 F5 键刷新页面，再继续操作。

2.9.5 相关功能

1、上游功能：<无>
2、相关功能：
任务向导
3、下游功能：

二、访问控制篇

3 网络设置

3.1 网卡设置

3.1.1 功能简介

功能代码：nicshow，在此可以查看、修改本机的网卡设置，以便正确地和上下游路由器及网络相连。

3.1.2 操作说明

1、点击“修改”链接进入修改界面，选择、输入网卡参数，点击“确定”按钮生效
2、DHCP 方式可以自动获得 IP 地址、网络掩码及 DNS 服务器 IP，静态方式和 PPPoE 方式只能设置/获得 IP 地址及网络掩码，不能设置/获得 DNS 服务器，所以需要另外设置 DNS 服务器 IP，请查看 DNS 解析功能
3、点击“状态”按钮，查看网卡状态

3.1.3 视频演示

网卡设置:http://www.trustcomputing.com.cn/help/cn/network/nic/nic_setting.html
WAN 网卡设置:http://www.trustcomputing.com.cn/help/cn/network/nic/update_wan.html
LAN 网卡设置:http://www.trustcomputing.com.cn/help/cn/network/nic/update_lan.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/network/nic/bbs.html

3.1.4 注意事项

1、链路聚合、VLAN、网桥等基于物理网卡的虚拟网卡的设置，在另外的功能中设置，在此只显示相关信息
2、如果网卡状态显示半双工，则网卡的“介质”可以强制选择除“自动”外的其它选项
3、网线的插拔会产生相应的系统日志，可通过 Email 接收获知 IP 地址等信息

3.1.5 相关功能

1、上游功能：
初始设置
2、相关功能：
DNS 解析
DDNS 服务
3、下游功能：
网卡状态
IP 地址对象
链路聚合
VLAN 设置
网桥设置
双机热备
NAT 策略
总控策略
路由设置
ARP 服务
DHCP 服务
IDP 网卡规则
IPS 状态
蜜罐规则
用户认证>资源组
系统日志
系统概要
4、任务向导
B1 初始化本机数据
B2 NAT 模式接入
B3 透明网桥模式接入
B4 路由模式接入
C5 WEB 透明协议过滤
C6 WEB 透明内容过滤
C7 WEB 透明防病毒
C8 FTP、POP3、SMTP 透明过滤
C9 POP3、SMTP 透明防病毒
C10 POP3、SMTP 透明防垃圾邮件

D1 服务器接入

3.2 链路聚合

3.2.1 功能简介

功能代码：bondingshow，链路聚合可以将二块或以上的物理网卡合并成一块虚拟网卡，以增强网络处理性能。

3.2.2 操作说明

1、点击“新建”按钮或“修改”链接进入新建、修改界面，选择、输入链路聚合参数，点击“确定”按钮生效
2、点击“状态”按钮，查看链路聚合网卡状态

3.2.3 视频演示

链路聚合设置:http://www.trustcomputing.com.cn/help/cn/network/bonding/bonding.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/network/bonding/bbs.html

3.2.4 注意事项

1、物理网卡 IP 的设置方式只能是静态，不能是 DHCP 或 PPPOE
2、在新建链路聚合网卡后，各成员物理网卡 IP 将被删除，代之以链路聚合网卡的 IP；如果出现连通性问题，可重启设备
3、需要交换机将这几块网卡相连

3.2.5 相关功能

1、上游功能：
网卡设置
2、相关功能：
VLAN 设置
网桥设置

双机热备
ARP 服务
ARP 状态

3、下游功能：

网卡状态
NAT 策略
总控策略

3.3 VLAN

3.3.1 功能简介

功能代码：vlanshow，创建、管理基于 802.1Q 协议的 VLAN Trunk 虚拟网卡，与二层 VLAN 交换机相连，可以构成以本机为中心的三层交换网络。

3.3.2 操作说明

1、点击“新建”按钮或“修改”链接进入新建、修改界面，选择、输入 VLAN 参数，点击“确定”按钮生效
2、点击“状态”按钮，查看 VLAN 网卡状态

3.3.3 视频演示

VLAN 设置示例: http://www.trustcomputing.com.cn/help/cn/network/vlan/vlan.html
---
官方讨论区: http://www.trustcomputing.com.cn/help/cn/network/vlan/bbs.html

3.3.4 注意事项

1、VLAN 路由的实现：交换机启用 Trunk 口与同一 VLAN 标识的 VLAN 所在的物理网卡连接，局域网 PC 的网关设成 VLAN IP，物理网卡的 IP 可以不设置
2、在总控策略中，选择 VLAN 网卡，用以过滤该 VLAN 网络的流量
3、如果 VLAN 有 IP 地址，那么系统自动生成相应的网络及 IP 地址对象，可以在总控策略中直接引用

3.3.5 相关功能

1、上游功能：
网卡设置
链路聚合
2、相关功能：

网桥设置
双机热备
ARP 服务
ARP 状态

3、下游功能：

网卡状态
NAT 策略
总控策略
IP 地址对象
IDP 网卡规则

3.4 网桥设置

3.4.1 功能简介

功能代码：bridgeshow，创建、管理网桥，成员可以是物理网卡、链路聚合或 VLAN 网卡，用于在不改变现有网络拓扑的前提下，接入本机实施控制。

3.4.2 操作说明

1、点击“新建”按钮或“修改”链接进入新建、修改界面，选择、输入网桥参数，点击“确定”按钮生效
2、点击“状态”按钮，查看网桥状态
3、在“初始设置”中，“运行方式”选择“透明网桥接入”，将清空所有 NAT 策略及网桥，并自动新建一个网桥

3.4.3 视频演示

网桥设置示例:http://www.trustcomputing.com.cn/help/cn/network/bridge/bridge.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/network/bridge/bbs.html

3.4.4 注意事项

1、网桥的 IP，就是其网卡成员的 IP 的集合，若其网卡成员均无 IP，则需要通过有 IP 的网卡进行管理
2、网桥不作为总控策略里的网卡，对网桥的访问控制，分解为对其成员网卡的总控策略
3、点击网卡成员-MAC 地址过滤规则列的链接，设置该网络内的 MAC 地址黑白名单

3.4.5 相关功能

1、上游功能：
网卡设置
链路聚合

 VLAN 设置

 初始设置

2、相关功能：

 ARP 服务

3、下游功能：

 网卡状态

 总控策略

4、任务向导

B3 透明网桥模式接入

C5 WEB 透明协议过滤

C6 WEB 透明内容过滤

C7 WEB 透明防病毒

C8 FTP、POP3、SMTP 透明过滤

C9 POP3、SMTP 透明防病毒

C10 POP3、SMTP 透明防垃圾邮件

3.5 双机热备

3.5.1 功能简介

功能代码：failovershow，创建、管理双机热备，基础网卡可以是物理网卡、链路聚合或 VLAN 网卡，用于网关的冗余和负载均衡。

3.5.2 操作说明

1、点击“修改”链接进入修改界面，选择、输入双机热备参数，点击“确定”按钮生效
2、点击“状态”按钮，查看双机热备状态

3.5.3 视频演示

双机热备设置:http://www.trustcomputing.com.cn/help/cn/network/failover/failover.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/network/failover/bbs.html

3.5.4 注意事项

1、一台设备的所有双机热备网卡只能处于一种状态，要么是 MASTER，要么是 BAKCUP
2、可以不设置数据同步网卡
3、双机热备网卡的 IP，一般作为网关 IP，起到网关冗余的作用，但总控策略中仍以基础网卡为控制网卡

3.5.5 相关功能

1、上游功能：
网卡设置
链路聚合
VLAN 设置
2、相关功能：

 会话策略

3、下游功能：

 网卡状态

 总控策略

3.6 路由设置

3.6.1 功能简介

功能代码：routeshow，创建、管理静态路由，可为局域网中三层交换机后面的网络提供回程路由。

3.6.2 操作说明

1、点击“新建”按钮或“修改”链接进入新建、修改界面，选择、输入路由参数，点击“确定”按钮生效
2、点击其它 TAB 按钮，查看、管理动态路由

3.6.3 视频演示

静态路由设置:http://www.trustcomputing.com.cn/help/cn/network/route/route.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/network/route/bbs.html

3.6.4 注意事项

1、策略路由在总控策略里设置
2、缺省路由在网卡里设置，可以有多个缺省路由
3、“网关地址”必须和本机的某个网卡的 IP 在同一个网络内，否则出错；“目的网络”及“网卡”是根据“网关地址”值自动判断出的
4、“流量”值只具有相对比较作用，不代表真实的流量

3.6.5 相关功能

1、上游功能：
网卡设置

 链路聚合

 VLAN 设置

2、相关功能：

 总控策略

IPSEC 连接

 测试工具

3、下游功能：

 网卡状态

4、任务向导

B2 NAT 模式接入

B4 路由模式接入

3.7 DNS 解析

3.7.1 功能简介

功能代码：nameshow，设置本机的名称，设置本机的 DNS 服务器 IP，用于日志及内部程序的 DNS 解析。

3.7.2 操作说明

1、根据提示分别输入相关的参数
2、DNS 服务器 IP 可以参考“常用 DNS 服务器地址”页面的信息
3、点击“测试”按钮，进入 nslookup 测试界面，测试本机的 DNS 解析连通性

3.7.3 视频演示

DNS 解析设置:http://www.trustcomputing.com.cn/help/cn/network/name/name.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/network/name/bbs.html

3.7.4 注意事项

1、只保留 114.114.114.114 等国家级 DNS 服务器 IP 及本地 ISP 提供的 DNS 服务器 IP，其它不稳定的 DNS 服务器 IP 一律删除
2、主机名会在系统实时 Email 报警中出现，以区别不同的设备，故要确保其唯一

3.7.5 相关功能

1、上游功能：
网卡设置

2、相关功能：

 系统概要

 测试工具

3、下游功能：

 DHCP 服务

 DNS 代理过滤

 WEB 代理协议过滤

 PPTP VPN

4、任务向导

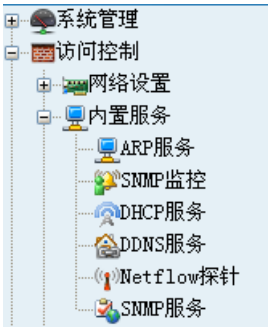
B1 初始化本机数据

C5 WEB 透明协议过滤

C6 WEB 透明内容过滤

C7 WEB 透明防病毒

4 内置服务



4.1 ARP 服务

4.1.1 功能简介

功能代码：macshow，设置 IP 与 MAC 地址的对应关系，防止 ARP 欺骗，定位 IP 地址使用者的身份，可以对 VLAN 网络进行绑定。

4.1.2 操作说明

1、点击“新建”按钮，可以新建一个 IP、MAC 对应关系定义；或者点击“更新”按钮，自动扫描网络中在线的 PC 设备等，可以以一个网络为整体快速新建定义
2、对于已存在的定义，可以选择序号后点击“绑定”、“临时”、“代理”按钮改变其绑定关系，或点击“删除”按钮删除
3、点击“状态”、“日志”按钮查看 ARP 缓存状态，或查看 ARP 日志

4.1.3 视频演示

1、手工单个绑定:http://www.trustcomputing.com.cn/help/cn/services/ipmac/mac_binding.html
2、自动扫描绑定:http://www.trustcomputing.com.cn/help/cn/services/ipmac/mac_update.html
3、ARP 状态示例:http://www.trustcomputing.com.cn/help/cn/services/ipmac/mac_status.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/services/ipmac/bbs.html

4.1.4 注意事项

1、为保证 IP、MAC 绑定效果，需要整个网段的所有 IP 均绑定，且 PC 客户端的网关 IP 设置成本设备的网卡 IP
2、为预防 ARP 病毒，需要在客户端安装 ARP 防火墙软件，绑定网关 IP 及正确的 MAC 地址
3、临时类型用于记录、占位，不起绑定作用；ARP 代理相当于增加克隆一个新 IP，用于 NAT 地址池、蜜罐等功能

4.1.5 相关功能

1、上游功能：
网卡设置
VLAN 设置
链路聚合设置
路由流控功能控制
2、相关功能：
ARP 防火墙软件
NAT 策略
蜜罐审计
网桥设置
用户定义
3、下游功能：
ARP 状态
ARP 日志
4、任务向导
C1 上网行为管理
C2 防控 ARP 病毒
D1 服务器接入

4.2 SNMP 监控

4.2.1 功能简介

功能代码：mac3layershow，通过监控三层交换机等网络设备的 SNMP 记录，实现隔着三层交换机绑定 PC 的 IP 和 MAC 地址。

4.2.2 操作说明

1、点击“新建”按钮或“修改”链接进入新建、修改界面，选择、输入 SNMP 监控参数，点击“确定”按钮生效
2、点击“状态”链接，查看当前 SNMP 监控状态
3、点击“日志”按钮，查看 SNMP 监控日志

4.2.3 视频演示

SNMP 监控服务:http://www.trustcomputing.com.cn/help/cn/services/mac3layer/mac3layer.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/services/mac3layer/bbs.html

4.2.4 注意事项

1、需要在 SNMP 代理所在的设备上开启 SNMP 服务，才能使用本功能，可以监控任何具备 SNMP 代理的网络设备
2、系统每 10 分钟检测一次
3、如果要阻拦不符合设置的 IP，需要打开 IPS 功能

4.2.5 相关功能

1、上游功能：
网卡设置
2、相关功能：
SNMP 软件

 SNMP 服务
 IPS 设置
 ARP 服务
 ARP 状态
 ARP 日志

3、下游功能：

 SNMP 监控日志

4、任务向导

C2 防控 ARP 病毒

4.3 DHCP 服务

4.3.1 功能简介

功能代码：dhcpdshow，提供 DHCP 服务器和 DHCP 中继两种类型的服务，为网络客户端自动获取 IP、DNS 服务器、缺省路由等提供配置服务。

4.3.2 操作说明

1、点击“修改”链接进入修改界面，选择、输入 DHCP 服务参数，点击“确定”按钮生效
2、点击“租借状态”列链接，查看 DHCP 客户端状态

4.3.3 视频演示

1、DHCP 服务器设置: http://www.trustcomputing.com.cn/help/cn/services/dhcp/dhcp_server.html
2、DHCP 中继设置:http://www.trustcomputing.com.cn/help/cn/services/dhcp/dhcp_relay.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/services/dhcp/bbs.html

4.3.4 注意事项

1、网络内出现多个 DHCP 服务器会对客户端获取 IP 产生干扰
2、当 DHCP 服务器不在本网段内，可以启用 DHCP 中继；VLAN 定义中包含 DHCP 中继 IP
3、在 ARP 设置中绑定的 MAC 的 IP，将固定分配给该 MAC 地址的机器

4.3.5 相关功能

1、上游功能：
网卡设置
DNS 解析
ARP 服务
路由流控功能控制

2、相关功能：

VLAN 设置

3、下游功能：<无>

4、任务向导

C1 上网行为管理

4.4 DDNS 服务

4.4.1 功能简介

功能代码：ddnsshow，如果外网网卡 IP 是动态获取的，可以通过将该 IP 绑定到一个域名的方法，实时得到该 IP，本功能用于通知 DDNS 服务提供商，更新该域名的 IP 地址。

4.4.2 操作说明

1、点击“修改”链接进入修改界面，选择、输入 DDNS 服务参数，点击“确定”按钮生效
2、在测试工具或 PC 中，查看绑定域名解析状态

4.4.3 视频演示

DDNS 服务:http://www.trustcomputing.com.cn/help/cn/services/ddns/ddns.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/services/ddns/bbs.html

4.4.4 注意事项

1、事先要在 DDNS 服务提供商的网站上注册域名、用户名及口令
2、还可以在内网服务器上运行花生壳等工具软件，实现同样的功能

4.4.5 相关功能

1、上游功能：
路由流控功能控制
网卡设置
2、相关功能：
测试工具
3、下游功能：<无>

4.5 Netflow 探针

4.5.1 功能简介

功能代码：netflowshow，将本机的流量转化成 netflow 数据流，发送给接收服务器，在接收服务器处保存、分析流量。

4.5.2 操作说明

1、根据提示分别输入相关的参数，点击“确定”按钮生效

4.5.3 视频演示

1、Netflow 探针设置:
http://www.trustcomputing.com.cn/help/cn/services/netflow/run_netflow.html
2、NetFlowAnalyzer 软件设置:
http://www.trustcomputing.com.cn/help/cn/services/netflow/NetFlowAnalyzer.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/services/netflow/bbs.html

4.5.4 注意事项

1、在接收服务器处安装 netflow analyzer 等分析软件，同时打开 PC 防火墙的接收端口
2、会话对象中可以设置“会话同步”的启用、停用，控制是否生成 netflow 流

4.5.5 相关功能

1、上游功能：
会话对象
总控策略
路由流控功能控制
2、相关功能：

 Netflow Analyzer 软件

 流量状态图表

3、下游功能：<无>

4、任务向导

A1 查看运行状态

C3 网络流量控制

C4 网络流量计费

D1 服务器接入

4.6 SNMP 服务

4.6.1 功能简介

功能代码：snmpshow，对外提供 SNMP 查询服务，用于网络设备的集中管理。

4.6.2 操作说明

1、根据提示分别输入相关的参数，点击“确定”按钮生效
2、修改网卡设置的“管理”选项为启用，才能从外部通过该网卡 IP 查询本机 SNMP 信息

4.6.3 视频演示

SNMP 设置:http://www.trustcomputing.com.cn/help/cn/services/snmp/snmp.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/services/snmp/bbs.html

4.6.4 注意事项

1、MIB-2 视图比系统视图能提供更多的查询参数
2、网卡的“管理”选项是否启用决定了外部能否通过该网卡 IP 查询 SNMP 信息

4.6.5 相关功能

1、上游功能：
网卡设置
2、相关功能：
SNMP 软件
3、下游功能：<无>
4、任务向导
A1 查看运行状态

C3 网络流量控制

5 基础策略

5.1 地址对象

5.1.1 功能简介

功能代码：ipshow，定义 IP 地址对象，一个地址对象包括多个 IP 及网段，用于总控策略、特殊应用等控制策略中，作为来源或目的地址。系统预定义了一些 IP 地址对象，如网卡网段、网卡 IP 等，可以直接使用。

5.1.2 操作说明

1、点击“新建”按钮或“修改”链接进入新建、修改界面，选择、输入 IP 地址参数，点击“确定”按钮生效
2、对于已存在且没有被引用的定义，可以选择序号后点击“删除”按钮删除
3、点击“来源功能统计”按钮，查看来源 IP 对象的各功能统计列表
4、在总控策略的新建或修改界面中，在“来源 IP”、“目的 IP”选项处，选择定义好的地址对象，加载该地址对象的 IP、网段内容；其它控制策略的实施与此类似

5.1.3 视频演示

IP 对象设置:http://www.trustcomputing.com.cn/help/cn/policy/ip_object/ip_object.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/policy/ip_object/bbs.html

5.1.4 注意事项

1、系统预定义的 IP 地址对象不能删除，修改网卡参数将同时修改基于网卡的 IP 地址对象的内容，例如 LAN_network、LAN_ip 等。当 LAN 网卡的网络号发生改变后，系统将自动修改 USER_ip 中的内容
2、USER_ip 应包括 SUPERUSER_ip 中的 IP 地址，SUPERUSER_ip 中列出的源 IP 将不受网络审计及应用过滤的控制，详情参见总控策略
3、被控制策略引用的 IP 地址对象，可以只修改其 IP 或网段内容，而不用再修改其所在的控制策略

5.1.5 相关功能

1、上游功能:
网卡设置
VLAN 设置
2、相关功能:
链路聚合
双机热备
流量统计
3、下游功能:
NAT 策略
总控策略
特殊应用
DNS 及 URL 库
PPTP VPN
PPPoE 接入
IPSEC 网关
IPSEC 连接
SSL 接入
4、任务向导
B2 NAT 模式接入
B3 透明网桥模式接入
B4 路由模式接入
C1 上网行为管理

