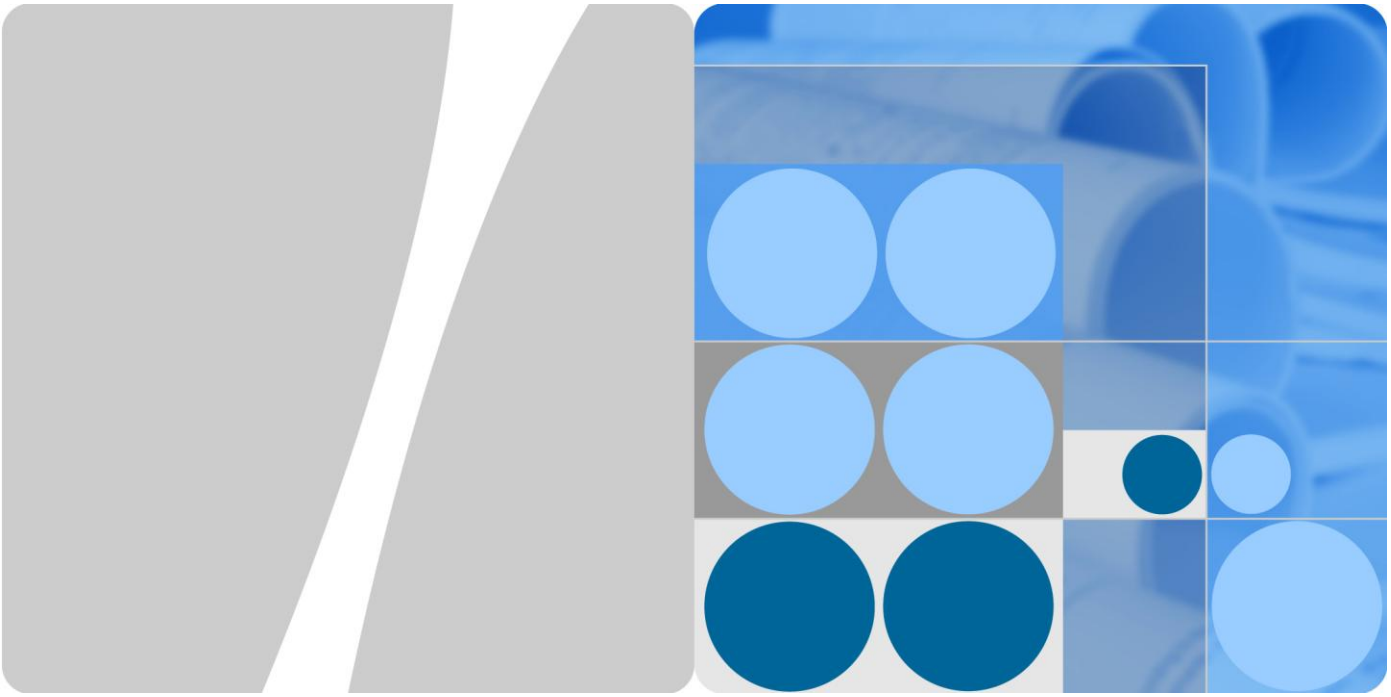


华为 SIG9800-X 系列 业务智能网关产品

产品概述

文档版本 01

发布日期 2012-10-12

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

前 言

概述

本文档介绍了 SIG 系统的软硬件组成、网络部署、业务与功能、操作与维护、可靠性设计、技术指标、设备遵循的标准和通过的认证。

本文档用于帮助读者了解 SIG 系统的定位、基本功能及主要规格，可以作为入门级学习的参考资料。

产品声明

- SIG 在提供业务、服务或维护过程中，将涉及个人数据的使用，同时具备相应的保护措施。您需遵循所适用国家的法律或公司用户隐私政策采取足够的措施，以确保用户的个人数据受到充分的保护。
- 根据您的要求，出于保障网络运营和服务的目的，可能涉及使用或存储个人用户某些通信内容。本公司无法单方采集或存储用户通信内容。建议您只有在所适用法律法规允许的目的和范围内方可启用相应的功能。在使用、存储用户通信内容的过程中，您应采取足够的措施以确保用户的通信内容受到严格保护。

