H3C SecPath ACG1000 系列应用控制网关

开局指导书

目录

1 特性简述

1.1 产品介绍

H3C SecPath ACG1000 是 H3C 公司新一代应用控制网关，ACG1000 融入了 H3C 最新的 BON（Business Oriented Network）设计理念，是面向客户业务而量身定制的全业务网关产品。

H3C SecPath ACG1000 系列应用控制网关能对网络中的网络社区、P2P/IM 带宽滥用、网络游戏、炒股、网络多媒体、非法网站访问等行为进行精细化识别和控制，并利用智能流控、智能阻断、智能路由等技术，配合创新的社交网络行为管理功能、清晰易管理日志等功能，提供完善的上网行为管理解决方案。从而保障网络关键应用和服务的带宽，对网络流量、用户上网行为进行深入分析与全面的审计，为用户全面了解网络应用模型和流量趋势，优化其带宽资源，开展各项业务提供有力的支撑。

1.2 系统介绍

1.2.1 ACG1000 面板介绍

H3C SecPath ACG1000 系列应用控制网关包括 ACG1000-XE1、ACG1000-PE、ACG1000-EE、ACG1000-AE、ACG1000-ME、ACG1000-TE、ACG1060-X1、ACG1070-X1、ACG1000-B、ACG1005、ACG1000-C 、ACG1010、ACG1020、ACG1000-S、ACG1030、ACG1040、ACG1050、ACG1000-M、ACG1000-T、ACG1060、ACG1000-A、ACG1070、ACG1000-E、ACG1000-P、ACG1000-X 、 ACG1000-AK110 、 ACG1000-AK120 、 ACG1000-AK130 、 ACG1000-AK140 、ACG1000-AK150、ACG1000-AK160、ACG1000-AK170、ACG1000-AK180、ACG1000-SE-PWR、ACG1000-SE、ACG 1000-BE-PWR、ACG 1000-BE、ACG1005-PWR 等多款产品，在不区分具体型号时，后续章节统称为 ACG1000 系列设备。

图1-1 ACG1000-B、ACG1005、ACG1000-C、ACG1010、ACG1020、ACG1000-AK110、ACG1000-AK120 设备前面板

表1-1 面板各区域说明

说明区域	区域说明	详细说明
①系统指示灯区	标识系统电源和系统运行状态	包括电源指示灯PWR和系统运行指示灯SYS： • PWR 蓝色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电 • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行
②USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接

		3G卡来支持3G上网功能
③Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
④业务接口区	系统管理和业务网络接口	10/100/1000BASE-T自适应以太网接口，缺省情况下，ge0是管理接口

图1-2 ACG1000-S、ACG1030、ACG1040、ACG1050、ACG1000-AK140 设备前面板

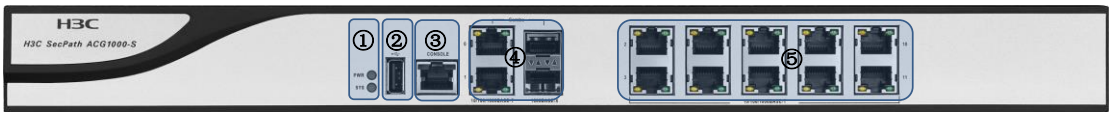


表1-2 面板各区域说明

说明区域	区域说明	详细说明
①系统指示灯区	标识系统电源和系统运行状态	包括电源指示灯PWR和系统运行指示灯SYS： • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电 • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行
②USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接3G卡来支持上网功能
③Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
④COMBO业务接口区	系统管理和业务网络接口	光电复用接口： 每一个SFP接口对应有一个复用的10/100/1000BASE-T接口，对应的两个接口在同一时刻只能有一个SFP或10/100/1000BASE-T接口被使用，缺省情况下，ge0是管理接口
⑤业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口

图1-3 ACG1000-M、ACG1000-T、ACG1060、ACG1000-A、ACG1070、ACG1000-AK160、ACG1000-AK170 设备前面板

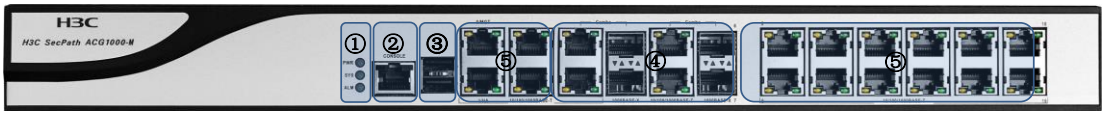


表1-3 面板各区域说明

说明区域	区域说明	详细说明
①系统指示灯区	标识系统电源和系统运行状态	包括电源指示灯PWR和系统运行指示灯SYS： • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电 • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行
②Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
③USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接3G卡来支持上网功能
④COMBO业务接口区	系统管理和业务网络接口	光电复用接口： 每一个SFP接口对应有一个复用的10/100/1000BASE-T接口，对应的两个接口在同一时刻只能有一个SFP或10/100/1000BASE-T接口被使用
⑤业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口，缺省情况下，ge0是管理接口

图1-4 ACG1000-E、ACG1000-P、ACG1000-X、ACG1000-AK180 设备前面板

表1-4 面板各区域说明

说明区域	区域说明	详细说明
①系统指示灯区	标识系统电源和系统运行状态	包括电源指示灯PWR和系统运行指示灯SYS： • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电 • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行
②Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
③USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接3G卡来支持上网功能

④管理接口区	系统管理接口	10/100自适应以太网管理接口①
⑤板载接口区	板载业务网络接口，板载为光电复用接口	光电复用接口：缺省情况下，系统识别板载区为槽位1，接口形态为ge1-0~ge1-3 每一个SFP接口对应有一个复用的10/100/1000BASE-T接口，对应的两个接口在同一时刻只能有一个SFP或10/100/1000BASE-T接口被使用
⑥、⑦、⑧扩展接口区	安装扩展接口子卡槽位	扩展插槽，各槽位对子卡的适配能力一致： 适配4COMBO子卡、1XG子卡、4XG子卡，可根据实际业务需求进行选择扩展

图1-5 ACG1000-AK130、ACG 1000-BE-PWR、ACG 1000-BE、ACG1005-PWR 设备前面板

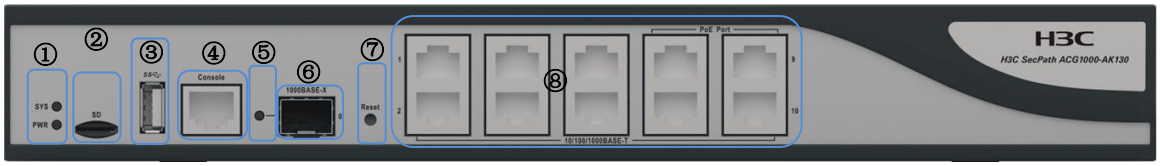


表1-5 面板各区域说明

说明区域	区域说明	详细说明
①统指示灯区	标识系统电源和系统运行状态	包括系统运行指示灯SYS和电源指示灯PWR： • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行 • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电
②SD接口区	支持SD扩展的接口	目前支持连接TF卡存储器用于存储
③USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接3G卡来支持上网功能
④Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
⑤SFP接口指示灯	光模块接口状态指示灯	指示光模块状态常亮表示光模块link，闪烁表示有数据收发，常灭表示未link
⑥ SFP接口	连接光模块的接口	1000BASE-X光模块接口, 接口形态为ge0
⑦ 按键	系统复位按键	长按该按键，进行软件复位重启系统。
⑧业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口，接口形态为ge1~ge10,缺省情况下，ge1是管理接口

图1-6 ACG1000-AK150、ACG1000-SE-PWR、ACG1000-SE 设备前面板

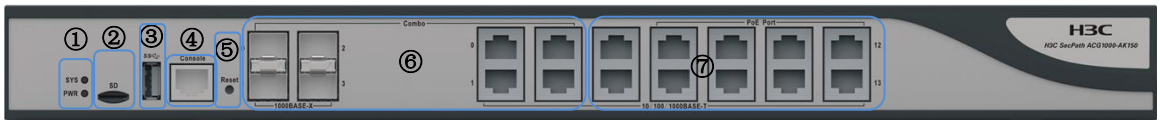


表1-6 面板各区域说明

说明区域	区域说明	详细说明
①统指示灯区	标识系统电源和系统运行状态	包括系统运行指示灯SYS和电源指示灯PWR： • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行 • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电
②SD接口区	支持SD扩展的接口	目前支持连接TF卡存储器用于存储
③USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本
④Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
⑤ 按键	系统复位按键	长按该按键，进行软件复位重启系统
⑥COMBO业务接口区	系统管理和业务网络接口	光电复用接口：接口形态为ge0~ge3, 缺省情况下，ge0是管理接口 每一个SFP接口对应有一个复用的10/100/1000BASE-T接口，对应的两个接口在同一时刻只能有一个SFP或10/100/1000BASE-T接口被使用
⑦业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口

图1-7 ACG1000-XE1

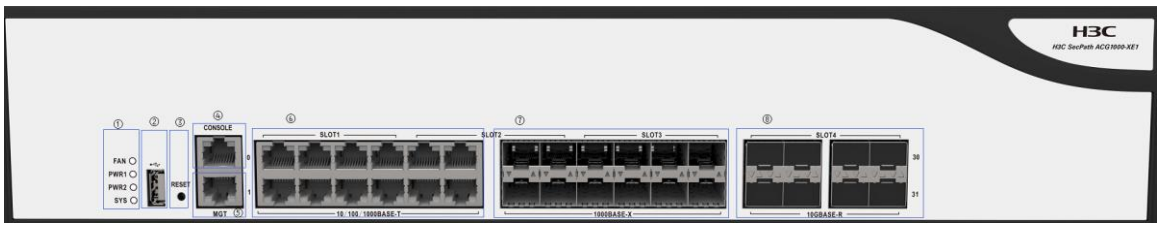


表1-7 面板各区域说明

说明区域	区域说明	详细说明
①系统指示灯区	标识系统电源和系统运行状态	包括电源指示灯PWR和系统运行指示灯SYS： • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电 • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行
②USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接4G卡来支持上网功能

③reset按键区	系统reset按键	系统reset按键： 支持长按恢复出厂设置
④Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
⑤MGT接口区	系统默认管理接口	10/100/1000BASE-T自适应以太网接口： 系统的默认管理口，可以通过该接口进行设备的调试、配置、维护、管理等工作
⑥千兆电口业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口
⑦千兆光口业务接口区	业务网络接口	1000BASE-X以太网接口
⑧万兆光口业务接口区	业务网络接口	10GBASE-R以太网接口

图1-8 ACG1000-PE、ACG1000-EE

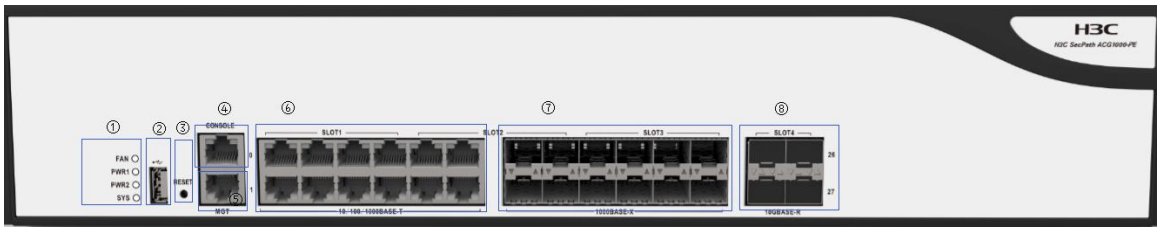


表1-8 面板各区域说明

说明区域	区域说明	详细说明
①系统指示灯区	标识系统电源和系统运行状态	包括电源指示灯PWR和系统运行指示灯SYS： • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电 • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行
②USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接4G卡来支持上网功能
③reset按键区	系统reset按键	系统reset按键： 支持长按恢复出厂设置
④Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
⑤MGT接口区	系统默认管理接口	10/100/1000BASE-T自适应以太网接口： 系统的默认管理口，可以通过该接口进行设备的调试、配置、维护、管理等工作

⑥千兆电口业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口
⑦千兆光口业务接口区	业务网络接口	1000BASE-X以太网接口
⑧万兆光口业务接口区	业务网络接口	10GBASE-R以太网接口

图1-9 ACG1000-AE

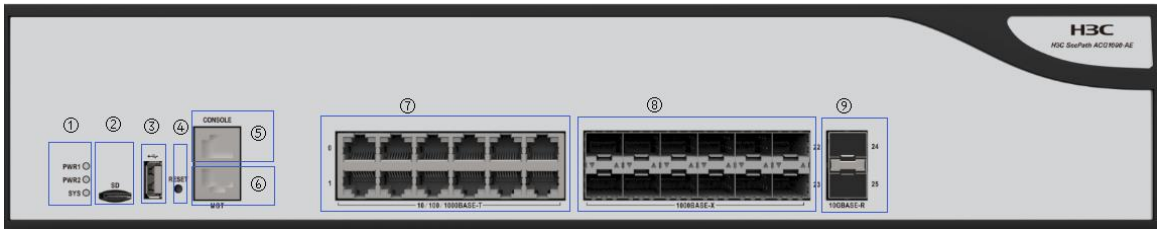


表1-9 面板各区域说明

说明区域	区域说明	详细说明
①系统指示灯区	标识系统电源和系统运行状态	包括电源指示灯PWR和系统运行指示灯SYS： • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电 • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行
②SD接口区	支持SD扩展的接口	目前支持连接TF卡存储器用于存储
③USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接4G卡来支持上网功能
④reset按键区	系统reset按键	系统reset按键： 支持长按恢复出厂设置
⑤Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
⑥MGT接口区	系统默认管理接口	10/100/1000BASE-T自适应以太网接口： 系统的默认管理口，可以通过该接口进行设备的调试、配置、维护、管理等工作
⑦千兆电口业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口
⑧千兆光口业务接口区	业务网络接口	1000BASE-X以太网接口
⑨万兆光口业务接口区	业务网络接口	10GEX以太网接口

图1-10 ACG1000-XE1、ACG1000-ME、ACG1000-TE、ACG1060-X1、ACG1070-X1

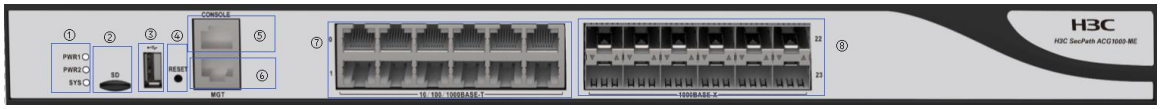


表1-10 面板各区域说明

说明区域	区域说明	详细说明
①系统指示灯区	标识系统电源和系统运行状态	包括电源指示灯PWR和系统运行指示灯SYS： • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电 • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行
②SD接口区	支持SD扩展的接口	目前支持连接TF卡存储器用于存储
③USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接4G卡来支持上网功能
④reset按键区	系统reset按键	系统reset按键： 支持长按恢复出厂设置
⑤Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
⑥MGT接口区	系统默认管理接口	10/100/1000BASE-T自适应以太网接口： 系统的默认管理口，可以通过该接口进行设备的调试、配置、维护、管理等工作
⑦千兆电口业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口
⑧千兆光口业务接口区	业务网络接口	1000BASE-X以太网接口

图1-11 ACG1000-K210

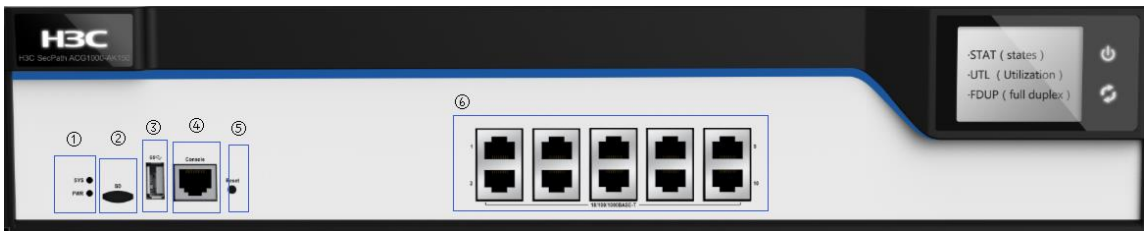


表1-11 面板各区域说明

说明区域	区域说明	详细说明

①统指示灯区	标识系统电源和系统运行状态	包括系统运行指示灯SYS和电源指示灯PWR： • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行 • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电
②SD接口区	支持SD扩展的接口	目前支持连接TF卡存储器用于存储
③USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接3G卡来支持上网功能
④Console接口区 A	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
⑤reset按键	系统复位按键	长按该按键，进行软件复位重启系统。
⑥业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口，接口形态为ge1~ge10,缺省情况下，ge1是管理接口

图1-12 ACG1000-K220

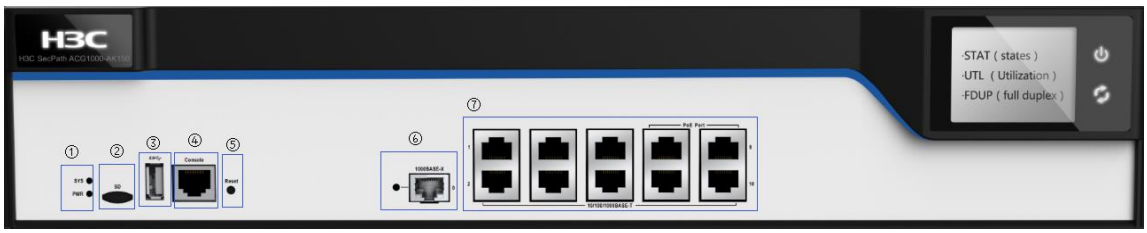


表1-12 面板各区域说明

说明区域	区域说明	详细说明
①统指示灯区	标识系统电源和系统运行状态	包括系统运行指示灯SYS和电源指示灯PWR： • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行 • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电
②SD接口区	支持SD扩展的接口	目前支持连接TF卡存储器用于存储
③USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接4G卡来支持上网功能
④Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
⑤reset按键	系统复位按键	长按该按键，进行软件复位重启系统。
⑥ SFP接口	连接光模块的接口	1000BASE-X光模块接口, 接口形态为ge0

		指示灯指示光模块状态常亮表示光模块link，闪烁表示有数据收发，常灭表示未link
⑦业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口，接口形态为ge1~ge10,缺省情况下，ge1是管理接口

图1-13 ACG1000-K230

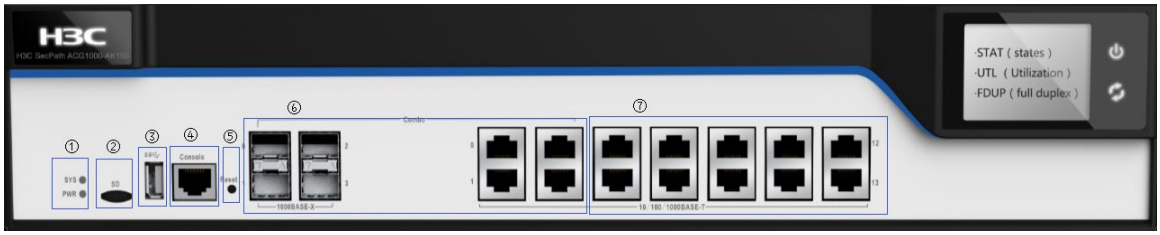


表1-13 面板各区域说明

说明区域	区域说明	详细说明
①统指示灯区	标识系统电源和系统运行状态	包括系统运行指示灯SYS和电源指示灯PWR： • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行 • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电
②SD接口区	支持SD扩展的接口	目前支持连接TF卡存储器用于存储
③USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本
④Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
⑤ 按键	系统复位按键	长按该按键，进行软件复位重启系统
⑥COMBO业务接口区	系统管理和业务网络接口	光电复用接口：接口形态为ge0~ge3, 缺省情况下，ge0是管理接口 每一个SFP接口对应有一个复用的10/100/1000BASE-T接口，对应的两个接口在同一时刻只能有一个SFP或10/100/1000BASE-T接口被使用
⑦业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口

图1-14 ACG1000-K240

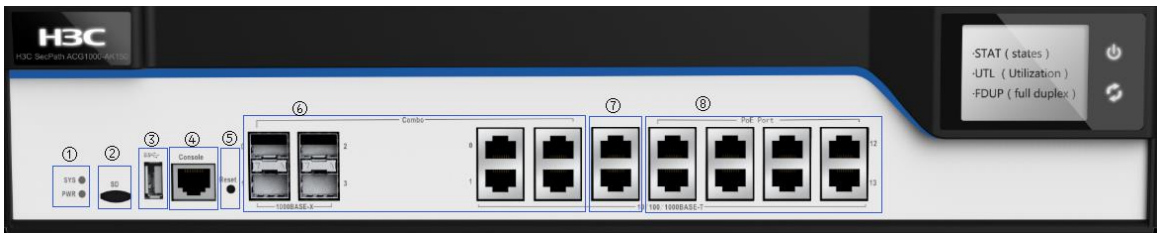


表1-14 面板各区域说明

说明区域	区域说明	详细说明
①统指示灯区	标识系统电源和系统运行状态	包括系统运行指示灯SYS和电源指示灯PWR： • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行 • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电
②SD接口区	支持SD扩展的接口	目前支持连接TF卡存储器用于存储
③USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本
④Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
⑤ 按键	系统复位按键	长按该按键，进行软件复位重启系统
⑥COMBO业务接口区	系统管理和业务网络接口	光电复用接口：接口形态为ge0~ge3, 缺省情况下，ge0是管理接口 每一个SFP接口对应有一个复用的10/100/1000BASE-T接口，对应的两个接口在同一时刻只能有一个SFP或10/100/1000BASE-T接口被使用
⑦业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口
⑧POE业务接口区	POE业务接口	10/100/1000BASE-T自适应以太网接口，支持POE供电

图1-15 ACG1000-K250、ACG1000-K260、ACG1000-K270

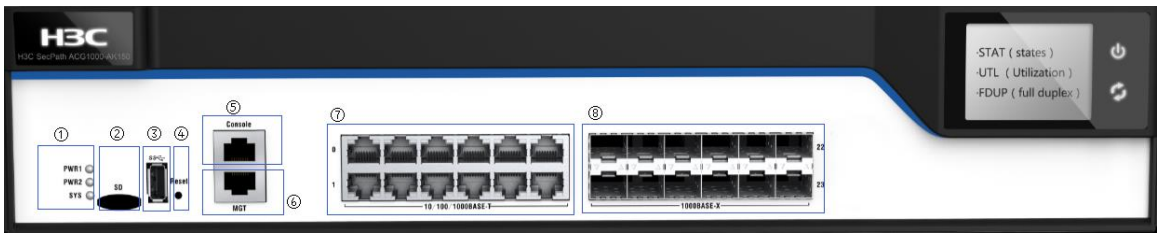


表1-15 面板各区域说明

说明区域	区域说明	详细说明
①系统指示灯区	标识系统电源和系统运行状态	包括电源指示灯PWR和系统运行指示灯SYS： • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电 • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行
②SD接口区	支持SD扩展的接口	目前支持连接TF卡存储器用于存储

③USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接4G卡来支持上网功能
④reset按键区	系统reset按键	系统reset按键： 支持长按恢复出厂设置
⑤Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作
⑥MGT接口区	系统默认管理接口	10/100/1000BASE-T自适应以太网接口： 系统的默认管理口，可以通过该接口进行设备的调试、配置、维护、管理等工作
⑦千兆电口业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口
⑧千兆光口业务接口区	业务网络接口	1000BASE-X以太网接口

图1-16 ACG1000-K280

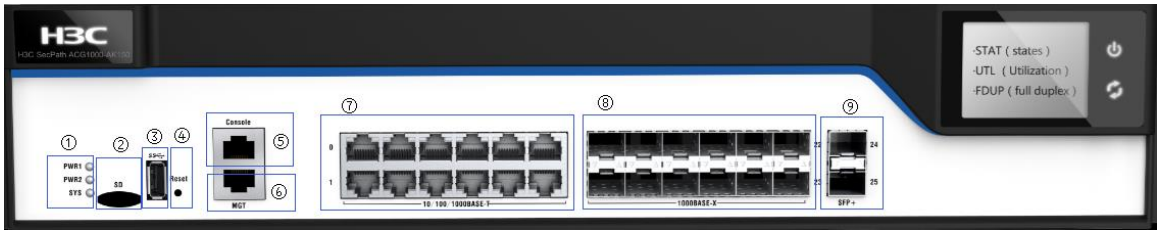


表1-16 面板各区域说明

说明区域	区域说明	详细说明
①系统指示灯区	标识系统电源和系统运行状态	包括电源指示灯PWR和系统运行指示灯SYS： • PWR 绿色常亮表示系统上电，常灭表示系统未上电或电源模块无法正常供电 • SYS 绿色常亮表示系统处于 uboot 状态或系统启动过程，绿色闪烁表示系统正常运行
②SD接口区	支持SD扩展的接口	目前支持连接TF卡存储器用于存储
③USB接口区	支持USB扩展的接口	通用串行数据接口： 目前支持连接USB存储器用于存储和加载软件版本，支持连接4G卡来支持上网功能
④reset按键区	系统reset按键	系统reset按键： 支持长按恢复出厂设置
⑤Console接口区	连接管理串口线的接口	通信串口，采用标准的RJ45连接器： 用来连接后台终端计算机的串口，以进行设备的调试、配置、维护、管理等工作

⑥MGT接口区	系统默认管理接口	10/100/1000BASE-T自适应以太网接口： 系统的默认管理口，可以通过该接口进行设备的调试、配置、维护、管理等工作
⑦千兆电口业务接口区	业务网络接口	10/100/1000BASE-T自适应以太网接口
⑧千兆光口业务接口区	业务网络接口	1000BASE-X以太网接口
⑨万兆光口业务接口区	业务网络接口	10GBASE-R以太网接口

这里，支持的扩展接口单板如下：

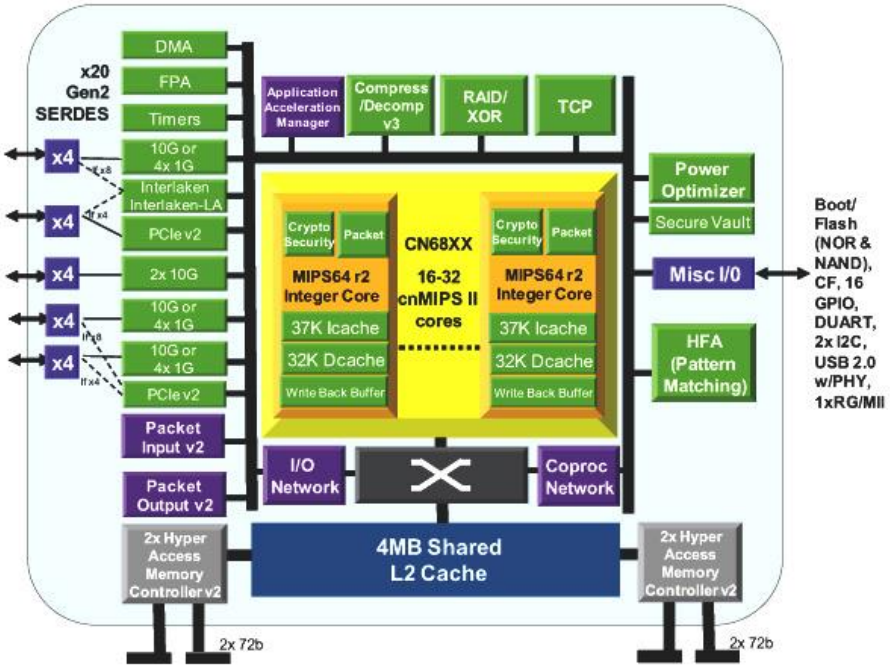
表1-17 支持的扩展接口卡

单板名称	单板类型	单板俗称	单板印丝名称	备注
4 Combo接口卡	业务卡	4COMBO子卡	NSQM1GC4	4个COMBO口，其中后一对电口支持断电和启动过程硬件bypass，不支持热插拔
1 SFP+接口卡	业务卡	1万兆	NSQM1TGS1	1个万兆SFP+，不支持热插拔
4 SFP+接口卡	业务卡	4万兆	NSQM1TGS4	4个万兆SFP+，不支持热插拔