5.2 时间对象

5.2.1 功能简介

功能代码：timeshow，定义时间对象，一个时间对象包括多个不重复的时间段，用于总控策略、特殊应用等控制策略中，作为生效策略时间。系统预定义了一些时间对象，如所有时间、没有时间、工作时间等，可以直接使用、修改。

5.2.2 操作说明

1、点击“新建”按钮或“修改”链接进入新建、修改界面，选择、输入时间参数，点击“确定”按钮生效
2、对于已存在且没有被引用的定义，可以选择序号后点击“删除”按钮删除
3、点击已存在定义所在行的“新建”或“修改”链接，只对该定义做“新建”或“修改”
4、在总控策略的新建或修改界面中，在“时间”选项处，选择定义好的时间对象，实施该时间对象的策略

5.2.3 视频演示

时间对象设置:http://www.trustcomputing.com.cn/help/cn/policy/time_object/time_object.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/policy/time_object/bbs.html

5.2.4 注意事项

1、系统预定义的时间对象不能删除
2、被控制策略引用的时间对象，可以只修改其时间段内容，而不用再修改其所在的控制策略

5.2.5 相关功能

1、上游功能：

系统时间

2、相关功能：<无>

3、下游功能：

NAT 策略

总控策略

特殊应用

DNS 及 URL 库

资源组

4、任务向导

B2 NAT 模式接入

B3 透明网桥模式接入

B4 路由模式接入

C1 上网行为管理

5.3 流量对象

5.3.1 功能简介

功能代码：trafficshow，定义流量对象，一个流量对象包括总流量配额、持续、上传流量阈值的定义，用于总控策略中，作为流量总量控制的依据。系统预定义了一些流量对象作为参考，可以直接使用、修改。

5.3.2 操作说明

1、点击“新建”按钮或“修改”链接进入新建、修改界面，选择、输入流量参数，点击“确定”按钮生效
2、对于已存在且没有被引用的定义，可以选择序号后点击“删除”按钮删除
3、第一个流量对象 Normal_tc 的“流量统计间隔”参数，是流量配额统计的间隔时间；动态（持续、上传）流量控制的统计间隔时间是固定的 1 分钟；在路由流控功能统计界面中，如果不启用“流量策略”，则这两个功能都停用
4、在总控策略的新建或修改界面中，在“流量”选项处，选择定义好的流量对象，实施该流量对象的策略

5.3.3 视频演示

流量对象设置:
http://www.trustcomputing.com.cn/help/cn/policy/traffic_object/traffic_object.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/policy/traffic_object/bbs.html

5.3.4 注意事项

1、系统预定义的流量对象不能删除
2、被控制策略引用的流量对象，可以只修改其流量参数，而不用再修改其所在的总控策略
3、系统每隔 1 小时自动生成流量统计日志，再发送到管理员 Email，方便其快速了解网络

流量情况

4、在 IPS 状态及 IPS 日志中查看被阻拦的 IP

5.3.5 相关功能

1、上游功能：

 路由流控功能控制

2、相关功能：

 IPS 设置

 IPS 状态

3、下游功能：

 总控策略

 流量日志

 流量统计

 流量统计日志

 在线主机

 用户组

4、任务向导

C1 上网行为管理

C3 网络流量控制

C4 网络流量计费

D1 服务器接入

5.4 会话对象

5.4.1 功能简介

功能代码：sessionshow，定义会话对象，用于总控策略中，实现状态过滤，可以针对某一条总控策略中单个源 IP 的最大会话数和最大新建会话速率的控制。系统预定义了一些会话对象作为参考，可以直接使用、修改。

5.4.2 操作说明

1、点击“新建”按钮或“修改”链接进入新建、修改界面，选择、输入会话参数，点击“确定”按钮生效
2、对于已存在且没有被引用的定义，可以选择序号后点击“删除”按钮删除
3、在总控策略的新建或修改界面中，在“会话”选项处，选择定义好的会话对象，实施该会话对象的策略

5.4.3 视频演示

会话对象设置:
http://www.trustcomputing.com.cn/help/cn/policy/session_object/session_object.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/policy/session_object/bbs.html

5.4.4 注意事项

1、被总控策略引用的会话对象，可以只修改其会话参数，而不用再修改其所在的总控策略
2、选择在线主机>流量明细功能，可以了解各源 IP、各控制策略的会话数统计，红色数字表明已达到最大会话数上限
3、会话超时是指会话建立后，若无新流量更新，从会话池中删除的倒计时间，又称老化时间

5.4.5 相关功能

1、上游功能：

 路由流控功能控制

2、相关功能：<无>

3、下游功能：

 总控策略

 在线主机

 会话状态

 Netflow 服务

 双机热备

4、任务向导

C1 上网行为管理

C3 网络流量控制

D1 服务器接入

5.5 QoS 对象

5.5.1 功能简介

功能代码：qosshow，定义 QoS 对象，用于总控策略中，作为实时带宽控制的依据，可以实现针对某一条总控策略中全体来源 IP 的带宽控制。具备树状带宽分配功能，可以实现对已知及未知流量的精确控制，以及空闲带宽的借用。系统预定义了一些 QoS 对象作为参考，可以直接使用、修改。

5.5.2 操作说明

1、点击“新建”按钮或“修改”链接进入新建、修改界面，选择、输入 QoS 参数，点击“确定”按钮生效
2、对于已存在且没有被引用的定义，可以选择序号后点击“删除”按钮删除
3、在总控策略的新建或修改界面中，在“QoS”选项处，选择定义好的 QoS 对象，实施该 QoS 对象的策略
4、“路由流控功能”中可以控制 QoS 策略整体是否实施，在 QoS 列表界面的“功能状态”处中有显示
5、点击“状态”按钮，查看 QoS 带宽分配状态

5.5.3 视频演示

QOS 策略应用:http://www.trustcomputing.com.cn/help/cn/policy/qos/qos_policy.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/policy/qos/bbs.html

5.5.4 注意事项

1、被总控策略引用的 QoS 对象，可以只修改其 QoS 参数，而不用再修改其所在的总控策略
2、选择在线主机>流量明细功能，可以了解各源 IP、各控制策略的平均带宽速率，与 QoS 对象定义的实时带宽不完全一样

5.5.5 相关功能

1、上游功能：


路由流控功能控制

2、相关功能：<无>

3、下游功能：


总控策略


QoS 状态


在线主机


会话状态


网卡状态


网络状态趋势

4、任务向导

C1 上网行为管理

C3 网络流量控制

5.6 NAT 策略

5.6.1 功能简介

功能代码：natshow，NAT 即网络地址转换，其中，来源 NAT 用于局域网通过外网网卡 IP 上外网；目的 NAT 又称端口转发，可用于将内网服务端口发布到外网，或拦截内网出网流量至本机代理服务程序，实现透明代理功能；双向 NAT 又称一对一 NAT，可以将某个内网 IP 全部转换到某个外网 IP。

5.6.2 操作说明

1、点击“新建”按钮或“修改”链接进入新建、修改界面，选择、输入 NAT 参数，点击“确定”按钮生效；可以先选择“序号”框再点击“新建”按钮，以方便在选择处插入新的 NAT 策略；系统为新建策略提供模板选择项，可以在此基础上调整
2、对于已存在的策略，可以选择序号后点击“删除”按钮删除
3、每一条 NAT 策略都对应一条总控策略，可以修改相对应的总控策略的时间对象，达到修改 NAT 策略生效时间的目的，点击“总控策略”列的链接查看相对应的总控策略
4、“路由流控功能”中可以控制 NAT 策略整体是否实施，在 NAT 策略列表界面的“功能状态”处中有显示
5、在“初始设置”中，如果“运行方式”选择“来源 NAT”，将清空所有 NAT 策略及网桥设置，并自动新建一条内网出外网的来源 NAT 策略

5.6.3 视频演示

NAT 策略演示:http://www.trustcomputing.com.cn/help/cn/policy/nat/nat_policy.doc
DNAT 策略设置:http://www.trustcomputing.com.cn/help/cn/policy/nat/dnat_policy.html
SNAT 策略设置:http://www.trustcomputing.com.cn/help/cn/policy/nat/snat_policy.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/policy/nat/bbs.html

5.6.4 注意事项

1、NAT 策略的匹配顺序是“马上生效”，即系统按从上到下的顺序用 NAT 策略去匹配数据流的源 IP、源端口、协议、目的 IP、目的端口 5 元素，如果匹配，则就按该匹配的 NAT 策略执行，而不再向下继续查找
2、由于新建、修改 NAT 策略会导致总控策略的序号发生变化，所以要在完成全部编辑操作后终止现有的会话
3、做来源 NAT 时，如果来源地址是内网路由器后面的网段，需要新建回程路由
4、DNAT 时的网卡为来源数据包进入网关时的网卡，SNAT 时的网卡为来源数据包穿出网关时的网卡
5、必要时系统自动为策略中非本机网卡 IP 的 IP 地址做 ARP 代理服务，使得通讯能正常进行

5.6.5 相关功能

1、上游功能：
初始设置
链路聚合
VLAN 设置
IP 地址对象
时间对象
路由流控功能控制
2、相关功能：
ARP 服务
ARP 状态
应用代理
会话状态
3、下游功能：
总控策略
4、任务向导
B2 NAT 模式接入
B3 透明网桥模式接入
B4 路由模式接入
C1 上网行为管理
C5 WEB 透明协议过滤
C6 WEB 透明内容过滤
C7 WEB 透明防病毒
C8 FTP、POP3、SMTP 透明过滤
C9 POP3、SMTP 透明防病毒
C10 POP3、SMTP 透明防垃圾邮件
D1 服务器接入

5.7 总控策略

序号	动作	网卡	来源	认证	目的	协议	端口	时间	流量	会话	QoS	日志	状态
	丢弃	ALL	ALL_network		ALL_network	IP		ALL_time				简单	
1	允许	»LAN	USER_ip		ALL_network	IP		ALL_time	Normal_tc	Normal_session		详细	MSTH
2	允许↑	»WAN	ALL_network		Server1	TCP*	666	ALL_time	Normal_tc	Normal_session		详细	MSTH
3	允许↑	»WAN	ALL_network		Server1	TCP*	888	ALL_time	Normal_tc	Normal_session		详细	MSTH
4	允许↑	»ALL	SUPERUSER_ip		ALL_network	IP		ALL_time	Normal_tc	Normal_session		简单	MSTH
5	允许	»ALL	USER_ip		ALL_network	IP		ALL_time	IP_tc	IP_session		简单	MSTH
6	允许	»LAN	USER_ip		ALL_network	TCP	1~65535	ALL_time	TCP_tc	TCP_session	TCP_qos	详细	MSTH
7	允许	»LAN	USER_ip		ALL_network	UDP	1~65535	ALL_time	UDP_tc	UDP_session	UDP_qos	简单	MSTH

5.7.1 功能简介

功能代码：pfshow，总控策略实现对网络访问控制策略的定义，由多个事先定义的对象作为基础，既可以实现对流量通过与否的判断，也可以实现对通过流量的路由、会话、带宽、总流量进行控制，还可以为日志记录、IDP 功能提供数据源。特殊应用、应用代理的自动策略是另外的、独立的控制策略，是对总控策略和 NAT 策略的补充，可方便管理员简化设置流程。

5.7.2 操作说明

1、可以先选择序号，再点击“新建”或“粘贴”按钮，相当于插入新定义；否则就是在最后添加新定义
2、对于已存在的策略，可以先选择序号再点击“删除”或“拷贝”按钮删除或拷贝定义
3、每一条 NAT 策略都对应一条总控策略，且均按顺序排在最前面，这样的总控策略其“动作”、“方向”、“来源 IP”、“目的 IP”、“协议”等项均不能再修改，如果要覆盖这条策略，可以在“规则匹配”处选择“继续检查”，并在其下新建相对应的策略；在列表界面中，点击“序号”列的链接查看相对应的 NAT 策略
4、“路由流控功能”中可以控制总控策略整体是否实施，在总控策略列表界面的“功能状态”处中有显示
5、初始设置中的“标准流控策略”及“粘贴”界面中的“还原初始规则”，都可以快速生成系统预定义的内网上网控制策略

5.7.3 视频演示

界面介绍:http://www.trustcomputing.com.cn/help/cn/policy/control/basic_operation.html
设置过程:http://www.trustcomputing.com.cn/help/cn/policy/control/control_policy.html
相关功能:http://www.trustcomputing.com.cn/help/cn/policy/control/related_function.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/policy/control/bbs.html

5.7.4 注意事项

1、总控策略匹配顺序由源 IP、源端口、协议、目的 IP、目的端口 5 元素及“规则匹配”选项决定，系统按从上到下的顺序进行匹配，在数据流的 5 元素与总控策略匹配的前提下，如果是“马上生效”，则按此策略实行，并会在列表界面的“动作”列中显示“允许↑”，如果是“继续检查”则即使当前匹配仍依次往下查找，并按最后一条匹配的总控策略实行；“动作”项是“拒绝”时，只能“继续检查”，不能“马上生效”，防止 WEB 管理被阻拦
2、总控策略内置的第一条策略是“拒绝所有”的策略，管理员一般只要在其后定义通过的策略即可，即遵循“除非允许，否则拒绝”的原则
3、“方向”一般选择“流入网卡”，此时的“网卡”是最靠近来源 IP 对象的网卡，会在列表界面中显示“»网卡”
4、由于新建、修改总控策略会导致其序号发生变化，所以要在完成全部编辑操作后终止现有的会话
5、“日志”选项是“简单”则只记录通过数据流的第一个数据包，“详细”则记录全部数据包，这些记录的数据包可以在“实时监控”、“网络审计”、“IDP 规则”功能中实时显示、记录、检查

5.7.5 相关功能

1、上游功能：
初始设置
链路聚合
VLAN 设置
IP 地址对象
时间对象
流量对象
会话对象
QoS 对象
NAT 策略
路由流控功能控制
2、相关功能：
特殊应用
3、下游功能：
流量统计
在线主机
会话状态
网络审计>总体设置
4、任务向导
B2 NAT 模式接入
B3 透明网桥模式接入
B4 路由模式接入
C1 上网行为管理
C3 网络流量控制

C4 网络流量计费
C5 WEB 透明协议过滤
C6 WEB 透明内容过滤
C7 WEB 透明防病毒
C8 FTP、POP3、SMTP 透明过滤
C9 POP3、SMTP 透明防病毒
C10 POP3、SMTP 透明防垃圾邮件
C11 QQ、MSN 过滤
C12 抓包分析并阻拦特定应用
D1 服务器接入
D2 SSL 接入
E2 WEB 门户认证
F1 PPTP、PPPOE 用户接入
F2 IPSEC VPN 接入

三、应用过滤篇

6 应用过滤

6.1 特殊应用总体设置

6.1.1 功能简介

功能代码：specappbasicshow，在此设置特殊应用整体启用状态，每个种类的来源地址及时间，进入每个种类设置界面还可以进一步选择通过或阻拦具体应用。每个具体应用无论是通过还是阻拦，均可以记录使用者的源 IP 及流量。

6.1.2 操作说明

1、选择所需的设置项，点击“确定”按钮生效
2、点击“状态”、“日志”按钮，进入查看特殊应用状态或日志的界面

6.1.3 视频演示

1、策略设置示例:
http://www.trustcomputing.com.cn/help/cn/appfilter/specapp/policy_setting.html
2、状态统计示例:
http://www.trustcomputing.com.cn/help/cn/appfilter/specapp/specappstatus.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/specapp/bbs.html

6.1.4 注意事项

1、总控策略必须启用，才能使特殊应用有效
2、如果启用了 DNS 及 URL 库域名过滤，则可能在 DNS 解析阶段就阻拦了相关的特殊应用
3、最好同时启用 WEB 审计过滤（WAF），这将过滤与具体特殊应用有关的网站
4、应用特征库的更新需要单独的 License，请咨询供应商

6.1.5 相关功能

1、上游功能:
总控策略
IP 地址对象
时间对象
许可证
上网管理功能控制
2、相关功能:
DNS 及 URL 库
WEB 审计过滤（WAF）
3、下游功能:
特殊应用状态
特殊应用日志
4、任务向导
C1 上网行为管理

6.2 特殊应用功能设置

6.2.1 功能简介

功能代码：specappshow，在此选择具体应用的实施方式：通过、阻拦或停用。最终策略应用方式，还取决于特殊应用总体设置中，本类应用的源 IP、时间等参数在此选择具体应用的实施方式：通过、阻拦或停用。最终策略应用方式，还取决于特殊应用总体设置中，本类应用的源 IP、时间等参数。

6.2.2 操作说明

1、选择序号列的选择框，再点击下方的“阻拦”、“通过”或“停用”按钮
2、点击下方的“状态”按钮，进入查看本类应用状态的界面
3、左/右键点击左边主菜单中本类名称链接，例如，网络视频等，可以直接进入到本类的状态界面
4、点击“来源数”列数字链接，查看该具体应用的状态

6.2.3 视频演示

1、策略设置示例:
http://www.trustcomputing.com.cn/help/cn/appfilter/specapp/policy_setting.html
2、状态统计示例:
http://www.trustcomputing.com.cn/help/cn/appfilter/specapp/specappstatus.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/specapp/bbs.html

6.2.4 注意事项

1、设置列表界面同时也是本类应用状态统计界面
2、此处显示的封包数、字节数不代表该应用的全部流量，只是定性分析的结果，在多个 IP

之间做相对比较有意义

6.2.5 相关功能

1、上游功能：

 特殊应用

 许可证

 上网管理功能控制

2、相关功能：

 来源功能统计

 DNS 及 URL 库

 WEB 审计过滤（WAF）

 在线主机

 流量统计

 流量日志

 会话状态

 日志统计

 系统概要

3、下游功能：

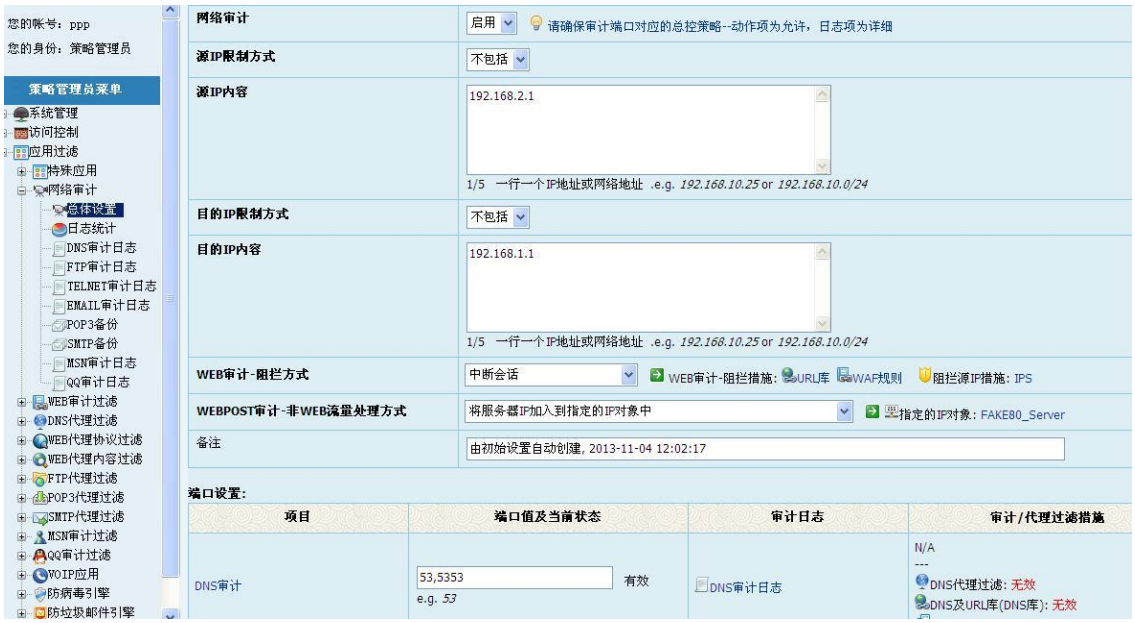
 特殊应用状态

 特殊应用日志

4、任务向导

C1 上网行为管理

6.3 网络审计



6.3.1 功能简介

功能代码：netauditshow，在此设置网络审计的整体启用状态、来源 IP 范围、目的 IP 范围、端口值等参数。网络审计可以记录下用户发出的数据包的应用层信息，并可以在此基础上做日志统计，分析出最活跃用户、最热门内容等信息，还可以查找某个源 IP 的上网记录。