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
危险	表示有高度潜在危险，如果不能避免，会导致人员死亡或严重伤害。
警告	表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
注意	表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
窍门	表示能帮助您解决某个问题或节省您的时间。
说明	表示是正文的附加信息，是对正文的强调和补充。

图形界面元素引用约定

格式	意义
“”	带双引号“”的格式表示各类界面控件名称和数据表，如单击“确定”。
>	多级菜单用“>”隔开。如选择“文件 > 新建 > 文件夹”，表示选择“文件”菜单下的“新建”子菜单下的“文件夹”菜单项。

修订记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 01 (2012-10-12)

第一次正式发布。

目 录

1 系统简介

基于 SIG 系统的深度运营解决方案，可以帮助网络服务提供商（如广电客户）客户应对目前网络转型所带来的挑战，通过流量的可视化，实现细粒度的流量管理，提供差异化、个性化的增值服务，助力客户实现精细化运营网络的目的。

对于其它行业用户，如企业、教育机构、政府机构，也可以通过 SIG 提供的网络可视化、智能流量管理等解决方案，有效控制企业/机构宝贵带宽资源的滥用，解决网络拥塞问题，保障关键业务的服务质量，减缓扩容压力，提升员工上网体验；同时还可有效管理员工的上网行为。

系统定位

SIG9800-X 系统（以下简称 SIG 系统）是基于华为成熟高端路由器硬件平台开发的大容量专用业务感知系统，能够按动态的灵活策略实现高密度大容量端口（10G POS、GE 和 10GE WAN/LAN 等）的带宽管理。

SIG 系统利用多项专利检测技术，通过高性能的硬件平台实现网络数据报文的分析和处理，并辅助提供智能的、灵活的业务控制手段，可以在各种网络中实现流量分析、带宽管理及网络安全防护等多种功能。同时，SIG 系统支持分布式部署和集中管理，可灵活扩展。

系统特点

- 业内领先的高性能硬件平台

  SIG9800-X 硬件平台继承了华为高端路由器的优良架构设计特性，提供电信路由器级别的高性能和高可用性。满足了设备数据处理的实时性、高性能、低功耗等要求，又满足了低网络时延、高传输质量的要求，性能超越业界同类产品。

- 全方位的网络安全防护

  通过具有 6500 万条以上网址的自研 URL 分类库，SIG 系统能够过滤绝大多数包含有害信息的站点。帮助客户净化网络环境，有助于客户开展相关的增值服务。

- 精细粒度的带宽管理

  在全面的应用识别、用户识别和流量流向识别的基础上，可针对 AS 域、链路、大客户、公众客户、虚通道（可用于扩展已有的业务对象，定制化能力更强）和子网等指定不同的带宽管理策略，通过 QoS 管理等方式实现基于不同应用的分时

段、分区域、分用户的细粒度的带宽控制，真正做到让带宽按需分配，提高网络带宽的利用率。

- 强大的流量和协议分析能力
  - SIG 系统采用业务感知技术，分析不同用户、区域、链路、AS 域组、子网、流向、虚通道等流量对象上的流量分布、流量趋势和流量流向，全面掌握网络中的流量、协议及业务分布，为合理规划网络、制定流量控制策略、深度挖掘网络商业价值提供依据。
  - 通过启发式行为分析检测，结合数据包协议分析和特征匹配技术，SIG 系统对网络层到应用层的数据进行全面分析，可以准确识别 P2P、VoIP、IM、Video、Game、Stock 等数十类多达 1100 种以上的应用协议，支持以协议特征、流量特征、连接数特征等多种组合条件进行数据分析及检测。
- 智能的知识库自动升级