1.2.2 系统结构介绍

H3C SecPath ACG 1000 系列应用控制网关产品采用了业界先进的分布式计算、集中式管理的体系结构，高性能专用硬件平台—ACG 应用控制网关作为最核心的设备，负责主要的计算和处理工作；审计功能负责对应用管理器的管理以及数据的分析和存储；客户端作为终端，负责查看配置工作。各个层次各司其职，又相互关联，达到最佳的可用性和稳定性。

图1-17 硬件架构



内置应用控制引擎系统，主要负责“快速地”与“准确地”执行流量实时分析、内容深度检测与智能分类、以及带宽优化与控制等任务，能对网络中的网络社区、P2P/IM 带宽滥用、网络游戏、炒股、网络多媒体、非法网站访问等行为进行精细化识别和控制。

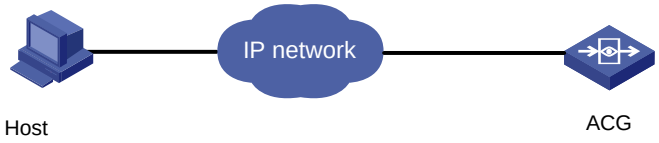
图1-18 智能流控和带宽保障

1.3 ACG1000 的管理

H3C SecPath ACG 1000 系列应用控制网关支持 Web 界面和命令行两种管理方式，管理员通过 Web 管理界面可以直观地管理和维护网络设备；通过命令行可以提供全面的配置、信息查看、故障诊断等。

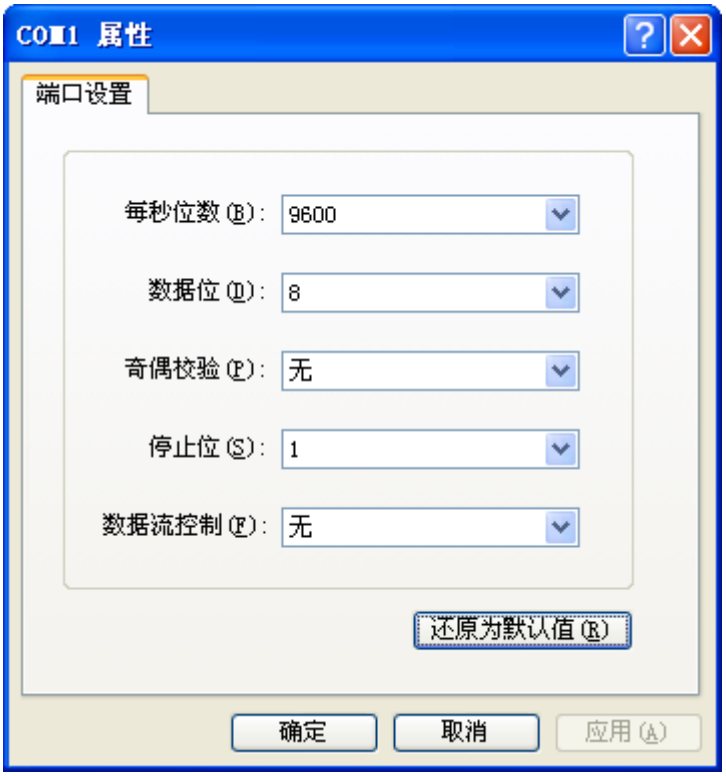
Web 网管的运行环境如图 1-19 所示：

图1-19 Web 网管运行环境



如图 1-20 所示，ACG1000 系列设备主机上自带 Console 口，可以用串口线对 ACG1000 进行命令行管理，其串口波特率默认为 9600。

图1-20 串口参数设置



2 部署方式

2.1 部属方式简介

ACG 路由部署模式：在不同的网络需求环境下对网络设备部署方式也有严格的要求，ACG 能够工作在三种模式下：路由模式、透明模式、旁路模式。如果 ACG 以三层对外连接（接口具有 IP 地址），则认为 ACG 工作在路由模式下；若 ACG 通过第二层对外连接（接口无 IP 地址），则 ACG 工作在透明模式下；若在不影响网络拓扑的前提下增加网络安全性，则使用旁路模式 ACG。

ACG ISP 路由部署模式：一般企业通常会申请多条线进行流量负载均衡。然而，一般的均衡是不会根据流量的流向做均衡的，如果网通的服务器通过电信访问，网速就会很慢。安全网关针对该问题，提供 ISP 路由功能，使不同 ISP 流量走专有路由通道，从而提高网络访问速度。

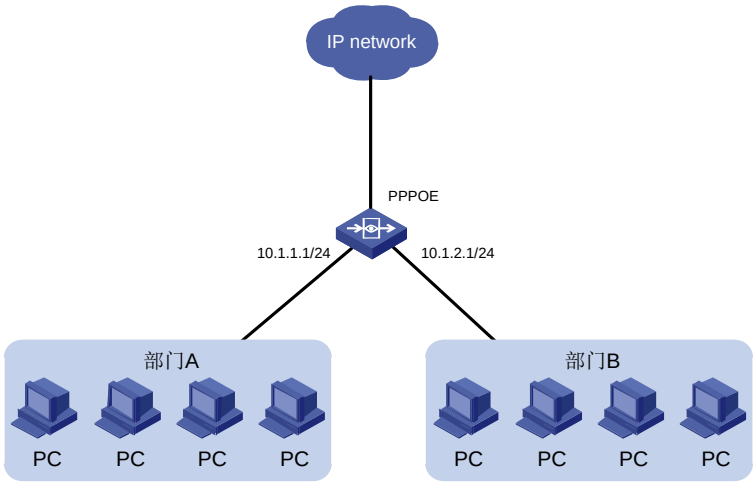
2.2 路由模式

2.2.1 组网需求

网络管理人员决定启用路由模式 ACG 实现直接与外网相连，现在需要在 ACG 上做适当配置。

2.2.2 组网图

图2-1 路由模式 ACG 组网图



2.2.3 配置思路

(1) 配置接口地址
(2) 配置路由
(3) 配置安全策略
(4) 配置源 NAT
(5) 保存配置
(6) 配置客户端 IP 等信息

2.2.4 配置步骤

(1) 登录 web 界面，进入网络配置>接口>物理接口，编辑各接口地址。

图2-2 配置接口地址

(2) 接口地址为 PPPOE，配置正确的用户名、密码，务必勾选更新网关，这样拨号成功后设备会自动生成默认路由，无需手动配置默认路由，管理方式根据访问需要进行选择。

图2-3 ge0 接口配置

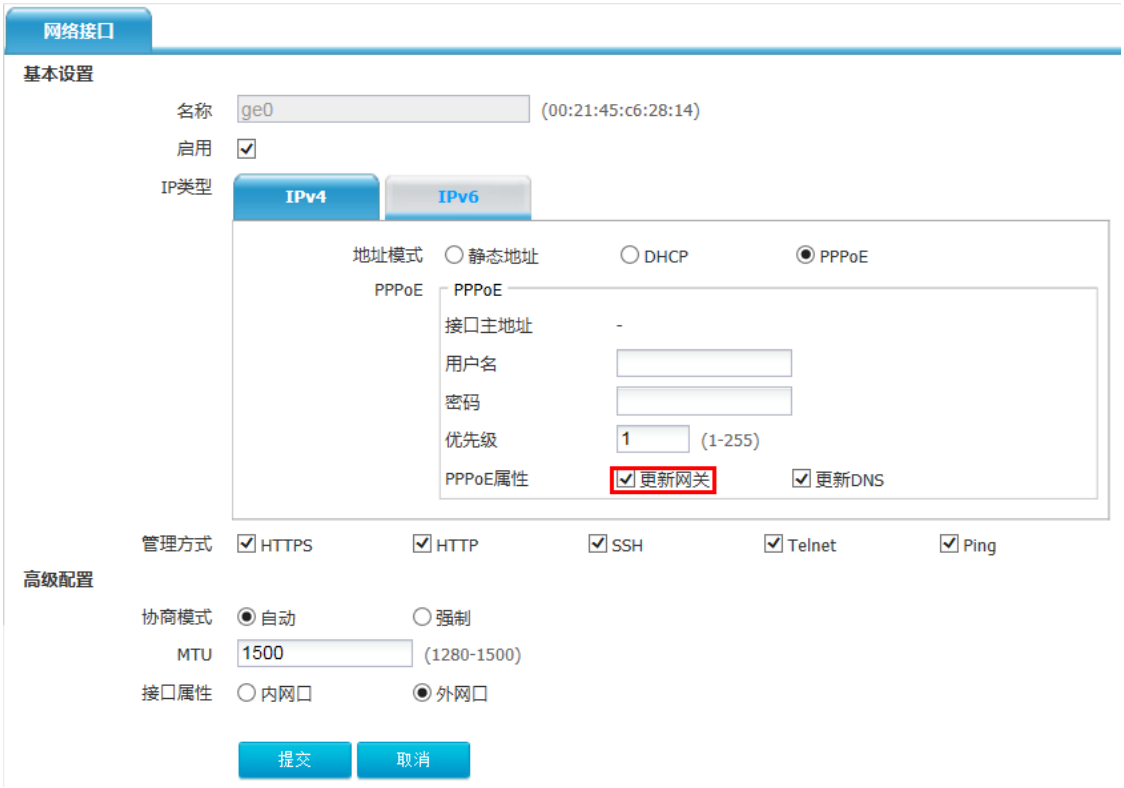


图2-4 ge1 接口配置

图2-5 ge2

(3) 配置路由，拨号成功后，进入“网络配置>路由>路由表”，可以看到系统自动生成的默认路由，协议为 PPPOE。

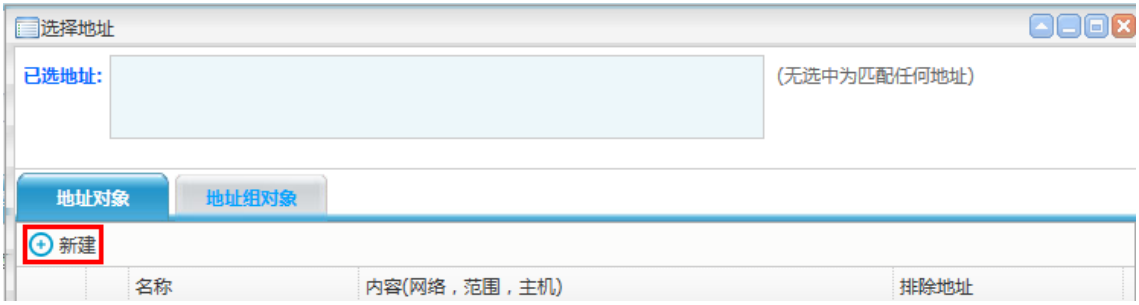
图2-6 配置安全策略：

点击匹配源，在源地址下拉格后点击选择地址。

图2-7 配置匹配源

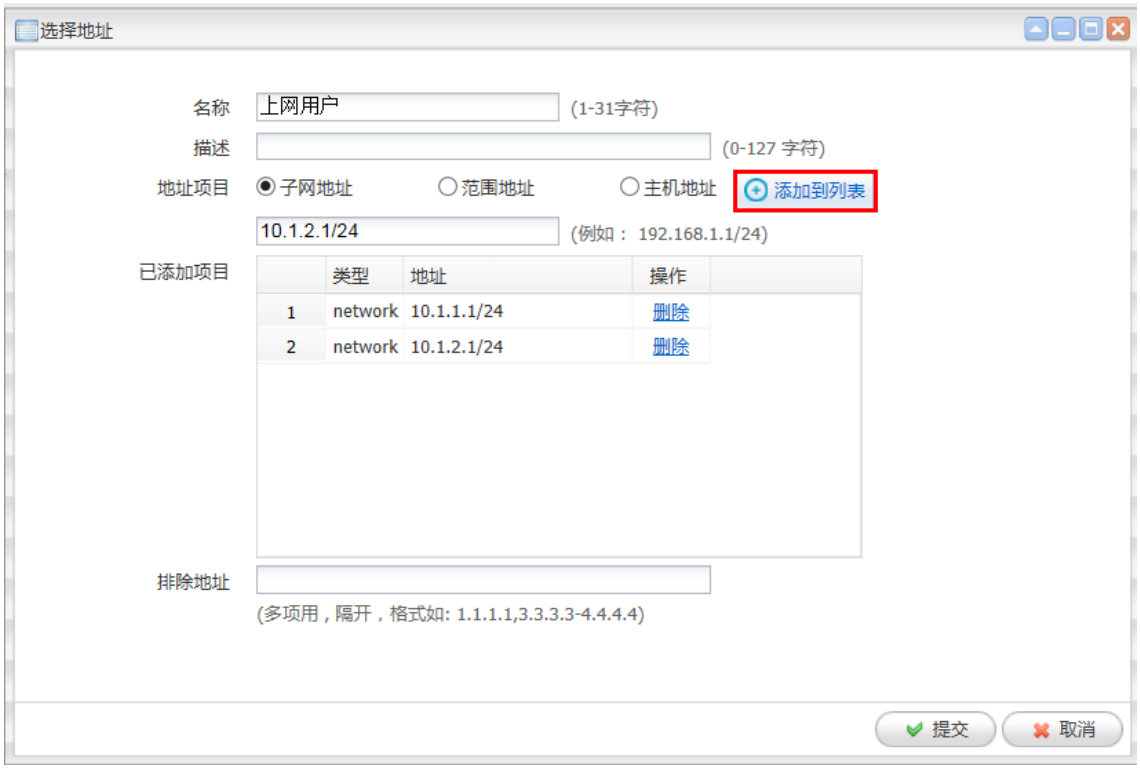
点击选择地址中，地址对象下方的<新建>。

图2-8 选择地址（一）



在名称处填写此地址的描述名称(便于选择地址使用)，输入上网地址（或网段）点击添加到列表提交。

图2-9 选择地址（二）



提交后，在匹配源中源地址项选择刚刚创建的上网用户后提交。

图2-10 提交配置

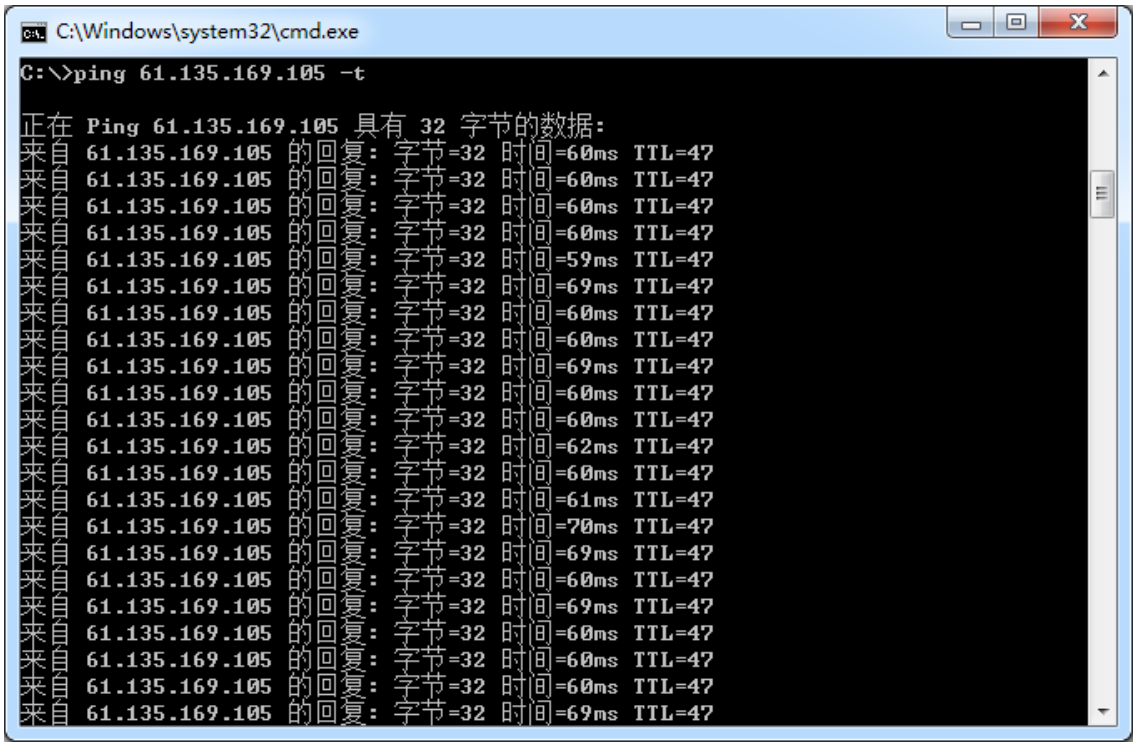
(4) 进入“网络配置>NAT>源 NAT”，点击页面左上角的<新建>按钮：将 IPV4 策略中匹配的上网地址调用在 NAT 中,转换类型为出接口,接口选择连接外网的接口，配置完成后点击提交。

图2-11 配置源 NAT 规则

(5) 保存配置。

(6) 配置客户端 IP、网关以及 DNS。。

图2-12 客户端



2.2.5 注意事项

使用 PPPOE 拨号时需要更新网关，在配置 IPV4 策略时添加上网地址后要点击添加到列表，如未点击添加到列表，则代表此策略不生效，NAT 转换时选择出接口正确。

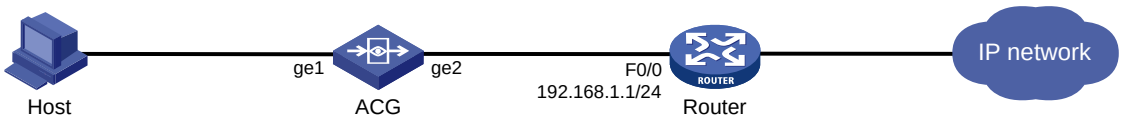
2.3 透明模式

2.3.1 组网需求

当固定网络环境中需要添加 ACG 1000，考虑到以路由模式添加对原网络改动幅度较大。选择以透明模式 ACG 加入网络。只需要更改 ACG 两端的接口在同一桥接口内即可。

2.3.2 组网图

图2-13 透明模式 ACG 组网图



2.3.3 配置思路

(1) 配置桥接口

(2) 配置安全策略

(3) 保存配置

(4) 配置客户端 IP 等信息

2.3.4 配置步骤

(1) 登录 Web 界面，进入“网络配置>接口>桥接口”，新建接口。

图2-14 新建桥接口

(2) 在新建接口内将 ge1、ge2 加入 bvi1 中，可以根据需要对桥接口进行 IP 地址配置。配置桥接口 IP 地址后，可以对 ACG 进行管理，管理方式根据访问需要进行选择。

图2-15 配置桥接口

(3) 进入“上网行为管理>策略配置>IPV4 策略”，点击页面左上角的<新建>按钮。

图2-16 配置安全策略

图2-17 匹配源地址 Any 行为允许

(4) 保存配置。

(5) 配置客户端 IP、网关以及 DNS。。

2.3.5 注意事项

- 透明模式需要配置桥接口，并把内外网接口加入到同一个桥接口下，数据便能通过二层转发。

安全策略按从上向下匹配的原则。状态为“ ”的上网策略才会生效。

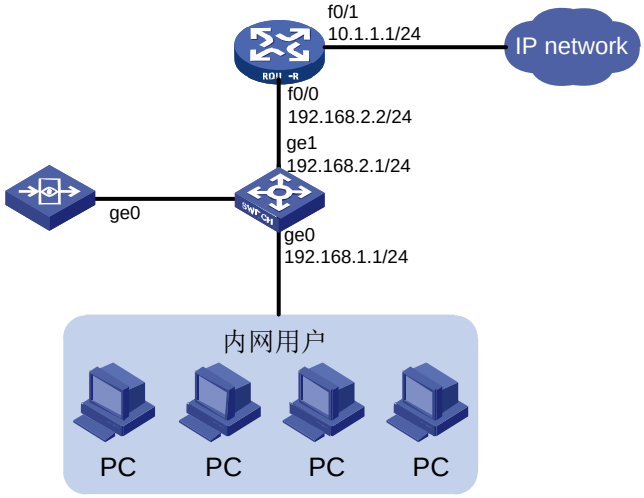
2.4 旁路模式

2.4.1 组网需求

公司新增一台 ACG 用于监控用户流量，为了不影响现网拓扑，使用旁路模式部署。

2.4.2 组网图

图2-18 旁路模式 ACG 组网图



2.4.3 配置思路

(1) 配置旁路模式

(2) 配置安全策略

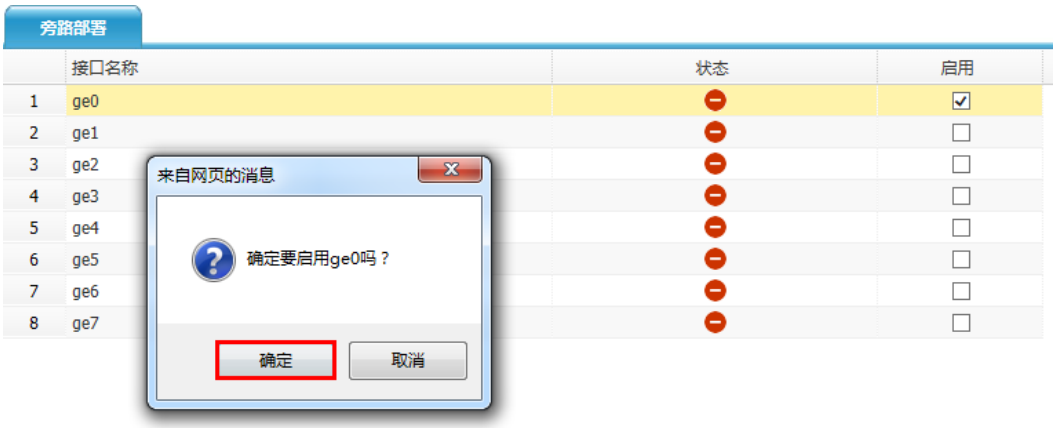
(3) 保存配置

(4) 配置客户端 IP 等信息

2.4.4 配置步骤

(1) 进入“系统管理>部署方式>旁路部署”，勾选 ge0 接口，在弹出的对话框中点击“确认”。

图2-19 配置旁路模式



(2) 进入“上网行为管理>策略配置>IPV4 策略”，点击页面左上角的<新建>按钮。

图2-20 新建安全策略

匹配源地址 Any 点击提交。

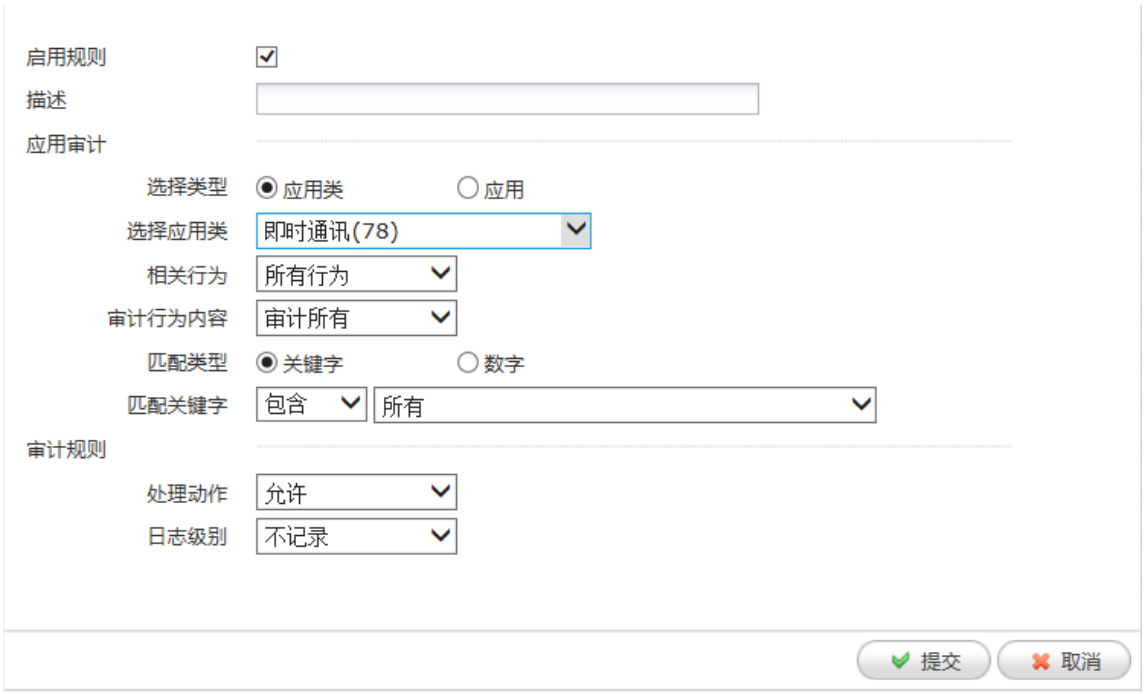
图2-21 配置安全策略

(3) 进入上网行为管理>策略配置>IPV4 策略，选择刚刚创建的策略，点击编辑。

图2-22 编辑策略

(4) 选择应用过滤，点击<新建>，配置需要的应用审计类型、处理动作、日志级别等，点击提交。

图2-23 配置应用策略



(5) 选择 URL 过滤，配置需要的过滤的 URL 分类、日志级别，点击提交。

(6) 保存配置。

(7) 配置客户端 IP、网关以及 DNS。

2.4.5 注意事项

- ACG 默认行为为拒绝所有，注意配置策略放行。
- 要将网络流量引向 ACG，使任何流量都通过 ACG 转发。

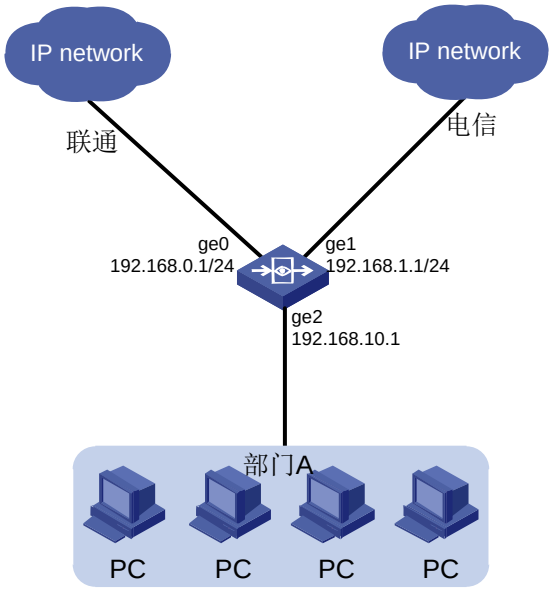
2.5 ISP 路由部署

2.5.1 组网需求

公司出口设备，出口使用不同运营商两条线路，正常情况下访问电信网络使用电信线路，访问联通网络使用联通线路。当一条线路出现故障时，所有用户使用另外一条线路访问外网。

2.5.2 组网图

图2-24 ISP 路由组网图



2.5.3 配置思路

(1) 配置接口地址
(2) 配置 Ipv4 地址对象
(3) 配置 ISP 路由
(4) 配置源 NAT
(5) 配置安全策略
(6) 保存配置
(7) 配置客户端 IP 等信息