6.3.2 操作说明

1、根据提示分别选择或输入相关的参数，端口值处不填，表示不启用该项网络审计
2、"WEB 审计"端口值中包含"555"，表示停用 WEB 审计过滤(WAF)及 DNS&URL 库(URL 库)过滤功能;"WEBPOST 审计"端口值中包含"444"，表示停用非标准 80 端口审计功能
3、点击“日志统计”按钮，进入查看日志分时统计的界面，还可以输入某个源 IP，进行该 IP 上网轨迹的查询

6.3.3 视频演示

总体设置示例:http://www.trustcomputing.com.cn/help/cn/appfilter/netaudit/netaudit.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/netaudit/bbs.html

6.3.4 注意事项

1、请确保审计端口对应的总控策略--动作项为允许，日志项为详细，例如，如果要审计 WEB，则必须保证在总控策略中有一条规则，其目的端口和此处的端口值相同，动作项是允许，日志项是详细
2、所有日志均保存在本机的存储器中，每天 0 时压缩打包一次，以节省空间，方便下载，另外有专门的审计管理员，负责对日志的管理

6.3.5 相关功能

1、上游功能：
总控策略
初始设置
上网管理功能控制
2、相关功能：
非标准 80 端口服务器 IP
DNS 及 URL 库(URL 库)
WAF 规则
聊天通信
IPS
3、下游功能：
各审计日志及日志统计
POP3 邮件备份
SMTP 邮件备份
MSN 审计过滤
QQ 审计过滤
4、任务向导
A2 查看当前日志内容
C1 上网行为管理
D1 服务器接入

6.4 WEB 审计过滤

6.4.1 功能简介

功能代码：wafshow，WEB 审计过滤是在 WEB 审计基础上的，对 HTTP 协议请求部分的过滤，由于不参与数据流的转发，因此网络吞吐性能不受影响。WEB 审计过滤可以看做一种广义的 WAF，它既可用于内网上网管理，又可用于保护 WEB 服务器，使其免受 SQL 注入等攻击。

6.4.2 操作说明

1、分为白名单和黑名单两种设置界面。黑名单界面“方式”选项中，“仅限于”是指仅过滤内容列表中的项目，“不包括”是指过滤不在内容列表中的项目，后者更严格一些
2、可以查看 WEB 审计日志“通过/阻拦”列的内容，判断该 URL 是否被阻拦，被阻拦的列显示"DENY_XXX"；对于通过的 URL，可以查看该 URL 各列的内容，用来确定阻拦该 URL 黑名单的类型及内容
3、在网络审计>总体设置中，可以设置来源 IP、目的 IP 范围，以及 WEB 审计端口范围，缩小审计范围可以提高审计效率

6.4.3 视频演示

1、WAF 规则设置:http://www.trustcomputing.com.cn/help/cn/appfilter/waf/waf_rules.html
2、DNS&URL 库:http://www.trustcomputing.com.cn/help/cn/appfilter/waf/webaudit_urldb.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/waf/bbs.html

6.4.4 注意事项

1、必须保证在总控策略中有一条规则，其目的端口包含此处的端口，动作项是允许，日志项是详细；必须保证网络审计总体设置状态有效
2、在初始设置中，启用“网络审计”选项，也可以启用 WEB 审计过滤;
如果“DMZ 区服务器 IP 地址及端口”中填写有 IP 地址(LAN 区或 DMZ 区 IP 地址)及端口 80(80 或者 80,110 这样), WAF 规则中的"CGI 参数"过滤将启用
3、只有在 TAB 名称右边有括号、括号里有数字的过滤类型，才是目前生效的类型

6.4.5 相关功能

1、上游功能：
网络审计>总体设置
初始设置
总控策略
上网管理功能控制
2、相关功能：
DNS 及 URL 库
IPS
DNS 代理过滤>总体设置
3、下游功能：
WEB 审计日志
4、任务向导
C1 上网行为管理
C12 抓包分析并阻拦特定应用
D1 服务器接入

6.5 DNS 代理过滤

6.5.1 功能简介

功能代码：dnsshow，DNS 代理首先是一个 DNS 转发器，它将客户端的请求转发到 DNS 服务器处，并将结果缓存起来；其次，它可以用来过滤客户端的请求，过滤措施包括内置的 DNS 及 URL 库和自定义域名规则；为了方便部署，可以通过 DNAT 策略，实现透明代理功能，不管客户端的 DNS 服务器怎么设置，均被强制重定向，先过滤再转发到本机的 DNS 服务器处查询，可以重定向到内置页面，也可以重定向到其它 WEB 服务器，方便用户了解被过滤的情况。

6.5.2 操作说明

1、根据提示分别选择或输入相关的参数。其中“DNS 转发服务器”即本机的 DNS 服务器；“库中域名过滤对应的 IP”是指 DNS 及 URL 库内的域名被统一解析成某个 IP，可以是本机内置的 WEB 服务器 IP（即各网卡的 IP），也可以是其它 WEB 服务器 IP，这样用户可以得到被过滤的提示，或者是 127.0.0.2，这样不会产生网络流量

2、当选择“启用服务+自动策略”项时，系统自动创建 DNAT 策略，实现透明代理的功能；如果选择“仅启用服务”项，则要么客户端要指定本机 IP 为 DNS 服务器 IP，要么管理员再新建 DNAT 策略（参见第 3 条），实现透明代理的功能。前者设置方便快速，但缺少时间、来源 IP、流量控制等策略控制，后者正好相反

3、如果选择“仅启用服务”项，可以点击“DNAT 策略执行点：无”的链接，进入新建 DNAT 策略的界面，系统自动设置好了相关参数，根据需要做一些调整，按“确定”按钮，即可生成 DNAT 策略

6.5.3 视频演示

1、总体设置示例:
http://www.trustcomputing.com.cn/help/cn/appfilter/dnsfilter/general_setting.html
2、DNS&URL 库:
http://www.trustcomputing.com.cn/help/cn/appfilter/dnsfilter/dnsurldbshow.html

3、域名规则设置: http://www.trustcomputing.com.cn/help/cn/appfilter/dnsfilter/dnsruleshow.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/dnsfilter/bbs.html

6.5.4 注意事项

1、为了加快 DNS 解析速度，必须将最快、最稳定的 DNS 服务器-通常是本地 ISP 的 DNS 服务器 IP 设置成第一、二位的本机 DNS 服务器，同时把其它 DNS 服务器删除，避免无法解析！
2、由于客户端 PC、浏览器也有 DNS 缓存功能，为了保证 DNS 代理过滤的效果，必要时需要清除 PC 的 DNS 缓存，方法是打开 DOS 窗口，运行 ipconfig/flushdns 命令，然后再清除浏览器的缓存
3、为防止客户端私设 hosts 文件，可以将客户端 PC 加入 windows 域管理，或启用 WEB 代理协议过滤，同时启用“本地 DNS 代理”选项
4、如果在初始设置中，选了“DNS 及 URL 库”中的一个或以上项目，则系统自动启用 DNS 代理过滤

6.5.5 相关功能

1、上游功能：
DNS 解析
NAT 策略
初始设置
上网管理功能控制
2、相关功能：
DNS 审计日志
3、下游功能：
DNS 及 URL 库
域名规则
DNS 代理日志
WEB 代理协议过滤
测试工具>Nslookup
DOS 命令：ipconfig/flushdns
4、任务向导
C1 上网行为管理

6.6 DNS&URL 库

6.6.1 功能简介

功能代码：dnsurldbshow，系统提供四个大类、二十几个分类的网站数据库，包括域名数据库和 URL 数据库，前者由 DNS 代理过滤实现，后者由 WEB 审计过滤（WAF）实现，既能够实现大规模的网址过滤功能，也能够达到阻拦相应网络应用的目的。域名过滤的来源 IP 由 DNS 代理总体设置及 DNAT 策略决定，URL 过滤的来源 IP 由网络审计总体设置及 WEB 审计 WAF 策略决定，各分类的生效时间可以单独设置。

域名库可以在 DNS 查询阶段过滤形如 https://www.xxx.com 和 http://www.xxx.com:82 这样的 URL，这是 URL 库难以做到的。URL 库中包含有任意位置的 URL 特征码，例如^tracker，可以过滤所有以 tracker 开头的 URL，这是域名库所无法做到的，因此，这两者是互补的关系。

6.6.2 操作说明

1、勾选各分类 DNS 及 URL 库，再点击下方的“启用”或“停用”按钮生效

2、如果要改变某一分类 DNS 及 URL 库的生效时间，则需要点击该行最右边“修改”链接，选择合适的时间对象，点击“确定”按钮生效

3、为了了解某个域名是否在 DNS 及 URL 库内，可以点击下方的“查询”按钮进行查询

4、为了取消 DNS 及 URL 库中的某个域名的过滤作用，可以为其单独新建一条域名规则，填入正确的解析后的 IP 地址

5、DNS 及 URL 库的更新需要单独的 License，请咨询供应商

6、为了避免点击“查询”按钮时出现的提示确认的窗口条，需要更改浏览器设置，具体操作是点击“工具>Internet 选项>安全(TAB)>自定义级别”，在打开的“安全设置”窗口中，找到“脚本”大类，将“允许网站使用脚本窗口提示获得信息”项设置成“启用”

6.6.3 视频演示

1、总体设置示例:

http://www.trustcomputing.com.cn/help/cn/appfilter/dnsfilter/general_setting.html

2、DNS&URL 库:

http://www.trustcomputing.com.cn/help/cn/appfilter/dnsfilter/dnsurldbshow.html

3、域名规则设置: http://www.trustcomputing.com.cn/help/cn/appfilter/dnsfilter/dnsruleshow.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/dnsfilter/bbs.html

6.6.4 注意事项

1、DNS 代理过滤总体设置状态必须是有效，DNS 及 URL 库的域名过滤才能发挥作用，同时，如果自定义域名规则有域名设置，则系统马上返回该设置，而不会再查询 DNS 及 URL 库
2、由于客户端 PC、浏览器也有 DNS 缓存功能，为了保证 DNS 代理过滤的效果，必要时需要清除 PC 的 DNS 缓存，方法是打开 DOS 窗口，运行 ipconfig/flushdns 命令，然后再清除浏览器的缓存
3、为防止客户端私设 hosts 文件，可以将客户端 PC 加入 windows 域管理；或启用 WEB 代理协议过滤，同时启用“本地 DNS 代理”选项
4、可以在初始设置中，选择“DNS 及 URL 库”中的一个或以上的大类，则系统自动启用 DNS 代理及 DNS 及 URL 库的域名过滤功能
5、DNS 代理过滤日志中，如果最右边“类型”一列有“-Modified”的后缀，则表明该域名已经被 DNS 及 URL 库或域名规则所修改

6.6.5 相关功能

1、上游功能：
DNS 代理过滤>总体设置
DNS 解析
NAT 策略
网络审计>总体设置
初始设置
许可证
上网管理功能控制
2、相关功能：
域名规则
WAF 规则
IPS
DNS 审计日志
特殊应用
3、下游功能：
DNS 代理日志
WEB 审计日志
WEB 代理协议过滤
测试工具>Nslookup
DOS 命令：ipconfig/flushdns
4、任务向导
C1 上网行为管理

6.7 自定义域名规则

6.7.1 功能简介

功能代码：dnsruleshow，为了防止上游 DNS 服务器或本机 DNS 及 URL 库对某个域名的污染，或者人为屏蔽某个域名，或者实现内网用户通过官网域名访问内网中托管的服务器，可以在此设置自定义的域名解析,即定义某些域名和某个 IP 之间多对一的关系,从而实现 DNS 服务器的 A 记录域名解析功能。

6.7.2 操作说明

1、点击“新建”按钮或“修改”链接进入新建、修改界面，选择、输入域名解析参数，点击“确定”按钮生效;其中“解析成的 IP”的正确的值可以通过本机的测试工具>Nslookup 查询得到
2、对于已存在的定义，可以先选择序号，再点击“删除”/“启用”/“停用”按钮删除/启用/停用
3、点击“日志”按钮查看 DNS 代理过滤日志

6.7.3 视频演示

1、总体设置示例:
http://www.trustcomputing.com.cn/help/cn/appfilter/dnsfilter/general_setting.html
2、DNS&URL 库:
http://www.trustcomputing.com.cn/help/cn/appfilter/dnsfilter/dnsurldbshow.html
3、域名规则设置: http://www.trustcomputing.com.cn/help/cn/appfilter/dnsfilter/dnsruleshow.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/dnsfilter/bbs.html

6.7.4 注意事项

1、DNS 代理过滤总体设置状态必须是有效，域名规则才能发挥作用，如果自定义域名规则有域名设置，则系统马上返回该设置，而不会再查询 DNS 及 URL 库
2、自定义的域名规则的生效时间是整个 24 小时，这一点和 DNS 及 URL 库域名过滤不一样；被过滤的来源 IP 由总体设置及 DNAT 策略决定，这一点和 DNS 及 URL 库域名过滤一样
3、DNS 代理过滤日志中，如果最右边“类型”一列有“-Modified”的后缀，则表明该域名已经被 DNS 及 URL 库域名过滤或域名规则所修改

6.7.5 相关功能

1、上游功能：
DNS 代理过滤>总体设置
初始设置
DNS 解析
NAT 策略
上网管理功能控制
2、相关功能：
DNS 及 URL 库
DNS 审计日志
3、下游功能：
DNS 代理日志
WEB 代理协议过滤
测试工具>Nslookup
DOS 命令：ipconfig/flushdns
4、任务向导
C1 上网行为管理
C12 抓包分析并阻拦特定应用

6.8 WEB 代理过滤

6.8.1 功能简介

功能代码：webproxybasicshow，WEB 代理过滤是网关级、在线过滤，既可以过滤内网出外网的流量，也可以过滤客户端到 WEB 服务器的流量，与 WEB 审计过滤相比，WEB 代理过滤能过滤服务器反馈的信息，包括被压缩、分包的内容。为了方便部署，可以通过 DNAT 策略，实现透明代理功能，客户端的 WEB 请求被强制重定向到本机 WEB 代理处，先过滤再转发到真实 WEB 服务器，返回的内容也是先过滤再转发到客户端处，根据设置还可以将返回的内容缓存起来，实现互联网加速功能。

6.8.2 操作说明

1、根据提示分别选择或输入相关的参数。如果启用“本地 DNS 代理”，那么 URL 请求的主机名会被 DNS 及 URL 库及 DNS 代理域名规则所过滤

2、当选择“启用服务+自动策略”项时，系统自动创建 DNAT 策略，实现透明代理的功能；如果选择“仅启用服务”项，则要么客户端要在浏览器中指定本机 IP 为 WEB 代理服务器 IP，要么管理员再新建 DNAT 策略（参见第 3 条），实现透明代理的功能。前者设置方便快速，但缺少时间、来源 IP、流量控制等策略控制，后者正好相反

3、如果选择“仅启用服务”项，可以点击“DNAT 策略执行点：无”的链接，进入新建 DNAT 策略的界面，系统自动设置好了相关参数，根据需要做一些调整，按“确定”按钮，即可生成 DNAT 策略

6.8.3 视频演示

1、自动策略示例:

http://www.trustcomputing.com.cn/help/cn/appfilter/webproxy/general_setting_auto.html
2、手工 NAT 策略:
http://www.trustcomputing.com.cn/help/cn/appfilter/webproxy/general_setting_manual.html
3、本地 DNS 代理:
http://www.trustcomputing.com.cn/help/cn/appfilter/webproxy/local_dnsproxy.html
4、WEB 协议过滤规则:
http://www.trustcomputing.com.cn/help/cn/appfilter/webproxy/webproxy_rule.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/webproxy/bbs.html

6.8.4 注意事项

1、WEB 代理会按管理员设置的本机的 DNS 服务器进行域名解析，为了加快解析速度，必须将最快、最稳定的 DNS 服务器-通常是本地 ISP 的 DNS 服务器 IP 设置成第一、二位的本机 DNS 服务器
2、如果启用“本地 DNS 代理”，与单纯的 DNS 代理过滤相比，WEB 代理的主机名过滤可以不受 PC 客户端 DNS 缓存的影响
3、如果启用 HTTPS 过滤，则客户端必须接受厂家的 CA 证书，才能继续浏览

6.8.5 相关功能

1、上游功能：
NAT 策略
DNS 解析
DNS 代理过滤
DNS 及 URL 库
域名规则
上网管理功能控制
2、相关功能：<无>
WEB 代理内容过滤>总体设置
网络审计>总体设置
WEB 审计日志
3、下游功能：
WEB 代理过滤规则
WEB 代理日志
4、任务向导
C5 WEB 透明协议过滤
C6 WEB 透明内容过滤
C7 WEB 透明防病毒

6.9 WEB 代理过滤规则

6.9.1 功能简介

功能代码：webproxyruleshow，在此设置 WEB 代理的过滤规则，分为白名单和黑名单两种类型，大部分的黑名单过滤都有相对应的站点白名单，以提高策略的灵活性。

6.9.2 操作说明

1、黑名单界面的“方式”选项中，“仅限于”是指仅过滤内容列表中的项目，“不包括”是指过滤不在内容列表中的项目，后者更严格一些；百名单界面的“方式”选项中，“仅限于”是指仅内容列表中的项目为白名单，“不包括”是指不在内容列表中的项目为白名单
2、可以查看 WEB 代理日志“状态代码”列的内容，判断该 URL 是否被阻拦，被阻拦的列显示"TCP_DENIED"；对于通过的 URL，可以查看该 URL 各列的内容，用来确定阻拦该 URL 黑名单的类型及内容

6.9.3 视频演示

1、WEB 协议过滤规则:
http://www.trustcomputing.com.cn/help/cn/appfilter/webproxy/webproxy_rule.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/webproxy/bbs.html

6.9.4 注意事项

1、必须保证 WEB 代理过滤总体设置状态有效
2、只有在 TAB 名称右边有括号、括号里有数字的过滤类型，才是目前生效的类型
3、可以在 WEB 代理>总体设置中，“仅启用服务”，再在 DNAT 策略中设置来源 IP、目的

IP 范围，还可以通过对应的总控策略设置生效时间，缩小透明 WEB 代理范围可以提高 WEB 代理效率

6.9.5 相关功能

1、上游功能：

 WEB 代理过滤>总体设置

 NAT 策略

 DNS 解析

 DNS 代理过滤>总体设置

 DNS 及 URL 库

 域名规则

 上网管理功能控制

2、相关功能：

 WEB 内容过滤>总体设置

 网络审计>总体设置

 WEB 审计日志

3、下游功能：

 WEB 代理日志

4、任务向导

C5 WEB 透明协议过滤

6.10 WEB 内容过滤

6.10.1 功能简介

功能代码：webfilterbasicshow，WEB 内容过滤主要是对内网出外网的 WEB 流量进行过滤，一是按关键词检查网页中的文字内容，二是防病毒过滤，它是网关级、在线过滤，可以对压缩、分包内容进行过滤，大规模的防病毒数据库会对网络吞吐量、延时有一定的影响。它必须在 WEB 代理的基础上进行，WEB 代理可以是本机的，也可以是部署在其它地方的。