  通过华为统一安全知识库升级网站，SIG 系统能够更新最新的协议特征库、恶意流量特征库和 URL 分类库。升级过程无需人工干预，操作简单，便于管理，而且升级过程不会中断系统业务正常运行。
- 强大灵活的管理能力和专业的报表

  SIG 系统通过 B/S 架构的专业网管系统，进行策略管理、用户管理和报表管理。专业的报表系统支持多种输出格式，同时具有柱状图、饼状图和曲线图等丰富的表现形式；提供按链路/区域/用户进行分业务的实时统计分析报表，通过对存储于后台数据库的分析数据进行更详尽的深度挖掘分析，为客户开展用户行为分析等新业务提供数据支持。
- 易于扩展的模块化架构设计

  SIG 系统支持前台分布式部署，后台集中统一分析，具备高可扩展性，可通过灵活的功能扩展来满足客户业务发展的需要，并可以随着新链路的接入而平滑扩容升级，保护客户已有的投资。
- 支持多种接口类型

  SIG9800-X 提供多种不同类型的接口板，支持 10G POS、10G WAN、10G LAN、GE 等丰富的网络接口类型。链路升级不需要进行设备替换，仅通过替换接口板的插卡即可完成，提升设备的使用周期。

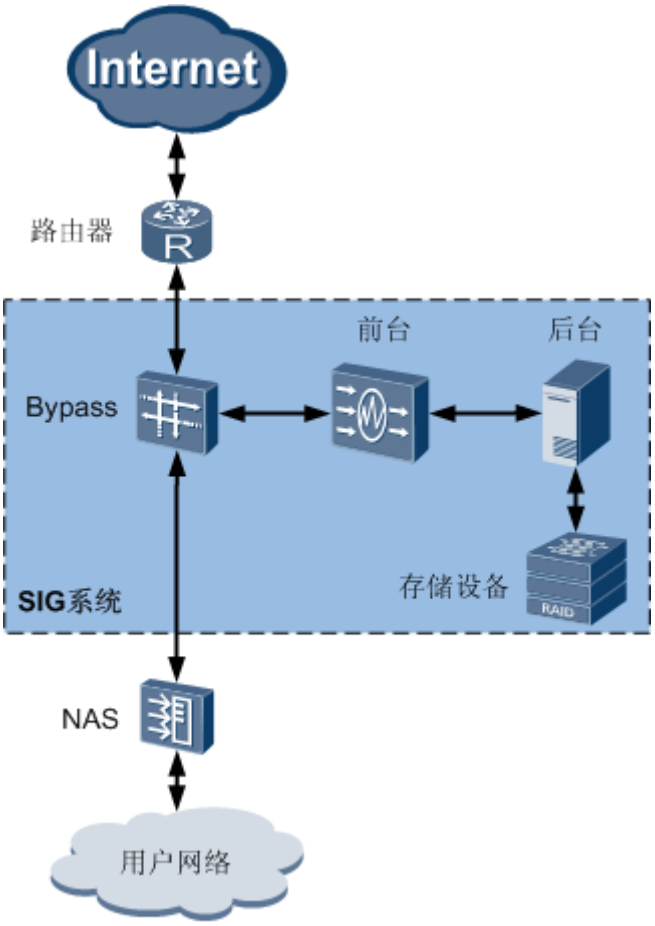
2 系统组成

2.1 硬件组成

SIG 系统主要由前台（SIG9800-X 设备）和后台（服务器）组成。根据网络部署模式和可靠性部署要求，可能还包括存储设备、Bypass 等设备。

SIG 系统典型物理组网如图 2-1 所示。其中前台通过 Bypass 设备直路部署于网络中，SIG 系统正常时流量经过 Bypass 设备到前台进行处理，SIG 系统异常时流量可以直接经过 Bypass 设备，不受前台直路部署的影响。