2.5.4 配置步骤

(1) 配置接口地址

进入“网络配置>接口>物理接口”，编辑 ge0、ge1、ge2 接口。

图2-25 编辑接口

图2-26 ge0


网络接口
基本设置
名称
ge0
(00:21:45:c6:28:14)
启用
IP类型
IPv4
IPv6
地址模式
静态地址
DHCP
PPPoE
接口主地址
192.168.0.1/24
从属IPv4列表
新建
管理方式
HTTPS
HTTP
SSH
Telnet
Ping
高级配置
协商模式
自动
强制
MTU
1500
(1280-1500)
接口属性
内网口
外网口
提交
取消

图2-27 ge1


网络接口
基本设置
名称
ge1
(00:21:45:c6:28:15)
启用
IP类型
IPv4
IPv6
地址模式
静态地址
DHCP
PPPoE
接口主地址
192.168.1.1/24
从属IPv4列表
新建
地址
操作
管理方式
HTTPS
HTTP
SSH
Telnet
Ping
高级配置
协商模式
自动
强制
MTU
1500
(1280-1500)
接口属性
内网口
外网口
提交
取消

图2-28 ge2

(2) 配置 Ipv4 地址对象

进入“对象管理>地址>IPv4 地址对象”，点击页面左上角的<新建>按钮，配置 IPv4 地址对象名称为上网网段，地址节点选择子网地址：192.168.2.0/24,点击<新建>，点击提交。

图2-29 配置地址对象

(3) 配置 ISP 路由

进入“网络配置>路由>ISP 路由>ISP 路由”，点击<新建>。

配置访问联通网络使用联通线路：

图2-30 配置 ISP 路由

图2-31 配置访问电信网络使用电信线路：

(4) 配置静态路由，进入“网络配置>路由>静态路由”，点击<新建>。

图2-32 联通

图2-33 电信

当某一接口 down 掉后，ISP 路由会失效，切换到另一线路，当 ISP 未匹配时，会匹配默认路由。

(5) 配置源 NAT

在源地址处选择上网网段，转换类型为出接口接口选择 ge0 和 ge2，配置完成后点击提交。

进入“网络配置>NAT>源 NAT”，点击<新建>。

图2-34 配置 SNAT

点击源地址下拉框，选择已配置好的 IPV4 地址对象。

图2-35 ge0

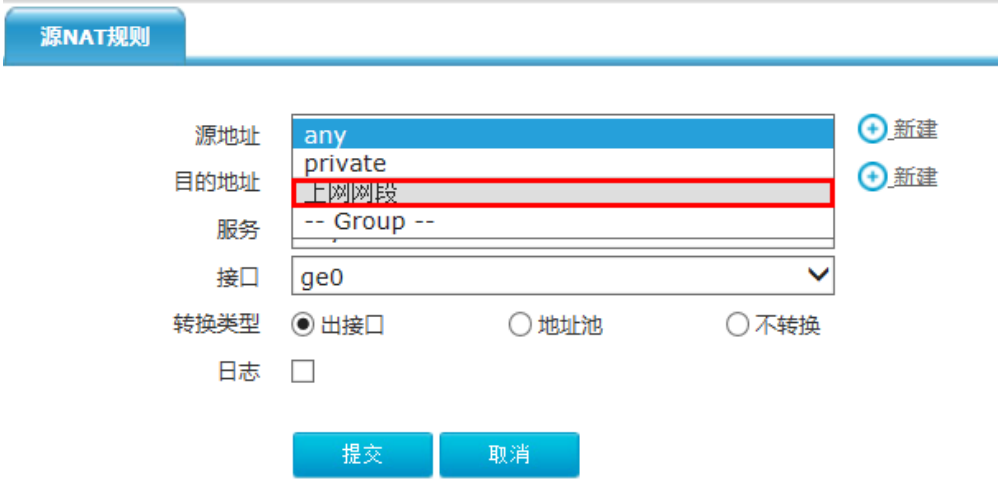
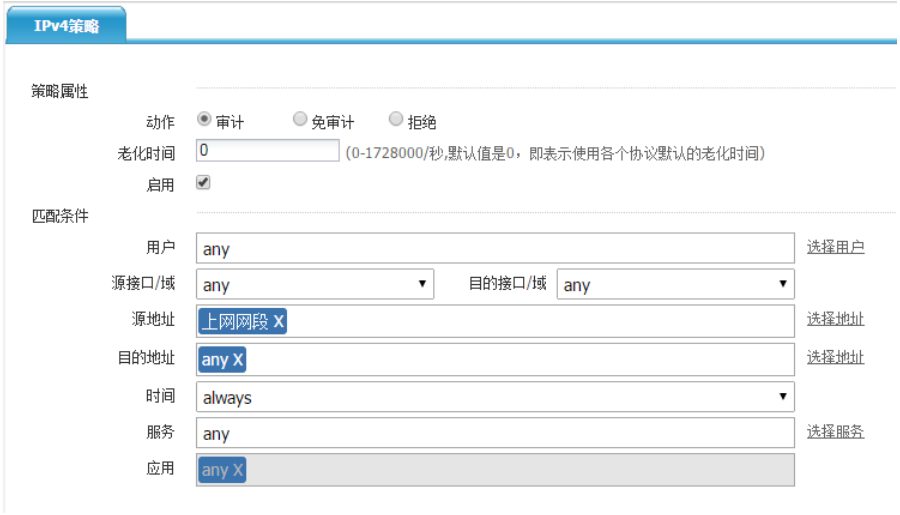


图2-36 ge1

(6) 配置安全策略，进入“上网行为管理>策略配置>IPV4 策略”，点击页面左上角的<新建>按钮。

图2-37 新建安全策略

图2-38 配置安全策略



(7) 保存配置。

(8) 配置客户端 IP、网关以及 DNS。

将部门某电脑 IP 地址设置为 192.168.2.10/24,网关设置地为 192.168.2.1，DNS 配置为 8.8.8.8（一般设置为当地的 DNS 即可）。电脑可正常上网。

2.5.5 注意事项

- IPV4 地址对象要与上网用户匹配。
- 源 NAT 要选择以配置的 IPV4 地址对象。
- 默认路由网关分别为 ISP 提供的 IP 地址。

安全策略按从上向下匹配的原则。状态为“ ”的上网策略才会生效。

3 版本升级

3.1 版本升级的内容

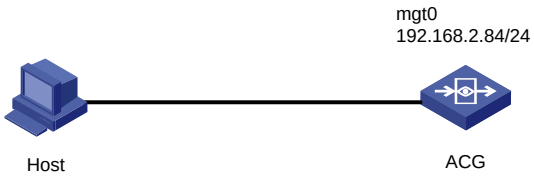
版本的升级包括软件、特征库文件升级。目的在于解决软件缺陷，更新最新的应用与 URL 特征。ACG 系统的软件需要解决软件缺陷或获取新软件特性，可通过 WEB 界面、命令行升级，当系统运行的主程序由于各种原因丢失或 WEB 界面和命令行均无法进入时，可进入底层 menuboot 程序进行主软件程序升级。

3.2 主控程序升级过程

3.2.1 WEB 界面下升级

1. 组网图

图3-1 WEB 界面下升级组网图



2. 配置步骤

(1) 从官方网站获取新软件版本文件，版本文件必须是以.bin 为后缀。

(2) 进入 WEB 管理界面，进入系统管理>系统设定>系统升级>手动升级，点击系统软件后的<浏览>按钮选择本地存储的升级文件，点击上传。

(3) 点击上传后会显示文件上传进度条，WEB 界面显示如下提示则表示文件上传成功，可进行下一步操作。

(4) 点击 WEB 界面右上角<保存>按钮保存当前配置。

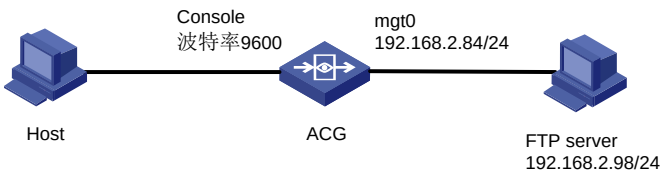
(5) 进入系统管理>系统设定>系统重启，选择系统重启提交后可重启设备。

(6) 点击提交后设备将进行重启，所有业务流量停止转发，同时页面停止响应，重启系统后再次 WEB 登录设备首页，检查首页版本信息升级成功。

3.2.2 命令行下升级

1. 组网图

图3-2 命令行下升级组网图



2. 配置步骤

(1) 从官方网站获取新软件版本文件，版本文件必须是以.bin 为后缀。

(2) 安装 3CDeamon，设置 tftp 和 ftp 服务器路径，为版本文件存放的位置。服务器设置为匿名登录。

(3) ping 服务器是否可达，排查基础连通性。在命令行 enable 节点下执行 ftp 升级命令：**copyftp** 192.168.2.98*xx.bin***version**，版本上传完成自行解压安装。提示两个 success 则表示版本校验成功且升级成功。

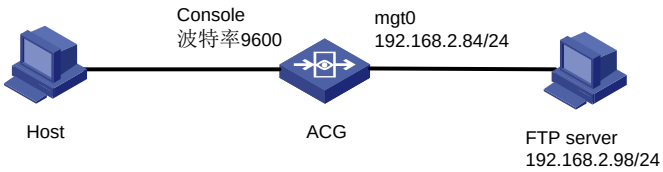
(4) 保存配置并重启系统，在命令行 enable 节点下执行保存配置命令：**save config**。

(5) 执行 reboot 重启设备，系统重启后在命令行界面，enable 节点下执行 **display version** 命令查看版本信息，升级成功。

3.2.3 Menuboot 下升级

1. 组网图

图3-3 Menuboot 下升级组网图



2. 配置步骤

(1) 重启设备，重启过程看到提示按 ctrl+b 则进入 uboot 界面。

(2) Uboot 界面下执行 **run menuboot_cf** 命令启动 **menuboot** 程序。

(3) 进入 **menuboot** 程序主界面，在选择项输入 0 可配置基本参数，参数说明如下(如果需要修改默认值需在冒号后输入，如不修改则回车进入下一项)：

- Startup image：即将上传的软件版本文件名称
- Startup menuboot：menuboot：程序文件名称，无需修改
- Startup bootrom[50MC1100.bin]：uboot 版本文件名称，无需修改
- Startup local：设备默认管理接口的 IP 地址，须设置且与服务器同一网段
- Startup mask：地址掩码，视实际情况进行设置
- Startup interface：上传版本文件使用的接口，一般为 ge0 或 mgt0
- Startup server：tftp/ftp 服务器的 IP 地址

(4) 在 menuboot 主界面选项输入 1 选择 ftp 方式进行文件上传，版本上传完成后会自动进行解压安装，两个 success 则表示版本校验成功且升级成功。

(5) 在 menuboot 程序主界面输入 r 选项，回车后可重启设备进入新系统。重启系统后命令行登录配置界面，enable 节点下执行 display version 命令，显示新版本信息，升级成功。

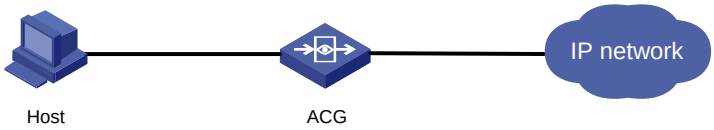
3.3 特征库升级

ACG 系统在线运行时需要周期性的更新特征库，才能更好进行应用识别控制和流量控制。在设备无法正常与互联网进行通信的情况下，可通过 WEB 页面进行特征库手动升级。若设备可正常与互联网进行通信，则可通过设置定期自动从服务器更新最新的特征库 (特征库升级的前提是已经购买并导入授权升级许可，如未购买则无法进行升级，授权许可证查看可参考相关章节)。

3.3.1 手动升级

1. 组网图

图3-4 手动升级组网图



2. 配置步骤

(1) 通过在线客户或售后热线电话获取特征库离线文件。

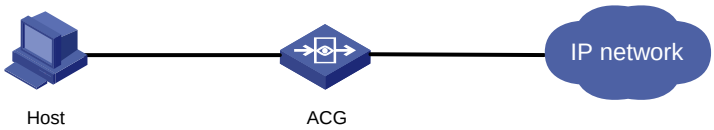
(2) 使用 WEB 管理界面，进入系统管理>系统设定>系统升级>手动升级，点击应用控制特征库后的<浏览>按钮选择本地存储的升级文件，点击**上传**。显示文件上传进度条，WEB 界面提示上传成功，可进行下一步操作。

(3) 进入监控>系统状态，首页上查看系统信息，检查首页版本信息，升级成功。升级特征库文件无需重启设备系统即可生效。

3.3.2 自动升级

1. 组网图

图3-5 自动升级组网图



2. 配置步骤

(1) 按拓扑设置默认路由使设备可访问互联网，进入系统管理>系统设定>DNS，设置主备 DNS。

(2) 点击提交设置完成，可在 WEB 界面进入系统管理>系统诊断工具，通过 ping 百度测试 DNS 解析是否正常。

(3) 登录 WEB 管理界面，进入系统管理>系统设定>系统升级>自动升级，选择默认升级服务器，设定周期。设备会在设定的周期内自动从服务器更新最新特征库版本。

(4) 首次安装设备上线，可通过立即在线升级方式更新特征库至最新，进入系统管理>系统设定>系统升级>自动升级，点击<立刻升级>按钮。

(5) 进入监控>系统状态，查看首页系统信息，升级成功。

3.4 注意事项

- 主程序升级需要重启设备，会造成断网，请避开业务高峰期升级。
- 主程序升级有一定风险，请务必保证升级过程中，设备供电稳定。

- 主程序升级前，请认真阅读相关文档。
- 升级不会导致配置、日志文件、库文件、license 丢失。
- 设备要连接互联网时才能升级库文件。
- 配置 DNS 才能检测库文件，自动更新。也可以手动方式检测最新库文件。
- 特征库在线升级过程中，设备需要从外网下载升级包，会占用一定网络带宽，且会影响设备的数据转发，所以建议将自动升级周期设置在业务低峰期。

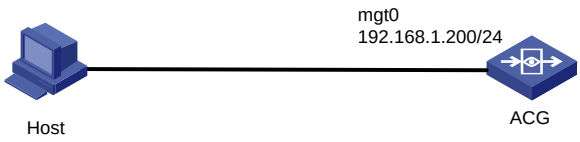
4 远程管理

设备管理主要有 Web 管理和命令行管理两种方式。管理员可通过 Web 可视化图形界面对 ACG 进行配置和管理维护。也可以通过命令行对 ACG 进行配置和管理维护。命令行下有 Console、telnet、SSH 三种方式，其中 Console 需要使用串口线连接设备， telnet、SSH 通过网络连接设备，telnet 方式相对较普遍，SSH 采用加密方式传输相对 telnet 较为安全，管理员可按需进行选择。

4.1 Web管理

4.1.1 组网图

图4-1 Web 管理组网图



4.1.2 配置步骤

(1) 配置管理员 IP 地址，打开网络连接，设置本地连接的 IP 地址为 192.168.1.2。

(2) 打开浏览器输入 https://192.168.1.1（默认），用户名 admin 默认密码 admin，忽略安全证书信息，即可登录设备管理界面的首页。

(3) 配置接口访问权限，进入网络管理>接口设置>物理接口，点击<编辑>按钮修改接口配置。配置接口 ge1-0 的主 IP 地址为 192.168.2.84/24，勾选管理方式可开启相关访问方式的权限：

- https：允许 https://192.168.2.84 访问管理
- http：允许 http://192.168.2.84 访问管理
- ssh：允许使用 ssh 方式管理
- telnet：允许使用 telnet 192.168.2.84 访问管理
- ping：允许 ping 此接口地址，如果不勾选，路由可达情况下 Ping 不通

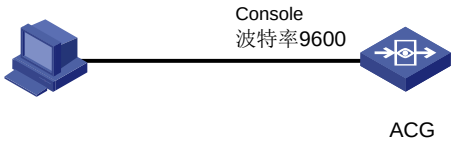
(4) 打开浏览器，在地址框输入 https://192.168.2.84，登录管理。

4.2 命令行下管理

4.2.1 Console 管理

1. 组网图

图4-2 Console 管理组网图



2. 配置步骤

(1) 准备 console 配置线，线两端为 com 口和 console 口，分别连接设备的 console 口和 PC 的 com 口。

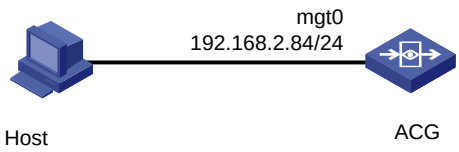
(2) 设置超级终端或 SecureCRT，以 SecureCRT 为例。点击<快速连接>按钮，弹出对话框，选择协议为“serial”，端口选择 PC 相应的 com 口。波特率选择 9600，其他选项默认。

(3) 连接完成后，按回车键会打印信息，验证连接效果，完成

4.2.2 telnet 管理

1. 组网图

图4-3 telnet 管理组网图



2. 配置步骤

(1) 开启管理接口的 telnet 管理权限，进入网络管理>接口设置>物理接口，编辑管理接口，管理方式中勾选 telnet 和 ping，点击提交。

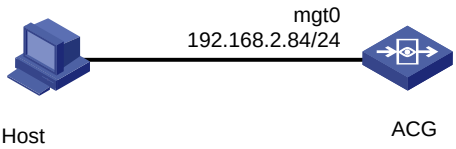
(2) 开启管理员 PC 的 telnet 功能， win7 操作系统 telnet 功能默认关闭，在 dos 框中使用 telnet 命令时会报错。进入开始菜单>控制面板，单击进入程序，选择打开或关闭 Windows 功能。在 window 功能对话框中选中 telnet 客户端，点击确定，等待操作完成。

(3) 使用 telnet 管理设备，点击开始>运行，输入 **cmd** 后回车，尝试 **ping** 检查连通性，在 DOS 窗口输入：telnet 192.168.2.84。回车后可输入管理员用户密码。

4.2.3 ssh 管理

1. 组网图

图4-4 ssh 管理组网图



2. 配置步骤

(1) 开启管理接口的 ssh 管理权限，管理方式中勾选 ssh 和 ping，点击提交。

(2) 使用 ssh 客户端软件，以 Secure CRT 为例，新建 ssh 连接，协议选择 ssh2，用户名 admin，其他默认，输入正确密码后登录设备命令行配置界面。（可先尝试 ping 一下管理 ip 进行连通性测试）

4.2.4 常用命令

表4-1 常用命令

命令	使用说明
enable	进入用户视图
configure terminal	进入系统视图
displayrunning-config	查看所有配置(空格键翻页)
save config	保存当前配置
erasestartup-config	恢复出厂配置，需重启设备才能生效
reboot	重启系统，重启前会提示是否保存当前配置
display version	查看版本信息、系统运行时间、设备序列号/型号、功能授权状态等信息
display date	查看系统当前时间(local time)
display interface	查看接口相关信息，包括IP地址、链路状态、MAC地址和工作模式
display cpu usage	查看设备cpu使用率(当前值、1分钟/5分钟/15分钟平均值
display memory	查看设备内存使用率(控制面、数据面)：

5 应用审计

5.1 应用审计简介

ACG1000 拥有应用审计功能，对特定应用支持审计和阻断，对内网用户访问外网进行审计控制，当前支持的应用主要有如下几种：

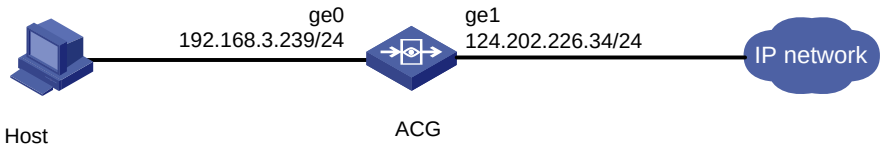
- 应用类：主要包括 IM 类、社区类、搜索引擎类、邮件类及流媒体类等。

同时支持移动终端，主要有如下几种：

- 支持移动客户端：IOS 系统和 Android。

5.2 组网图

图5-1 应用审计组网图



5.3 应用审计

5.3.1 用户需求

对内网用户访问外网进行审计。

5.3.2 配置思路

(1) 配置设备的接口、NAT、路由，使内网用户能够访问外网。

(2) 配置审计策略。

(3) 使用 PC 登录 QQ，查看审计日志。

5.3.3 配置步骤

(1) 进入“网络管理>接口>物理接口”，点击操作。

图5-2 配置物理接口 ge0

图5-3 配置物理接口 ge1

(2) 配置 NAT

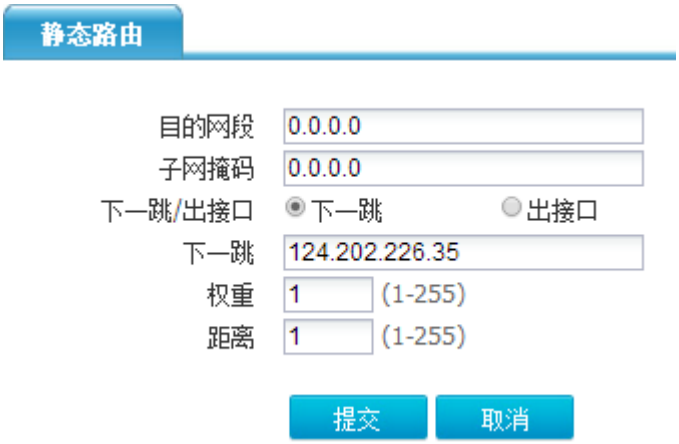
进入“网络配置>NAT>源 NAT”，点击<新建>。

图5-4 配置 NAT 规则

(3) 配置静态路由

进入“网络配置>路由>静态路由”，点击<新建>。

图5-5 配置静态路由



(4) 配置审计策略

进入“上网行为管理>策略配置>IPv4 策略”，点击<新建>。

图5-6 配置 IPv4 策略

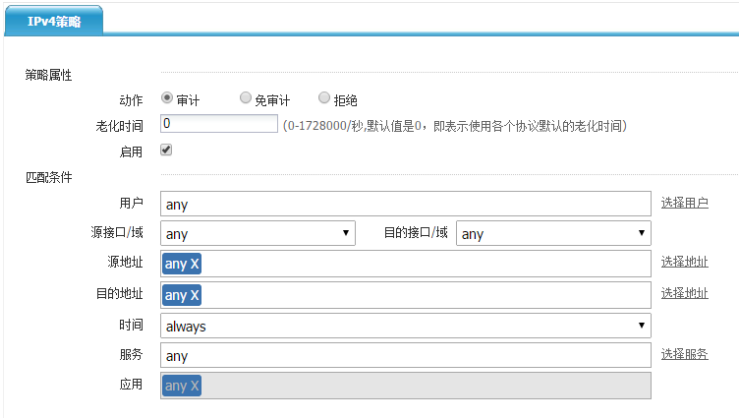
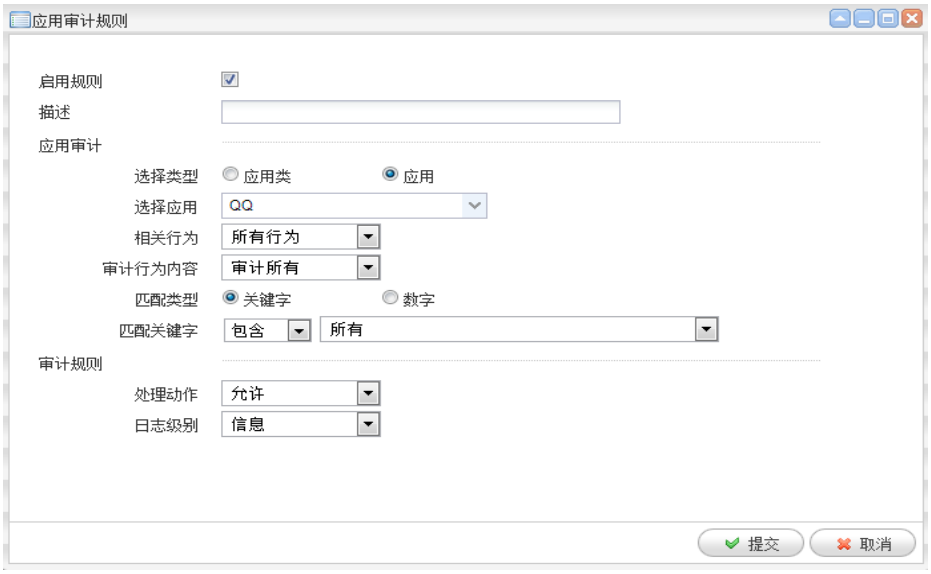


图5-7 配置应用审计策略



(5) 设备下挂的 PC 登录 QQ

进入“日志查询>应用审计日志>IM 聊天软件日志”