6.10.2 操作说明

1、根据提示分别选择或输入相关的参数。如果启用“防病毒检测”，那么必须事先启用防病毒引擎
2、当选择“启用服务+自动策略”项时，系统自动创建 DNAT 策略，实现透明代理的功能；如果选择“仅启用服务”项，则要么客户端要在浏览器中指定本机 IP 为 WEB 代理服务器 IP，要么管理员再新建 DNAT 策略（参见第 3 条），实现透明代理的功能。前者设置方便快速，但缺少时间、来源 IP、流量控制等策略控制，后者正好相反
3、如果选择“仅启用服务”项，可以点击“DNAT 策略执行点：无”的链接，进入新建 DNAT 策略的界面，系统自动设置好了相关参数，根据需要做一些调整，按“确定”按钮，即可生成 DNAT 策略

6.10.3 视频演示

1、自动策略:
http://www.trustcomputing.com.cn/help/cn/appfilter/webfilter/general_setting_auto.html
2、手工 NAT 策略:
http://www.trustcomputing.com.cn/help/cn/appfilter/webfilter/general_setting_manual.html
3、关键词库:
http://www.trustcomputing.com.cn/help/cn/appfilter/webfilter/keywords_blacklist.html

---

官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/webfilter/bbs.html

6.10.4 注意事项

1、如果使用本机的 WEB 代理，则可以先调试好 WEB 代理，再启用 WEB 内容过滤，此时 WEB 代理“仅启用服务”即可

2、可以在总体设置中，“仅启用服务”，再在 DNAT 策略中设置来源 IP、目的 IP 范围，还可以通过对应的总控策略设置生效时间，缩小透明 WEB 内容过滤范围可以提高 WEB 内容过滤效率

3、WEB 内容过滤日志只记录被阻拦的 URL，正常的 URL 可以查看 WEB 审计日志或 WEB 代理日志

4、为提高 WEB 内容过滤效率，可以在 PC 客户端上安装免费的杀毒软件，在总体设置中停用“防病毒检测”；或者在防病毒引擎设置中，选择 ClamAV 的“近期流行”数据库，以提高检查性能

6.10.5 相关功能

1、上游功能：

DNAT 策略

防病毒引擎

WEB 代理协议过滤

上网管理功能控制

2、相关功能：

WEB 代理过滤规则

WEB 代理日志

网络审计>总体设置

WEB 审计日志

3、下游功能：

WEB 内容过滤日志

关键词库

关键词规则

关键词例外

防病毒例外

4、任务向导

C6 WEB 透明内容过滤

C7 WEB 透明防病毒

6.11 关键词库

6.11.1 功能简介

功能代码：keywordsdbshow，系统内置了七十多种分类关键词词库，管理员在此选择启用哪些分类词库，还可以添加新的关键词。根据总体设置，过滤的范围可以是“头部标识”、“纯内容”或“整个 HTML 文件”，检测到关键词后，可以“阻拦并记录”或“仅记录”。

6.11.2 操作说明

1、根据需要选择合适的分类，即选择“序号”列的选择框，再点击“确定”按钮生效
2、点击“修改”链接，进入到修改界面，添加或修改关键词，再点击“确定”按钮生效
3、正常 URL 请查看 WEB 审计日志或 WEB 代理日志，被阻拦的 URL 请查看 WEB 内容过滤日志

6.11.3 视频演示

1、关键词库:
http://www.trustcomputing.com.cn/help/cn/appfilter/webfilter/keywords_blacklist.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/webfilter/bbs.html

6.11.4 注意事项

1、必须保证 WEB 代理内容过滤总体设置状态有效，开启后会产生一定的延时
2、源 IP、域名、文件后缀等白名单在“关键词例外”中单独设置
3、DNS 及 URL 库也可以达到过滤网站的目的，请确认一下该功能是否启用
4、为提高 WEB 内容过滤效率，可以在 PC 客户端上安装免费的杀毒软件，在总体设置中停用“防病毒检测”；或者在防病毒引擎设置中，选择 ClamAV 的“近期流行”数据库，以提高检查性能

6.11.5 相关功能

1、上游功能：

 WEB 内容过滤>总体设置

 上网管理功能控制

2、相关功能：

 关键词规则

 关键词例外

 DNS 及 URL 库

 WEB 代理过滤规则

 WEB 代理日志

 网络审计>总体设置

 WEB 审计日志

3、下游功能：

 WEB 内容过滤日志

4、任务向导

C6 WEB 透明内容过滤

6.12 关键词规则

6.12.1 功能简介

功能代码：keywordsruleshow，用于多个网页编码的关键词设置，大规模的关键词过滤请使用关键词库。

6.12.2 操作说明

1、选择网页编码 TAB，按照提示的格式，在内容框里输入关键词，不必在 Unicode 网页编码中重复输入该关键词，点击“确定”按钮生效

6.12.3 视频演示

1、关键词库:
http://www.trustcomputing.com.cn/help/cn/appfilter/webfilter/keywords_blacklist.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/webfilter/bbs.html

6.12.4 注意事项

1、必须保证 WEB 代理内容过滤总体设置状态有效，开启后会产生一定的延时
2、源 IP、域名、文件后缀等白名单在“关键词例外”中单独设置
3、DNS 及 URL 库也可以达到过滤网站的目的，请确认一下该功能是否启用
4、为提高 WEB 内容过滤效率，可以在 PC 客户端上安装免费的杀毒软件，在总体设置中停用“防病毒检测”；或者在防病毒引擎设置中，选择 ClamAV 的“近期流行”数据库，以提高检查性能

6.12.5 相关功能

1、上游功能：

 WEB 内容过滤>总体设置

 上网管理功能控制

2、相关功能：

 关键词库

 关键词例外

 DNS 及 URL 库

 WEB 代理过滤规则

 WEB 代理日志

 网络审计>总体设置

 WEB 审计日志

3、下游功能：

 WEB 内容过滤日志

4、任务向导

C6 WEB 透明内容过滤

6.13 关键词例外

6.13.1 功能简介

功能代码：keywordsexpshow，在此设置关键词过滤的白名单，由于关键词过滤主要是针对网页文字做过滤，因此对于非文本文件的二进制文件可以通过“不检查的文件后缀”白名单进行屏蔽以提高效率。

6.13.2 操作说明

1、选择白名单类型 TAB，按照提示的格式，在内容框里输入白名单内容，点击“确定”按钮生效

6.13.3 视频演示

1、关键词库:
http://www.trustcomputing.com.cn/help/cn/appfilter/webfilter/keywords_blacklist.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/webfilter/bbs.html

6.13.4 注意事项

1、必须保证 WEB 代理内容过滤总体设置状态有效
2、为提高 WEB 内容过滤效率，可以在 PC 客户端上安装免费的杀毒软件，在总体设置中停用“防病毒检测”；或者在防病毒引擎设置中，选择 ClamAV 的“近期流行”数据库，以提高检查性能

6.13.5 相关功能

1、上游功能：

WEB 内容过滤>总体设置

上网管理功能控制

2、相关功能：

关键词库

关键词规则

WEB 代理过滤规则

WEB 代理日志

网络审计>总体设置

WEB 审计日志

3、下游功能：

WEB 内容过滤日志

4、任务向导

C6 WEB 透明内容过滤

C7 WEB 透明防病毒

6.14 防病毒例外

6.14.1 功能简介

功能代码：avexpshow，在此设置 WEB 防病毒过滤的白名单，由于防病毒过滤主要是针对二进制文件、javascript 文件做检查，因此对于视频文件、图片文件等可以通过“不检查的文件后缀”白名单进行屏蔽以提高效率。

6.14.2 操作说明

1、选择白名单类型 TAB，按照提示的格式，在内容框里输入白名单内容，点击“确定”按钮生效

6.14.3 视频演示

1、关键词库:
http://www.trustcomputing.com.cn/help/cn/appfilter/webfilter/keywords_blacklist.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/webfilter/bbs.html

6.14.4 注意事项

1、必须保证 WEB 代理内容过滤总体设置状态有效
2、为提高 WEB 内容过滤效率，可以在 PC 客户端上安装免费的杀毒软件，在总体设置中停用“防病毒检测”；或者在防病毒引擎设置中，选择 ClamAV 的“近期流行”数据库，以提高检查性能

6.14.5 相关功能

1、上游功能：

 WEB 内容过滤>总体设置

 防病毒引擎

 上网管理功能控制

2、相关功能：

 关键词库

 关键词规则

 WEB 代理过滤规则

 WEB 代理日志

 网络审计>总体设置

 WEB 审计日志

3、下游功能：

 WEB 内容过滤日志

4、任务向导

C7 WEB 透明防病毒

6.15 FTP 代理过滤

6.15.1 功能简介

功能代码：ftpfiltershow，通过代理的方式对客户端发出的 FTP 指令进行过滤，可以防止用户上传、删除 FTP 文件，也可以保护 FTP 服务器不受非法攻击。

6.15.2 操作说明

1、根据提示选择、输入合适的参数，点击“确定”按钮生效
2、当选择“启用服务+自动策略”项时，系统自动创建 DNAT 策略，实现透明代理的功能；如果选择“仅启用服务”项，则要么在 FTP 客户端中指定本机 IP 为代理服务器 IP，要么管理员再新建 DNAT 策略（参见第 3 条），实现透明代理的功能。前者设置方便快速，但缺少时间、来源 IP、流量控制等策略控制，后者正好相反
3、如果选择“仅启用服务”项，可以点击“DNAT 策略执行点：无”的链接，进入新建 DNAT 策略的界面，系统自动设置好了相关参数，根据需要做一些调整，按“确定”按钮，即可生成 DNAT 策略

6.15.3 视频演示

1、FTP 过滤示例:http://www.trustcomputing.com.cn/help/cn/appfilter/ftpfilter/ftpfilter.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/ftpfilter/bbs.html

6.15.4 注意事项

1、文件后缀区分大小写
2、FTP 审计日志是基于完整会话的，它只记录了客户端发出的命令，且必须等客户端终止操作才能全部显示；FTP 代理日志不是基于完整会话的，可以记录服务器反馈信息，但显示比较繁杂
3、目的端口在最小数据端口至最大数据端口之间的非 FTP 的流量将被阻拦

6.15.5 相关功能

1、上游功能：

 DNAT 策略

 上网管理功能控制

2、相关功能：

 网络审计

 FTP 审计日志

3、下游功能：

 FTP 过滤日志

4、任务向导

C8 FTP、POP3、SMTP 透明过滤

6.16 POP3 代理过滤

6.16.1 功能简介

功能代码：pop3filtershow，通过代理的方式对客户端以 POP3 方式收取的邮件进行过滤，主要是防病毒和防垃圾邮件。

6.16.2 操作说明

1、根据提示选择、输入合适的参数，点击“确定”按钮生效
2、当选择“启用服务+自动策略”项时，系统自动创建 DNAT 策略，实现透明代理的功能；如果选择“仅启用服务”项，则要么在邮件客户端中指定本机 IP 为代理服务器 IP，要么管理员再新建 DNAT 策略（参见第 3 条），实现透明代理的功能。前者设置方便快速，但缺少时间、来源 IP、流量控制等策略控制，后者正好相反
3、如果选择“仅启用服务”项，可以点击“DNAT 策略执行点：无”的链接，进入新建 DNAT 策略的界面，系统自动设置好了相关参数，根据需要做一些调整，按“确定”按钮，即可生成 DNAT 策略

6.16.3 视频演示

1、POP3 过滤示例: http://www.trustcomputing.com.cn/help/cn/appfilter/pop3filter/pop3filter.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/pop3filter/bbs.html

6.16.4 注意事项

1、启用“防病毒检测”，必须先启用防病毒引擎；启用“防垃圾邮件检测”，必须先启用防垃圾邮件引擎

2、POP3 审计日志是基于完整会话的，它只记录了客户端发出的命令，且必须等客户端终止操作才能全部显示；POP3 代理日志也是基于完整会话的，它还记录检测到的病毒或垃圾邮件

3、对于检测到的病毒邮件，系统删除该邮件，并发送处理邮件给用户；对于检测到的垃圾邮件，系统在邮件标题最前面加上[SPAM]字样，仍让用户收取，用户可根据标题中是否包含[SPAM]字样，进行邮件分拣

4、"重命名附件"选项中的"危险附件"包括:

.exe, .com, .bat, .pif, .eml, .url, .hlp, .chm, .vbs, .wsf, .wsh, .htm, .html 等，如被阻拦，建议发送压缩文档

6.16.5 相关功能

1、上游功能：

DNAT 策略

防病毒引擎

防垃圾邮件引擎

上网管理功能控制

2、相关功能：

网络审计

Email 审计日志

POP3 邮件备份

3、下游功能：

POP3 过滤日志

4、任务向导

C8 FTP、POP3、SMTP 透明过滤

C9 POP3、SMTP 透明防病毒

C10 POP3、SMTP 透明防垃圾邮件

6.17 SMTP 代理过滤

6.17.1 功能简介

功能代码：smtpfiltershow，通过代理的方式对客户端以 SMTP 方式发送的邮件进行过滤，主要是防病毒、防垃圾邮件以及对发信人的过滤。

6.17.2 操作说明

1、根据提示选择、输入合适的参数，点击“确定”按钮生效
2、当选择“启用服务+自动策略”项时，系统自动创建 DNAT 策略，实现透明代理的功能；如果选择“仅启用服务”项，则要么在邮件客户端中指定本机 IP 为代理服务器 IP，要么管理员再新建 DNAT 策略（参见第 3 条），实现透明代理的功能。前者设置方便快速，但缺少时间、来源 IP、流量控制等策略控制，后者正好相反
3、如果选择“仅启用服务”项，可以点击“DNAT 策略执行点：无”的链接，进入新建 DNAT 策略的界面，系统自动设置好了相关参数，根据需要做一些调整，按“确定”按钮，即可生成 DNAT 策略

6.17.3 视频演示

1、SMTP 过滤示例：http://www.trustcomputing.com.cn/help/cn/appfilter/smtpfilter/smtpfilter.html
---
官方讨论区：http://www.trustcomputing.com.cn/help/cn/appfilter/smtpfilter/bbs.html

6.17.4 注意事项

1、启用“防病毒检测”，必须先启用防病毒引擎；启用“防垃圾邮件检测”，必须先启用防垃圾邮件引擎
2、SMTP 审计日志是基于完整会话的，它只记录了客户端发出的命令，且必须等客户端终

止操作才能全部显示；SMTP 代理日志也是基于完整会话的，它还记录检测到的病毒或垃圾邮件

3、对于检测到的病毒邮件，系统拒绝发送该邮件；对于检测到的垃圾邮件，系统在邮件标题最前面加上“头部标识”，例如：[SPAM]等字样，再发送出去，接收方可根据标题中是否包含[SPAM]字样，进行邮件分拣

6.17.5 相关功能

1、上游功能：

 DNAT 策略

 防病毒引擎

 防垃圾邮件引擎

 上网管理功能控制

2、相关功能：

 网络审计

 Email 审计日志

 SMTP 邮件备份

3、下游功能：

 SMTP 过滤日志

4、任务向导

C8 FTP、POP3、SMTP 透明过滤

C9 POP3、SMTP 透明防病毒

C10 POP3、SMTP 透明防垃圾邮件

6.18 MSN 审计过滤

6.18.1 功能简介

功能代码：msnfiltershow，MSN 审计过滤有两个功能，一是记录 MSN 聊天内容，二是控制哪些 MSN 账号可以登录、哪些账号可以被邀请聊天。

6.18.2 操作说明

1、根据提示选择、输入合适的参数，点击“确定”按钮生效
2、当选择“启用服务+自动策略”项时，系统自动创建控制策略，实现日志记录及账号控制的功能；如果选择“仅启用服务”项，则需要管理员确认有以下内容的总控策略存在：动作项为允许，协议是 TCP，目的端口包含 1863，日志项为详细。前者设置方便快速，但缺少时间、来源 IP、流量控制等策略控制，后者正好相反
3、“白名单”模式时，只有在账号列表中的账号才能登录或被邀请；“黑名单”模式时，在账号列表中的账号将被禁止登录或被邀请

6.18.3 视频演示

1、MSN 过滤示例:http://www.trustcomputing.com.cn/help/cn/appfilter/msnfilter/msnfilter.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/msnfilter/bbs.html

6.18.4 注意事项

1、特殊应用>聊天通信中也有 MSN 项，如果该项是通过，则相当于“+自动策略”，且受本功能对账号的控制；如果该项是阻拦，则本功能失效；如果该项是停用，则不影响本功能的使用

2、如果账号被阻拦，则在日志中会加上“-blocked”的后缀
3、初始设置中启用“网络审计”，将启用 MSN 审计过滤；网络审计>总体设置只显示 MSN 审计过滤当前状态，不涉及其功能开关

6.18.5 相关功能

1、上游功能：
总控策略
特殊应用>网络通信
初始设置
网络审计
上网管理功能控制
2、相关功能：<无>
3、下游功能：
MSN 审计过滤日志
4、任务向导
C1 上网行为管理
C11 QQ、MSN 过滤

6.19 QQ 审计过滤

6.19.1 功能简介

功能代码：qqfiltershow，QQ 审计过滤有两个功能，一是记录 QQ 聊天命令，二是控制哪些 QQ 账号可以登录。如果用被禁止的 QQ 号登陆，系统会阻拦该用户使用 QQ 五分钟，所以不能在同一台 PC 上同时使用一个允许的号和一个禁止的号。

6.19.2 操作说明

1、根据提示选择、输入合适的参数，点击“确定”按钮生效
2、当选择“启用服务+自动策略”项时，系统自动创建控制策略，实现日志记录及账号控制的功能；如果选择“仅启用服务”项，则需要管理员确认有以下内容的总控策略存在：动作项为允许，协议是 UDP，目的端口包含 8000，日志项为详细。前者设置方便快速，但缺少时间、来源 IP、流量控制等策略控制，后者正好相反
3、“白名单”模式时，只有在账号列表中的账号才能登录；“黑名单”模式时，在账号列表中的账号将被禁止登录

6.19.3 视频演示

1、QQ 过滤示例:http://www.trustcomputing.com.cn/help/cn/appfilter/qqfilter/qqfilter.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/qqfilter/bbs.html

6.19.4 注意事项

1、特殊应用>网络通信中也有 QQ 项，如果该项是通过，则相当于“+自动策略”，且受本功能对账号的控制；如果该项是阻拦，则本功能失效；如果该项是停用，则不影响本功能的使用
2、如果账号被阻拦，则在日志中会加上“-blocked”的后缀

3、初始设置中启用“网络审计”，将启用 QQ 审计过滤；网络审计>总体设置只显示 QQ 审计过滤当前状态，不涉及其功能开关

6.19.5 相关功能

1、上游功能：
总控策略
特殊应用>网络通信
初始设置
网络审计
上网管理功能控制
2、相关功能：<无>
3、下游功能：
QQ 审计过滤日志
4、任务向导
C1 上网行为管理
C11 QQ、MSN 过滤

6.20 H323 代理

6.20.1 功能简介

功能代码：h323proxyshow，提供 H.323 网关应用层代理，方便客户端连接 VOIP 应用。

6.20.2 操作说明

1、根据提示选择、输入合适的参数，点击“确定”按钮生效

2、当选择“启用服务+自动策略”项时，系统自动创建 DNAT 策略，实现透明代理的功能；如果选择“仅启用服务”项，则要么在 VOIP 客户端中指定本机 IP 为代理服务器 IP，要么管理员再新建 DNAT 策略（参见第 3 条），实现透明代理的功能。前者设置方便快速，但缺少时间、来源 IP、流量控制等策略控制，后者正好相反

3、如果选择“仅启用服务”项，可以点击“DNAT 策略执行点：无”的链接，进入新建 DNAT 策略的界面，系统自动设置好了相关参数，根据需要做一些调整，按“确定”按钮，即可生成 DNAT 策略