图2-1 SIG 系统物理组网



NAS（Network Access Server）网络接入服务器

2.1.1 前台

前台设备型号包括 SIG9800-X3、SIG9800-X8 和 SIG9800-X16。在使用 SIG 系统前，您需要了解前台设备的功能、外观和技术参数。

功能

SIG 前台采用华为公司专用硬件平台，主要实现流量监控、策略执行和应用，以及上报统计数据。

外观

SIG9800-X3/X8/X16 采用一体化机箱，SIG9800-X3 直流机箱高度是 4U（1U=44.45mm），SIG9800-X3 交流机箱高度是 5U，SIG9800-X8 直流机箱高度是 14U，SIG9800-X16 直流机箱高度是 32U，均可以安装在 N68E-22 机柜和深度尺寸不小于 800mm 的 IEC（International Electrotechnical Commission）19 英寸标准机柜中。设备外观分别如图 2-2、图 2-3 和图 2-4 所示。

图2-2 SIG9800-X3 直流和交流设备外观图

图2-3 SIG9800-X8 直流设备外观图

图2-4 SIG9800-X16 直流设备外观图

技术参数

SIG9800-X3/X8/X16 设备的技术参数分别如表 2-1、表 2-2 和表 2-3 所示。

表2-1 SIG9800-X3 的物理规格

项目	参数
外形尺寸（宽×深×高）[a]	直流电源机箱：442mm×650mm×175mm（4U） 交流电源机箱：442mm×650mm×220mm（5U）
安装	可安装在 N68E 机柜或 19 英寸标准机柜中
典型功耗	配置 1 块接口线路处理板 LPUF-40-A、2 块业务板 SPUA 和 2 块 MPU 的情况下： • 直流：1245 W • 交流：1283 W
最大功率	配置 1 块接口线路处理板 LPUF-40-A、2 块业务板 SPUA 和 2 块 MPU 的情况下： • 直流：1352 W

项目		参数
		• 交流：1393 W
散热值		3569 BTU/小时
重量	空机箱	直流：15kg 交流：25kg
	满配置	配置 1 块接口线路处理板 LPUF-40-A、2 块业务板 SPUA 和 2 块 MPU 的情况下： • 直流：42kg • 交流：52kg
直流输入电压	额定电压	-48V
	最大电压范围	-72V～-38V
交流输入电压	额定电压	175V AC～275V AC；50/60Hz
	最大电压范围	90V AC～275V AC；50/60Hz
系统可靠性	MTBF(年)	25
	MTTR(小时)	0.5
工作环境温度[b]	长期[c]	0°C～45°C
	短期	-5°C～55°C
存储温度		-40°C～70°C
工作环境相对湿度	长期	5%RH～85%RH，不结露
	短期	0%RH～95%RH，不结露
存储相对湿度		0%RH～95%RH
长期工作海拔高度		小于 3000m
存储海拔高度		小于 5000m
说明 a.“宽”为不带挂耳的尺寸。 b.温度和湿度，是指在机架前后没有保护板的情况下，距地板以上 1.5m 和距机架前方 0.4m 处测量的数值。 c.短期是指连续不超过 48 小时和每年累计不超过 15 天。超过上述值为长期。		