图5-8 查看聊天软件日志

5.4 应用控制

5.4.1 用户需求

对内网用户访问外网进行控制。

5.4.2 配置思路

(1) 配置设备的接口、NAT、路由，使内网用户能够访问外网。

(2) 配置审计策略。

(3) 使用 PC 访问百度，查看阻断日志。

5.4.3 配置步骤

(1) 进入“网络管理>接口>物理接口”，点击操作。

图5-9 配置接口 ge0

图5-10 配置接口 ge1

(2) 配置 NAT

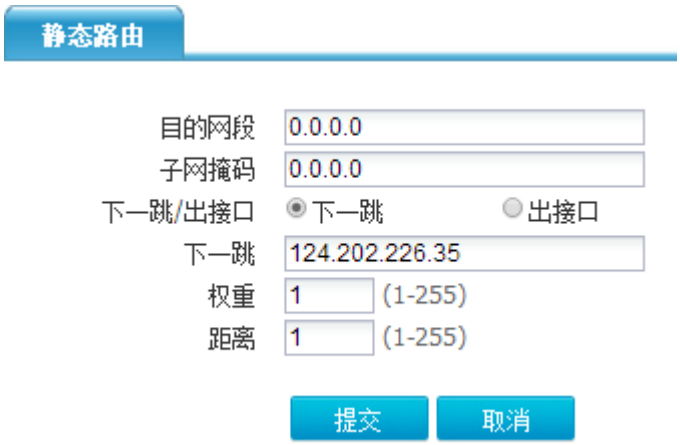
进入“网络配置>NAT>源 NAT”，点击<新建>。

图5-11 配置 nat

(3) 配置静态路由

进入“网络配置>路由>静态路由”，点击<新建>。

图5-12 配置静态路由



(4) 配置审计策略

进入“上网行为管理>策略配置>IPv4 策略”，点击<新建>。

图5-13 配置 IPv4 策略

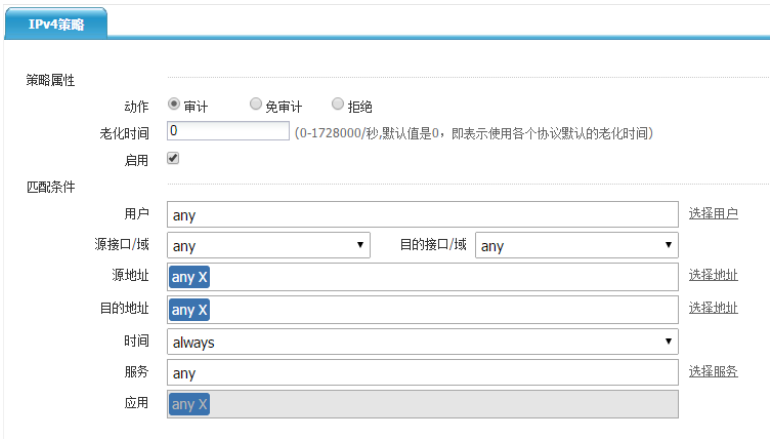
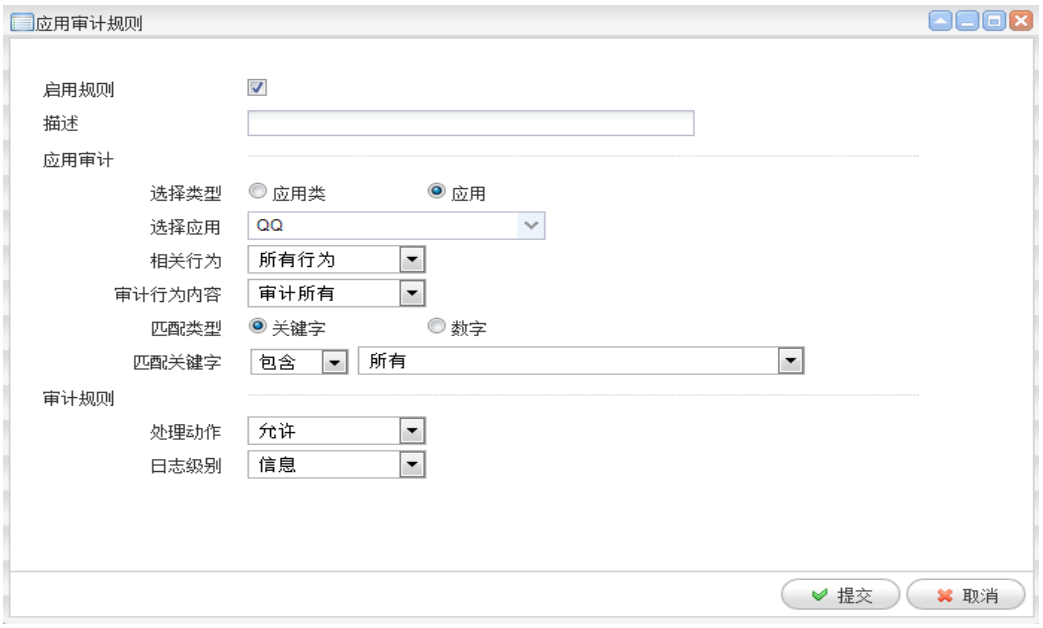
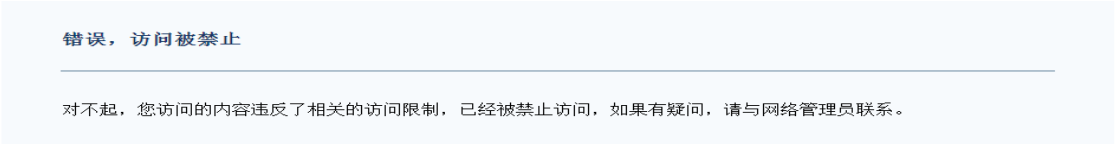


图5-14 配置应用审计规则



(5) 设备下挂的 PC 访问百度

图5-15 禁止访问页面



(6) 进入“日志查询>应用审计日志>搜索引擎日志”

图5-16 搜索引擎日志

5.5 恶意URL白名单

5.5.1 用户需求

公司内网用户通过 ACG 上网，某些情况下由于发布新特征库误判导致某些网站不能访问，于是需要手动添加 url 白名单，使内网用户能够正常访问网络。

5.5.2 配置思路

(1) 将 ACG 接口配置相应 IP 地址

(2) 在 ACG 上建立 IPV4 地址对象并配置源 NAT 转换

(3) 在 ACG 上配置静态路由

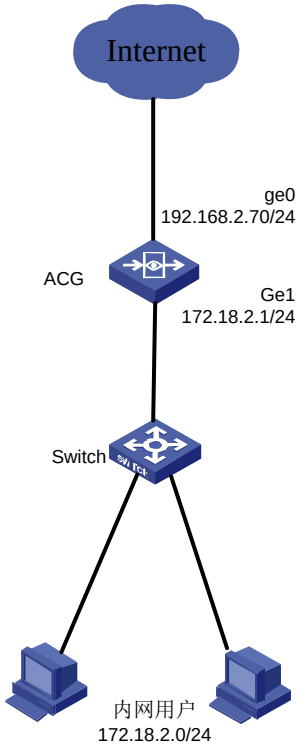
(4) 在 ACG 上配置安全策略开启 URL 过滤功能

(5) 配置 PC 地址

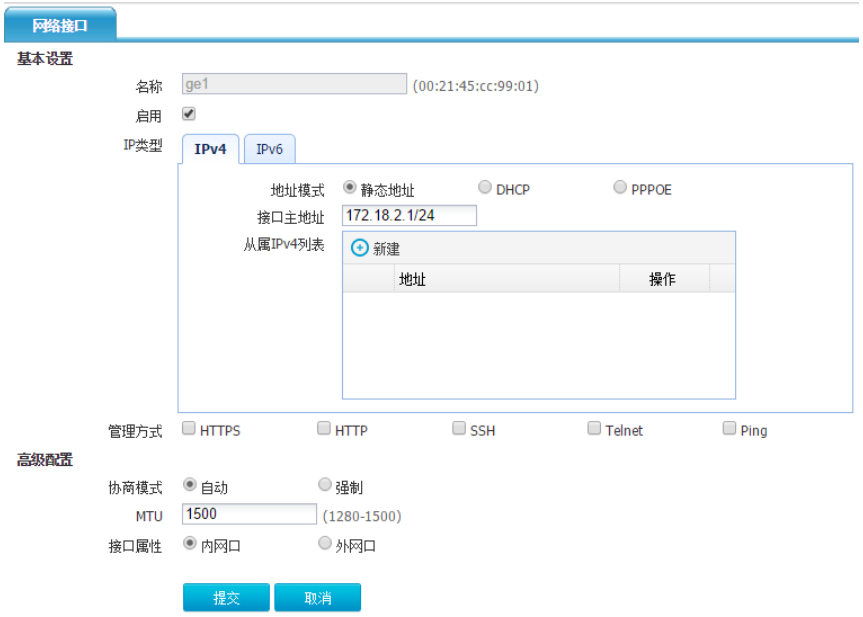
(6) 测试结果。PC 访问网站被阻断后，配置恶意 URL 白名单后，重新访问

5.5.3 配置步骤

图5-17 恶意 URL 白名单组网示意图



(1) 登录 web 界面，进入网络配置>接口>物理接口，编辑 Ge0、Ge1 接口地址。



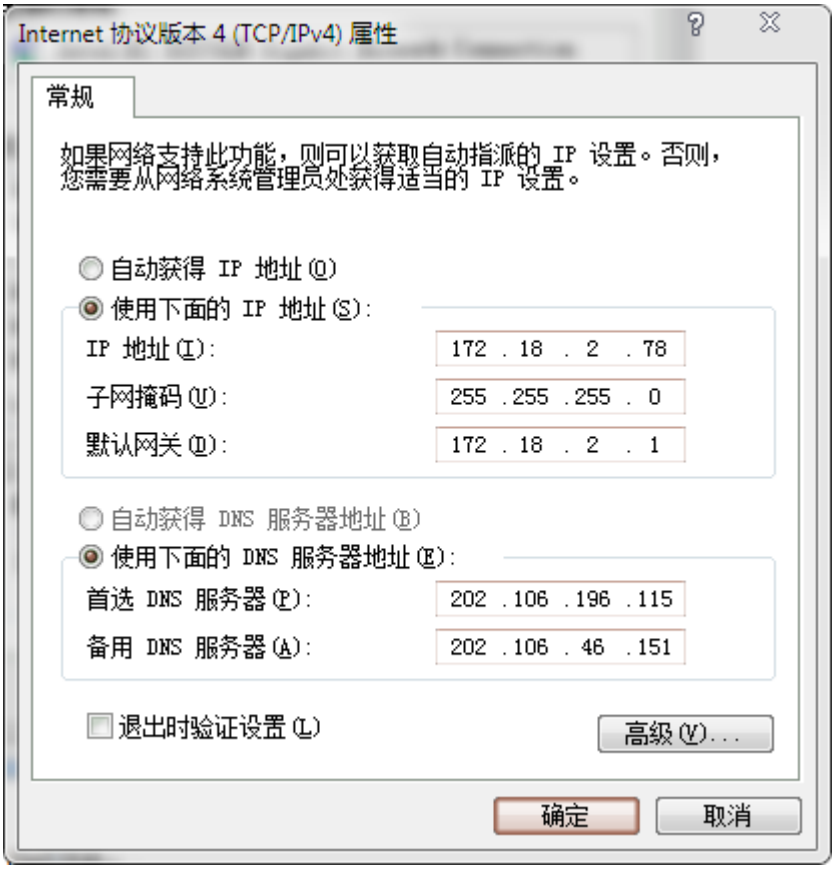
(2) 配置地址对象并配置源 NAT 转换。ACG 上建立 IPV4 地址对象，将内网网段添加到 IPV4 地址对象中进入对象管理>地址>IPv4 地址对象，点击页面左上角的<新建>按钮，配置 IPv4 地址对象。名称为内网用户，地址节点选择子网地址：172.18.2.0/24,点击新建，点击提交。

(3) 配置源 NAT 在源地址处选择上网网段，转换类型为出接口接口选择 ge0，配置完成后点击提交。进入“网络配置>NAT>源 NAT”，点击新建。

(4) 在 ACG 上配置静态路由进入“网络配置>路由>静态路由”，点击新建

(5) 在 ACG 上配置安全策略开启 URL 过滤功能进入“上网行为管理>策略配置>IPV4 策略”，点击新建策略，开启 URL 过滤功能。

(6) 配置客户端 IP



(7) 进入“对象管理>URL>恶意 URL 白名单”，点击新建。

图5-18 配置恶意 URL 白名单

配置完恶意 URL 后客户端重新访问该网站可顺利访问

5.5.4 注意事项

恶意 url 白名单是精确匹配。例：被阻断的网站为 qq.com，新建恶意 URL 白名单 www.qq.com 后还是不能访问，只能是 qq.com，才能访问。

6 策略路由

6.1 策略路由特性

策略路由，也叫做基于策略的路由，是指在决定一个 IP 包的下一跳转发地址时，不是简单的根据目的或源 IP 地址来决定，而是综合考虑多种因素决定。它转发分组到特定网络需要基于预先配置的策略，这个策略可能指定从一个特定的网络发送的通信应该被转发到一个指定的接口。

6.2 策略路由

6.2.1 配置需求

- ACG 设备两个出口，一条为静态地址线路，另一条为 ADSL 线路
- 部门一电脑通过静态地址上网，
- 部门一电脑通过 ADLS 线路上网

6.2.2 配置思路

(1) 配置接口地址

(2) 配置地址对象

(3) 配置策略路由

(4) 配置源 NAT

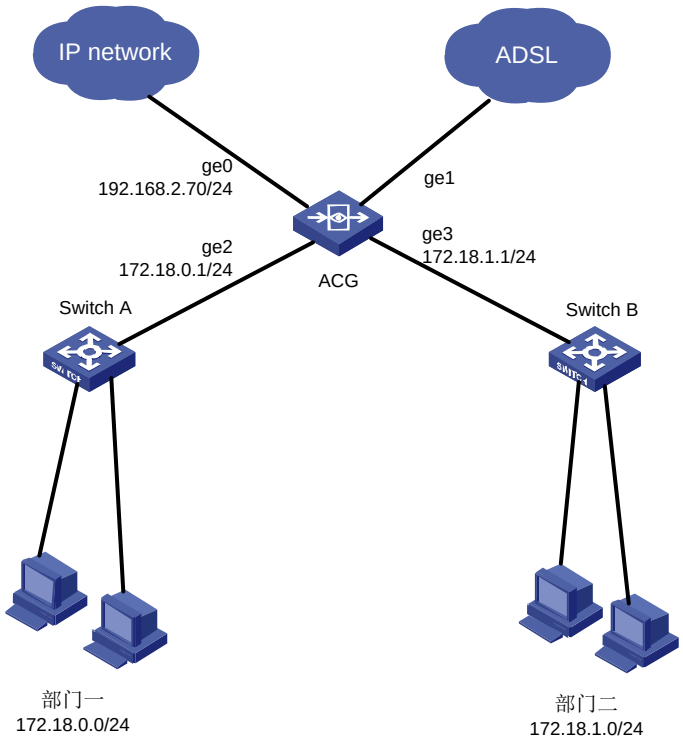
(5) 配置上网行为管理策略

(6) 保存配置

(7) 配置客户端 IP 等信息

6.2.3 配置步骤

图6-1 策略路由组网示意图：



(2) 在 ACG A 进入“网络配置>接口>网络接口”，点击<新建>按钮，配置 ge0 地址为 192.168.2.70/24，ge2 接口为 172.16.0.1/24，ge3 接口为 172.16.1.1/24。

图6-2 配置接口 ge0

(3) ge1 接口地址模式选择 PPPoE，配置正确的用户名、密码，务必勾选“更新网关”，这样 ADSL 拨号成功后设备会自动生成默认路由，无需手动配置默认路由。

图6-3 配置接口 ge1

图6-4 配置接口 ge2

图6-5 配置接口 ge3

(4) 在 ACG 上进入“地址对象>地址>IPV4 地址对象”，点击<新建>。配置地址对象

- 名称为“部门一”，地址节点选择“子网地址”：“172.18.0.0/24”，点击“添加到列表”，点击提交。
- 名称为“部门二”，地址节点选择“子网地址”：“172.18.1.0/24”,点击“添加到列表”点击提交。

图6-6 配置地址对象

图6-7 配置地址对象

(5) 配置策略路由

配置部门一通过静态地址上网，部门二通过 ADSL 上网。

进入“网络配置>路由>策略路由”，点击<新建>

配置部门一固定通过静态地址线路上网，选择静态下一跳，并点击添加到列表：

图6-8 配置策略路由


策略路由
入接口
ge2
源地址
部门一
新建
目的地址
any
新建
用户
any
服务
any
应用
any
时间
always
下一跳信息
网关
192.168.2.1
权重
1
添加到列表
类型
网关
出接口
权重
操作
1
网关
192.168.2.1
-
1
删除
提交
取消

图6-9 配置策略路由

(6) 配置源 NAT

在 ACG 进入“网络配置>NAT>源 NAT”，点击<新建>

分别配置两条源 NAT 转换，转换类型为“出接口”,接口选择连接外网的接口，配置完成后点击提交。

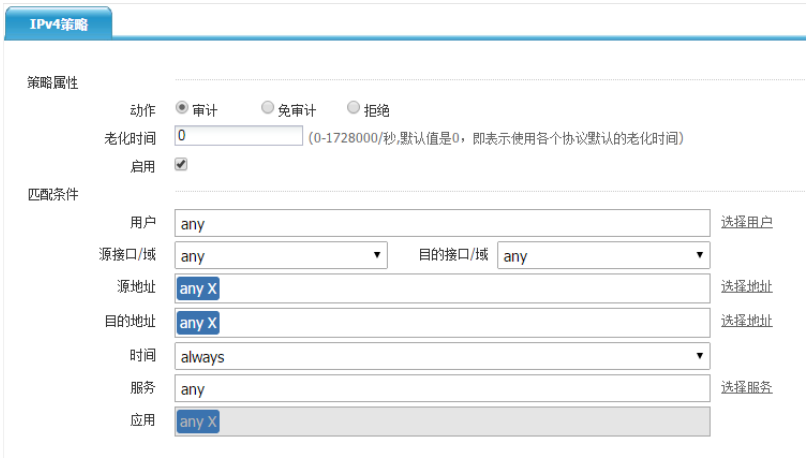
图6-10 配置 SNAT

图6-11 配置 SNAT

(7) 配置上网行为管理

在 ACG 进入“上网行为管理>策略配置>IPV4 策略”，点击<新建>，配置一条全通策略

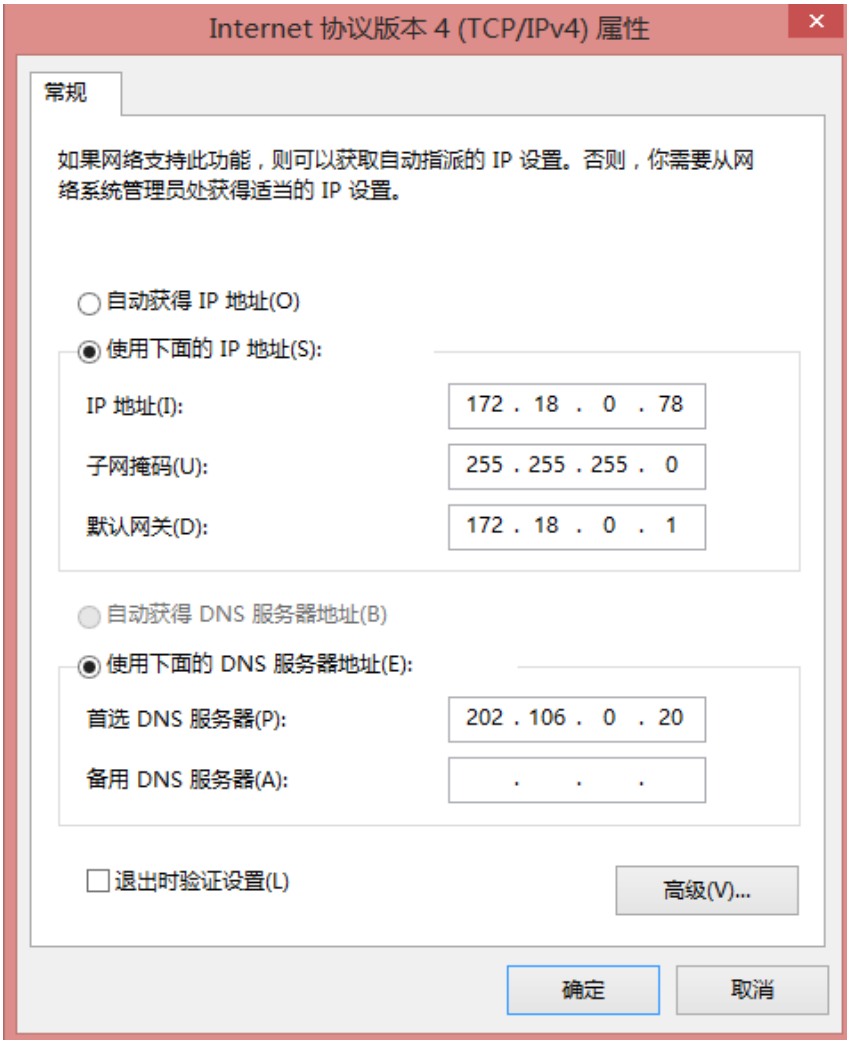
图6-12 配置安全策略



(8) 配置客户端 IP 等配置，使其能够访问外网。

将部门一电脑 IP 地址设置为 172.18.0.78/24,网关设置地为 172.18.0.1/24，DNS 配置为 202.106.0.20（一般设置为当地的 DNS 即可）。电脑可正常上网。

图6-13 配置客户端



6.2.4 注意事项

- 分清入口和报文源地址对象，精确匹配策略路由引用的地址对象，尽量不要使用 any
- 分清入口和报文源地址对象，并配置正确下一跳地址

7 流控

7.1 流控简介

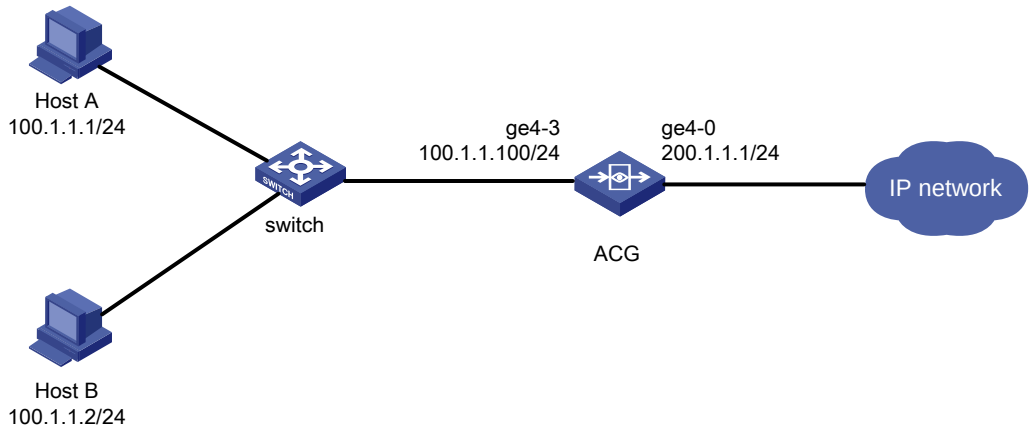
流量管理是通过流量分析，对各种上网流量大小进行精细控制的一种方法。传统的流量管理功能仅仅是对带宽进行限制，无法根据应用、服务、用户进行带宽限制，ACG 的流量管理具有如下特点：

- 使用虚拟线路和管道，实现层次化的流量管理
- 支持优先级，确保高优先级的应用能够获得带宽

- 支持保障带宽和最大带宽
- 支持弹性带宽或带宽借用，充分利用网络资源
- 能够根据应用、服务、用户、IP 地址组进行流量控制
- 能够分别对 Ingress/Egress 流量进行控制
- 能够保障用户公平使用带宽
- 能够自动分辨低时延的特殊应用，避免上行拖垮下载的特殊情况

7.2 组网图

图7-1 流控组网图



7.3 应用带宽限制

7.3.1 用户需求

接口转发的流量不能超过其绑定的线路策略所设定的最大带宽。匹配优酷等流媒体的应用上下行流量不能超过其带宽限制。

7.3.2 配置思路

(1) 绑定出接口，限制上下行最大带宽。

(2) 子通道对优酷等流媒体进行最大带宽限制。

(3) 配置每 ip 限速对内网多台 Host 进行带宽分配。

7.3.3 配置步骤

(1) 进入“上网行为管理>流量管理>流量策略”，点击<新建>限制接口上下行带宽分别为 1M。

图7-2 配置线路策略

(2) 新建流量策略 youku 匹配应用”优酷”，最大带宽为 300K，保障带宽为 200K。

图7-3 配置流量控制

(3) 配置每 ip 限速对内网多台 Host 进行带宽分配限制，并点击提交。

图7-4 配置流量控制

7.4 应用带宽保障

7.4.1 用户需求

接口转发的流量不能超过其绑定的线路策略最大带宽。匹配优酷的应用上下行流量不能超过其带宽限制，在带宽拥塞的情况下可以达到其保障带宽。

7.4.2 配置思路

(1) 绑定出接口，限制上下行最大带宽。

(2) 子通道对优酷等流媒体进行保障带宽限制。

(3) 配置每 ip 限速对内网多台 PC 进行带宽分配。

7.4.3 配置步骤

(1) 进入“上网行为管理>流量管理>流量策略”，点击<新建>限制接口上下行带宽分别为 100M：

图7-5 配置线路策略

(2) 新建流量策略 ge4-3 匹配应用”优酷”，最大带宽为 5M，保障带宽为 3M。

图7-6 配置流量控制

(3) 配置每 ip 限速对内网多台 Host 进行带宽分配限制，并点击提交。

图7-7 配置流量控制

8 日志

8.1 日志简介

ACG1000 拥有日志管理功能，可以记录并输出各种日志信息，当前支持的日志主要有如下几种：

- 应用审计日志：主要包括 IM 聊天软件日志、社区日志、搜索引擎日志、邮件日志、命令日志及其他应用日志。
- 网站访问日志：主要包括访问网站日志及恶意 URL 日志。
- 安全防护日志：主要是网络层攻击日志，包括异常包攻击日志、Flood 攻击日志等。
- 系统日志：包括系统日志与操作日志。

8.2 支持本地日志、第三方日志

H3C 系列支持本地日志及第三方日志两种日志记录方式。

- 本地日志：可以通过配置日志模块中的日志过滤部分，将产生的日志记录在本地数据库中，如**错误!未找到引用源。**及**错误!未找到引用源。**所示。

- 第三方日志：可以通过配置日志模块中的日志服务器及日志过滤部分，将日志发送到远程日志服务器，在日志服务器上查看日志信息，如**错误!未找到引用源。**、**错误!未找到引用源。**及**错误!未找到引用源。**所示。

图8-1 日志过滤统一配置

点击**错误!未找到引用源。**的<高级配置>按钮，出现审计等日志的过滤配置，如**错误!未找到引用源。**所示。

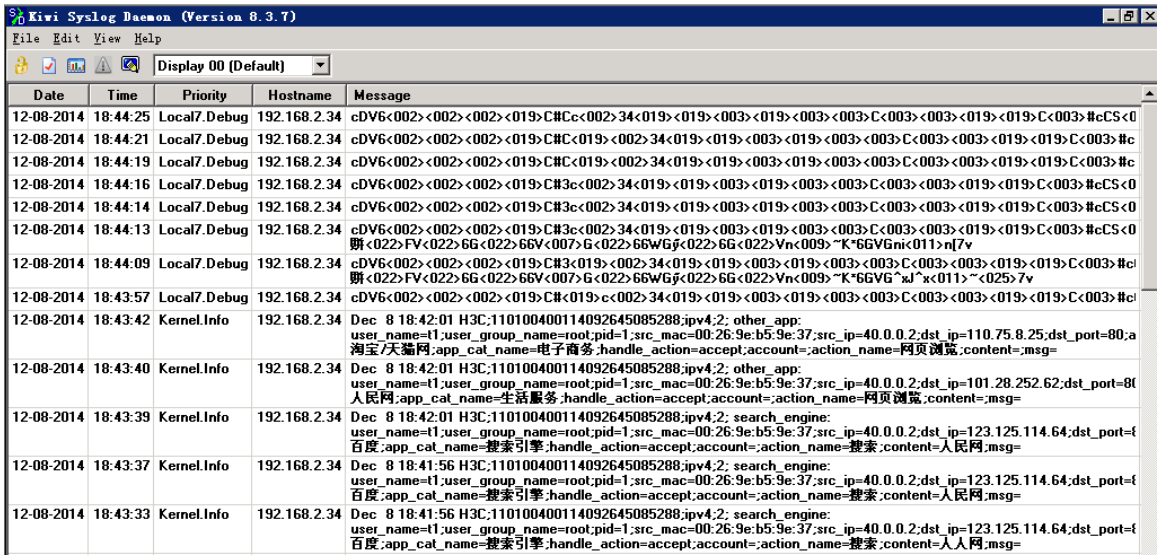
图8-2 日志过滤高级配置

图8-3 日志服务器配置

说明

日志加密：如**错误!未找到引用源。**所示，在日志服务器页面，勾选服务器 IP 地址后面的加密复选框，可对发送到远程服务器的日志加密，如下图所示：

图8-4 Syslog Server



上图中下半部分为未加密情况下在远程日志服务器上得到的日志情况，上半部分为加密后在远程服务器上得到的日志。

8.3 应用审计日志

8.3.1 IM 聊天软件日志

1. 日志查看

打开 web 页面，点击“日志查询>应用审计日志>IM 聊天软件日志”，可以查看 IM 聊天软件日志，如**错误!未找到引用源。**所示。

2. 日志查询

在 IM 聊天软件日志页面，点击<查询>按钮，弹出日志过滤条件对话框，根据对话框的选项，可以根据日期、时间段、用户、源地址、目的地址、应用分类、应用、行为、账号、内容、处理动作、日志级别查询所需要的日志信息，如**错误!未找到引用源。**所示。