6.20.3 视频演示

官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/voip/bbs.html

6.20.4 注意事项

1、需要定义内部网络，只能从内部网络连接非内部网络主机

6.20.5 相关功能

1、上游功能：

DNAT 策略

安全防护功能控制

2、相关功能：<无>

3、下游功能：<无>

6.21 H.323 网守

6.21.1 功能简介

功能代码：h323gkshow，提供 H.323 网守服务，方便客户端连接 VOIP 应用。

6.21.2 操作说明

1、根据提示选择、输入合适的参数，点击“确定”按钮生效
2、当选择“启用服务+自动策略”项时，系统自动创建控制策略，实现 H.323 网守的功能；如果选择“仅启用服务”项，则要么在 VOIP 客户端中指定本机 IP 为代理服务器 IP，要么管理员再新建控制策略（参见第 3 条），允许相关的流量通过。前者设置方便快速，但缺少时间、来源 IP、流量控制等策略控制，后者正好相反
3、如果选择“仅启用服务”项，则需要确保总控策略中有一条或多条允许的策略，其目的 IP 为本机网卡 IP，目的端口包含 1719(UDP)、1503、1720、1721、1731、Q931 端口范围、H245 端口范围和 T120 及 RTP 端口范围

6.21.3 视频演示

官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/voip/bbs.html

6.21.4 注意事项

1、需要定义公网地址，可以是域名或 IP 地址

6.21.5 相关功能

1、上游功能：

 DNAT 策略

 安全防护功能控制

2、相关功能：<无>

3、下游功能：<无>

6.22 SIP 代理

6.22.1 功能简介

功能代码：sipproxyshow，提供 SIP 网关应用层代理，方便客户端连接 VOIP 应用。

6.22.2 操作说明

1、根据提示选择、输入合适的参数，点击“确定”按钮生效
2、当选择“启用服务+自动策略”项时，系统自动创建 DNAT 策略，实现透明代理的功能；如果选择“仅启用服务”项，则要么在 VOIP 客户端中指定本机 IP 为代理服务器 IP，要么管理员再新建 DNAT 策略（参见第 3 条），实现透明代理的功能。前者设置方便快速，但缺少时间、来源 IP、流量控制等策略控制，后者正好相反
3、如果选择“仅启用服务”项，可以点击“DNAT 策略执行点：无”的链接，进入新建 DNAT 策略的界面，系统自动设置好了相关参数，根据需要做一些调整，按“确定”按钮，即可生成 DNAT 策略

6.22.3 视频演示

官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/voip/bbs.html

6.22.4 注意事项

1、需要定义内部网络，只能从内部网络连接非内部网络主机

6.22.5 相关功能

1、上游功能：

 DNAT 策略

 安全防护功能控制

2、相关功能：<无>

3、下游功能：<无>

6.23 TFTP 代理

6.23.1 功能简介

功能代码：tftpproxyshow，提供 TFTP 应用层代理，方便客户端连接 VOIP 应用。

6.23.2 操作说明

1、根据提示选择、输入合适的参数，点击“确定”按钮生效
2、当选择“启用服务+自动策略”项时，系统自动创建 DNAT 策略，实现透明代理的功能；如果选择“仅启用服务”项，则要么在 TFTP 客户端中指定本机 IP 为代理服务器 IP，要么管理员再新建 DNAT 策略（参见第 3 条），实现透明代理的功能。前者设置方便快速，但缺少时间、来源 IP、流量控制等策略控制，后者正好相反
3、如果选择“仅启用服务”项，可以点击“DNAT 策略执行点：无”的链接，进入新建 DNAT 策略的界面，系统自动设置好了相关参数，根据需要做一些调整，按“确定”按钮，即可生成 DNAT 策略

6.23.3 视频演示

官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/voip/bbs.html

6.23.4 注意事项

1、需要定义内部网络，只能从内部网络连接非内部网络主机

6.23.5 相关功能

1、上游功能：

 DNAT 策略

 安全防护功能控制

2、相关功能：<无>

3、下游功能：<无>

6.24 防病毒引擎

6.24.1 功能简介

功能代码：avshow，防病毒引擎本身不过滤网络流量，只是被应用过滤程序调用，检查传输的文件。目前可以在两种引擎中做选择，选中的引擎生效。目前有 WEB、POP3、SMTP 流量可以做网关级的防病毒检查，一般只用于过滤客户端发出的流量。

6.24.2 操作说明

1、根据提示选择、输入合适的参数，点击“确定”按钮生效；各应用过滤程序均有“防病毒检测”选项，需要同步启用才能最终生效
2、对于 ClamAV 数据库，“近期流行”的数据库是本年度的特征库，数量较精简，对网络吞吐量及延时影响较小；如果要扫描压缩的网页，就要启用“扫描压缩文件”选项，不过会产生一定的延时
3、防病毒数据库的更新需要单独的 License，请咨询供应商

6.24.3 视频演示

1、防病毒引擎示例:http://www.trustcomputing.com.cn/help/cn/appfilter/antivirus/antivirus.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/antivirus/bbs.html

6.24.4 注意事项

1、对于 ClamAV 引擎，实际文件超过设定的最大文件大小等值，会当做无毒文件处理
2、测试代码不适用于 ClamAV“近期流行”的数据库，因为它是本年度的特征库，不包括这个测试代码

6.24.5 相关功能

1、上游功能：


上网管理功能控制

2、相关功能：


WEB 内容过滤>总体设置


POP3 代理过滤


SMTP 代理过滤


防病毒数据库

3、下游功能：


防病毒日志

4、任务向导

C7 WEB 透明防病毒

C9 POP3、SMTP 透明防病毒

6.25 防病毒数据库

6.25.1 功能简介

功能代码：avdbshow，在此显示当前的防病毒数据库容量等信息，并可以查询某一具体的病毒名称。

6.25.2 操作说明

1、在防病毒引擎设置中选择不同的引擎，在此查看相关数据库信息
2、输入病毒名称，点击“查询”按钮查询

6.25.3 视频演示

1、防病毒引擎:http://www.trustcomputing.com.cn/help/cn/appfilter/antivirus/antivirus.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/antivirus/bbs.html

6.25.4 注意事项

1、防病毒数据库更新状态只和许可证有关，但当防病毒引擎停用时，防病毒数据库也停止更新

6.25.5 相关功能

1、上游功能：
防病毒引擎
许可证

上网管理功能控制

2、相关功能：<无>

3、下游功能：

防病毒日志

4、任务向导

C7 WEB 透明防病毒

C9 POP3、SMTP 透明防病毒

6.26 防垃圾邮件引擎

6.26.1 功能简介

功能代码：antispamshow，防垃圾邮件引擎本身不过滤网络流量，只是被邮件过滤程序调用，检查传输的邮件。目前有 POP3、SMTP 流量可以做网关级的防垃圾邮件检查，既可以是过滤客户端发出的流量，也可以过滤到服务器的流量。

6.26.2 操作说明

1、根据提示选择、输入合适的参数，点击“确定”按钮生效；各应用过滤程序均有“防垃圾邮件检测”选项，需要同步启用才能最终生效
2、“贝叶斯分类”是一种智能分析方法，可以不依靠特征值检测，一般都启用它
3、启用“邮件头部报告”后，系统在每一封邮件的头部嵌入检测报告，可以做进一步的分析
4、“分数”值越小，检测越严格，误判的可能性也越大
5、系统将判断出的 POP3 垃圾邮件的标题最前面加上“垃圾邮件标识”，用户可以根据这个标识做邮件分拣

6.26.3 视频演示

1、防垃圾邮件引擎: http://www.trustcomputing.com.cn/help/cn/appfilter/antispam/antispam.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/appfilter/antispam/bbs.html

6.26.4 注意事项

1、对于 POP3 垃圾邮件邮件，系统标记再转发；对于 SMTP 垃圾邮件，系统阻止其发送
2、防垃圾邮件检测不适用于 WEB 邮件

6.26.5 相关功能

1、上游功能：

 上网管理功能控制

2、相关功能：

 POP3 代理过滤

 SMTP 代理过滤

3、下游功能：

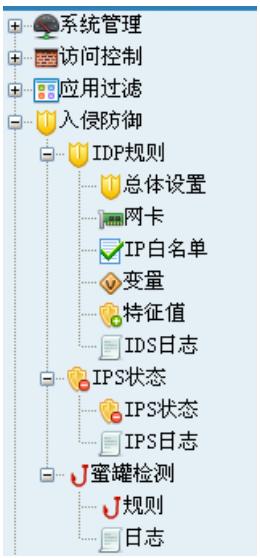
 防垃圾邮件日志

4、任务向导

C10 POP3、SMTP 透明防垃圾邮件

四、入侵防御篇

7 入侵检测与防御



7.1 IDP 总体设置

7.1.1 功能简介

功能代码：idpbasicshow，入侵检测与防御（IDP）的作用是根据定义好的特征值检查与之匹配的数据包，再根据设置记录、阻拦该数据包。管理员可以对检测的网络、端口值、IP 白名单等做定制，系统内置了四十八大类、一万多条特征值规则供管理员选择使用，还可以自定义特征值规则。

7.1.2 操作说明

1、根据提示选择、输入合适的参数，点击“确定”按钮生效
2、“检测间隔”是指相同数据包检测记录的间隔，可以防止同一事件在短时期内被反复记录
3、点击“IPS 功能”链接，查看当前的 IPS 状态
4、点击“IDS 日志”链接，查看当前的 IDS 日志

7.1.3 视频演示

1、IDP 总体设置:http://www.trustcomputing.com.cn/help/cn/idp/idp_basic/idp_basic.html
2、IDP 与总控策略“日志”项的关系:
http://www.trustcomputing.com.cn/help/cn/idp/idp_basic/pf_ids_brief_log.html
3、IDP 与总控策略“规则匹配”项的关系:
http://www.trustcomputing.com.cn/help/cn/idp/idp_basic/pf_ids_pass_quick.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/idp/idp_basic/bbs.html

7.1.4 注意事项

1、被检测的数据流由总控策略的日志项所控制，如果数据流对应的总控策略的日志项是“详细”则全部检查，是“简单”则只检查第一个数据包，是“无”则不检测

7.1.5 相关功能

1、上游功能:
总控策略
安全防护功能控制
2、相关功能:
SNMP 监控
流量策略
网络审计
URL 库
WAF 规则
用户登录防护(NPC)
3、下游功能:
IDP 规则>网卡
IDP 规则>IP 白名单
IDP 规则>变量
IDP 规则>特征值
IDS 日志
IPS 状态
IPS 日志
4、任务向导
D1 服务器接入
D3 入侵检测与防御

7.2 IDP 网卡规则

7.2.1 功能简介

功能代码：idpnicshow，确定哪些网络的数据包被检测，缩小检测范围，提高检测效率。

7.2.2 操作说明

1、如果没有启用某个特定的网卡，则全部网络都检测，此时，第一行显示“全部”；如果启用了某个网卡，则就启用的网络受检测，其它停用的网络不检测。根据以上原则，查看当前状态，或点击某一块网卡的“修改”链接，修改设置
2、点击“总体设置状态”右边的状态链接，查看当前 IDS 功能状态

7.2.3 视频演示

1、IDP 检测网卡设置:http://www.trustcomputing.com.cn/help/cn/idp/idpnic/idpnic.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/idp/idpnic/bbs.html

7.2.4 注意事项

1、必须保证 IDS、总控策略功能状态为有效，否则本功能无直接效果
2、系统自动列出当前的 VLAN 网卡，其数目由 VLAN 网卡设置管理

7.2.5 相关功能

1、上游功能：
总控策略
IDP 规则>总体设置
安全防护功能控制
2、相关功能：

网卡设置
VLAN 设置
IPSEC VPN 总体设置
PPTP VPN 总体设置
PPPoE 接入总体设置
IDP 规则>IP 白名单
IDP 规则>变量
IDP 规则>特征值

3、下游功能：

IDS 日志
IPS 状态
IPS 日志

4、任务向导

D3 入侵检测与防御

7.3 IDP IP 白名单

7.3.1 功能简介

功能代码：idpipshow，设置某个 IP 或网段的 IDS 白名单方式和 IPS 方式，防止重要的 IP 被检测或被阻拦。

7.3.2 操作说明

1、点击“新建”按钮或“修改”链接进入新建、修改界面，选择、输入参数，点击“确定”按钮生效
2、对于已存在的定义，可以选择序号后点击“删除”按钮删除
3、点击“总体设置状态”右边的状态链接，查看当前 IDS 功能状态

7.3.3 视频演示

1、未启用 IDP IP 白名单:
http://www.trustcomputing.com.cn/help/cn/idp/idpip_exp/idpip_exp.html
2、启用 IDS 白名单: http://www.trustcomputing.com.cn/help/cn/idp/idpip_exp/idpip_ids_exp.html
3、启用 IPS 白名单: http://www.trustcomputing.com.cn/help/cn/idp/idpip_exp/idpip_ips_exp.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/idp/idpip/bbs.html

7.3.4 注意事项

1、必须保证 IDS、总控策略功能状态为有效，否则本功能无直接效果
2、如果某 IP 的 IPS 方式是“覆盖”，则 IPS 日志中有“override from xx seconds”的字样

7.3.5 相关功能

1、上游功能：

总控策略
IDP 规则>总体设置
安全防护功能控制

2、相关功能：

IDP 规则>网卡
IDP 规则>变量
IDP 规则>特征值

3、下游功能：

IDS 日志
IPS 状态
IPS 日志

4、任务向导

D3 入侵检测与防御

7.4 IDP 变量

7.4.1 功能简介

功能代码：idpvarshow，根据实际网络环境，定制端口值等包含在 IDP 特征值规则里的变量，缩小检测范围，提高检测效率。

7.4.2 操作说明

1、根据提示输入合适的参数，点击“确定”按钮生效
2、点击“引用规则”列链接，查看某类特征值规则
3、点击“总体设置状态”右边的状态链接，查看当前 IDS 功能状态

7.4.3 视频演示

1、IDP 规则的变量设置:http://www.trustcomputing.com.cn/help/cn/idp/idpvar/idpvar.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/idp/idpvar/bbs.html

7.4.4 注意事项

1、必须保证 IDS、总控策略功能状态为有效，否则本功能无直接效果

7.4.5 相关功能

1、上游功能：
总控策略
IDP 规则>总体设置
安全防护功能控制
2、相关功能：

IDP 规则>网卡
IDP 规则>IP 白名单
IDP 规则>特征值

3、下游功能：

IDS 日志
IPS 状态
IPS 日志

4、任务向导

D3 入侵检测与防御

7.5 IDP 特征值规则

7.5.1 功能简介

功能代码：idsruleshow，根据实际网络环境，定制启用哪些 IDP 特征值规则大类，缩小检测范围，提高检测效率。

7.5.2 操作说明

1、根据提示选择合适的类别，点击“启用”或“停用”按钮生效
2、点击“查看”链接，进入到该大类规则设置界面，在此可以“启用”、“停用”、修改具体 IDP 规则
3、在最上方"ID:"处输入特征值规则 ID 号，查询该特征值规则
4、点击“总体设置状态”右边的状态链接，查看当前 IDS 功能状态

7.5.3 视频演示

1、IDP 特征值规则设置:http://www.trustcomputing.com.cn/help/cn/idp/idprules/idprules.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/idp/idprules/bbs.html

7.5.4 注意事项

1、必须保证 IDS、总控策略功能状态为有效，否则本功能无直接效果

7.5.5 相关功能

1、上游功能：
总控策略
IDP 规则>总体设置

 许可证

 安全防护功能控制

2、相关功能：

 IDP 规则>网卡

 IDP 规则>IP 白名单

 IDP 规则>变量

3、下游功能：

 IDS 日志

 IPS 状态

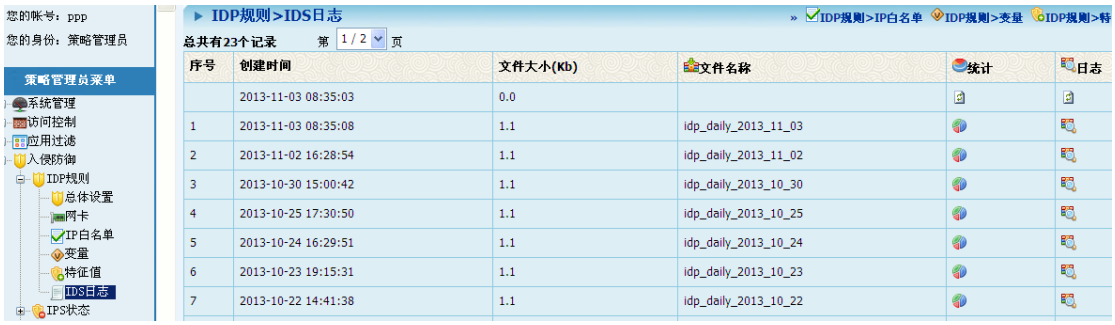
 IPS 日志

4、任务向导

D1 服务器接入

D3 入侵检测与防御

7.6 IDS 日志



7.6.1 功能简介

功能代码：idplogshow，在此可以浏览当前及历史日志记录，还可以查看日志统计。

7.6.2 操作说明

1、点击“日志”列链接查看日志内容
2、点击“统计”列链接查看日志统计
3、选择上方的页数或选择其它日志种类查看
4、点击当前菜单位置提示的第一个位置链接，可以转到 IDP 功能设置界面

7.6.3 视频演示

1、IDS 日志操作:http://www.trustcomputing.com.cn/help/cn/idp/idslog/idslog.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/idp/idslog/bbs.html

7.6.4 注意事项

1、必须保证 IDS、IDS 日志、总控策略功能状态为有效，否则没有日志产生
2、查看当前日志时，如果内容不是最新的，需要点击“确定”按钮刷新

7.6.5 相关功能

1、上游功能：
总控策略
IDP 规则>总体设置
IDP 规则>网卡
IDP 规则>IP 白名单

IDP 规则>变量
IDP 规则>特征值
安全防护功能控制

2、相关功能：

IPS 状态
IPS 日志

3、下游功能：<无>

4、任务向导

A2 查看当前日志内容
A3 查看当前日志统计
D3 入侵检测与防御

7.7 IPS 状态

7.7.1 功能简介

功能代码：ipsstatusshow，查看当前被阻拦的 IP，每个网络分为客户端和服务器两种类型显示，还可以解除被阻拦的 IP 或添加新的需要阻拦的 IP。完整记录可以查询 IPS 日志。

7.7.2 操作说明

1、点击“修改”链接，进入到查看阻拦 IP 的界面，在此可以“新建”、“删除”、“修改”具体的 IP
2、点击上方“总共有 x 个被阻拦的 IP”的链接，查看 IPS 日志

7.7.3 视频演示

1、IPS 状态操作:http://www.trustcomputing.com.cn/help/cn/idp/ipsstatus/ipsstatus.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/idp/ipsstatus/bbs.html

7.7.4 注意事项

1、必须保证 IDS、IPS、总控策略功能状态为有效，否则系统不会阻拦 IP
2、系统根据特征值规则的设置，将检测出特征值的数据包的源 IP 或目的 IP 自动阻拦，同样根据规则设置，在阻拦时长过后，系统自动解除被阻拦的 IP；同时，管理员可以查看、管理查看当前被阻拦的 IP
3、因为登录 WEB 界面时用户名+口令错误而被系统阻拦的特征值 ID 为 20000
4、因为通过 SNMP 监控 IP&MAC 地址而被系统阻拦的特征值 ID 为 22000
5、因为日志审计中包含设定的监控关键词而被系统阻拦的特征值 ID 为 30000，可以查看功能统计>系统实时报警设置
6、被流量策略阻拦的特征值 ID 为 40000+总控策略序号，例如：40007 就是匹配总控策略 7 的数据包被其流量策略所阻拦而产生的，可以进一步查看该流量策略，如 udp_tc 等
7、被"网络审计>WEB 审计-阻拦方式"所阻拦的特征值 ID 为 60001，可以查看网络审计>总