表2-2 SIG9800-X8 的物理规格

项目	描述
外形尺寸（宽×深×高）[a]	442mm×650mm×620mm（14U）

项目		描述
安装		可安装在 N68E 或 19 英寸标准机柜中
重量	空机箱	43.2kg
	满配置	配置 2 块接口线路处理板 LPUF-40-A、6 块业务板 SPUA、1 块 SFU 和 2 块 SRU 的情况下： 79kg
典型功耗		配置 2 块接口线路处理板 LPUF-40-A、6 块业务板 SPUA、1 块 SFU 和 2 块 SRU 的情况下： 2860W
最大功率		配置 2 块接口线路处理板 LPUF-40-A、6 块业务板 SPUA、1 块 SFU 和 2 块 SRU 的情况下： 3436W
散热值		9084 BTU/小时
直流（DC）输入电压	额定电压	-48V
	最大电压范围	-72V～-38V
交流（AC）输入电压	额定电压	175V AC～275V AC；50/60Hz
	最大电压范围	90V AC～275V AC；50/60Hz
系统可靠性	MTBF(年)	25
	MTTR(小时)	0.5
工作环境温度 [b]	长期 [c]	0°C～45°C
	短期	-5°C～55°C
	备注	温度变化速率限制：30°C/小时
存储温度		-40°C～70°C
工作环境相对湿度	长期	5%RH～85%RH，不结露
	短期	0%RH～95%RH，不结露
存储相对湿度		0%RH～95%RH
长期工作海拔高度		小于 3000 米
存储海拔高度		小于 5000 米

项目	描述
说明 a.“宽”为不带挂耳的尺寸。 b.温度和湿度，是指在机架前后没有保护板的情况下，距地板以上 1.5m 和距机架前方 0.4m 处测量的数值。 c.短期是指连续不超过 48 小时和每年累计不超过 15 天。超过上述值为长期。	

表2-3 SIG9800-X16 的物理规格

项目		描述
外形尺寸（宽×深×高）[a]		442mm×650mm×1420mm（32U）
安装		可安装在 N68E 或 19 英寸标准机柜中
重量	空机箱	94.4kg
	满配置	配置 4 块接口线路处理板 LPUF-40-A、12 块业务板 SPUA、4 块 SFU 和 2 块 MPU 的情况下： 240kg
典型功耗		配置 4 块接口线路处理板 LPUF-40-A、12 块业务板 SPUA、4 块 SFU 和 2 块 MPU 的情况下： 5450W
最大功率		配置 4 块接口线路处理板 LPUF-40-A、12 块业务板 SPUA、4 块 SFU 和 2 块 MPU 的情况下： 6595W
散热值		17390 BTU/小时
直流（DC）输入电压	额定电压	-48V
	最大电压范围	-72V～-38V
交流（AC）输入电压	额定电压	175V AC～275V AC；50/60Hz
	最大电压范围	90V AC～275V AC；50/60Hz
系统可靠性	MTBF(年)	25
	MTTR(小时)	0.5
工作环境温度 [b]	长期 [c]	0°C～45°C
	短期	-5°C～55°C
	备注	温度变化速率限制：30°C/小时
存储温度		-40°C～70°C

项目		描述
工作环境相对湿度	长期	5%RH～85%RH，不结露
	短期	0%RH～95%RH，不结露
存储相对湿度		0%RH～95%RH
长期工作海拔高度		小于 3000 米
存储海拔高度		小于 5000 米
说明 a.“宽”为不带挂耳的尺寸。 b.温度和湿度，是指在机架前后没有保护板的情况下，距地板以上 1.5m 和距机架前方 0.4m 处测量的数值。 c.短期是指连续不超过 48 小时和每年累计不超过 15 天。超过上述值为长期。		