图8-5 IM 聊天软件日志查看

	用户	应用	账号	行为	处理动作	系统	终端	级别	时间	操作
1	t1	QQ	480828690	收消息	放行	windows	-	信息	2014-12-08 14:36:06	详细
2	t1	QQ	480828690	收消息	放行	windows	-	信息	2014-12-08 14:30:37	详细
3	t1	QQ	480828690	收消息	放行	-	-	信息	2014-12-08 14:25:06	详细
4	t1	QQ	480828690	登录	放行	-	-	信息	2014-12-08 14:25:05	详细
5	192.168.2.2	QQ	18397281	收消息	放行	windows	-	信息	2014-12-08 14:14:20	详细
6	192.168.2.2	QQ	18397281	发消息	放行	windows	-	信息	2014-12-08 14:10:23	详细
7	192.168.2.2	QQ	18397281	收消息	放行	windows	-	信息	2014-12-08 14:09:18	详细
8	192.168.2.2	QQ	18397281	收消息	放行	windows	-	信息	2014-12-08 14:04:17	详细
9	192.168.2.2	QQ	18397281	发消息	放行	windows	-	信息	2014-12-08 14:01:59	详细
10	192.168.2.2	QQ	18397281	收消息	放行	windows	-	信息	2014-12-08 13:59:14	详细
11	192.168.2.2	QQ	18397281	收消息	放行	windows	-	信息	2014-12-08 13:53:35	详细
12	192.168.2.2	QQ	18397281	收消息	放行	windows	-	信息	2014-12-08 13:48:25	详细
13	192.168.2.2	QQ	18397281	收消息	放行	windows	-	信息	2014-12-08 13:43:21	详细
14	192.168.2.2	QQ	18397281	收消息	放行	windows	-	信息	2014-12-08 13:38:15	详细
15	192.168.2.2	QQ	18397281	收消息	放行	windows	-	信息	2014-12-08 13:37:29	详细
16	192.168.2.2	QQ	18397281	收消息	放行	windows	-	信息	2014-12-08 13:37:15	详细
17	192.168.2.2	QQ	18397281	收消息	放行	windows	-	信息	2014-12-08 13:36:15	详细
18	192.168.2.2	QQ	18397281	收消息	放行	windows	-	信息	2014-12-08 13:35:17	详细
19	192.168.2.2	QQ	18397281	收消息	放行	windows	-	信息	2014-12-08 13:35:16	详细
20	192.168.2.2	QQ	18397281	收消息	放行	windows	-	信息	2014-12-08 13:35:15	详细

图8-6 日志过滤条件

例如，查询日期为 2015 年 02 月 28 日，应用为“QQ”，行为为“发消息”且账号为“18397281”的日志，过滤条件如**错误!未找到引用源。**所示，查询结果如**错误!未找到引用源。**所示。

图8-7 IM 聊天软件日志过滤条件示例

图8-8 IM 聊天软件日志查询结果

8.3.2 社区日志

1. 日志查看

打开 web 页面，点击“日志查询>应用审计日志>社区日志”，可以查看社区日志，如**错误!未找到引用源。**所示。

图8-9 社区日志查看

2. 日志查询

在社区日志页面，点击<查询>按钮，弹出日志过滤条件对话框，根据对话框的选项，可以根据日期、时间段、用户、源地址、目的地址、应用分类、应用、行为、账号、内容、处理动作、日志级别查询所需要的日志信息。

例如，查询日期为2015年02月28日，应用为“QQ空间”，行为为“发表”的日志，账号为“18397281”过滤条件如**错误!未找到引用源。**所示，查询结果如**错误!未找到引用源。**所示。

图8-10 社区日志过滤条件

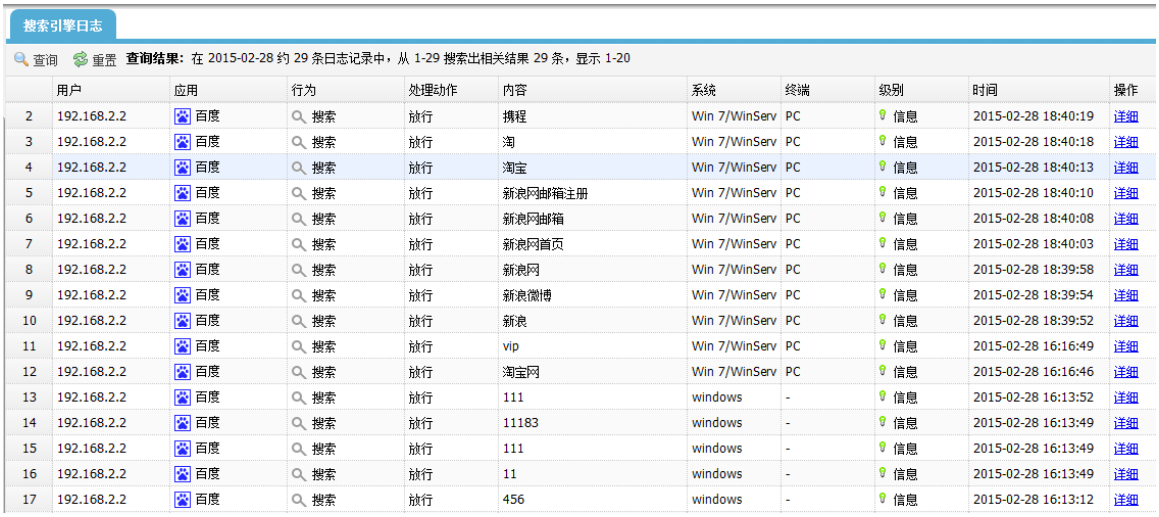
图8-11 社区日志查询结果

8.3.3 搜索引擎日志

1. 日志查看

打开 web 页面，点击“日志查询>应用审计日志>搜索引擎日志”，可以查看搜索引擎日志，如**错误!未找到引用源。**所示。

图8-12 搜素引擎日志查看



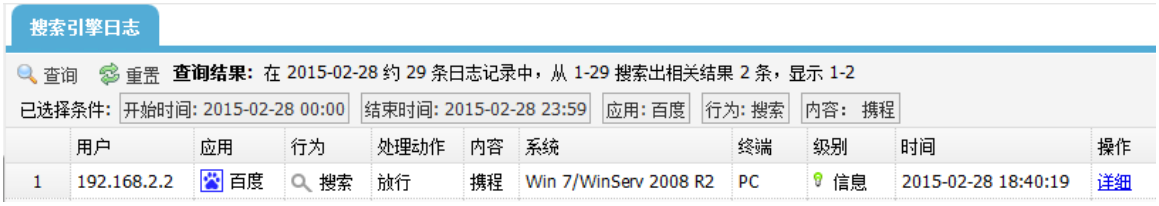
2. 日志查询

在搜索引擎日志页面，点击<查询>按钮，弹出日志过滤条件对话框，根据对话框的选项，可以根据日期、时间段、用户、源地址、目的地址、应用分类、应用、行为、内容、处理动作、日志级别查询所需要的日志信息。

例如，查询日期为 2015 年 02 月 28 日，应用为“百度”，行为为“搜索”，且内容为“携程”的日志，过滤条件如**错误!未找到引用源。**所示，查询结果如**错误!未找到引用源。**所示。

图8-13 搜索引擎日志过滤条件

图8-14 搜索引擎日志查询结果



8.3.4 邮件日志

1. 日志查看

打开 web 页面，点击“日志查询>应用审计日志>邮件日志”，可以查看邮件日志，如**错误!未找到引用源。**所示。

图8-15 邮件日志查看结果

2. 日志查询

在邮件日志页面，点击<查询>按钮，弹出日志过滤条件对话框，根据对话框的选项，可以根据日期、时间段、用户、源地址、目的地址、应用分类、应用、行为、发送地址、接收地址、账号、主题、处理动作、日志级别查询所需要的日志信息。

例如，查询发件人为“ambertest@sina.com”的日志，过滤条件如**错误!未找到引用源。**所示，查询结果如**错误!未找到引用源。**所示。

图8-16 邮件日志过滤条件

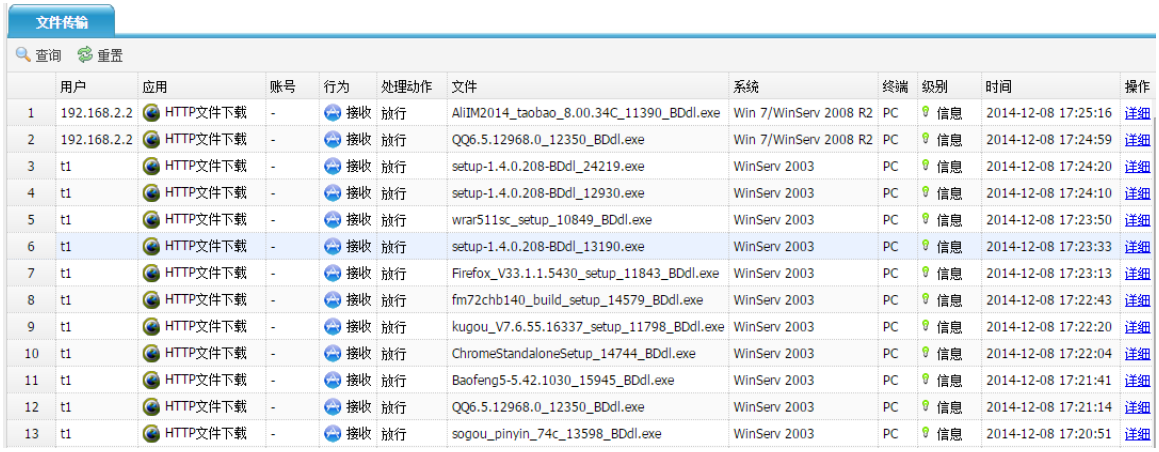
图8-17 邮件日志查询结果

8.3.5 文件传输日志

1. 日志查看

打开 web 页面，点击“日志查询>应用审计日志>文件传输日志”，可以查看命令日志，如**错误!未找到引用源。**所示。

图8-18 文件传输日志查看结果



	用户	应用	账号	行为	处理动作	文件	系统	终端	级别	时间	操作
1	192.168.2.2	HTTP文件下载	-	接收	放行	AliIM2014_taobao_8.00.34C_11390_BDdl.exe	Win 7/WinServ 2008 R2	PC	信息	2014-12-08 17:25:16	详细
2	192.168.2.2	HTTP文件下载	-	接收	放行	QQ6.5.12968.0_12350_BDdl.exe	Win 7/WinServ 2008 R2	PC	信息	2014-12-08 17:24:59	详细
3	t1	HTTP文件下载	-	接收	放行	setup-1.4.0.208-BDdl_24219.exe	WinServ 2003	PC	信息	2014-12-08 17:24:20	详细
4	t1	HTTP文件下载	-	接收	放行	setup-1.4.0.208-BDdl_12930.exe	WinServ 2003	PC	信息	2014-12-08 17:24:10	详细
5	t1	HTTP文件下载	-	接收	放行	wrar511sc_setup_10849_BDdl.exe	WinServ 2003	PC	信息	2014-12-08 17:23:50	详细
6	t1	HTTP文件下载	-	接收	放行	setup-1.4.0.208-BDdl_13190.exe	WinServ 2003	PC	信息	2014-12-08 17:23:33	详细
7	t1	HTTP文件下载	-	接收	放行	Firefox_V33.1.1.5430_setup_11843_BDdl.exe	WinServ 2003	PC	信息	2014-12-08 17:23:13	详细
8	t1	HTTP文件下载	-	接收	放行	fm72chb140_build_setup_14579_BDdl.exe	WinServ 2003	PC	信息	2014-12-08 17:22:43	详细
9	t1	HTTP文件下载	-	接收	放行	kugou_V7.6.55.16337_setup_11798_BDdl.exe	WinServ 2003	PC	信息	2014-12-08 17:22:20	详细
10	t1	HTTP文件下载	-	接收	放行	ChromeStandaloneSetup_14744_BDdl.exe	WinServ 2003	PC	信息	2014-12-08 17:22:04	详细
11	t1	HTTP文件下载	-	接收	放行	Baofeng5-5.42.1030_15945_BDdl.exe	WinServ 2003	PC	信息	2014-12-08 17:21:41	详细
12	t1	HTTP文件下载	-	接收	放行	QQ6.5.12968.0_12350_BDdl.exe	WinServ 2003	PC	信息	2014-12-08 17:21:14	详细
13	t1	HTTP文件下载	-	接收	放行	sogou_pinyin_74c_13598_BDdl.exe	WinServ 2003	PC	信息	2014-12-08 17:20:51	详细

2. 日志查询

在文件传输日志页面，点击<查询>按钮，弹出日志过滤条件对话框，根据对话框的选项，可以根据开始时间、结束时间、用户、源地址、目的地址、应用、行为、账号、文件、处理动作、日志级别查询所需要的日志信息。

例如，查询应用为“HTTP 文件下载”，行为为“接收”，文件为“QQ”的日志，过滤条件如**错误!未找到引用源。**所示，查询结果如**错误!未找到引用源。**所示。

图8-19 文件传输日志过滤条件

图8-20 文件传输日志查询结果

8.3.6 股票/娱乐日志

1. 日志查看

打开 web 页面，点击“日志查询>应用审计日志>股票/娱乐日志”，可以查看股票/娱乐日志，这类日志主要包括应用分类为流媒体、股票软件等日志，如**错误!未找到引用源。**所示。

图8-21 股票/娱乐日志查看

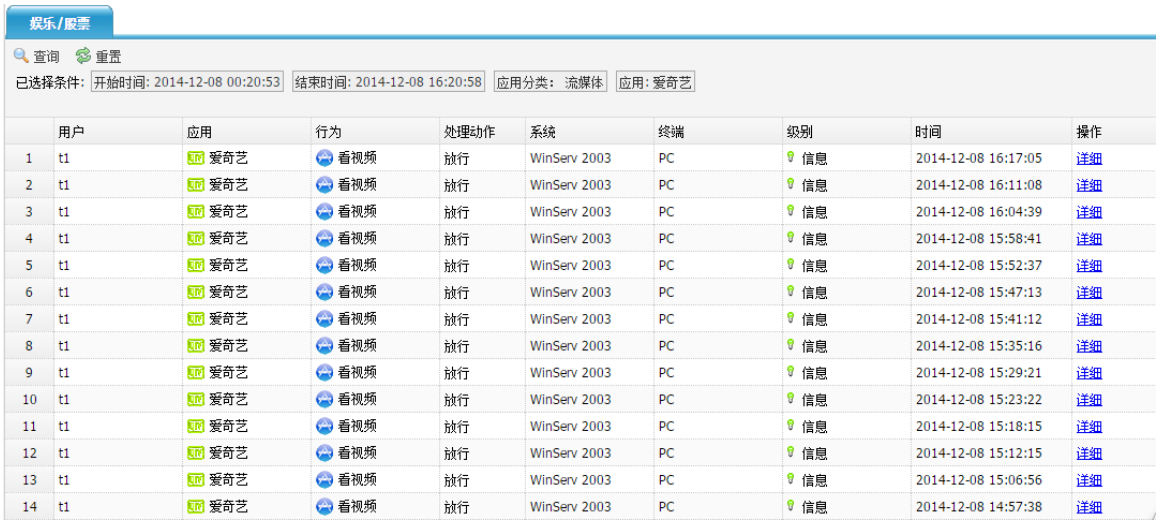
2. 日志查询

在股票/娱乐日志页面，点击<查询>按钮，弹出日志过滤条件对话框，根据对话框的选项，可以根据日期、时间段、用户、源地址、目的地址、应用分类、应用、行为、账号、处理动作、日志级别查询所需要的日志信息。

例如，查询应用为“爱奇艺”的日志，过滤条件如**错误!未找到引用源。**所示，查询结果如**错误!未找到引用源。**所示。

图8-22 股票/娱乐日志过滤条件

图8-23 股票/娱乐日志查询结果



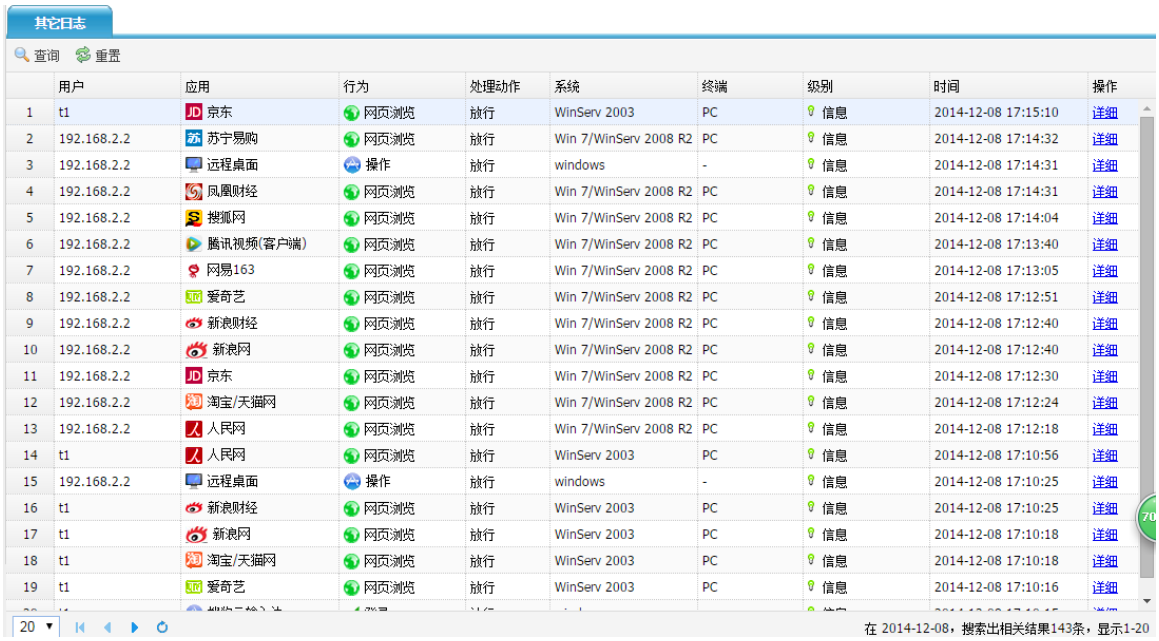
	用户	应用	行为	处理动作	系统	终端	级别	时间	操作
1	t1	爱奇艺	看视频	放行	WinServ 2003	PC	信息	2014-12-08 16:17:05	详细
2	t1	爱奇艺	看视频	放行	WinServ 2003	PC	信息	2014-12-08 16:11:08	详细
3	t1	爱奇艺	看视频	放行	WinServ 2003	PC	信息	2014-12-08 16:04:39	详细
4	t1	爱奇艺	看视频	放行	WinServ 2003	PC	信息	2014-12-08 15:58:41	详细
5	t1	爱奇艺	看视频	放行	WinServ 2003	PC	信息	2014-12-08 15:52:37	详细
6	t1	爱奇艺	看视频	放行	WinServ 2003	PC	信息	2014-12-08 15:47:13	详细
7	t1	爱奇艺	看视频	放行	WinServ 2003	PC	信息	2014-12-08 15:41:12	详细
8	t1	爱奇艺	看视频	放行	WinServ 2003	PC	信息	2014-12-08 15:35:16	详细
9	t1	爱奇艺	看视频	放行	WinServ 2003	PC	信息	2014-12-08 15:29:21	详细
10	t1	爱奇艺	看视频	放行	WinServ 2003	PC	信息	2014-12-08 15:23:22	详细
11	t1	爱奇艺	看视频	放行	WinServ 2003	PC	信息	2014-12-08 15:18:15	详细
12	t1	爱奇艺	看视频	放行	WinServ 2003	PC	信息	2014-12-08 15:12:15	详细
13	t1	爱奇艺	看视频	放行	WinServ 2003	PC	信息	2014-12-08 15:06:56	详细
14	t1	爱奇艺	看视频	放行	WinServ 2003	PC	信息	2014-12-08 14:57:38	详细

8.3.7 其他应用日志

1. 日志查看

打开 web 页面，点击“日志查询>应用审计日志>其他应用日志”，可以查看其他应用日志，这类日志主要包括应用分类为 P2P 软件、网络协议等日志，如**错误!未找到引用源。**所示。

图8-24 其他应用日志查看



2. 日志查询

在其他日志页面，点击<查询>按钮，弹出日志过滤条件对话框，根据对话框的选项，可以根据开始时间、结束时间、用户、源地址、目的地址、应用分类、应用、行为、账号、内容、处理动作、日志级别查询所需要的日志信息。

例如，查询应用分类为“生活服务”，应用为“人民网”，行为为“网页浏览”，且日志级别为“信息”的日志，过滤条件如**错误!未找到引用源。**所示，查询结果如**错误!未找到引用源。**所示。

图8-25 其他应用日志过滤条件

图8-26 其他应用日志查询结果

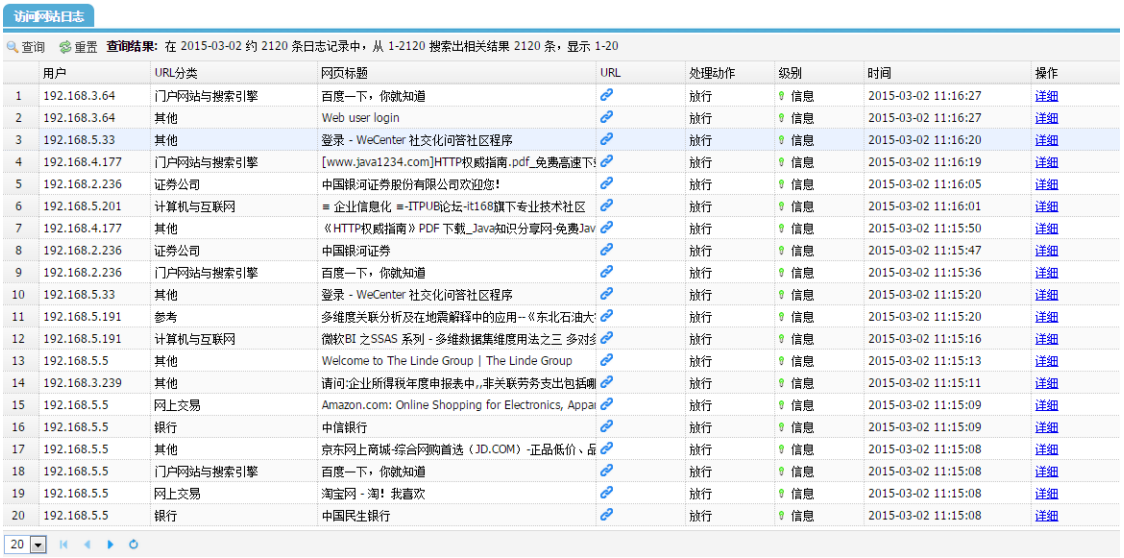
8.4 网站访问日志

8.4.1 访问网站日志

1. 日志查看

打开 web 页面，点击“日志查询>网站访问>访问网站日志”，可以查看访问网站日志，如[错误!未找到引用源。](#)所示。

图8-27 访问网站日志查看



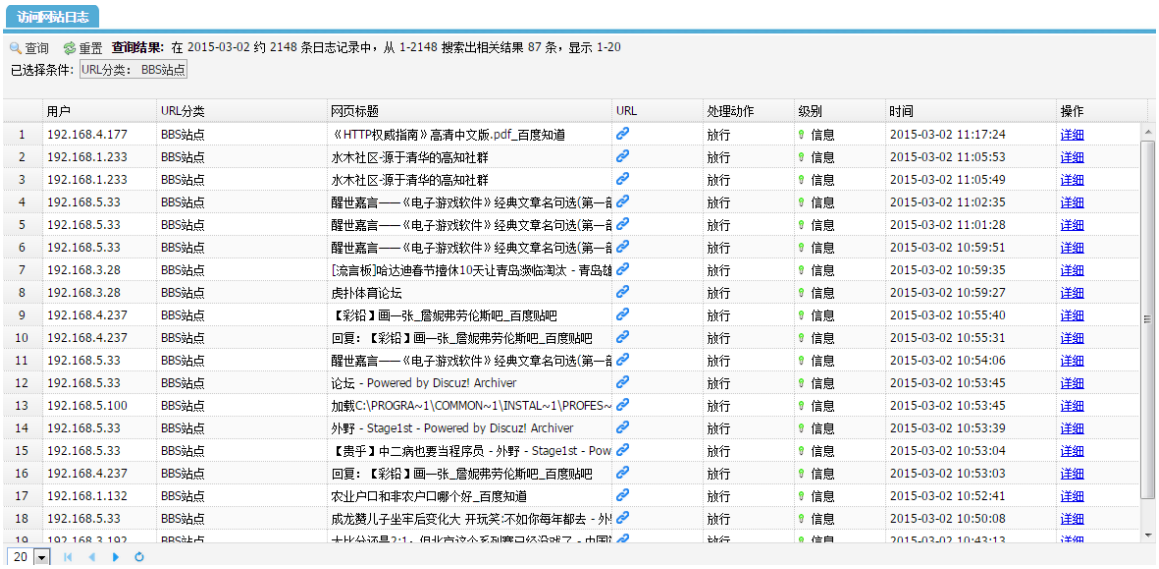
2. 日志查询

在访问网站日志页面，点击<查询>按钮，弹出日志过滤条件对话框，根据对话框的选项，可以根据日期、时间段、用户、源地址、目的地址、URL 分类、URL、处理动作、日志级别查询所需要的日志信息。