体设置

8、被"网络审计>WEBPOST 审计-非 WEB 流量处理方式"所阻拦的特征值 ID 为 60002，可以查看网络审计>总体设置及相关的 IP 对象定义：FAKE80_Server

7.7.5 相关功能

1、上游功能：

总控策略

用户登录防护

SNMP 监控 IP&MAC

系统实时报警

流量策略

网络审计

IDP 规则>总体设置

安全防护功能控制

2、相关功能：

IPS 日志

非标准 80 端口服务器 IP

IDP 规则>网卡

IDP 规则>IP 白名单

IDP 规则>变量

IDP 规则>特征值

网卡设置

URL 库

WAF 规则

蜜罐审计

网络状态趋势

3、下游功能：<无>

4、任务向导

A1 查看运行状态

C1 上网行为管理

D1 服务器接入

D3 入侵检测与防御

7.8 蜜罐检测

7.8.1 功能简介

功能代码：honeypotshow，蜜罐检测（HoneyPot）是建立一个虚拟的服务器，提供虚拟的 Ping、WEB、Telnet 等服务，诱导“黑客”扫描、攻击该服务器，同时记录客户端的扫描、攻击行为及指令，有益于查找可疑的“黑客”。

7.8.2 操作说明

1、点击“新建”按钮或“修改”链接进入新建、修改界面，选择、输入参数，点击“确定”按钮生效
2、对于已存在的定义，可以选择序号后点击“删除”按钮删除
3、点击“网络审计”按钮，查看当前网络审计设置，并进一步查询 WEB、Telnet 等相关审计日志，找到与蜜罐有关的记录

7.8.3 视频演示

1、ICMP 及端口服务:
http://www.trustcomputing.com.cn/help/cn/idp/honeypot/honeypot_ping_scanport.html
2、内置 WEB 服务:
http://www.trustcomputing.com.cn/help/cn/idp/honeypot/honeypot_webserver.html
3、内置 Telnet 服务:
http://www.trustcomputing.com.cn/help/cn/idp/honeypot/honeypot_telnet.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/idp/honeypot/bbs.html

7.8.4 注意事项

1、每一个虚拟服务器的 IP 均不得与同网段其它 IP 冲突，必须是一个空闲的 IP; 如果做了 IP&MAC 地址绑定，则要确认此 IP 的 MAC 地址未绑定或是本网段网卡 MAC 地址的代理
2、目前只有 WEB、TELNET 等内部服务器，其它服务只是开放相应的端口或提供代理转发服务

3、必须启用 WEB、TELNET 等网络审计，才能记录“黑客”发出的应用层指令
4、可以"记录并阻拦"蜜罐日志的监控关键词，再启用系统实时报警和 IPS 功能，监控关键词可以设为蜜罐服务器的 IP 等，如果有蜜罐日志产生，源 IP 就会被 IPS 系统阻拦，其 IDP 特征值 ID 为 30000。此时界面按钮区有"IPS 状态"和"IPS 日志"这两个按钮

7.8.5 相关功能

1、上游功能：
安全防护功能控制
2、相关功能：
网络审计
IPS 设置
IPS 状态
系统实时报警
ARP 服务设置
网卡设置
3、下游功能：
蜜罐日志
WEB 审计日志
Telnet 审计日志
IPS 日志
4、任务向导
D3 入侵检测与防御

五、远程接入篇

8 用户认证

8.1 认证方法

8.1.1 功能简介

功能代码：authshow，用户认证方法根据认证服务器的不同，分为本地和 RADIUS、LDAP 认证，本地认证将认证数据库建立在本机中，使用更简洁、方便，其它认证适用于用户单位已有认证服务器的情况。用户认证的过程是：首先使用本地用户名、口令登陆内置的 WEB 用户门户，网址是 https://网卡 IP:3443，如果是用户所在的用户组是本地认证方法，则点击“网络登陆”按钮即可通过认证，如果是其它方法，则点击之后需要再输入该方法的用户名、口令才能完成认证，网络认证成功后，对应的总控策略才能对用户认证时所在的源 IP 进行控制。

8.1.2 操作说明

1、点击“新建”按钮或“修改”链接进入新建、修改界面，选择、输入参数，点击“确定”按钮生效
2、对于已存在且没有被引用的定义，可以选择序号后点击“删除”按钮删除
3、点击“测试”列链接，进入测试界面，输入用户名、口令，点击“确定”按钮测试认证的有效性；对于本地（local）认证，就是登陆用户门户，网址是 https://网卡 IP:3443
4、新建完认证方法后，需要在用户组的“认证方法”选项中将其选中使用，一个认证方法

可以为多个用户组所使用

8.1.3 视频演示

1、认证方法设置:
http://www.trustcomputing.com.cn/help/cn/auth/auth_method/auth_method.html
---
2、简介-管理员设置策略:
http://www.trustcomputing.com.cn/help/cn/auth/auth_intro/admin_make_rules.html
3、简介-用户登录上网:
http://www.trustcomputing.com.cn/help/cn/auth/auth_intro/user_login_browse.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/auth/auth_intro/bbs.html

8.1.4 注意事项

1、在路由流控功能控制中，可以对本地 WEB 用户门户服务进行控制
2、认证的名称可以是中文或英文，以方便用户认证时理解

8.1.5 相关功能

1、上游功能：
路由流控功能控制
2、相关功能：<无>
3、下游功能：
用户组
认证日志
总控策略
WEB 用户门户
4、任务向导
D2 SSL 接入
E1 实名制查看用户状态
E2 WEB 门户认证

8.2 用户

8.2.1 功能简介

功能代码：usershow，用户的集合是用户组，总控策略的“用户认证”选项对应的是用户组。用户姓名用于在各种状态统计中标识源 IP 身份；登录账号和口令用于登录内置的 WEB 用户门户以及 PPTP/PPPOE/SSLVPN 等拨号 VPN 服务；绑定 IP 用于强制用户只能在该 IP 处使用登录账号和口令登录；网络保护检查（NPC）是指当用户点击“网络登录”按钮时，系统自动检查用户 PC 防火墙是否启用；用户的有效性还有时间限制。

8.2.2 操作说明

1、点击“新建”按钮或“修改”链接进入新建、修改界面，选择、输入参数，点击“确定”按钮生效
2、对于已存在的定义，可以选择序号后点击“删除”按钮删除
3、用户在第一次登录内置的 WEB 用户门户时，需要强制性的修改口令，修改后，在日志列有*号标记
4、在状态统计页面中，点击某 IP 的“*+”链接，进入到新建用户的界面，该 IP 即为绑定 IP

8.2.3 视频演示

1、用户设置:http://www.trustcomputing.com.cn/help/cn/auth/user/user.html
2、用户设置之客户端证书登录:
http://www.trustcomputing.com.cn/help/cn/auth/user/user_certlogin.html
3、用户组设置:http://www.trustcomputing.com.cn/help/cn/auth/usergroup/usergroup.html
---
4、简介-管理员设置策略:
http://www.trustcomputing.com.cn/help/cn/auth/auth_intro/admin_make_rules.html
5、简介-用户登录上网:
http://www.trustcomputing.com.cn/help/cn/auth/auth_intro/user_login_browse.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/auth/user/bbs.html

8.2.4 注意事项

1、新建用户时，口令可以不填，缺省为 12345678
2、新建用户组时，所添加的用户，其口令也是 12345678
3、登录账号不能重名，一个登录账号只能属于一个用户组
4、用户登录内置的 WEB 用户门户，仅仅是第一步，还需要点击“网络认证”按钮，才能真正的激活相应的总控策略；如果用户所在的用户组没有被总控策略所引用，则无需进行网络认证

8.2.5 相关功能

1、上游功能：
 路由流控功能控制
2、相关功能：
 用户组
 本地认证
 ARP 服务
3、下游功能：
 认证日志
 总控策略
 WEB 用户门户
 状态统计功能
4、任务向导
C1 上网行为管理
D2 SSL 接入
E1 实名制查看用户状态
E2 WEB 门户认证
F1 PPTP、PPPOE 用户接入

8.3 用户组

8.3.1 功能简介

功能代码：ugshow，用户组对应的是总控策略的“用户认证”选项，如果一条总控策略具有“用户认证”选项——其动作选项一般是允许，则相应的源 IP 必须用该用户组内的用户进行认证，认证通过后，认证所在的源 IP 才被允许使用该总控策略所对应的流量。与 PPPOE 接入方式相比，用户登录后的流量仍然走以太网，性能、稳定性有保障。

8.3.2 操作说明

1、点击“新建”按钮或“修改”链接进入新建、修改界面，选择、输入参数，点击“确定”按钮生效
2、对于已存在且未被引用的定义，可以选择序号后点击“删除”按钮删除
3、可以直接添加、修改“用户帐号”列表内容，相当于批量新建、删除用户定义，新建用户的口令是 12345678，用户姓名与登录账号相同

8.3.3 视频演示

1、用户组设置:http://www.trustcomputing.com.cn/help/cn/auth/usergroup/usergroup.html
2、用户设置:http://www.trustcomputing.com.cn/help/cn/auth/user/user.html
3、简介-管理员设置策略:
http://www.trustcomputing.com.cn/help/cn/auth/auth_intro/admin_make_rules.html
4、简介-用户登录上网:
http://www.trustcomputing.com.cn/help/cn/auth/auth_intro/user_login_browse.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/auth/usergroup/bbs.html

8.3.4 注意事项

1、用户组的“有效期至”、“最大在线时间”选项，只适用于新建用户时有用，在用户定义中可以做进一步的修改

2、为防止用户“网络登录”后，不点击“网络登出”按钮，直接关机，导致其他用户可以私改 IP，不用认证顶替改用户上网，需要设置“WEB 门户认证用户流量空闲登出”选项，这样，当两次流量统计结果相同时，系统判定该用户空闲，进而强制登出该用户，收回该 IP

8.3.5 相关功能

1、上游功能：
 认证方法
 路由流控功能控制
2、相关功能：
 用户
3、下游功能：
 认证日志
 总控策略
 流量对象
 WEB 用户门户
 PPTP VPN
 PPPOE 接入
4、任务向导
D2 SSL 接入
E2 WEB 门户认证
F1 PPTP、PPPOE 用户接入

8.4 资源

8.4.1 功能简介

功能代码：resshow，用户登录内置的 WEB 用户门户，网址是 https://网卡 IP:3443，左边菜单有“资源”菜单项，点击后显示用户可用的网络资源。一个资源组对应一个用户组，一个资源可以是多个资源组成员。

8.4.2 操作说明

1、点击“新建”按钮或“修改”链接进入新建、修改界面，选择、输入参数，点击“确定”按钮生效
2、对于已存在且未被引用的定义，可以选择序号后点击“删除”按钮删除

8.4.3 视频演示

1、资源设置:http://www.trustcomputing.com.cn/help/cn/auth/resource/resource.html
2、资源组设置:
http://www.trustcomputing.com.cn/help/cn/auth/resourcegroup/resourcegroup.html
3、简介-管理员设置策略:
http://www.trustcomputing.com.cn/help/cn/auth/auth_intro/admin_make_rules.html
4、简介-用户登录上网:
http://www.trustcomputing.com.cn/help/cn/auth/auth_intro/user_login_browse.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/auth/resource/bbs.html

8.4.4 注意事项

1、资源的名称可以是中文或英文，以方便用户理解
2、需要新建相应的总控策略与每一资源定义相匹配

8.4.5 相关功能

1、上游功能：

 路由流控功能控制

2、相关功能：<无>

3、下游功能：

 资源组

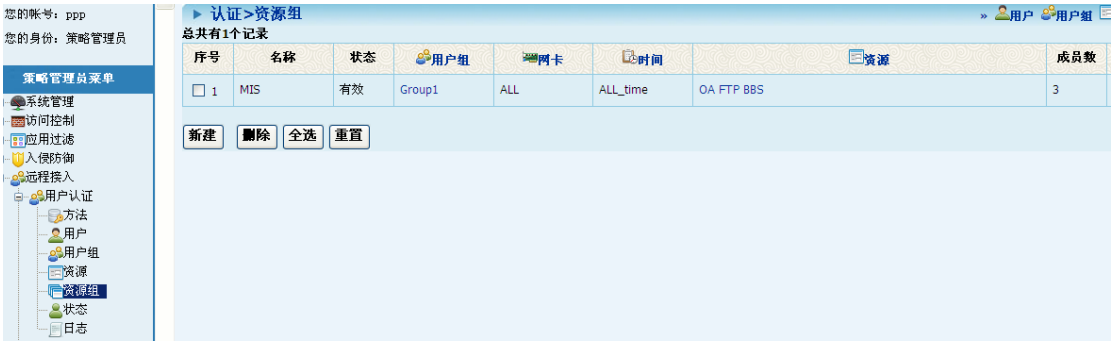
 用户组

 认证日志

 总控策略

 WEB 用户门户

8.5 资源组



8.5.1 功能简介

功能代码：resgroupshow，用户登录内置的 WEB 用户门户，网址是 https://网卡 IP:3443，左边菜单有“资源”菜单项，点击后显示用户可用的网络资源。一个资源组对应一个用户组，一个资源可以是多个资源组成员。

8.5.2 操作说明

1、点击“新建”按钮或“修改”链接进入新建、修改界面，选择、输入参数，点击“确定”按钮生效
2、对于已存在且未被引用的定义，可以选择序号后点击“删除”按钮删除

8.5.3 视频演示

1、资源组设置:
http://www.trustcomputing.com.cn/help/cn/auth/resourcegroup/resourcegroup.html
2、资源设置:http://www.trustcomputing.com.cn/help/cn/auth/resource/resource.html
---
3、简介-管理员设置策略:
http://www.trustcomputing.com.cn/help/cn/auth/auth_intro/admin_make_rules.html
4、简介-用户登录上网:
http://www.trustcomputing.com.cn/help/cn/auth/auth_intro/user_login_browse.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/auth/resourcegroup/bbs.html

8.5.4 注意事项

1、资源组的名称可以是中文或英文，以方便用户理解
2、系统根据登录用户所在用户组的资源组定义，按照“网卡”、“时间”等条件显示可用的

资源

8.5.5 相关功能

1、上游功能：

 资源

 路由流控功能控制

2、相关功能：

 网卡设置

 时间设置

3、下游功能：

 用户组

 认证日志

 总控策略

 WEB 用户门户

4、任务向导

D2 SSL 接入

8.6 用户状态

8.6.1 功能简介

功能代码：userstatusshow，根据用户网络登录的状态，分类显示用户信息，包括登录、登出时间、IP，总在线时间等，方便管理员查看认证运行状态。

8.6.2 操作说明

1、选择最上方的“用户组”、“状态”下拉框，分类显示用户状态
2、根据实际情况，选择“序号”列选择框，再点击“登录”、“登出”按钮，强制性网络登录、网络登出用户
3、点击某一用户“日志”列的“流量”、“日志”链接，显示该用户的流量统计、认证日志

8.6.3 视频演示

1、简介-管理员设置策略:
http://www.trustcomputing.com.cn/help/cn/auth/auth_intro/admin_make_rules.html
2、简介-用户登录上网:
http://www.trustcomputing.com.cn/help/cn/auth/auth_intro/user_login_browse.html
3、用户设置:http://www.trustcomputing.com.cn/help/cn/auth/user/user.html
4、用户组设置:http://www.trustcomputing.com.cn/help/cn/auth/usergroup/usergroup.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/auth/auth_intro/bbs.html

8.6.4 注意事项

1、用户必须自己做过一次网络登录，管理员才能强制“登录”、“登出”用户，因为需要知道上次用户登录的 IP

8.6.5 相关功能

1、上游功能：

 用户

 用户组

 总控策略

 路由流控功能控制

2、相关功能：

 WEB 用户门户

 认证日志

3、下游功能：<无>

4、任务向导

A1 查看运行状态

D2 SSL 接入

E1 实名制查看用户状态

E2 WEB 门户认证

9 拨号接入

9.1 PPTP 总体设置

9.1.1 功能简介

功能代码：pptpshow，PPTP VPN 的作用是保障合法用户安全连接上内网资源，让外部用户和内网用户一样使用内网资源。远程用户不需要安装 VPN 客户端，直接在 windows 中建立拨号连接，输入相应的用户名和口令，即可与 VPN 服务器后的内网相连，而且，信息在加密的 VPN 隧道内流动，不会被截获、篡改。

9.1.2 操作说明

1、根据提示输入合适的参数，点击“确定”按钮生效。当选择“启用服务+自动策略”项时，系统自动创建控制策略，让相关数据包通过；如果选择“仅启用服务”项，则需要新建总控策略，允许以下三种流量通过：一是协议是 TCP、目的 IP 是 ALLNIC_ip、目的端口是 1723 的全部流量，二是协议是 GRE 的全部流量，三是网卡是 PPP 的全部流量

2、系统内置了两个 IP 地址定义，即 PPTP_localip 和 PPTP_network，用于 PPTP 设置，左/右键点击它们，进入修改 IP 地址定义的界面
3、点击“用户组”列链接，查看用户组定义，只有启用某个用户组的“PPTP 组”选项，才能使之在“用户组”框里显示出来

9.1.3 视频演示

1、PPTP 管理员设置:http://www.trustcomputing.com.cn/help/cn/vpn/pptp/pptp_admin.html
2、PPTP 用户使用:http://www.trustcomputing.com.cn/help/cn/vpn/pptp/pptp_user.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/vpn/pptp/bbs.html

9.1.4 注意事项

1、只有“用户组”内有组成员，PPTP VPN 才有用户数据库
2、在总控策略中选择"PPP"作为网卡，来过滤、记录用户拨号连接后的流量，如果设置了“详细”日志，还可以进行网络审计和 IDP 等 7 层内容过滤
3、对于“用户地址池”，如果用户有绑定 IP，则以绑定 IP 为准，绑定 IP 不能和任何已有的 IP 重复，否则系统随机在用户地址池中分配一个 IP 给用户用

9.1.5 相关功能

1、上游功能：
用户组
用户
DNS 解析
IP 地址对象
安全防护功能控制
2、相关功能：
总控策略
NAT 策略
IDP 网卡规则
3、下游功能：
PPTP 状态
PPTP 日志
4、任务向导
F1 PPTP、PPPOE 用户接入

9.2 PPTP 用户状态

9.2.1 功能简介

功能代码：pptpstatus，在此查看当前已登录的 PPTP 用户信息，管理员还可以强制中断某个用户的连接。

9.2.2 操作说明

1、根据需要点击某个用户所在列的“删除”链接，中断该用户的连接
2、点击表格题头的“日志”连接，查看 PPTP VPN 日志

9.2.3 视频演示

1、PPTP 管理员设置:http://www.trustcomputing.com.cn/help/cn/vpn/pptp/pptp_admin.html
2、PPTP 用户使用:http://www.trustcomputing.com.cn/help/cn/vpn/pptp/pptp_user.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/vpn/pptp/bbs.html

9.2.4 注意事项

1、“用户地址”前半部分是用户物理网卡的 IP 地址，后半部分是系统分配的虚拟 IP 地址，如果该用户有绑定 IP, 则系统分配的虚拟 IP 地址就是该绑定 IP
2、远程用户需要知道 PPTP VPN 服务器的 IP 地址，并能和它连通才能建立 PPTP VPN 连接