2.1.2 后台

华为 RH2288 V2 机架式服务器

在行业的绝大多数场景中，后台推荐使用华为 RH2288 V2 服务器。该服务器无需配套存储设备和交换机使用。

功能

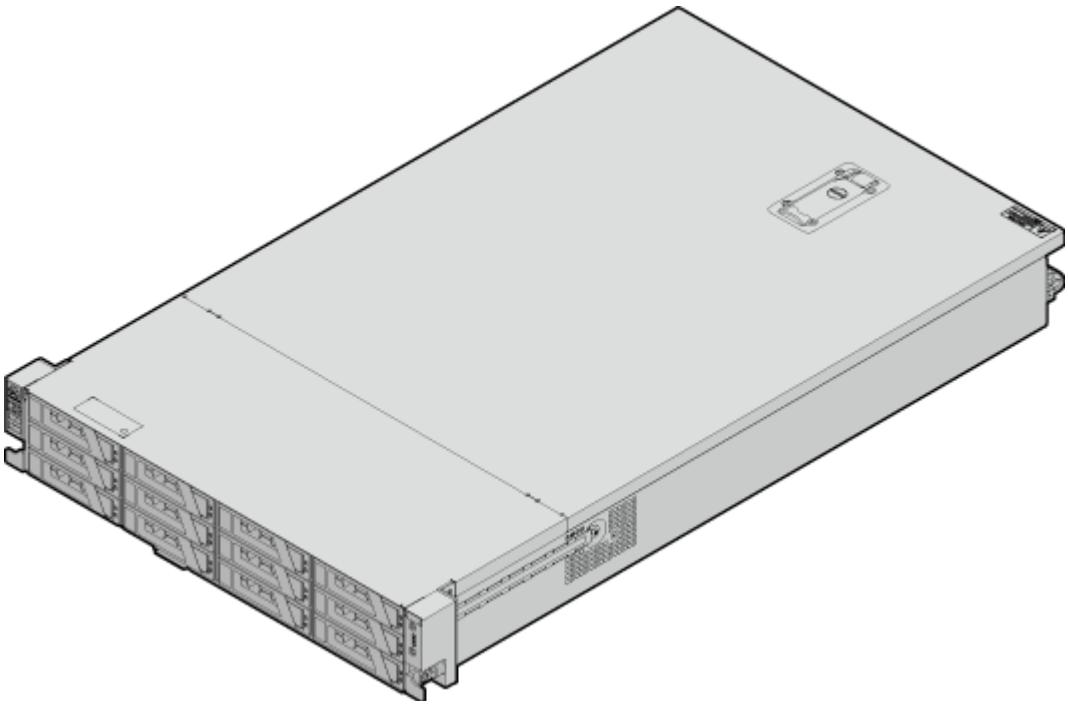
在 SIG 系统中主要完成策略配置、报表统计等功能。

外观

RH2288 V2 服务器高度为 2U，可以安装在满足 IEC（International Electrotechnical Commission）297 标准的宽 19 英寸、深 1000mm 以上的通用机柜中。需要注意，由于进深不同，该服务器无法使用 SIG 前台设备的 19 英寸标准机柜。

设备外观如图 2-5 所示。

图2-5 RH2288 V2 外观



技术参数

RH2288 V2 的技术参数如表 2-4 所示。

表2-4 RH2288 V2 技术参数

名称		参数
外形尺寸（宽×深×高）[a]		87.3 mm(2U)×447 mm×760 mm
功率		422W
满配重量		36.4Kg
额定输入电压	额定电压	交流模块：100V AC ～ 120V AC 或200V AC ～ 240V AC 直流模块：－36V DC ～－72V DC
工作环境温度[b]	长期[c]	10°C ～ 35°C
工作环境湿度		8%～85% 非凝结
存储环境湿度		5%～95% 非凝结

名称	参数
说明 a：“宽”为不带挂耳的尺寸。 b：温度和湿度，是指在机架前后没有保护板的情况下，距地板以上 1.5m 和距机架前方 0.4m 处测量的数值。 c：短期是指连续不超过 48 小时和每年累计不超过 15 天。超过上述值为长期。	

华为 T8223 刀片服务器

在对后台可靠性要求非常严苛的场景下，后台推荐使用华为 T8223 刀片服务器。T8223 刀片服务器需要配合存储设备及交换机共同组成后台系统。

功能

在 SIG 系统中主要完成策略配置、报表统计等功能。

外观

T8223 机箱高度为 14U，可以安装在 N68E-22 或 19 英寸标准机柜中。设备前视图和后视图如图 2-6 所示。

图2-6 T8223 机箱前、后视图

技术参数

T8223 的技术参数如表 2-5 所示。

表2-5 T8223 的技术参数

名称		参数
外形尺寸（宽×深×高）[a]		436mm×450mm×619.5mm
最大功率		2600W（配套 SIG 使用时的最大功率）
重量	空机箱	30kg
	满配置	105kg
直流输入电压	额定电压	－48V～-60V
	最大电压范围	－40.5V～－72V
工作环境温度[b]	长期[c]	5℃～40℃
	短期	－5℃～55℃
存储环境温度		－40℃～70℃
工作环境湿度	长期	5%～85%
	短期	5%～90%
存储环境湿度		10%～95%