例如，查询 URL 分类为“BBS 站点”的日志，过滤条件如**错误!未找到引用源。**所示，查询结果如**错误!未找到引用源。**所示。

图8-28 访问网站日志过滤条件

图8-29 访问网站日志查询结果

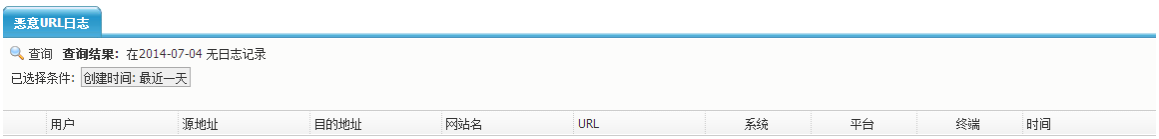


8.4.2 恶意 URL 日志

1. 日志查看

打开 web 页面，点击“日志查询>网站访问>恶意 URL 日志”，可以查看恶意 URL 日志，如**错误! 未找到引用源。**所示。

图8-30 恶意 URL 日志



2. 日志查询

在恶意 URL 日志页面，点击<查询>按钮，弹出日志过滤条件对话框，根据对话框的选项，可以根据日期、时间段、用户、源地址、目的地址、网站名查询所需要的日志信息，如**错误!未找到引用源。**所示。

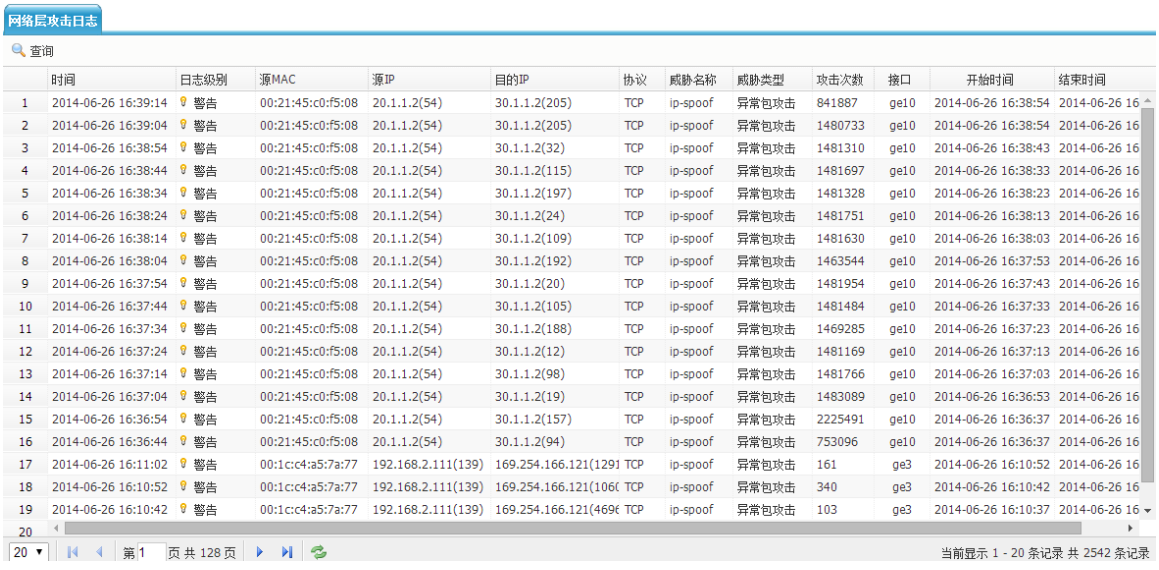
图8-31 恶意 URL 日志过滤条件

8.5 安全防护日志

1. 日志查看

打开 web 页面，点击“日志查询>安全防护日志>网络层攻击日志”，可以查看恶意 URL 日志，如**错误!未找到引用源。**所示。

图8-32 网络层攻击日志查看



2. 日志查询

在网层攻击日志页面，点击<查询>按钮，弹出日志过滤条件对话框，根据对话框的选项，可以根据开始时间、结束时间、日志级别、源 IP 地址、目的 IP 地址、威胁名称、协议查询所需要的日志信息。

例如，查询日志级别为“警告”，源地址为“192.168.2.211”，威胁类型为“异常包攻击”且协议为“TCP”的日志，过滤条件如**错误!未找到引用源。**所示，查询结果如**错误!未找到引用源。**所示。

图8-33 网络层攻击日志过滤条件

图8-34 网络层攻击日志查询结果

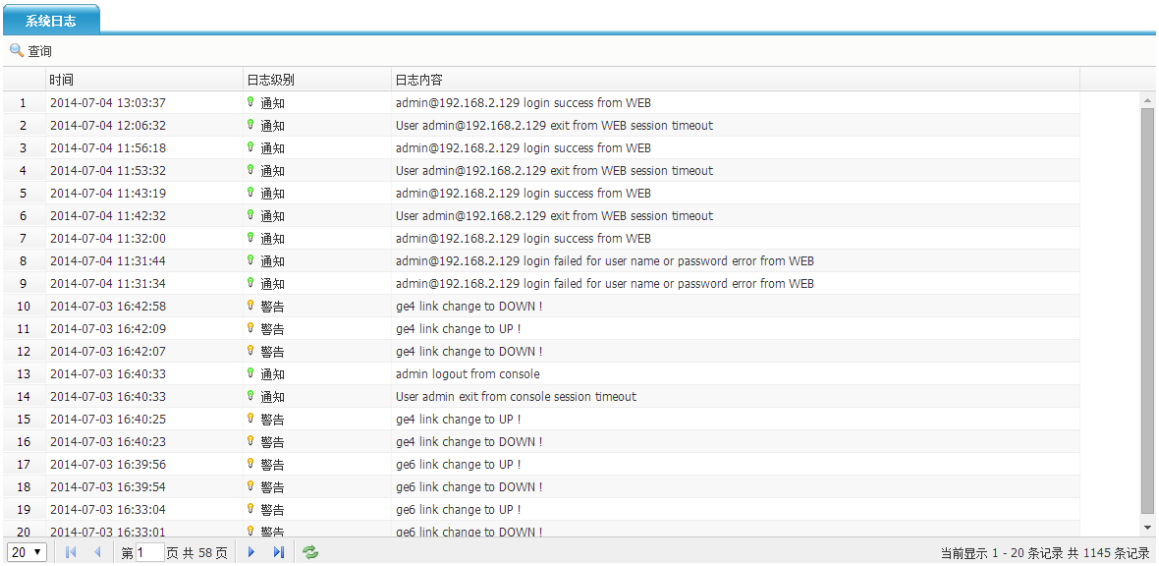
8.6 系统日志

8.6.1 系统日志

1. 日志查看

打开 web 页面，点击“日志查询>系统日志>系统日志”，可以查看系统日志，如**错误!未找到引用源。**所示。

图8-35 系统日志查看



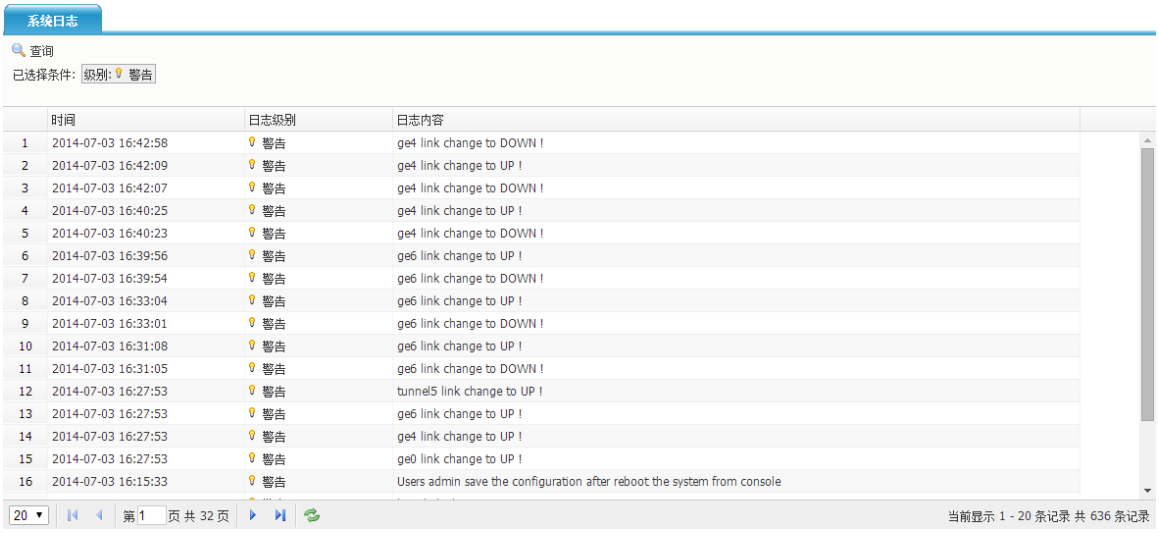
2. 日志查询

在系统日志页面，点击<查询>按钮，弹出日志过滤条件对话框，根据对话框的选项，可以根据开始时间、结束时间、日志级别、日志内容查询所需要的日志信息。

例如，查询日志级别为“警告”的日志，过滤条件如**错误!未找到引用源。**所示，查询结果如**错误!未找到引用源。**所示。

图8-36 系统日志过滤条件

图8-37 系统日志查询结果

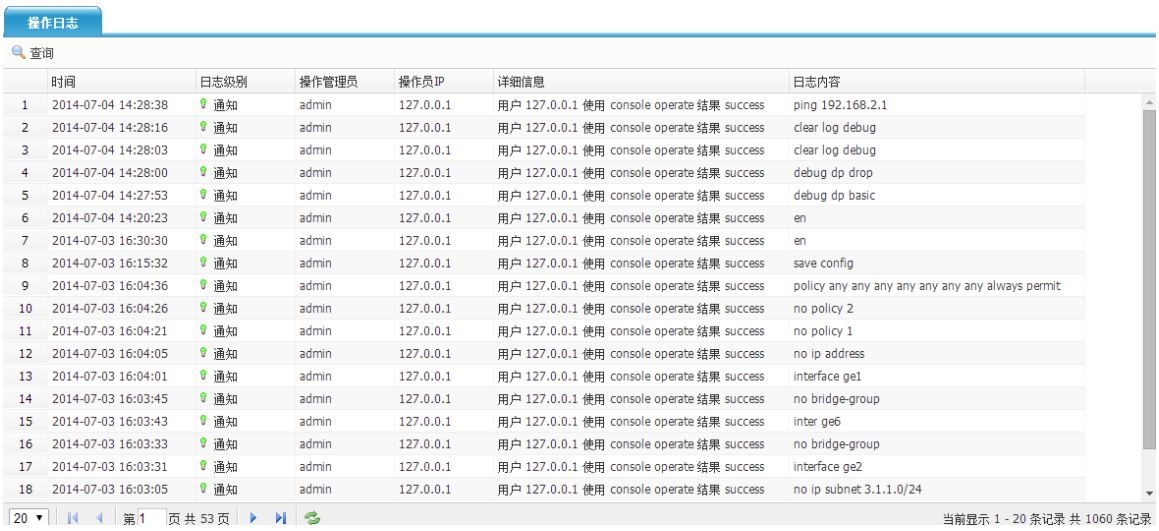


8.6.2 操作日志

1. 日志查看

打开 web 页面，点击“日志查询>系统日志>操作日志”，可以查看操作日志，如**错误!未找到引用源。**所示。

图8-38 操作日志查看



2. 日志查询

在操作日志页面，点击<查询>按钮，弹出日志过滤条件对话框，根据对话框的选项，可以根据开始时间、结束时间、操作管理员、操作 IP、日志级别、日志内容查询所需要的日志信息。

例如，查询 2014 年 7 月 4 日且日志级别为“通知”的日志，过滤条件如**错误!未找到引用源。**所示，查询结果如**错误!未找到引用源。**所示。

图8-39 操作日志过滤条件

图8-40 操作日志查询结果

	时间	日志级别	操作管理员	操作员IP	详细信息	日志内容
1	2014-07-04 14:28:38	通知	admin	127.0.0.1	用户 127.0.0.1 使用 console operate 结果 success	ping 192.168.2.1
2	2014-07-04 14:28:16	通知	admin	127.0.0.1	用户 127.0.0.1 使用 console operate 结果 success	clear log debug
3	2014-07-04 14:28:03	通知	admin	127.0.0.1	用户 127.0.0.1 使用 console operate 结果 success	clear log debug
4	2014-07-04 14:28:00	通知	admin	127.0.0.1	用户 127.0.0.1 使用 console operate 结果 success	debug dp drop
5	2014-07-04 14:27:53	通知	admin	127.0.0.1	用户 127.0.0.1 使用 console operate 结果 success	debug dp basic
6	2014-07-04 14:20:23	通知	admin	127.0.0.1	用户 127.0.0.1 使用 console operate 结果 success	en

9 组网特性

9.1 HA

9.1.1 HA 特性

HA 是 High Availability 缩写，即高可用性，可防止网络中由于单个网关产品的设备故障或链路故障导致网络中断，保证网络服务的连续性和安全强度。

随着网络的快速普及和应用的日益深入，各种增值业务（如 IPTV、视频会议等）得到了广泛部署，网络中断可能影响大量业务、造成重大损失。因此，作为业务承载主体的基础网络，其可靠性日益成为受关注的焦点。

在实际网络中，总避免不了各种非技术因素造成的网络故障和服务中断。因此，提高系统容错能力、

提高故障恢复速度、降低故障对业务的影响，是提高系统可靠性的有效途径。

本产品通过双机热备来实现 HA。

9.1.2 路由模式 HA 主备

1. 配置需求

- 设备 ACG A 配置为主设备，设备 ACG B 配置成为备设备。
- 设备 ACG A 的 ge1-3 接口作为 HA 接口和设备 ACG B 的 ge1-3 接口相连。
- 设备 ACG A 和设备 ACG B 配置 mgt0、ge1-0 和 ge1-2 为监控接口。
- 设备 ACG A 和设备 ACG B 配置自动同步 session，配置，特征库。

2. 配置思路

(1) 按照拓扑搭建测试环境；

(2) 在 ACG A 配置网络接口；

(3) 在在 ACG A 上配置两条静态路由，下一跳分别指向 Switch A 和 Switch B

(4) 配置 IPV4 策略

(5) 在在 ACG A 开启 HA；

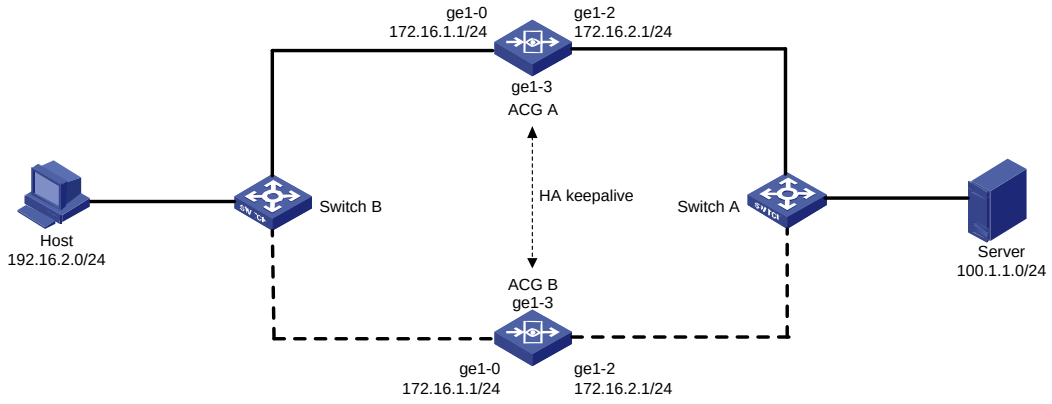
(6) 在 ACG B 开启 HA；

(7) 在 ACG A 查看 HA 状态是否同步

(8) 分别在 ACG A 和 ACG B 配置管理 IP

3. 配置步骤

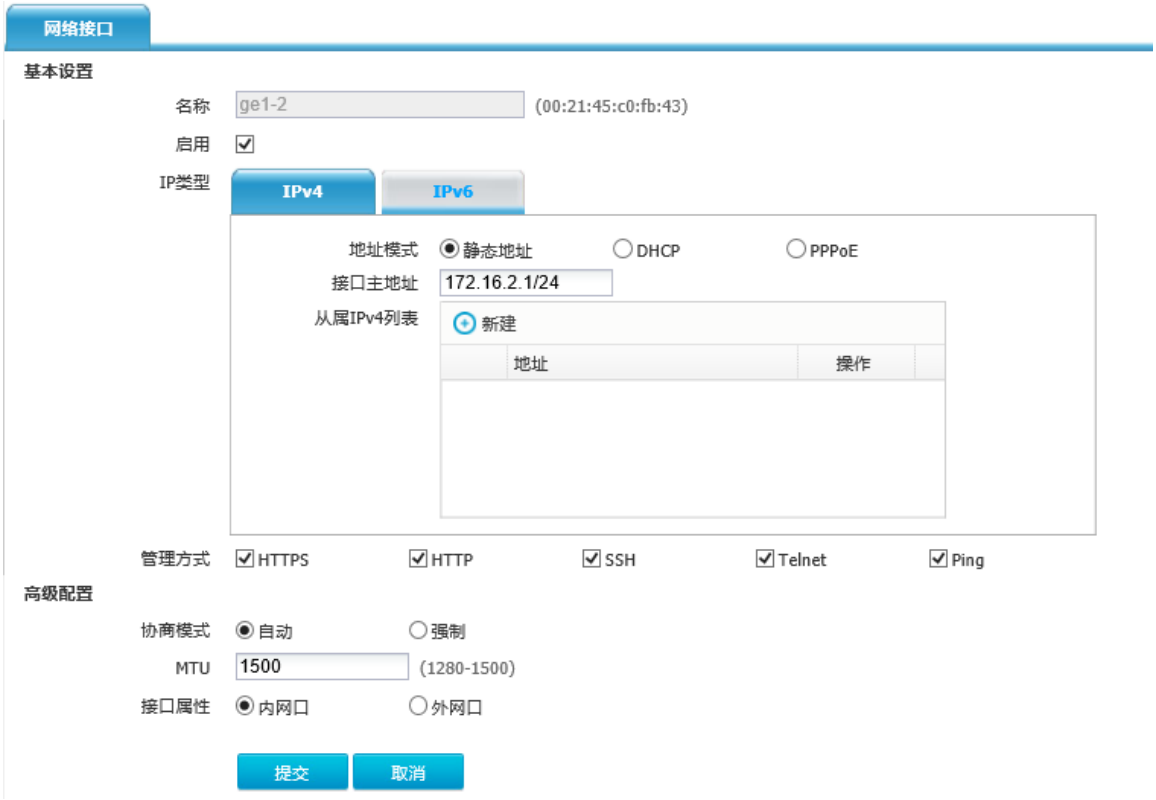
图9-1 HA 组网示意图



(1) 在 ACG A 进入“网络配置>接口>网络接口”，点击<新建>按钮，配置 ge1-0 地址为 172.16.1.1/24，ge1-2 接口为 172.16.2.1、24

图9-2 配置接口 ge1-0

图9-3 配置 ge1-2



(2) 在 ACG A 上进入“网络配置>路由>静态路由”，点击<新建>。配置两条静态路由，下一跳分别指向 Switch A 和 Switch B。

图9-4 配置静态路由

图9-5 配置静态路由

(3) 在 ACG A 进入“上网行为管理>策略配置>IPV4 策略”，点击<新建>，配置一条全通策略。

图9-6 配置安全策略

(4) 在 ACG A 进入“系统管理>高可用性>HA 全局配置”，开启主-备工作模式

图9-7 配置 HA

在 ACG B 进入“系统管理>高可用性>HA 全局配置”，开启主-备工作模式。

图9-8 配置 HA

在 ACG A 进入系统管理>高可用性>HA 监控，查看 HA 状态是否同步。不同步的话，点击<同步配置>，进行同步，此时备墙重启。

图9-9 HA 监控

同步完成后再次查看 HA 状态是否相同。

图9-10 HA 监控

在 ACG A 进入系统管理>高可用性>HA 接口管理地址，点击<新建管理 ip>。

图9-11 HA 接口管理地址

使用管理 IP 登录 ACG A 后，进入系统管理>高可用性>HA 监控，点击<主备切换>。

图9-12 HA 监控

图9-13 HA 监控

4. 注意事项

- 进行 HA 的两台设备，应为同一个硬件型号。设备之间通过 HA 接口直连， HA 接口可以任何以太网接口，也可以是 AGG 接口（聚合接口），此接口一旦选中为 HA 接口后，不能作为其他用途。要求作为 HA 的两台设备为同一个硬件型号，选择同样的接口作为 HA 接口。
- 心跳口，必须是物理接口和聚合接口。心跳口不能和其他功能一起使用，比如不能加入桥，加入聚合，配置 NAT。接口配置成 HA 心跳口后，接口上的有关于地址的配置都会被删除
- 要配置成监控接口的接口，一般应是网络中重要的接口，比如通往 internet 的接口。如果此接口的状态发生改变。表明网络中发生重大故障，需要启用备设备，主备设备会立刻切换。如果主设备和备设备的监控接口都发生故障，表明此时网络发生严重错误，此时主备切换也无法修复错误，所以主备不会发生切换
- 手动同步配置后，会自动重启备设备，重新加载备设备的驱动。HA 的相关配置在配置同步时不会同步。配置自动同步选项不会影响手动同步配置的效果。
- 管理地址可以和接口主地址处于同一网段。接口没有配置主地址也可以配置管理地址，但是如果接口的主地址是 PPPOE 或者 DHCP 地址，则无法配置管理地址。管理员可以通过管理地址访问备设备的 telnet 服务和 web ui。但是备设备无法通过管理地址主动访问外部地址，除非应用制定了源地址为管理地址（比如说制指定地址的 ping 命令）。

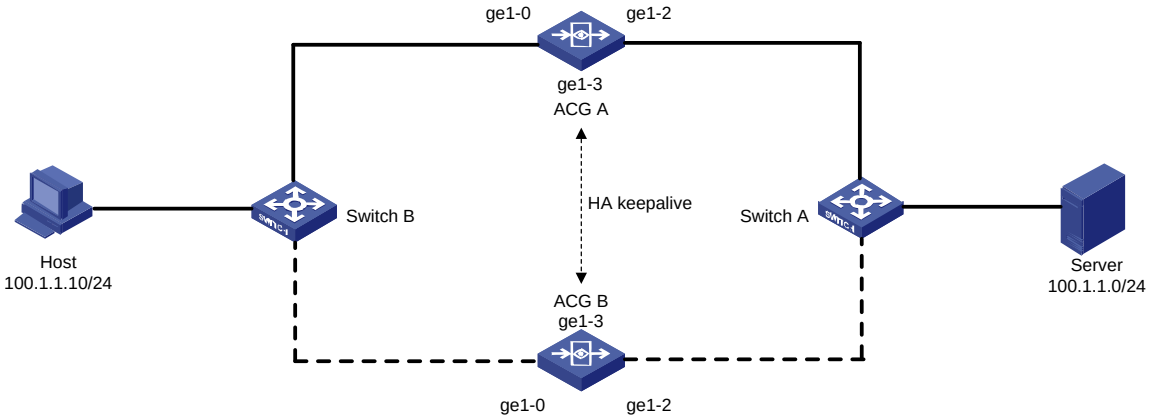
9.1.3 透明模式 HA 主备

1. 配置需求

- 设备 ACG A 配置为主设备，设备 ACG B 配置成为备设备。
- 设备 ACG A 的 ge1-3 接口作为 HA 接口和设备 ACG B 的 ge1-3 接口相连。
- 设备 ACG A 和设备 ACG B 配置 mgt0、ge1-0 和 ge1-2 为监控接口。
- 设备 ACG A 和设备 ACG B 配置自动同步 session，配置，特征库。

2. 组网图

图9-14 HA 组网示意图：



3. 配置思路

(1) 按照拓扑搭建测试环境；

(2) 在 ACG A 配置网桥接口；

(3) 配置 IPV4 策略；

(4) 在 ACG A 开启 HA；

(5) 在 ACG B 开启 HA；

(6) 在 ACG A 查看 HA 状态是否同步；

(7) 分别在 ACG A 和 ACG B 配置管理 IP；

4. 配置步骤

(1) 在 ACG A 进入“网络配置>接口>网桥接口”，点击<新建>按钮，把 ge1-0 和 ge1-2 加入桥。

图9-15 配置桥接口

(2) 在 ACG A 进入“上网行为管理>策略配置>IPV4 策略”，点击<新建>，配置一条全通策略

图9-16 配置安全策略

(3) 在 ACG A 进入“系统管理>高可用性>HA 全局配置”，开启主-备工作模式：

图9-17 配置 HA

(4) 在 ACG B 进入“系统管理>高可用性>HA 全局配置”，开启主-备工作模式

图9-18 配置 HA

(5) 在 ACG A 进入“系统管理>高可用性>HA 监控”，查看 HA 状态是否同步。不同步的话，点击<同步配置>按钮，进行同步，此时备墙重启。

图9-19 HA 监控

(6) 同步完成后再次查看 HA 状态是否相同

图9-20 HA 监控

(7) 在 ACG A 进入“系统管理>高可用性>HA 接口管理地址”，点击<新建管理 ip>。

图9-21 配置 HA 接口管理地址

（8） 使用管理 IP 登录 ACG A 后，进入“系统管理>高可用性>HA 监控”，点击<主备切换>按钮。

图9-22 主备切换

图9-23 切换后的效果图

5. 注意事项

- 进行 HA 的两台设备，应为同一个硬件型号。设备之间通过 HA 接口直连， HA 接口可以任何以太网接口，也可以是 AGG 接口（聚合接口），此接口一旦选中为 HA 接口后，不能作为其他用途。要求作为 HA 的两台设备为同一个硬件型号，选择同样的接口作为 HA 接口。
- 心跳口，必须是物理接口和聚合接口。心跳口不能和其他功能一起使用，比如不能加入桥，加入聚合，配置 NAT。接口配置成 HA 心跳口后，接口上的有关于地址的配置都会被删除
- 要配置成监控接口的接口，一般应是网络中重要的接口，比如通往 internet 的接口。如果此接口的状态发生改变。表明网络中发生重大故障，需要启用备设备，主备设备会立刻切换。如果主设备和备设备的监控接口都发生故障，表明此时网络发生严重错误，此时主备切换也无法修复错误，所以主备不会发生切换

- 如果设备工作在桥模式，在成为备设备后，设备会将加入桥的接口关闭打开一次，用来刷新上下游交换机的 fdb 表并将加入桥的接口关闭打开一次，用来刷新上下游交换机的 fdb 表。设备刚变成备状态，会从主设备获取配置信息，但是不会立刻加载。如果主备设备的信息不一致。需要重启备设备。
- 手动同步配置后，会自动重启备设备，重新加载备设备的驱动。HA 的相关配置在配置同步时不会同步。配置自动同步选项不会影响手动同步配置的效果。
- 管理地址可以和接口主地址处于同一网段。接口没有配置主地址也可以配置管理地址，但是如果接口的主地址是 PPPOE 或者 DHCP 地址，则无法配置管理地址。管理员可以通过管理地址访问备设备的 telnet 服务和 web ui。但是备设备无法通过管理地址主动访问外部地址，除非应用制定了源地址为管理地址（比如说制指定地址的 ping 命令）。