9.2.5 相关功能

1、上游功能：
PPTP 总体设置
用户组
用户
总控策略

 IP 地址对象

 安全防护功能控制

2、相关功能：

 PPTP 日志

3、下游功能：<无>

4、任务向导

A1 查看运行状态

E1 实名制查看用户状态

F1 PPTP、PPPOE 用户接入

9.3 PPPOE 总体设置

9.3.1 功能简介

功能代码：pppoeshow，PPPOE 接入的作用是保障只有合法用户才能接入内网网络，合法用户的身份是由用户名和口令来保证，而不是通过源 IP 或 MAC 地址来保证。用户不需要安装接入客户端，直接在 windows 中建立拨号连接，输入相应的用户名和口令，即可与 PPPOE 服务器相连，之后，信息在 PPPOE 通道内流动，不受 ARP 广播包的影响。目前，只能在少量用户环境下（<10 人）使用 PPPOE 接入功能。

9.3.2 操作说明

1、根据提示输入合适的参数，点击“确定”按钮生效。当选择“启用服务+自动策略”项时，系统自动创建控制策略，让相关数据包通过；如果选择“仅启用服务”项，则需要新建总控策略，允许网卡是 PPP 的全部流量通过

2、系统内置了两个 IP 地址定义，即 PPPOE_localip 和 PPPOE_network，用于 PPPOE 接入设置，左/右键点击它们，进入修改 IP 地址定义的界面

3、点击“用户组”列链接，查看用户组定义，只有启用某个用户组的“PPTP 组”选项，才能使之在“用户组”框里显示出来

9.3.3 视频演示

1、PPPoE 管理员设置:http://www.trustcomputing.com.cn/help/cn/vpn/pppoe/pppoe_admin.html

2、PPPoE 用户使用:http://www.trustcomputing.com.cn/help/cn/vpn/pppoe/pppoe_user.html

---

官方讨论区:http://www.trustcomputing.com.cn/help/cn/vpn/pppoe/bbs.html

9.3.4 注意事项

1、只有“用户组”内有组成员，PPPOE 接入才有用户数据库
2、在 NAT 策略中选择"PPPOE_network"作为来源地址做来源 NAT，外网网卡作为 NAT 网卡，使用户上公网
3、在总控策略中选择"PPP"作为网卡，来过滤、记录用户拨号连接后的流量，如果设置了“详细”日志，则还可以进行网络审计和 IDP 等 7 层内容过滤
4、对于“用户地址池”，如果用户有绑定 IP，则以绑定 IP 为准，绑定 IP 不能和任何已有的 IP 重复，否则系统随机在用户地址池中分配一个 IP 给用户用

9.3.5 相关功能

1、上游功能：
用户组
用户
总控策略
DNS 解析
IP 地址对象
安全防护功能控制
2、相关功能：
IDP 网卡规则
NAT 策略
3、下游功能：
PPPOE 状态
PPPOE 日志
4、任务向导
F1 PPTP、PPOE 用户接入

9.4 PPPOE 用户状态

9.4.1 功能简介

功能代码：pppoestatus，在此查看当前已登录的 PPPOE 用户信息，管理员还可以强制中断某个用户的连接。

9.4.2 操作说明

1、根据需要点击某个用户所在列的“删除”链接，中断该用户的连接
2、点击表格题头的“日志”连接，查看 PPPOE 接入日志

9.4.3 视频演示

1、PPPoE 管理员设置:http://www.trustcomputing.com.cn/help/cn/vpn/pppoe/pppoe_admin.html
2、PPPoE 用户使用:http://www.trustcomputing.com.cn/help/cn/vpn/pppoe/pppoe_user.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/vpn/pppoe/bbs.html

9.4.4 注意事项

1、“用户地址”是系统分配的虚拟 IP 地址，不包括物理网卡的 IP 地址，如果该用户有绑定 IP，则系统分配的虚拟 IP 地址就是该绑定 IP
2、用户不需要知道 PPPOE 服务器的 IP 地址，使用广播包就能和它连通，进而建立 PPPOE 连接

9.4.5 相关功能

1、上游功能：
PPPOE 总体设置
用户组

用户

IP 地址对象

安全防护功能控制

2、相关功能：

总控策略

PPPOE 日志

3、下游功能：<无>

4、任务向导

F1 PPTP、PPPOE 用户接入

10 IPSEC VPN

10.1 IPSEC VPN 总体设置

10.1.1 功能简介

功能代码：ipsecbasicshow，IPSEC VPN 分为“PC 到内网”和“内网到内网”两种方式，前者和 PPTP VPN 类似，后者的认证过程发生在两台 VPN 网关间，当它们相互认证成功后，两个内网里的 PC 可以直接请求对方的资源，不需要安装软件或建立拨号连接，信息在加密的 VPN 隧道内流动，不会被截获、篡改。

10.1.2 操作说明

1、根据提示输入合适的参数，点击“确定”按钮生效
2、当选择“启用服务+自动策略”项时，系统自动创建控制策略，让相关数据包通过；如

果选择“仅启用服务”项，则需要新建总控策略，允许以下三种流量通过：一是协议是 UDP、目的 IP 是 ALLNIC_ip、目的端口是 500 以及 4500 的全部流量，二是协议是 ESP 的全部流量，三是网卡是 IPSEC 的全部流量

10.1.3 视频演示

1、IPSEC 总体设置: http://www.trustcomputing.com.cn/help/cn/vpn/ipsec/basic/ipsec_basic.html
2、两个局域网之间互联-本地方设置:
http://www.trustcomputing.com.cn/help/cn/vpn/ipsec/lan_to_lan/lan_to_lan_wuhan.html
3、两个局域网之间互联-远程方设置:
http://www.trustcomputing.com.cn/help/cn/vpn/ipsec/lan_to_lan/lan_to_lan_beijing.html
4、PC 到局域网之间互联-局域网方设置:
http://www.trustcomputing.com.cn/help/cn/vpn/ipsec/pc_to_lan/pc_to_lan.html
5、PC 到局域网之间互联-PC 方设置:
http://www.trustcomputing.com.cn/help/cn/vpn/ipsec/pc_to_lan/vpn_client.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/vpn/ipsec/bbs.html

10.1.4 注意事项

1、当 IKE 选择"启用服务+自动策略"项时，系统允许所有通过 VPN 隧道-IPSEC 网卡的流量；为了在 VPN 隧道内做访问控制，需要另外在总控策略中新建策略，先拒绝所有网卡是 IPSEC 的流量，再允许必要的到内网服务器的流量，或者选择"仅启用服务"项，再在总控策略中允许需要通过的流量
2、特殊应用中的设置会影响到 VPN 隧道内的流量的连通性，例如阻拦"危险应用"中的"微软 Netbios"会导致不能访问网络共享，如果需要访问，则要停用"微软 Netbios"
3、为了让内网中的 IPSEC VPN 流量穿越本机 SNAT 策略，需要 VPN 软件客户端和 VPN 服务器同时启用 NAT-T 功能
4、如果 IPSEC 日志中出现 INVALID_ID，表明连接设置中的"本地内网"不符合远程 VPN 网关的设置；如果 IPSEC 日志中出现 INVALID_HASH，表明连接设置中的"本地内网"与其它 VPN 网关重复，而其它 VPN 网关已与远程 VPN 网关相连
5、对于非正式许可证设备，初始设置中具有启用 IPSEC VPN 的功能

10.1.5 相关功能

1、上游功能：
安全防护功能控制
初始设置
2、相关功能：
IPSEC VPN 软件
总控策略
特殊应用

 会话状态
 实时监控
 IDP 网卡规则

3、下游功能：

 IPSEC VPN>网关设置
 IPSEC VPN>网关状态
 IPSEC VPN>连接设置
 IPSEC VPN>连接状态
 IPSEC VPN>日志

4、任务向导

F2 IPSEC VPN 接入

10.2 IPSEC VPN 本机设置

10.2.1 功能简介

功能代码：localkeyshow，如果 IPSEC 网关定义中“认证方法”是“RSA Keys”选项，则需要在此生成本机的 RSA 密钥，并发给通讯的其它方，在网关设置中使用。如果 IPSEC 网关定义中“认证方法”是“X.509 Certificates”选项，则需要在此生成本机的 CSR 请求，并发给 CA 中心，等 CA 中心签发证书后，再导入 CA 证书和本机证书。

10.2.2 操作说明

1、根据提示输入合适的参数，点击“确定”按钮生效
2、根据具体设置，在 IPSEC 网关设置中填写远程网关的 RSA 公钥等信息

10.2.3 视频演示

1、IPSEC 本机设置: http://www.trustcomputing.com.cn/help/cn/vpn/ipsec/localkey/localkey.html
2、IPSEC 总体设置: http://www.trustcomputing.com.cn/help/cn/vpn/ipsec/basic/ipsec_basic.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/vpn/ipsec/bbs.html

10.2.4 注意事项

1、在“RSA 密钥”界面中只显示公钥。可以只输入公钥，私钥由公钥导出或公私钥对一起输入

10.2.5 相关功能

1、上游功能：
IPSEC VPN>总体设置

总控策略

安全防护功能控制

2、相关功能：

会话状态

实时监控

3、下游功能：

IPSEC VPN>网关设置

IPSEC VPN>网关状态

IPSEC VPN>连接设置

IPSEC VPN>连接状态

IPSEC>日志

4、任务向导

F2 IPSEC VPN 接入

10.3 IPSEC VPN 网关

10.3.1 功能简介

功能代码：gatewayshow，IPSEC 网关定义又称为第一阶段协商，一个 IPSEC 网关可以为多个 IPSEC 连接所用。

10.3.2 操作说明

1、点击“新建”按钮或“修改”链接进入新建、修改界面，选择、输入参数，点击“确定”按钮生效；系统为新建策略提供模板选择项，可以在此基础上调整
2、对于已存在且未被引用的定义，可以选择序号后点击“删除”按钮删除
3、点击“网关状态”按钮，查看当前 IPSEC 网关状态
4、点击左边主菜单“连接”链接，查看 IPSEC 连接定义
5、在 IPSEC 连接新建、修改界面的“IPSEC 网关”选项处，选择此处定义的网关

10.3.3 视频演示

1、IPSEC 总体设置: http://www.trustcomputing.com.cn/help/cn/vpn/ipsec/basic/ipsec_basic.html
---
2、两个局域网之间互联-本地方设置:
http://www.trustcomputing.com.cn/help/cn/vpn/ipsec/lan_to_lan/lan_to_lan_wuhan.html
3、两个局域网之间互联-远程方设置:
http://www.trustcomputing.com.cn/help/cn/vpn/ipsec/lan_to_lan/lan_to_lan_beijing.html
---
4、PC 到局域网之间互联-局域网方设置:
http://www.trustcomputing.com.cn/help/cn/vpn/ipsec/pc_to_lan/pc_to_lan.html
5、PC 到局域网之间互联-PC 方设置:
http://www.trustcomputing.com.cn/help/cn/vpn/ipsec/pc_to_lan/vpn_client.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/vpn/ipsec/bbs.html

10.3.4 注意事项

1、必须保证 IPSEC 总体设置状态为有效，否则本功能无直接效果
2、IPSEC 网关双方必须使用完全一样的认证、加密等参数设置才能建立网关
3、对于“PC 到内网”的方式，“远程 IKE 地址”为 ALL_network
4、系统预定义了两个 IPSEC 网关，一个是内网到内网，一个是 PC 到内网
5、如果修改了相关的网卡 IP 或 IP 对象后，系统自动更新 IPSEC 网关定义

10.3.5 相关功能

1、上游功能：
 IPSEC VPN>总体设置
 总控策略
 IP 地址对象
 安全防护功能控制
2、相关功能：<无>
3、下游功能：
 IPSEC VPN>网关状态
 IPSEC VPN>连接设置
 IPSEC VPN>连接状态
 IPSEC VPN>日志
4、任务向导
F2 IPSEC VPN 接入

10.4 IPSEC VPN 连接

10.4.1 功能简介

功能代码：connectionshow，IPSEC 连接定义又称为第二阶段协商，一个 IPSEC 网关可以为多个 IPSEC 连接所用。

10.4.2 操作说明

1、点击“新建”按钮或“修改”链接进入新建、修改界面，选择、输入参数，点击“确定”按钮生效；系统为新建策略提供模板选择项，可以在此基础上调整
2、对于已存在的定义，可以选择序号后点击“删除”按钮删除
3、点击“连接状态”按钮，查看当前 IPSEC 连接状态
4、点击左边主菜单“网关”链接，查看 IPSEC 网关定义
5、在总控策略中选择"IPSEC"作为网卡，来过滤 VPN 连接后的流量

10.4.3 视频演示

1、IPSEC 总体设置：http://www.trustcomputing.com.cn/help/cn/vpn/ipsec/basic/ipsec_basic.html
---
2、两个局域网之间互联-本地方设置：
http://www.trustcomputing.com.cn/help/cn/vpn/ipsec/lan_to_lan/lan_to_lan_wuhan.html
3、两个局域网之间互联-远程方设置：
http://www.trustcomputing.com.cn/help/cn/vpn/ipsec/lan_to_lan/lan_to_lan_beijing.html
---
4、PC 到局域网之间互联-局域网方设置：
http://www.trustcomputing.com.cn/help/cn/vpn/ipsec/pc_to_lan/pc_to_lan.html
5、PC 到局域网之间互联-PC 方设置：
http://www.trustcomputing.com.cn/help/cn/vpn/ipsec/pc_to_lan/vpn_client.html
---
官方讨论区：http://www.trustcomputing.com.cn/help/cn/vpn/ipsec/bbs.html

10.4.4 注意事项

1、必须保证 IPSEC 总体设置状态为有效，否则本功能无直接效果
2、IPSEC 连接双方必须使用完全一样的认证、加密等参数设置才能建立连接
3、对于“PC 到内网”的方式，“远程内网”为 ALL_network，同时需要停用“连接发起者”选项
4、系统预定义了两个 IPSEC 连接，一个是内网到内网，一个是 PC 到内网
5、如果修改了相关的网卡 IP 或 IP 对象后，系统自动更新 IPSEC 连接定义

10.4.5 相关功能

1、上游功能：
IPSEC VPN>总体设置
IPSEC VPN>网关设置
总控策略
IP 地址对象
安全防护功能控制
2、相关功能：
IPSEC VPN>网关状态
路由设置
会话状态
实时监控
3、下游功能：
IPSEC VPN>连接状态
IPSEC VPN>日志
4、任务向导
A1 查看运行状态
F2 IPSEC VPN 接入

11 SSL 接入及 SSLVPN

11.1 SSL 接入

11.1.1 功能简介

功能代码：sslshow，本程序负责接收、解密客户端发出的 SSL 数据包，再向真实的服务器发起普通 TCP 连接，再将返回的内容用 SSL 加密转发给客户端，这样可以防止客户端直接和真实服务器通讯，导致数据包被窃听。例如，可以在 HTTPS 和 HTTP、POP3S 和 POP3、SMTPS 和 SMTP 等协议之间做转换，还可以安装专门的 stunnel 客户端软件，实现任意 TCP 流量的加密和转发。

11.1.2 操作说明

1、点击“新建”按钮或“修改”链接进入新建、修改界面，选择、输入参数，点击“确定”按钮生效
2、对于已存在的定义，可以选择序号后点击“删除”按钮删除
3、必要时，需要新建总控策略，目的 IP 是 ALLNIC_ip，保证数据包通过

11.1.3 视频演示

SSL 接入设置:http://www.trustcomputing.com.cn/help/cn/vpn/ssl/ssl_server.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/vpn/ssl/bbs.html

11.1.4 注意事项

1、“接入 IP”和“接入端口”是 SSL 客户端设置的服务器 IP 及端口，其中，“接入 IP”的值永远是 ALLNIC_ip，即本机所有网卡的 IP，另外，“接入端口”的值不能重复
2、“外联 IP”、“外联端口”是指真实服务器的 IP 和端口，本程序负责在 SSL 客户端和真实

服务器之间转发

11.1.5 相关功能

1、上游功能：

网卡设置

安全防护功能控制

2、相关功能：

总控策略

会话状态

实时监控

3、下游功能：<无>

4、任务向导

D2 SSL 接入

11.2 SSLVPN 总体设置

11.2.1 功能简介

功能代码：sslvpn，本程序服务端以 SSL 协议作为加密、认证手段，以 TCP 或 UDP 协议为封装形式，实现虚拟局域网即 VPN 功能，用于远程应用接入、异地 FQ 上网和客户端组网互联，同时，还具备 Windows、Linux、Mac OS X、安卓、iOS 等操作系统下的客户端软件。为了方便客户端的部署，厂家提供 Windows 客户端软件安装包制作源程序，管理员通过封装客户端配置文件再制作专门的安装文件，供用户通过 WEB 门户下载，可以实现即装即用、随机启动运行、自动连接 VPN 网关的效果。

与传统 SSLVPN 相比，本 SSLVPN 有以下优势：

1）VPN 性能更好

用户操作层与数据通讯层分离，提高了数据处理的性能，对外公开的可以只有一个数据通讯端口，用户可以事先在内网中登陆 WEB 门户修改缺省口令、下载安装软件，外网 VPN 隧道建立后可以以虚拟 IP 的方式登陆 WEB 门户，既安全高效又方便了管理员和用户；

2）数据穿透力更强

传统 SSLVPN 只能通过 TCP 协议进行数据传输，遇到只开放 DNS（53/UDP）端口的 WEB 认证网络时就无法连通，本 SSLVPN 既可以用 TCP 协议也可以用 UDP 协议，使得数据穿透力更强，使用范围更广；

3）服务端更安全

取消了公网 SSLVPN WEB 用户登陆及管理后台界面，避免了服务器信息泄露和黑客攻击，所有来自公网的扫描和攻击，例如 SQL 注入、XSS 攻击、域名劫持、钓鱼网站、挂马、拖库、搜索引擎爬虫扫描、弱口令扫描、WEB 服务器缺陷扫描等都不在是有效的威胁；

4）客户端更安全方便

具备 Windows、Linux、Mac OS X、安卓、iOS 等操作系统下的客户端软件，通过安装、运行包含定制配置文件的客户端软件，杜绝了 ActiveX、Java Applet 等浏览器插件带来的客户端不安全性和局限性，摆脱了对浏览器的依赖，可以实现开机自动运行以及自动重连的功能；

5）口令机制更完善

强制用户修改缺省口令，保证了口令安全的健壮性，划清了与管理员的责任，也避免了维护

RADIUS、AD、LDAP 数据库或/及 CA、RA、PKI 等数字证书公钥基础设施的繁琐；

6）资源定义更灵活

资源定义与访问控制策略分离，需要公开的资源可以显示在 WEB 门户中，需要保密的资源可以不定义、不显示出来，但仍旧可以连接；

7）VPN 使用更有效率

SSL 协议可以只用于加密和建立 VPN 隧道，用户认证、访问控制可以在 VPN 隧道建立后进行，对于自身加密的应用（HTTPS 等），甚至可以直接用 DNAT 端口映射+用户认证，而不用 VPN 以提高性能，与传统的 SSLVPN 需要用户 WEB 登陆才能建立 VPN 隧道的使用体验一致，但策略实施更灵活、使用和管理更方便；

8）VPN 隧道内流量的管控能力更细致

VPN 建立后，还可以对 VPN 隧道内的流量进行基于用户名/IP 地址、时间、流量、会话、QoS 的 NAT 地址转换和 ACL 访问控制，以及网络审计、上网行为管理、WEB 过滤、入侵检测与防御等 7 层内容过滤，提升了 VPN 管理员及运营商的管控能力；

9）具备无线接入、虚拟化及云计算的能力

无线用户连接上 WIFI 后，可以再连接本 SSLVPN 以确保安全；通过部署虚拟化产品（UTMWALL-VM），将本 SSLVPN 集成到应用系统的 Windows 环境里，节省了硬件、空间、电力等费用，使得远程应用接入方式又多了一种选择；还可以将本 SSLVPN 随应用系统或独立部署到公有云、私有云中，实现云 VPN 功能，让云计算更安全。