说明

a：“宽”为不带挂耳的尺寸。

b：温度和湿度，是指在机架前后没有保护板的情况下，距地板以上 1.5m 和距机架前方 0.4m 处测量的数值。

c：短期是指连续不超过 48 小时和每年累计不超过 15 天。超过上述值为长期。

2.1.3 存储设备

在使用 SIG 系统前，您需要了解存储设备的功能、外观和技术参数。需要注意，当选用 RH2288 V2 服务器作为后台服务器时，则不需要配置存储设备。

功能

存储设备推荐使用华为 S2600T 磁盘阵列。其主要负责存储系统中的策略、用户信息、报表数据等所有数据文件，保证后台数据的可靠性。

外观

S2600T 由控制框和磁盘扩展框组成，可以安装在 N68E-22 或 19 英寸标准机柜中。控制框外观如图 2-7 和图 2-8 所示，磁盘框外观如图 2-9 和图 2-10 所示。

图2-7 S2600T 控制框前视图

图2-8 S2600T 控制框后视图

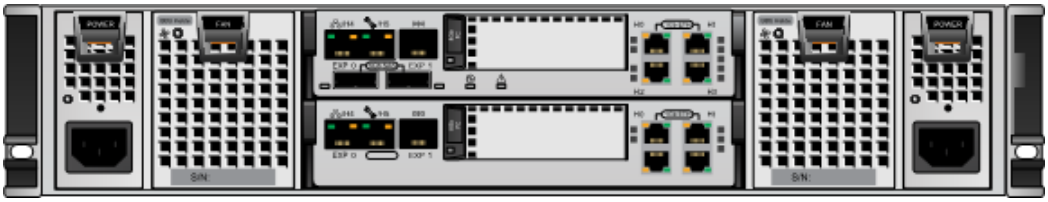


图2-9 S2600T 硬盘框前视图

图2-10 S2600T 硬盘框后视图

技术参数

S2600T 的技术参数如表 2-6 和表 2-7 所示。

表2-6 S2600T 控制框的技术参数

名称		参数
外形尺寸（宽×深×高）[a]		446mm×582mm×86.1mm
重量	空框 [b]	22.98kg
	满配置	30.9kg
功率	峰值功率	380W
	运行功率	350W
	空载功率	280W
交流输入电压	额定电压	110V，50Hz/60Hz 220V，50Hz/60Hz
	最大电压范围	100V～127V 或 200V～240V
直流输入电压	额定电压	-48V
	最大电压范围	-36V～-76V
可靠性	MTBF	700000 小时
	MTTR	2 小时
温度	工作环境温度 [c]	海拔低于 1800m 时：5℃～40℃ 海拔为 1800m～3000m 时：5℃～30℃
	存储环境温	-20℃～60℃

名称		参数
	度	
湿度	工作环境湿度	5% RH～90% RH
	存储环境湿度	5% RH～95% RH
说明 a：“宽”为不带挂耳的尺寸。 b：空框重量是指不安装硬盘时的重量。 c：温度和湿度，是指在机架前后没有保护板的情况下，距地板以上 1.5m 和距机架前方 0.4m 处测量的数值。		

表2-7 磁盘框的技术参数

名称		参数
外形尺寸（宽×深×高）[a]		446mm×412mm×175mm
重量	空框 [b]	25.2kg
	满配置	42.6kg
功率	峰值功率	527W
	运行功率	441W
	空载功率	370W
交流输入电压	额定电压	110V，50Hz/60Hz 220V，50Hz/60Hz
	最大电压范围	100V～127V 或 200V～240V
直流输入电压	额定电压	-48V
	最大电压范围	-36V～-76V
可靠性	MTBF	700000 小时
	MTTR	2 小时
温度	工作环境温度 [c]	海拔低于 1800m 时：5℃～40℃ 海拔为 1800m～3000m 时：5℃～30℃
	存储环境温度	-20℃～60℃