9.1.4 路由模式 HA 主主

1. 配置需求

- 设备 ACG A 配置为主设备，设备 ACG B 配置成为主设备。
- 设备 ACG A 的 ge1-3 接口作为 HA 接口和设备 ACG B 的 ge1-3 接口相连。
- 设备 ACG A 和设备 ACG B 配置 mgt0、ge1-0 和 ge1-2 为监控接口。
- 设备 ACG A 和设备 ACG B 配置自动同步 session，自动同步 monitor_ip。

2. 配置思路

(1) 按照拓扑搭建测试环境；

(2) 在 ACG A 配置网络接口；

(3) 在 ACG A 上配置两条静态路由，下一跳分别指向 Switch A 和 Switch B

(4) 配置 IPV4 策略

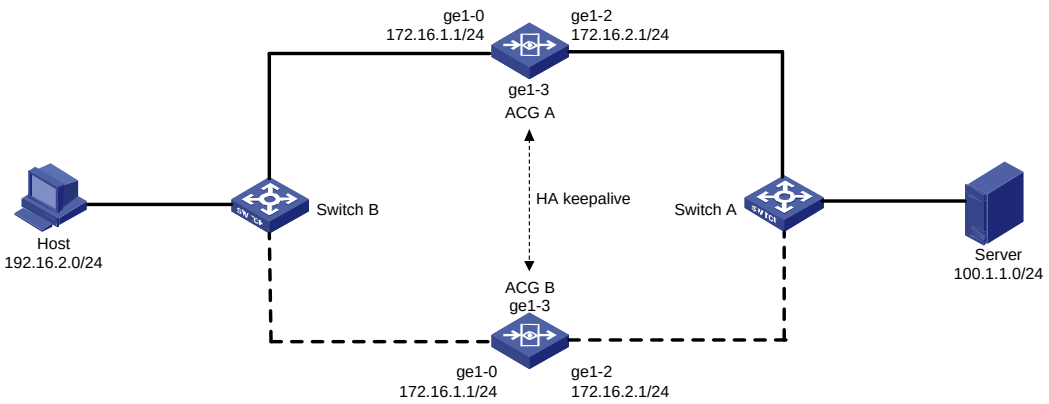
(5) 在 ACG A 开启 HA；

(6) 在 ACG B 开启 HA；

(7) 在 ACG A 查看 HA 状态是否同步

3. 配置步骤

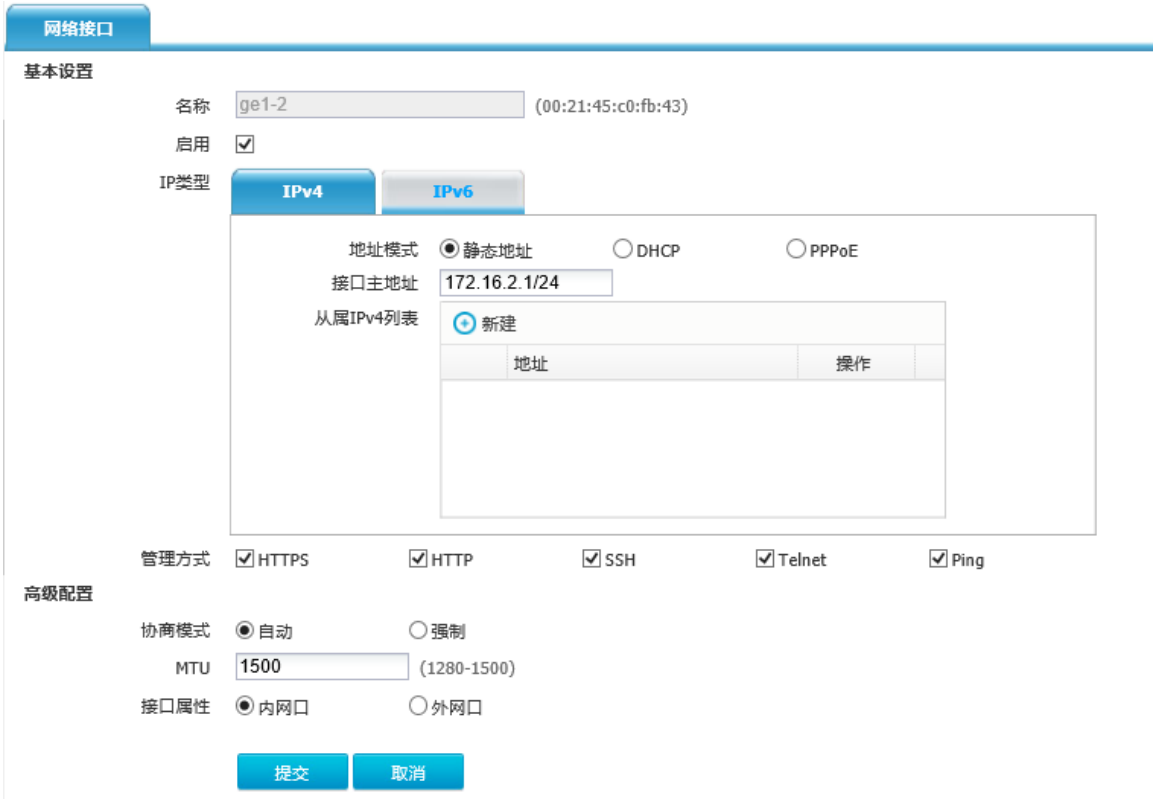
图9-24 HA 组网示意图



(2) 在 ACG A 进入“网络配置>接口>网络接口”，点击<新建>按钮，配置 ge1-0 地址为 172.16.1.1/24，ge1-2 接口为 172.16.2.1、24

图9-25 配置接口 ge1-0

图9-26 配置 ge1-2



(3) 在 ACG A 上进入“网络配置>路由>静态路由”，点击<新建>。配置两条静态路由，下一跳分别指向 Switch A 和 Switch B。

图9-27 配置静态路由

图9-28 配置静态路由

(4) 在 ACG A 进入“上网行为管理>策略配置>IPV4 策略”，点击<新建>，配置一条全通策略。

图9-29 配置安全策略

(5) 在 ACG A 进入“系统管理>高可用性>HA 全局配置”，开启主-主工作模式

图9-30 配置 HA

在 ACG B 进入“系统管理>高可用性>HA 全局配置”，开启主-主工作模式。

图9-31 配置 HA

图9-32 在 ACG A 进入系统管理>高可用性>HA 监控，查看 HA 状态是否同步。

4. 注意事项

- 进行 HA 的两台设备，应为同一个硬件型号。设备之间通过 HA 接口直连， HA 接口可以任何以太网接口，也可以是 AGG 接口（聚合接口），此接口一旦选中为 HA 接口后，不能作为其他用途。要求作为 HA 的两台设备为同一个硬件型号，选择同样的接口作为 HA 接口。
- 心跳口，必须是物理接口和聚合接口。心跳口不能和其他功能一起使用，比如不能加入桥，加入聚合，配置 NAT。接口配置成 HA 心跳口后，接口上的有关于地址的配置都会被删除
- 要配置成监控接口的接口，一般应是网络中重要的接口，比如通往 internet 的接口。如果此接口的状态发生改变。表明网络中发生重大故障，需要主主切换。如果主主设备的监控接口都发生故障，表明此时网络发生严重错误，此时主主切换也无法修复错误，所以主主不会发生切换

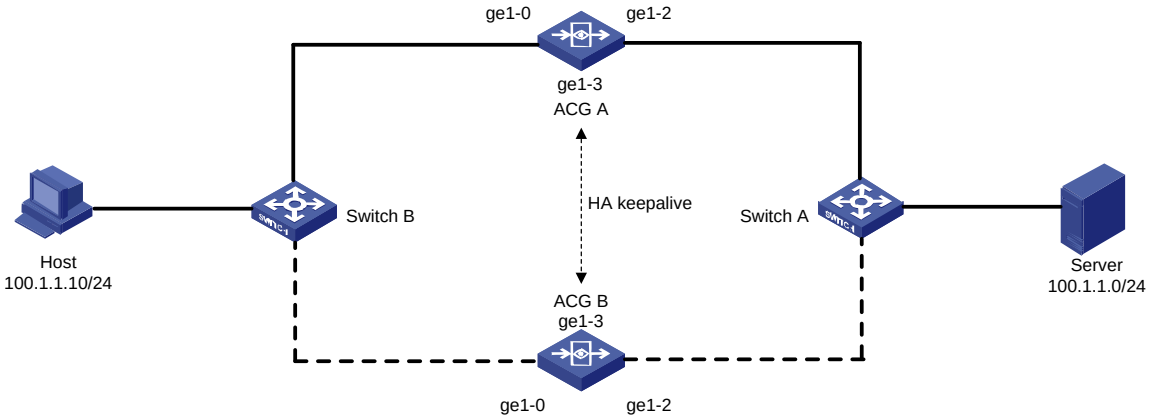
9.1.5 透明模式 HA 主主

1. 配置需求

- 设备 ACG A 配置为主设备，设备 ACG B 配置成为主设备。
- 设备 ACG A 的 ge1-3 接口作为 HA 接口和设备 ACG B 的 ge1-3 接口相连。
- 设备 ACG A 和设备 ACG B 配置 mgt0、ge1-0 和 ge1-2 为监控接口。
- 设备 ACG A 和设备 ACG B 配置自动同步 session，自动同步 monitor_ip。

2. 组网图

图9-33 HA 组网示意图：



3. 配置思路

(1) 按照拓扑搭建测试环境；

(2) 在 ACG A 配置网桥接口；

(3) 配置 IPV4 策略；

(4) 在 ACG A 开启 HA；

(5) 在 ACG B 开启 HA；

(6) 在 ACG A 查看 HA 状态是否同步；

(7) 分别在 ACG A 和 ACG B 配置管理 IP；

4. 配置步骤

(1) 在 ACG A 进入“网络配置>接口>网桥接口”，点击<新建>按钮，把 ge1-0 和 ge1-2 加入桥。

图9-34 配置桥接口

(2) 在 ACG A 进入“上网行为管理>策略配置>IPV4 策略”，点击<新建>，配置一条全通策略

图9-35 配置安全策略

(3) 在 ACG A 进入“系统管理>高可用性>HA 全局配置”，开启主-备工作模式：

图9-36 配置 HA

(4) 在 ACG B 进入“系统管理>高可用性>HA 全局配置”，开启主-主工作模式

图9-37 配置 HA

(5) 在 ACG A 进入“系统管理>高可用性>HA 监控”，查看 HA 状态是否同步。

图9-38 HA 监控

5. 注意事项

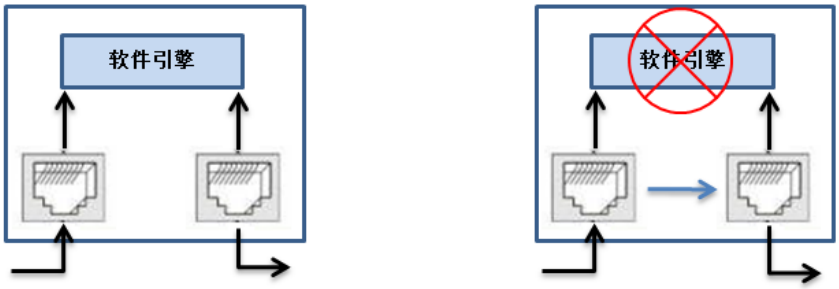
- 进行 HA 的两台设备，应为同一个硬件型号。设备之间通过 HA 接口直连， HA 接口可以任何以太网接口，也可以是 AGG 接口（聚合接口），此接口一旦选中为 HA 接口后，不能作为其他用途。要求作为 HA 的两台设备为同一个硬件型号，选择同样的接口作为 HA 接口。
- 心跳口，必须是物理接口和聚合接口。心跳口不能和其他功能一起使用，比如不能加入桥，加入聚合，配置 NAT。接口配置成 HA 心跳口后，接口上的有关于地址的配置都会被删除
- 要配置成监控接口的接口，一般应是网络中重要的接口，比如通往 internet 的接口。如果此接口的状态发生改变。表明网络中发生重大故障，需要主主切换。如果主主设备的监控接口都发生故障，表明此时网络发生严重错误，此时主主切换也无法修复错误，所以主主不会发生切换

9.2 BYPass功能

9.2.1 组网需求

H3C ACG1000 具有电口 BYPass 的硬件特性，当软件系统进程异常重启、手工重启或供电故障(断电)时，支持 BYPass 功能的接口会自动切换到 BYPass 状态，直接将接收到的网络流量在二层进行转发出去，不再进入上层软件处理，以保证设备在软件故障或掉电故障时仍能够维持网络业务的连续性。

图9-39 Bypass 模式切换示意图：



9.2.2 配置思路组网步骤

图9-40 Bypass 物理连接示意图：

9.2.3 配置步骤

BYPass 功能无需手工页面配置或命令行配置，测试时 BYPass 接口划入到桥中，将设备 1 进行 Ping 设备 2，拔掉电源观察 Host 之间断 3 个 ICMP 报文又正常恢复。

9.2.4 注意事项

(1) 使用时需将通信接口配置在同一个 BYPass 接口对中。

(2) BYPass 功能需要配置为二层模式，不支持三层模式。

9.3 链路负载均衡

9.3.1 链路负载均衡产生背景

信息时代，工作越来越离不开网络，为了规避运营商出口故障带来的网络可用性风险，和解决网络带宽不足带来的网络访问问题，企业往往会租用两个或多个运营商出口（如：电信、网通等）。如何合理运用多个运营商出口，既不造成资源浪费，又能很好的服务于企业，因而产生了多链路负载均衡的需求。传统的策略路由也可以在一定程度上解决该问题，但是策略路由配置不方便，而且不够灵活，无法动态适应网络结构变化，且策略路由无法根据带宽进行报文分发，造成高吞吐量的链路无法得到充分利用。负载均衡技术，通过动态算法，也能够在多条链路中进行负载均衡，算法配置简单，且具有自适应能力，能很好的解决上述问题。

9.3.2 链路负载均衡特性

多链路负载均衡，根据链路情况，可配置不同的策略，比路由更灵活的控制流量的走向，以适应不同的场景。目前负载方式暂支持两种分别为带宽比策略和优先级策略

- 带宽比策略，依据链路带宽的不同，每个链路承载相应比例的流量，尽量发挥各个链路的带宽的可用性。
- 优先级一般适用于多个不同链路，每个链路的花费不一样，尽量优选性价比高的链路走流量，其他链路做备份使用。

9.3.3 链路负载均衡

组网需求

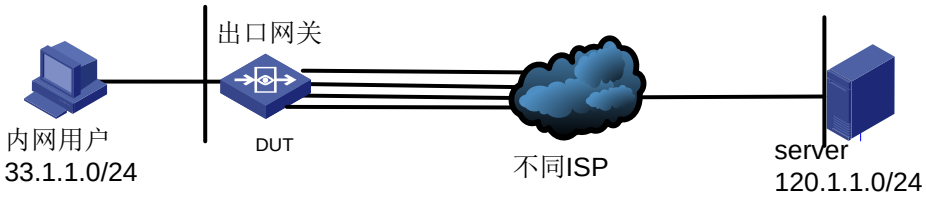
为了规避运营商出口故障带来的网络可用性风险，和解决网络带宽不足带来的网络访问问题，公司租用多个运营商出口流量在多个出口按照带宽比进行负载均衡保证内网访问公网的可靠性。

配置思路

(1) 配置接口地址
(2) 配置出口路由
(3) 配置地址对象
(4) 配置源 NAT
(5) 配置 IPV4 策略
(6) 配置地址探测对象
(7) 配置链路负载均衡
(8) 保存配置

配置步骤

图9-41 链路负载均衡组网示意图：



(9) 配置接口地址

在 ACG A 进入“网络配置>接口>网络接口”，点击<新建>按钮，配置 ge1-0 地址为 11.1.1.2/24，ge1-1 接口为 12.1.1.2/24，ge1-2 接口为 13.1.1.2/24,ge1-3 接口为 14.1.1.2/24.内网接口 ge2-0 接口 IP 为 33.1.1.1/24

图9-42 配置接口 ge1-0

图9-43 配置接口 ge1-1

图9-44 配置接口 ge1-2

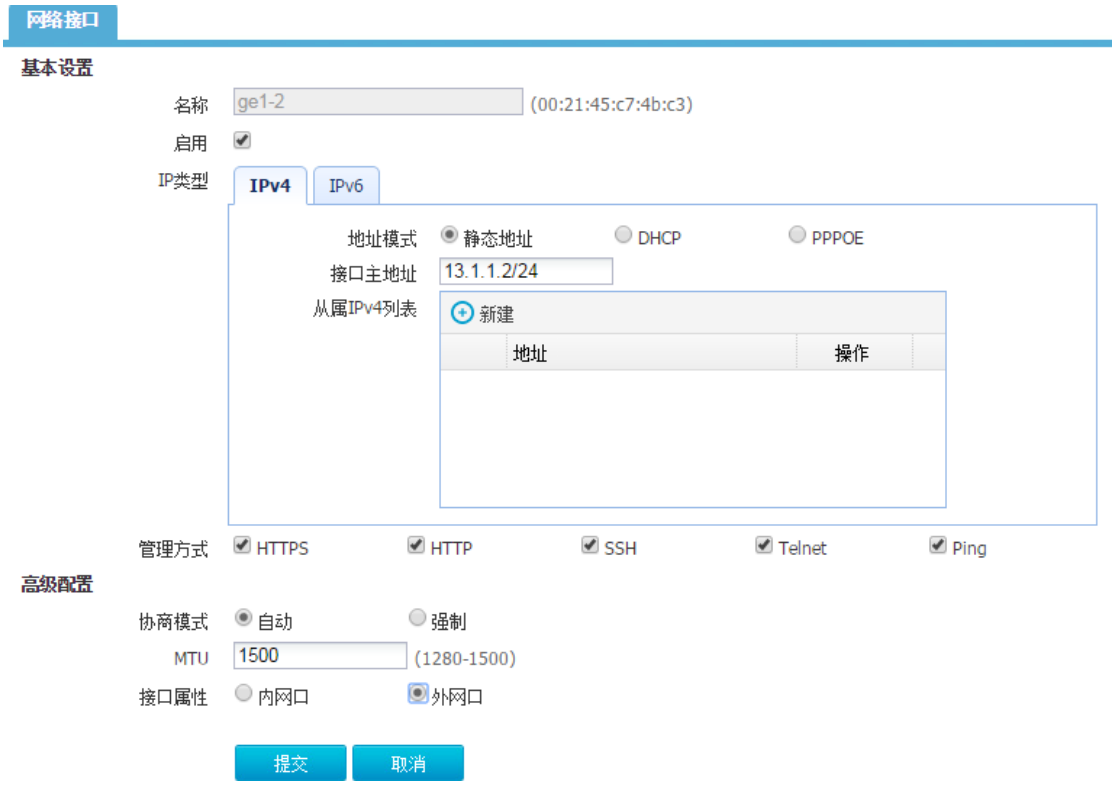


图9-45 配置接口 ge1-3

图9-46 配置接口 ge2-0

(10) 配置出口路由

在 ACG 上进入“网络配置>静态路由”，点击<新建>。配置四条默认路由。

图9-47 配置出口路由

(11) 配置地址对象

在 ACG 上进入“地址对象>地址>IPV4 地址对象”，点击<新建>。配置地址对象

名称为“内网网段”，地址节点选择“子网地址”：“33.1.1.0/24”，点击“添加到列表”，点击提交。

图9-48 配置地址对象

(12) 配置源 NAT

在 ACG 进入“网络配置>NAT>源 NAT”，点击<新建>

分别配置四条源 NAT 转换，转换类型为“出接口”,接口选择连接外网的接口，配置完成后点击提交。

图9-49 配置 SNAT

图9-50 配置 SNAT

图9-51 配置 SNAT

图9-52 配置 SNAT

(13) 配置 IPV4 策略

在 ACG 进入“上网行为管理>策略配置>IPV4 策略”，点击<新建>，配置一条全通策略

图9-53 配置安全策略

(14) 配置地址探测对象

在 ACG 进入“对象管理>地址>地址探测”，点击<新建>，配置四个地址探测对象，探测对象为出接口下一跳地址。

图9-54 配置地址探测对象

	名称	探测目标	类型	出接口	间隔时间	重试次数	状态	操作
1	120	120.1.1.2	PING	any	4	4		
2	出口地址一	11.1.1.1	PING	any	10	4		
3	出口地址二	12.1.1.1	PING	any	10	4		
4	出口地址三	13.1.1.1	PING	any	10	4		
5	出口地址四	14.1.1.1	PING	any	10	4		

(15) 配置链路负载均衡

在 ACG 进入“网络配置>链路负载均衡”，点击<新建>，配置链路负载均衡。其中两条带宽 10M，两条 50M，配置阈值为 100，开启健康检查，并且指定接口 ge1-3 为过载保护接口，配置完成后提交。

图9-55 配置负载均衡组 ge1-0

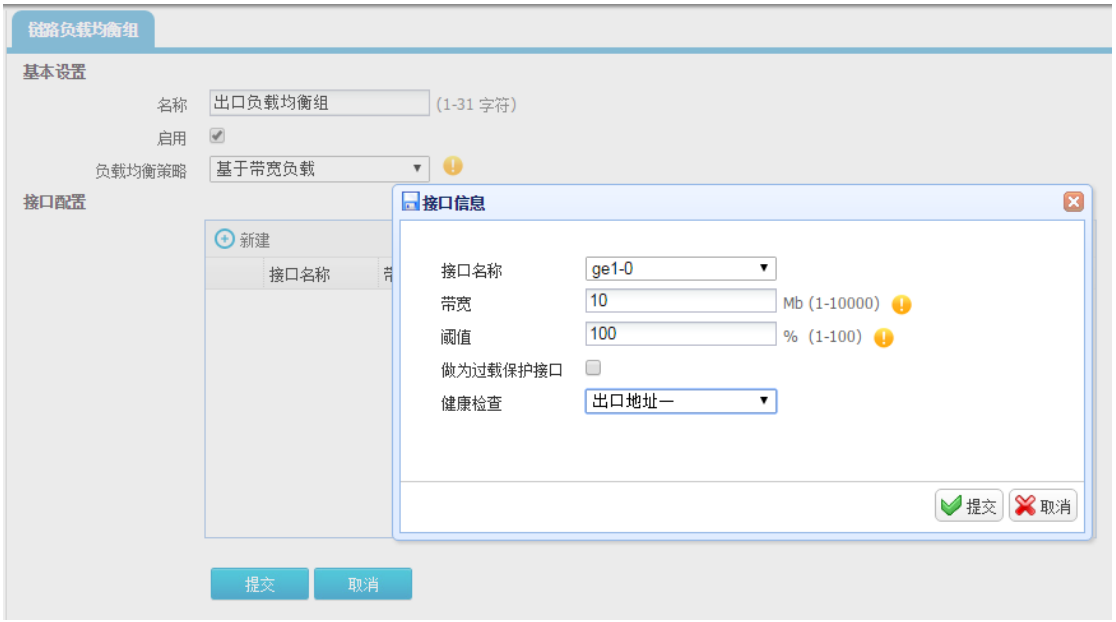


图9-56 配置负载均衡组 ge1-1

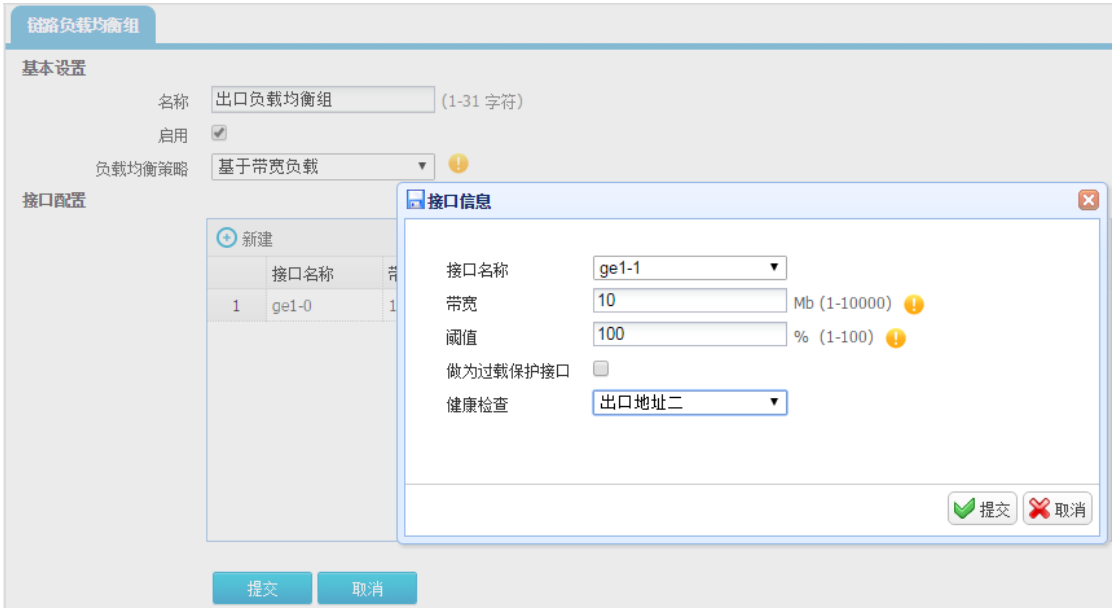


图9-57 配置负载均衡组 ge1-2

图9-58 配置负载均衡组 ge1-3

注意事项

- 采用带宽比负载均衡时，接口组里的所有接口都需要配置带宽，否则该接口组不生效。
- 接口不再同一负载均衡组下不做负载
- 基于优先级的是谁的优先级高先走谁接口达到阀值后在找第二优先级的接口走，相同优先级，接口流量满了后才从其它接口转发
- 会话保持是相同源 IP 的流出口一样。如果未达到阈值的话。和带宽比负载不冲突，也就是会话保持优先于带宽

负载方式为优先级同时开启会话保持，先走优先级。会话保持对优先级无效，因为优先级强调的本来就是优先先走哪个接口，这俩互斥

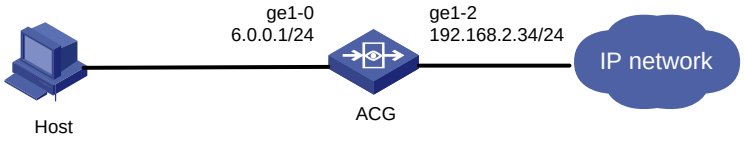
9.4 服务质量管理

9.4.1 服务质量管理简介

目前支持 TCP、DNS、PING 这几种探测方式，根据用户所需探测的服务可配置 20 条不同的探测服务。主要功能为收集每次探测结果，分析数据，通过图表和曲线直观描述探测结果。