11.2.2 操作说明

1、根据提示输入合适的参数，点击“确定”按钮生效。当选择“启用服务+自动策略”项时，系统自动创建控制策略，让相关数据包通过；如果选择“仅启用服务”项，则需要新建总控策略，允许以下二种流量通过：一是协议是服务协议（缺省是 TCP）、目的 IP 是 ALLNIC_ip、目的端口是服务端口（缺省是 443）的全部流量，二是网卡是 PPP 的全部流量

3、点击“用户组”列链接，查看 SSLVPN 用户组定义，系统内置了一个用户组即 SSLVPN_usergroup，内置了 10 个用户，可以在此基础上新建多个用户组，配合总控策略的用户认证选项，实现基于策略的远程应用访问控制

4、SSLVPN 部署流程一般是：设置好 SSLVPN 服务端参数，设置好 SSLVPN 用户组、资源组，设置好针对 PPP 网卡的、带用户认证选项的总控策略，设置好针对 SSLVPN_network 的回程路由或 SNAT 策略；下载客户端配置文件，制作客户端软件安装程序，上传到网站，通知用户登录 WEB 门户，用户修改缺省口令并下载客户端软件安装程序，安装后运行

11.2.3 视频演示

1、SSLVPN 管理员设置:

http://www.trustcomputing.com.cn/help/cn/vpn/sslvpn/sslvpn_admin.html

2、SSLVPN 用户使用:

http://www.trustcomputing.com.cn/help/cn/vpn/sslvpn/sslvpn_user.html

---

官方讨论区:http://www.trustcomputing.com.cn/help/cn/vpn/sslvpn/bbs.html

11.2.4 注意事项

1、系统内置了三个 IP 地址定义，即 SSLVPN_network、SSLVPN_route 和 SSLVPN_localip，用于 SSLVPN 设置，左/右键点击它们，进入修改 IP 地址定义的界面，其中，SSLVPN_localip 的内容由 SSLVPN_network 的内容自动生成，不需要修改
2、如果启用了“客户端软件用户名密码认证”，则用户必须登陆 WEB 门户修改缺省口令，才能通过 SSLVPN 客户端连接成功，此口令既是 WEB 门户的口令，也是 SSLVPN 客户端的口令，有关用户的操作请查看《UTMWALL 网关 SSLVPN 用户手册》
3、如果启用了“VPN 建立后客户端相互连通”，则还要关闭用户 PC 的防火墙才能相互连通
4、“路由地址池”是 SSLVPN 客户端连接成功后加载到本机的路由，设置为 0.0.0.0/1 128.0.0.0/1 将会使 VPN 隧道成为缺省路由，为了能连通“路由地址池”中的设备，还必须在网关上设置针对 SSLVPN_network 的回程路由或 SNAT 策略
5、在总控策略中选择"PPP"作为网卡，来过滤、记录用户连接 SSLVPN 后的流量，如果设置了“详细”日志，则还可以进行网络审计和 IDP 等 7 层内容过滤

11.2.5 相关功能

1、上游功能：
用户组
用户
资源组
IP 地址对象
安全防护功能控制
2、相关功能：
总控策略
NAT 策略
IDP 网卡规则
WEB 门户
3、下游功能：
SSLVPN 状态
SSLVPN 日志
4、任务向导
F3 SSLVPN 远程接入

11.3 SSLVPN 用户状态

11.3.1 功能简介

功能代码：sslvpnstatus，在此查看当前已登录的 SSLVPN 用户信息，管理员还可以强制中断某个用户的连接。

11.3.2 操作说明

1、根据需要点击某个用户所在列的“删除”链接，中断该用户的连接
2、点击表格题头的“日志”连接，查看 SSLVPN 日志

11.3.3 视频演示

1、SSLVPN 管理员设置:
http://www.trustcomputing.com.cn/help/cn/vpn/sslvpn/sslvpn_admin.html
2、SSLVPN 用户使用:
http://www.trustcomputing.com.cn/help/cn/vpn/sslvpn/sslvpn_user.html
---
官方讨论区:http://www.trustcomputing.com.cn/help/cn/vpn/pptp/bbs.html

11.3.4 注意事项

1、如果启用了“客户端软件用户名密码认证”，则 SSLVPN 客户端连接成功后，系统自动以此用户名及虚拟 IP 地址进行 WEB 门户的“网络登录”操作 ，退出时，也是同步进行 WEB 门户的“网络登出”操作，同时，在总控策略中，可以设置用户认证选项，这样就实现了基于用户组角色的远程访问控制
2、单独删除一个用户的连接后，用于客户端软件有定时重连的功能，所以会在 10 秒钟内自动连上；点击“全部删除”按钮后，SSLVPN 服务端被终止，用户要等待 5 分钟后才能连上

11.3.5 相关功能

1、上游功能：
SSLVPN 总体设置
用户组
用户
总控策略

IP 地址对象
安全防护功能控制

2、相关功能：

SSLVPN 日志
用户认证状态

3、下游功能：<无>

4、任务向导

A1 查看运行状态
E1 实名制查看用户状态
F3 SSLVPN 远程接入

任务向导篇

A 状态统计

A1 查看运行状态

步骤一	步骤二	步骤三	步骤四	其它步骤
•查看系统运行状态： 系统概要 流量图表 CPU 趋势 内存趋势 功能统计 许可证 IPS 状态 系统日志	**•查看网络流量状态：** 带宽趋势 会话趋势 网卡状态 QoS 状态 IPSEC 连接 ARP 状态 ARP 日志 SNMP 监控日志	**•查看用户使用情况：** 在线主机 流量统计 流量日志 应用状态 日志图表 日志统计 用户状态 PPTP 状态	**•在线工具调试:** 实时监控 会话状态 测试工具	**•网管工具查询：** 设置好 SNMP 和 Netflow 服务，再通过外部工具查看系统状态

A2 查看当前日志内容

步骤一	步骤二	步骤三	步骤四	其它步骤
•本机及流量日志： 系统日志 系统状态 关键词审计 包过滤 ARP SNMP 监控 流量 特殊应用	**•网络审计日志：** DNS MSN QQ WEB 浏览 WEB POST 搜索关键词 发信发言 FTP TELNET Email	**•应用过滤日志：** DNS 代理 WEB 协议过滤 WEB 内容过滤 FTP 过滤 POP3 过滤 SMTP 过滤 防病毒 防垃圾邮件	**•IDP 及远程接入日志：** IPS IDS 蜜罐 用户认证 IPSEC PPTP PPPOE	**•日志统计及其它记录：** 日志图表 小时统计表 日期统计表 日志统计 POP3 备份 SMTP 备份 流量统计

A3 查看当前日志统计

步骤一	步骤二	步骤三	步骤四	其它步骤
•本机及流量日志： 系统日志 系统状态 关键词审计 包过滤 ARP SNMP 监控 流量 特殊应用	**•网络审计日志：** DNS MSN QQ WEB 浏览 WEB POST 搜索关键词 发信发言 FTP TELNET Email	**•应用过滤日志：** DNS 代理 WEB 协议过滤 WEB 内容过滤 FTP 过滤 POP3 过滤 SMTP 过滤 防病毒 防垃圾邮件	**•IDP 及远程接入日志：** IPS IDS 蜜罐 用户认证 IPSEC PPTP PPPOE	**•整体日志统计：** 日志图表 小时统计表 日期统计表 日志内容

B 初始设置

B1 初始化本机数据

步骤一	步骤二	步骤三	步骤四	其它步骤
初始设置	设置网卡及缺省网关 设置主机名及 DNS 服务器	设置本机时间 设置菜单界面 下载并安装证书	设置路由流控功能 设置上网管理功能 设置安全防护功能	查看功能统计 查看系统状态 查看网络状态 测试工具 查看本机许可证

B2 NAT 模式接入

步骤一	步骤二	步骤三	步骤四	其它步骤
初始设置 或者按以下步骤分步设置: 设置网卡及缺省网关 查看网卡状态	设置 NAT 策略	设置总控策略 设置地址策略 设置时间策略 设置及查看路由	测试网络连通性 查看总控策略应用情况 查看总控策略流量统计	查看在线主机 查看会话状态 系统日志

B3 透明网桥模式接入

步骤一	步骤二	步骤三	步骤四	其它步骤
初始设置 或者按以下步骤分步设置: 设置网卡及缺省网关 查看网卡状态	设置网桥	设置总控策略 设置地址策略 设置时间策略	测试网络连通性 查看总控策略应用情况 查看总控策略流量统计	查看在线主机 查看会话状态 系统日志

B4 路由模式接入

步骤一	步骤二	步骤三	步骤四	其它步骤
初始设置 或者按以下步骤分步设置: 设置网卡及缺省网关 查看网卡状态	设置及查看路由	设置总控策略 设置地址策略 设置时间策略	测试网络连通性 查看总控策略应用情况 查看总控策略流量统计	查看在线主机 查看会话状态 系统日志

C 内网管理

C1 上网行为管理

步骤一	步骤二	步骤三	步骤四	其它步骤
首先使用: 初始设置 再查看并调整: 总控 NAT 时间 流量 会话 QoS 策略	设置上网用户 IP 范围 设置特权用户 IP 范围 绑定 IP&MAC 地址 绑定 IP&用户姓名 设置 DHCP 服务	特殊应用 远程应用 P2P 下载 网络游戏 网络视频 聊天通信 网银支付 证券交易 MSN 管理 QQ 管理	网络审计策略 DNS&URL 库 DNS 代理过滤>总体设置 DNS 代理过滤>DNS 代理规则 WEB 审计过滤>WAF 规则	活跃用户 热门内容 流量状态 功能统计 在线主机 流量统计 ARP 状态 应用状态 IPS 状态 审计日志

C2 防控 ARP 病毒

步骤一	步骤二	步骤三	步骤四	其它步骤
绑定本地网段 IP 及 MAC 地址	查看本地 ARP 情况： 系统日志 系统日志统计 ARP 日志 ARP 日志统计	SNMP 监控远程 IP 及 MAC 地址	通过 SNMP 查看远程 ARP 情况： SNMP 监控 ARP 日志 SNMP 监控 ARP 日志统计	客户端安装 ARP 防火墙软件，绑定网关 IP 和 MAC 地址

C3 网络流量控制

步骤一	步骤二	步骤三	步骤四	其它步骤
设置会话策略 控制单点不同应用的会话数及新建会话速率 设置流量策略 对持续流量、上传流量和总流量的控制进行分类设置	设置 QoS 策略 控制来源对象带宽	设置总控策略 根据网络流量分类生成总控策略，将会话、流量、QoS 策略安装到各总控策略中	查看运行状态: 带宽趋势 会话趋势 在线主机 会话状态 流量统计 QoS 状态	设置 SNMP 服务 和 Netflow 服务 ，再通过外部工具查看系统状态

C4 网络流量计费

步骤一	步骤二	步骤三	步骤四	其它步骤
设置流量策略 控制单点不同应用的流量配额及清除、登出策略	设置总控策略 根据网络流量分类生成总控策略，将流量策略安装到各总控策略中	查看运行状态: 流量统计 在线主机		设置好 Netflow 服务 ，再通过外部工具查看系统状态

C5 WEB 透明协议过滤

步骤一	步骤二	步骤三	步骤四	其它步骤
设置成透明网桥模式(可选): 设置网卡及缺省网关 设置网桥	WEB 透明代理安全策略(可选): 设置 NAT 策略 设置总控策略	WEB 代理总体设置: 设置 DNS 服务器 WEB 代理总体设置	HTTP 协议过滤规则: 设置 URL、文件后缀等过滤规则及作用的站点	查看日志及统计: WEB 代理日志 WEB 代理日志统计

C6 WEB 透明内容过滤

步骤一	步骤二	步骤三	步骤四	其它步骤
设置成透明网桥模式(可选): 设置网卡及缺省网关 设置网桥	WEB 代理内容过滤总体设置: 设置 DNS 服务器 WEB 代理协议过滤 WEB 代理内容过滤	透明代理设置(可选): 设置 DNAT 策略 设置总控策略	WEB 代理内容过滤策略: 关键词规则 关键词库 关键词例外	查看日志及统计: WEB 过滤日志 WEB 过滤日志统计

C7 WEB 透明防病毒

步骤一	步骤二	步骤三	步骤四	其它步骤
设置成透明网桥模式(可选): 设置网卡及缺省网关 设置网桥	WEB 代理内容过滤总体设置: 设置 DNS 服务器 WEB 代理协议过滤 WEB 代理内容过滤	透明代理策略(可选): 设置 DNAT 策略 设置总控策略	WEB 防病毒策略: 防病毒引擎 防病毒例外 关键词例外	查看日志及统计: 防病毒日志 日志统计 WEB 过滤日志 日志统计 防病毒数据库

C8 FTP、POP3、SMTP 透明过滤

步骤一	步骤二	步骤三	步骤四	其它步骤
设置成透明网桥模式(可选) 设置网卡及缺省网关 设置网桥	FTP、POP3、SMTP 过滤策略: FTP 过滤 POP3 过滤 SMTP 过滤	透明代理设置(可选): 设置 DNAT 策略 设置总控策略	查看日志及统计: FTP 过滤日志 日志统计 POP3 过滤日志 日志统计 SMTP 过滤日志 日志统计	

C9 POP3、SMTP 透明防病毒

步骤一	步骤二	步骤三	步骤四	其它步骤
设置成透明网桥模式(可选) 设置网卡及缺省网关 设置网桥	POP3、SMTP 防病毒策略： POP3 过滤 SMTP 过滤	透明代理设置(可选)： 设置 DNAT 策略 设置总控策略	防病毒总体设置： 防病毒设置 防病毒数据库	查看日志及统计: 防病毒日志 日志统计 POP3 过滤日志 日志统计 SMTP 过滤日志 日志统计

C10 POP3、SMTP 透明防垃圾邮件

步骤一	步骤二	步骤三	步骤四	其它步骤
设置成透明网桥模式(可选)： 设置网卡及缺省网关 设置网桥	POP3、SMTP 防垃圾邮件策略： POP3 过滤 SMTP 过滤	透明代理设置(可选)： 设置 DNAT 策略 设置总控策略	防垃圾邮件总体设置： 防垃圾邮件总体设置	查看日志及统计: 防垃圾邮件日志 日志统计 POP3 过滤日志 日志统计 SMTP 过滤日志 日志统计

C11 QQ、MSN 过滤

步骤一	步骤二	步骤三	步骤四	其它步骤
设置总控策略(可选): 生成对应的总控策略，日志必须设成"详细"	QQ、MSN 过滤策略： QQ 过滤 MSN 过滤 聊天通信	查看日志及统计: QQ 过滤日志 日志统计 MSN 过滤日志 日志统计		

C12 抓包分析并阻拦特定应用

步骤一	步骤二	步骤三	步骤四	其它步骤
依次打开以下功能，并右击主菜单项，让窗口在 TAB 中重新打开 实时监控 会话状态 WEB 日志 DNS 日志 应用状态 在线主机	查看特殊应用: 远程控制 P2P 下载 网络游戏 网络视频 聊天通信 网银支付 证券交易	确认目的地址是 Blocked_Server 的总控策略存在，将需要阻拦的服务器 IP 输入到 Blocked_Server 这个 IP 地址对象的"成员"中	将需要阻拦的 WEB URL 按格式输入到 WAF 的域名等规则中	新建或修改 DNS 代理过滤的自定义域名规则，将需要阻拦的域名输入到"域名"中，"解析成的 IP"设置成内置的 WEB 服务器 IP 或 127.0.0.1 等其它无关 IP

D 对外服务

D1 服务器接入

步骤一	步骤二	步骤三	步骤四	其它步骤
初始设置 或者按以下步骤分步设置: 设置网卡及缺省网关 查看网卡状态	设置 DNAT 策略 设置总控策略 设置会话策略 设置流量策略 绑定 IP&MAC 地址	启用 Netflow 服务 设置网络审计 WEB 审计过滤>WAF 规则 IDP 总体设置 IDP 特征值	测试网络连通性 查看总控策略应用情况 查看总控策略流量统计 查看 ARP 状态 查看 IPS 状态	在线主机 会话状态 流量日志 WEB URL 日志 WEB POST 日志

D2 SSL 接入

步骤一	步骤二	步骤三	步骤四	其它步骤
启用功能: SSL 接入功能 设置 SSL 策略: 设置 SSL 服务策略	用户组及用户管理: 用户 用户组 资源 资源组 认证方法	设置总控策略: 将用户组策略安装到各总控策略中	启用功能: 用户认证功能 用户登录 WEB 门户，查看使用资源列表	查看用户状态: 在线主机 用户状态 用户认证日志 用户认证日志统计

D3 入侵检测与防御

步骤一	步骤二	步骤三	步骤四	其它步骤
IDP 总体设置： IDP 总体设置 启用 IDS、IPS 和日志	设置 IDP 策略： 特征值 网卡 IP 白名单 变量	查看 IDP 状态及日志： IPS 状态 IPS 日志 IPS 日志统计 IDS 日志 IDS 日志统计	设置蜜罐规则： 设置蜜罐规则 查看蜜罐日志： 蜜罐日志 蜜罐日志统计	查看网络审计日志： WEB 浏览 FTP TELNET Email

E 用户管理

E1 实名制查看用户状态

步骤一	步骤二	步骤三	步骤四	其它步骤
设置用户资料： 用户认证 设置用户姓名、绑定 IP	设置显示方式： 本地认证方法	查看用户状态： ARP 状态 在线主机 流量统计 应用状态 日志图表 日志统计 用户状态 PPTP 状态	查看日志统计： 查看日志统计	

E2 WEB 门户认证

步骤一	步骤二	步骤三	步骤四	其它步骤
用户组及用户管理： 用户组管理 用户管理 认证方法	设置总控策略： 将用户组策略安装到各总控策略中；协议设置成 HTTP 将启用 WEB 重定向认证	启用功能： 用户认证功能 用户登录 WEB 门户，修改口令	查看用户状态： 在线主机 用户状态 用户认证日志 用户认证日志统计	

F 远程接入

F1 PPTP、PPPOE 用户接入

步骤一	步骤二	步骤三	步骤四	其它步骤
用户组及用户管理： 用户组管理 启用 PPTP 组或 PPPOE 组 用户管理	总体设置： PPTP 总体设置 PPPOE 总体设置	设置总控策略： 总控策略 允许到本机网卡的 GRE 协议的通讯，允许 PPP 网卡的通讯	查看用户状态及日志： PPTP 状态 PPPOE 状态 PPTP 日志 PPPOE 日志 PPTP 统计 PPPOE 统计	启用功能： 用户认证功能 用户登录 WEB 门户，修改口令

F2 IPSEC VPN 接入

步骤一	步骤二	步骤三	步骤四	其它步骤
IPSEC 总体设置： IPSEC 总体设置 启用 IKE	IPSEC 策略设置： IPSEC 网关设置 IPSEC 连接设置 本机证书设置	设置总控策略： 总控策略 允许到本机网卡的 ESP 协议的通讯，允许 IPSEC 网卡的通讯	查看日志状态： IPSEC 日志 IPSEC 网关状态 IPSEC 连接状态	在线工具调试: 实时监控 会话状态 测试工具

F3 SSLVPN

步骤一	步骤二	步骤三	步骤四	其它步骤
总体设置： SSLVPN 总体设置 设置用户地址池 设置路由地址池 定制客户端软件安装程序	设置 SSLVPN 用户组及用户： 用户组 启用 SSLVPN 组 用户	设置针对 PPP 网卡的总控策略： 总控策略 允许到本机网卡的服务协议、服务端口的通讯，允许 PPP 网卡的通讯，加上 SSLVPN 用户组的用户认证选项 NAT 路由 设置针对 SSLVPN_network 的 SNAT 策略或回程路由	启用 WEB 门户： 用户认证功能 用户登录 WEB 门户，修改缺省口令，下载客户端软件，安装使用	查看用户状态及日志： SSLVPN 状态 SSLVPN 日志 SSLVPN 统计 实时监控 会话状态