9.4.2 组网图

图9-59 服务质量管理组网图



9.4.3 PING 服务质量管理

配置需求

对目标进行 PING 服务质量管理探测。

配置思路

(1) 配置设备的接口、路由、NAT、安全策略、DNS。

(2) 配置 PING 服务质量管理条目。

(3) 查看该管理条目的探测结果。

配置步骤

(4) 进入“网络管理>接口>物理接口”，点击操作。

图9-60 配置物理接口 ge1-2

图9-61 配置物理接口 ge1-0

(5) 配置 NAT

进入“网络配置>NAT>源 NAT”，点击<新建>。

图9-62 配置 NAT 规则

(6) 配置静态路由

进入“网络配置>路由>静态路由”，点击<新建>。

图9-63 配置静态路由

(7) 配置 IPv4 策略

进入“上网行为管理>策略配置>IPv4 策略”，点击<新建>。

图9-64 配置 IPv4 策略

(8) 配置 DNS

进入“网络配置>DNS 服务器”。

图9-65 配置 DNS 服务器

(9) 配置 PING 服务质量管理条目

进入“网络优化>服务质量管理”，点击<新建>。

图9-66 配置服务质量管理

图9-67 查看服务质量管理条目成功率结果

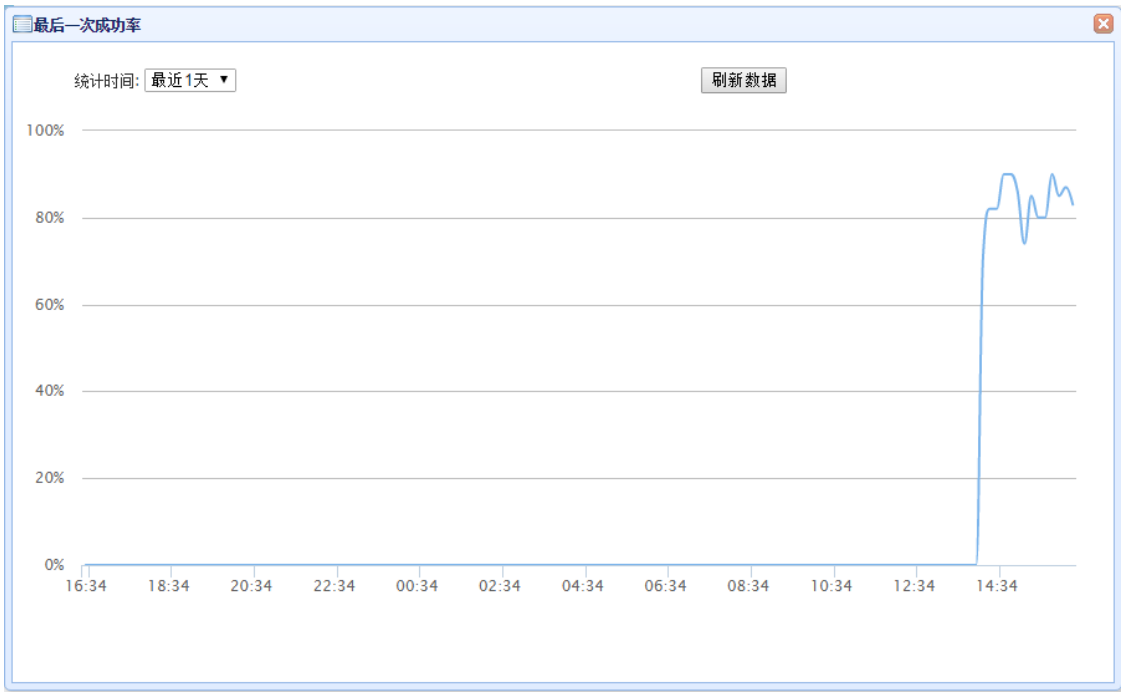
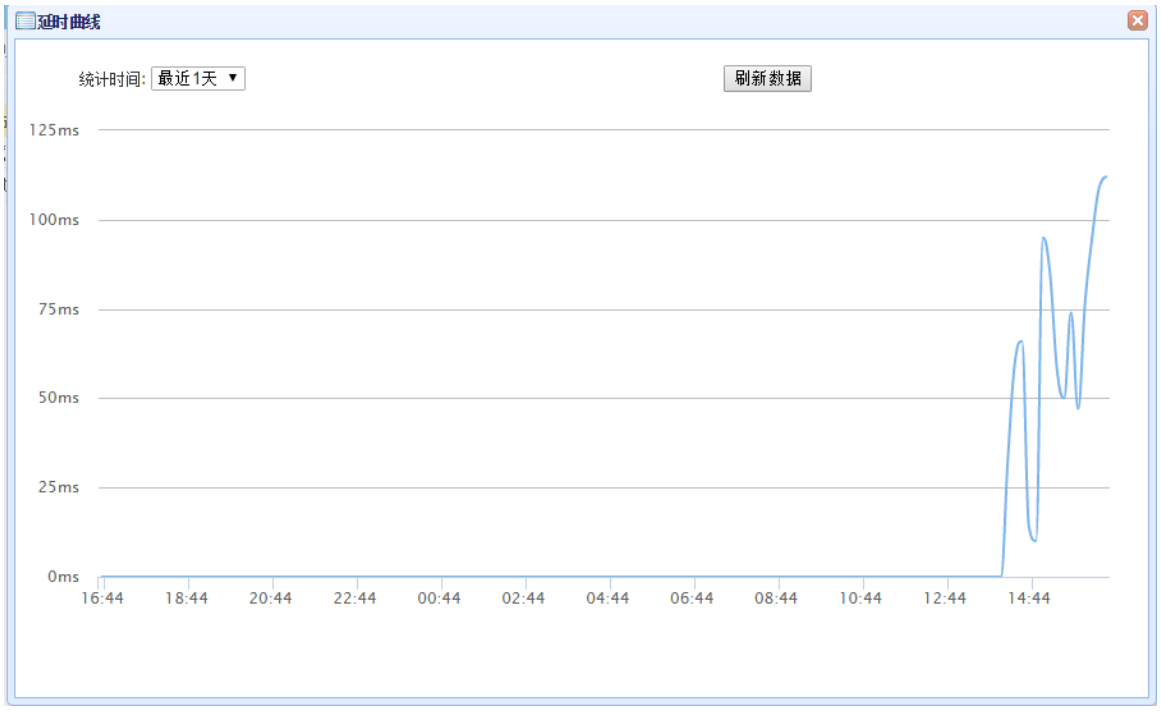


图9-68 查看服务质量管理条目延时结果



9.4.4 DNS 服务质量管理

配置需求

对目标进行 DNS 服务质量管理探测。

配置思路

(1) 配置设备的接口、路由、NAT、安全策略、DNS。

(2) 配置 DNS 服务质量管理条目。

(3) 查看该管理条目的探测结果。

配置步骤

(4) 进入“网络管理>接口>物理接口”，点击操作。

图9-69 配置物理接口 ge1-2

图9-70 配置物理接口 ge1-0

(5) 配置 NAT

进入“网络配置>NAT>源 NAT”，点击<新建>。

图9-71 配置 NAT 规则

(6) 配置静态路由

进入“网络配置>路由>静态路由”，点击<新建>。

图9-72 配置静态路由

(7) 配置 IPv4 策略

进入“上网行为管理>策略配置>IPv4 策略”，点击<新建>。

图9-73 配置 IPv4 策略

(8) 配置 DNS

进入“网络配置>DNS 服务器”。

图9-74 配置 DNS 服务器

(9) 配置 DNS 服务质量管理条目

进入“网络优化>服务质量管理”，点击<新建>。

图9-75 配置服务质量管理

图9-76 查看服务质量管理条目成功率结果

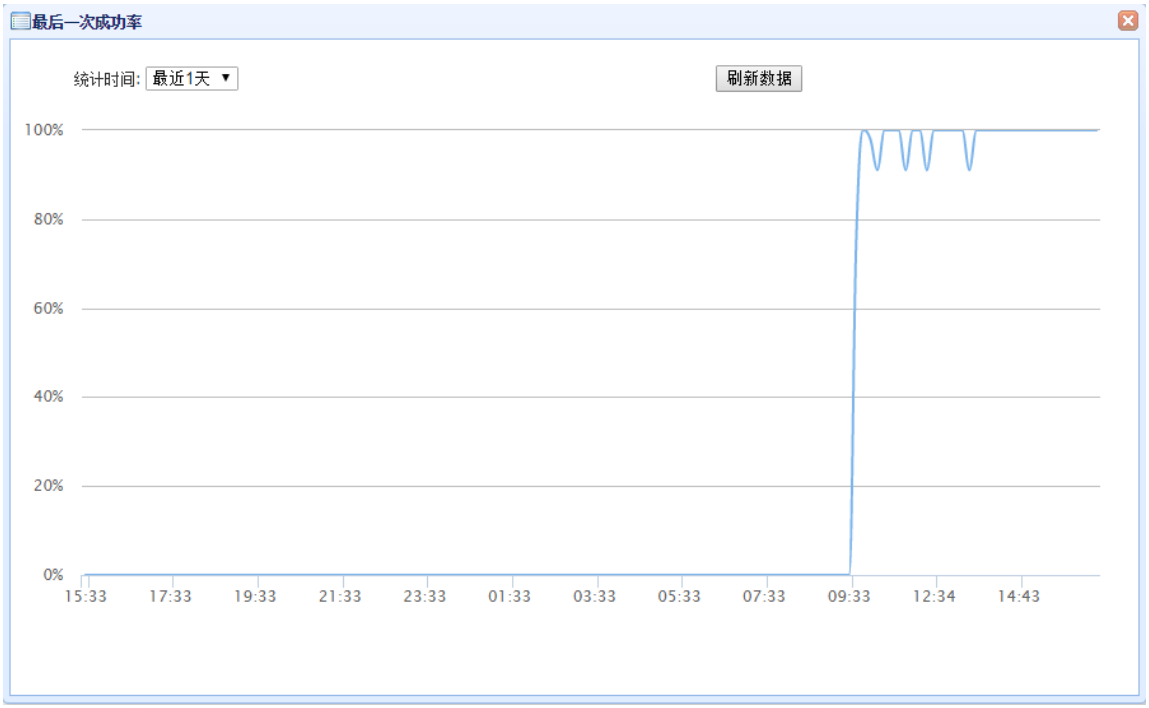
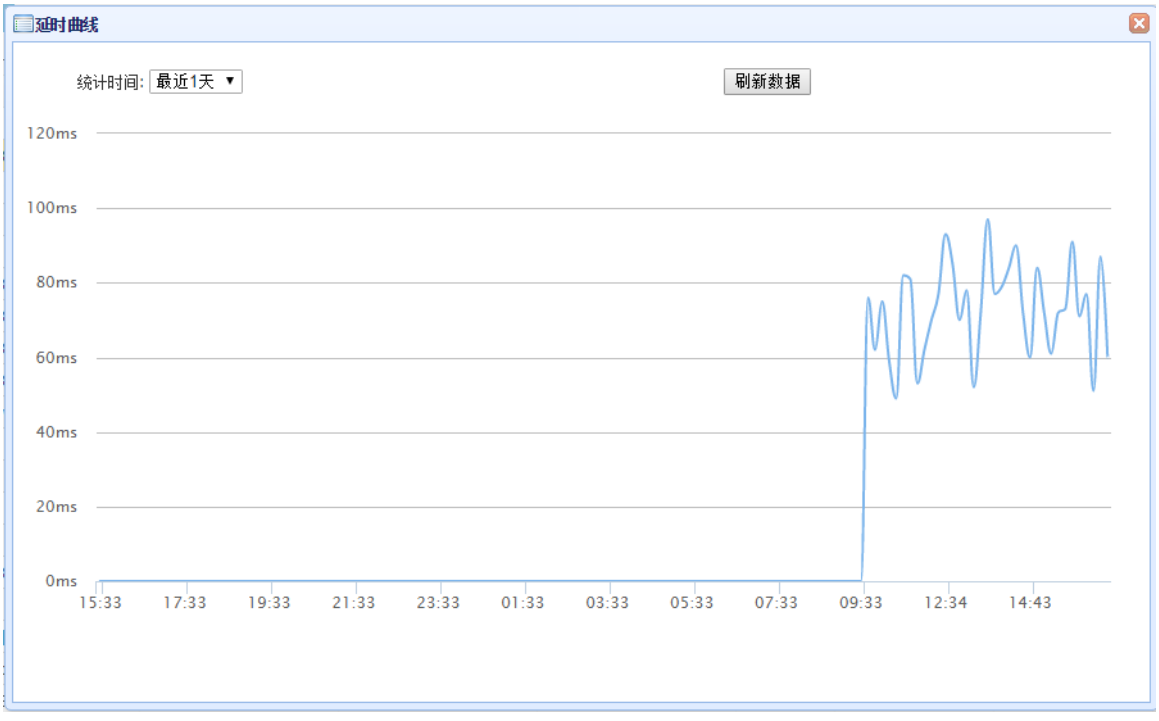


图9-77 查看服务质量管理条目延时结果



9.4.5 TCP 服务质量管理

配置需求

对目标进行 TCP 服务质量管理探测。

配置思路

(1) 配置设备的接口、路由、NAT、安全策略、DNS。

(2) 配置 TCP 服务质量管理条目。

(3) 查看该管理条目的探测结果。

配置步骤

(4) 进入“网络管理>接口>物理接口”，点击操作。

图9-78 配置物理接口 ge1-2

图9-79 配置物理接口 ge1-0

(5) 配置 NAT

进入“网络配置>NAT>源 NAT”，点击<新建>。

图9-80 配置 NAT 规则

(6) 配置静态路由

进入“网络配置>路由>静态路由”，点击<新建>。

图9-81 配置静态路由

(7) 配置 IPv4 策略

进入“上网行为管理>策略配置>IPv4 策略”，点击<新建>。

图9-82 配置 IPv4 策略

(8) 配置 DNS

进入“网络配置>DNS 服务器”。

图9-83 配置 DNS 服务器

(9) 配置 TCP 服务质量管理条目

进入“网络优化>服务质量管理”，点击<新建>。

图9-84 配置服务质量管理

图9-85 查看服务质量管理条目成功率结果

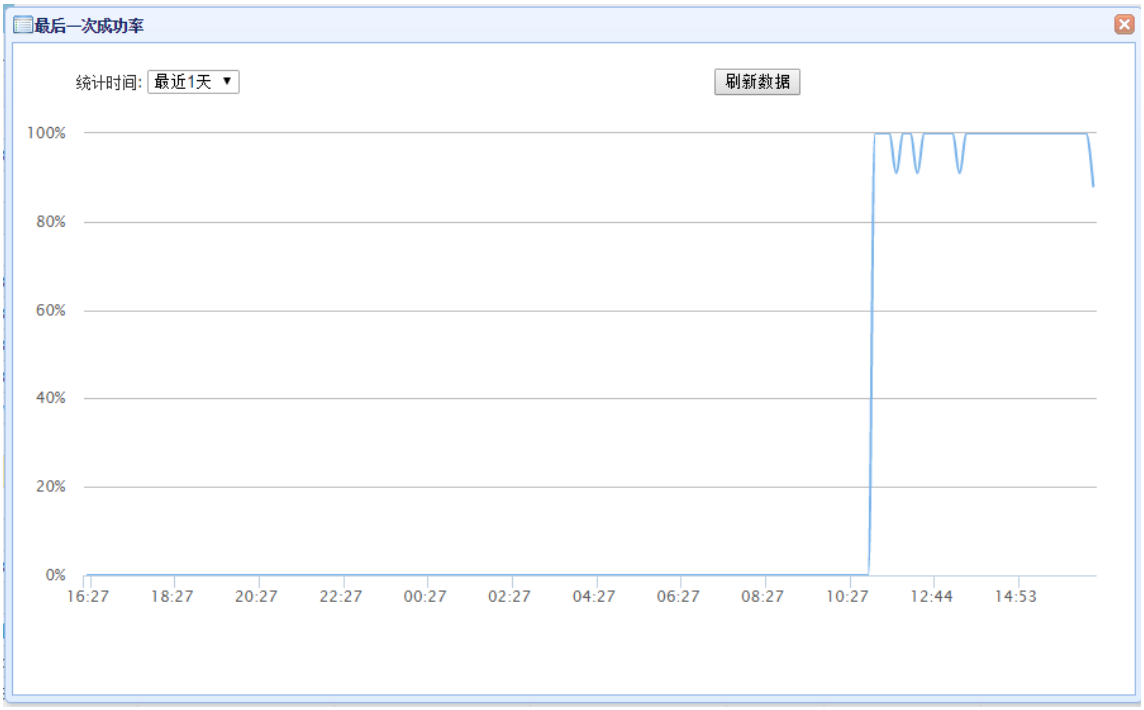
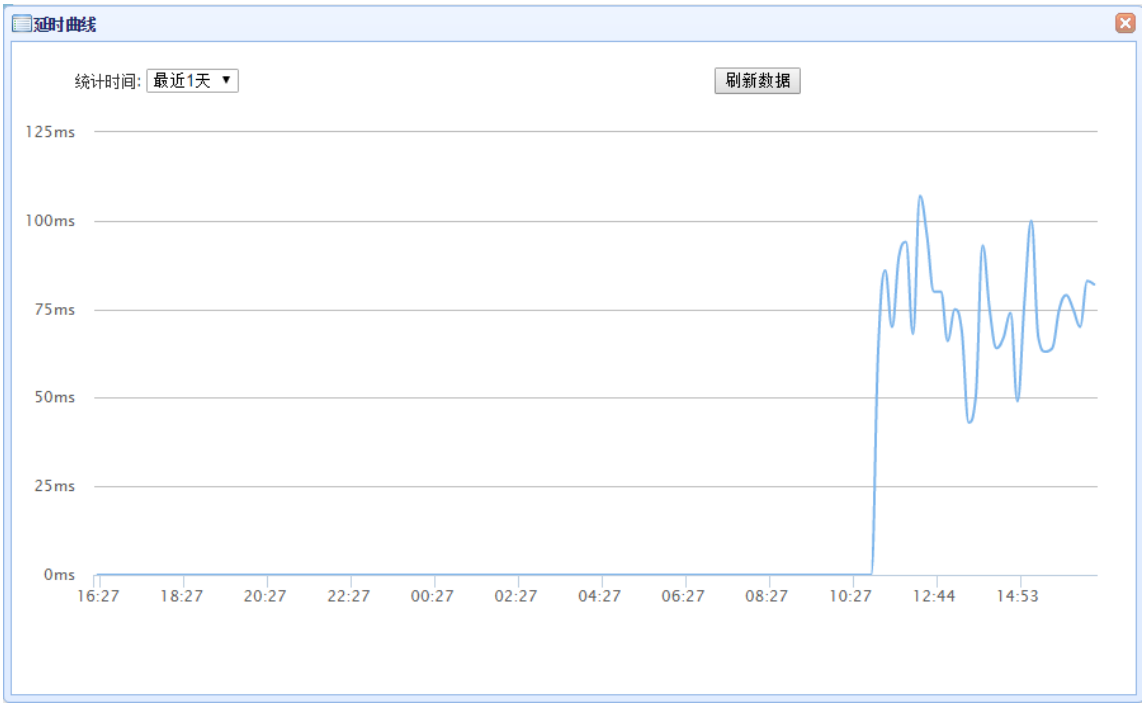


图9-86 查看服务质量管理条目延时结果



10 日志分析与管理平台（R0303 以及以下版本）

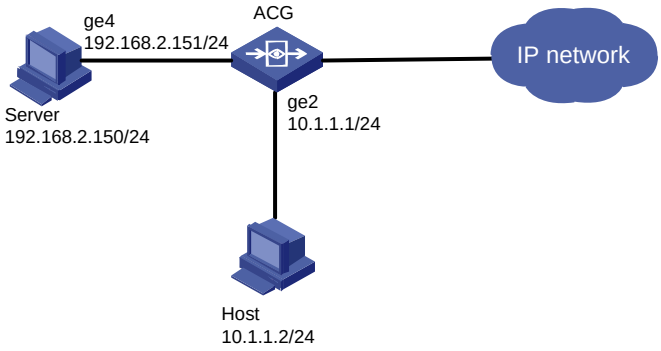
10.1 日志分析与管理平台简介

日志分析与管理平台是我公司自主研发的业界领先的设备集中管理产品，可以管理大量ACG设备，可以通过设备发送的数据进行独立的分析，日志分析与管理平台的特点包括：流量监控，设备管理，策略管理，日志查询，统计报表，数据库备份等重要功能。

10.2 日志分析与管理平台与ACG设备连接

10.2.1 组网图

图10-1 日志分析与管理平台管理设备组网图



10.2.2 配置步骤

(1) 配置 ACG 设备的日志服务器，登录 web 界面，进入系统管理>日志设定>日志服务器，填写服务器 IP，开启启用按钮。

(2) 配置设备的日志过滤，进入系统管理>日志设定>日志过滤，选择要过滤的和记录的日志类型。

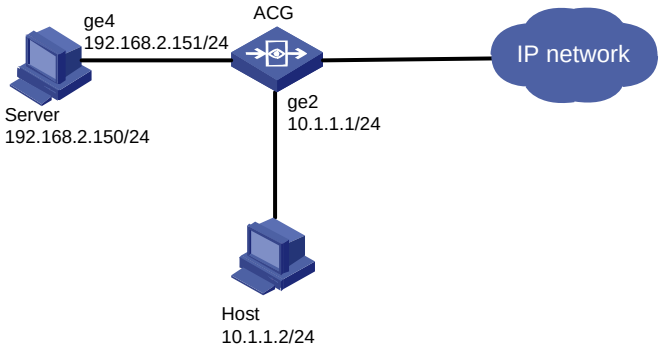
(3) 配置安全策略审计，进入上网行为管理〉策略配置〉IPV4 策略。新建一条策略，匹配条件为默认 any，开启应用审计和 URL 审计，点击确定提交。

(4) 日志分析与管理平台添加该设备，输入正确的 IP 地址、用户名、密码，使日志分析与管理平台正确添加该设备。

10.3 日志分析与管理平台日志查询

10.3.1 组网图

图10-2 日志分析与管理平台管理日志组网图



10.3.2 配置步骤

(1) 确保设备和日志分析与管理平台配置正确，包括添加策略，配置日志服务器，配置日志过滤，并且日志分析与管理平台正确添加该设备。

(2) 确保服务器上五项服务正常开启，在服务器上，进入控制面板>管理工具>服务，进入服务确保日志分析与管理平台的五项服务正常开启。

(3) 确保设备和日志分析与管理平台可以连通，日志分析与管理平台添加设备后设备显示正常在线状态。

(4) 各项信息配置无误后，点击日志查询查询日志类型，其中包括设备操作日志、系统事件日志、NAT 日志、上网行为日志、用户综合日志等。

10.4 日志分析与管理平台自动备份还原

10.4.1 配置部署

(1) 配置数据库自动备份，登录日志分析与管理平台，系统管理〉数据库备份还原，选择是否备份报表文件，填写备份路径，选择自动备份数据库开启，点击确定按钮，成功配置自动备份数据库，选择自动备份数据库关闭，点击确定按钮，成功配置关闭自动备份数据库。

(2) 配置立即备份当月数据库路径，点击立即备份当月数据库。

(3) 配置立即备份全部数据库路径，点击立即备份全部数据库。

(4) 在还原路径上填写正确的备份路径，还原自动备份数据库、当月数据库、全部数据库，确保备份还原数据库信息正确。

10.4.2 注意事项

(1) 配置好数据库自动备份设置以后，可以修改路径备份立即当月或者备份立即全部，不会对之前配置的自动备份产生影响。

(2) 配置好自动备份后，下个月以后的每月第一天 0 点开始进行自动备份。

(3) 立即备份全部数据库的备份信息，不会在备份结果中显示，备份结果中只会显示立即备份当月和自动备份数据库的信息。

(4) 数据库还原路径，允许多个文件还原，也允许单次还原，并且在还原时要严格按照备份顺序进行还原。

(5) 在还原时，不允许全部数据库和当月数据进行同时还原。

11 日志分析与管理平台（R0304 以及以上版本）

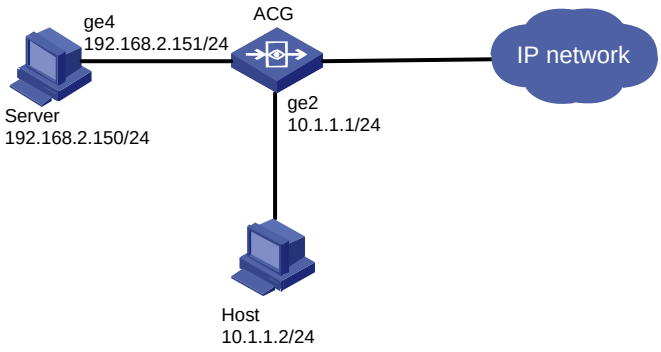
11.1 日志分析与管理平台简介

日志分析与管理平台是我公司自主研发的业界领先的设备集中管理产品，可以管理大量ACG设备，可以通过设备发送的数据进行独立的分析，日志分析与管理平台的特点包括：流量监控，设备管理，策略管理，日志查询，统计报表，数据库备份等重要功能。

11.2 日志分析与管理平台与ACG设备连接

11.2.1 组网图

图11-1 日志分析与管理平台管理设备组网图



11.2.2 配置步骤

(1) 配置 ACG 设备的日志服务器，登录 web 界面，进入系统管理>日志设定>日志服务器，填写服务器 IP，开启启用按钮。

(2) 配置设备的日志过滤，进入系统管理>日志设定>日志过滤，选择要过滤的和记录的日志类型。

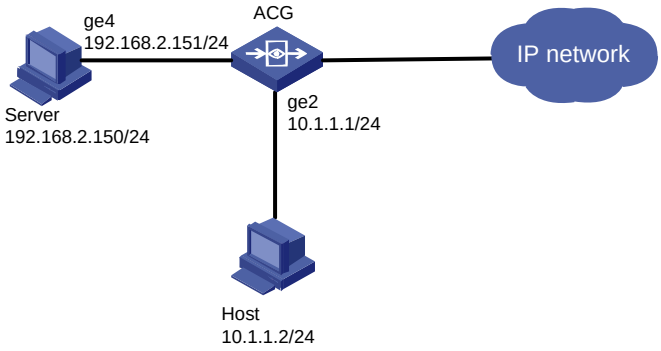
(3) 配置安全策略审计，进入上网行为管理〉策略配置〉IPV4 策略。新建一条策略，匹配条件为默认 any，开启应用审计和 URL 审计，点击确定提交。

(4) 日志分析与管理平台添加该设备，输入正确的 IP 地址、用户名、密码，使日志分析与管理平台正确添加该设备。

11.3 日志分析与管理平台日志查询

11.3.1 组网图

图11-2 日志分析与管理平台管理日志组网图



11.3.2 配置步骤

(1) 确保设备和日志分析与管理平台配置正确，包括添加策略，配置日志服务器，配置日志过滤，并且日志分析与管理平台正确添加该设备。

(2) 确保设备和日志分析与管理平台可以连通，日志分析与管理平台添加设备后设备显示正常在线状态。

(3) 各项信息配置无误后，点击日志查询查询日志类型，其中包括设备操作日志、系统事件日志、NAT 日志、上网行为日志、用户综合日志等。

11.4 关闭/启动服务

如系统出现异常需要重新启动服务，可以通过关闭/开启命令来重启服务。无需将整个服务器重启。

如需关闭服务，需要执行如下命令：

```
sh /home/datacenter_init/datacenter_shutdown.sh
```

手动关闭服务后，需要手动执行脚本启动所有服务。启动服务需要执行如下命令：

```
sh /home/datacenter_init/datacenter_start.sh
```