名称		参数
湿度	工作环境湿度	5% RH～90% RH
	存储环境湿度	5% RH～95% RH
说明 a：“宽”为不带挂耳的尺寸。 b：空框重量是指不安装硬盘时的重量。 c：温度和湿度，是指在机架前后没有保护板的情况下，距地板以上 1.5m 和距机架前方 0.4m 处测量的数值。		

2.1.4 Bypass

在使用 SIG 系统前，您需要了解 Bypass 的功能、外观和技术参数。

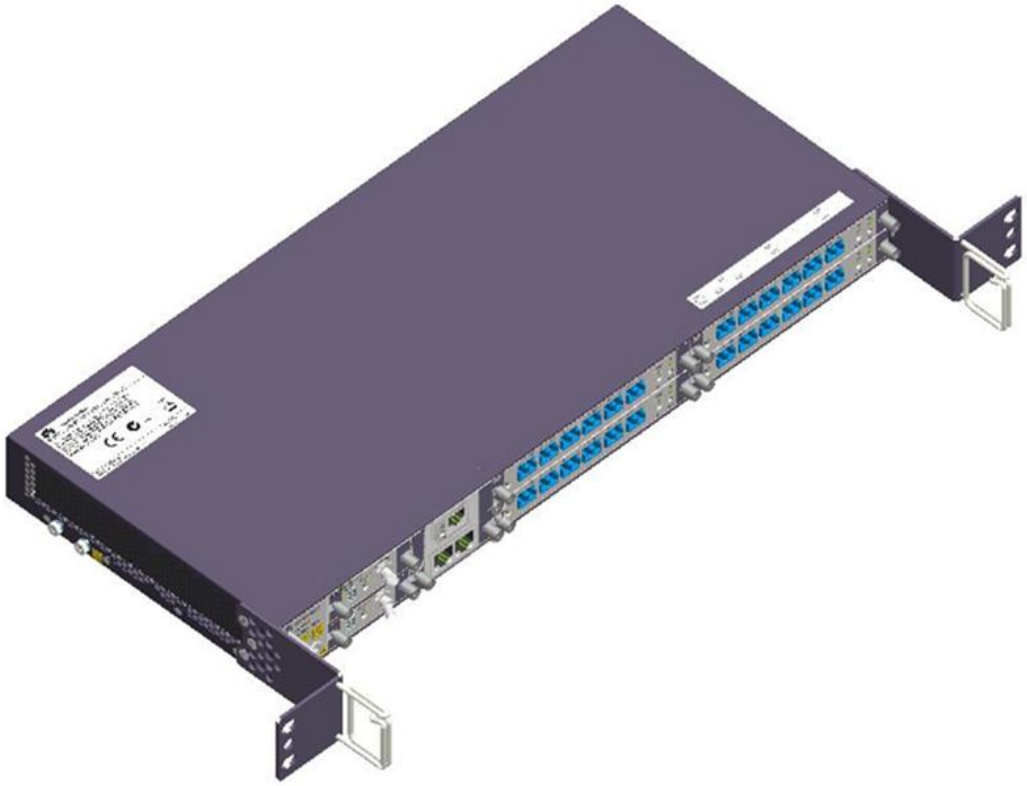
功能

外置 Bypass 推荐使用 OPLINK Bypass OPSSP，Bypass OPSSP 提供链路级的高可靠性，采用双通道光线路保护单板。

外观

Bypass OPSSP 机箱高度为 1U，可以安装在 N68E-22 或 19 英寸标准机柜中。设备外观如图 2-11 所示。

图2-11 Bypass OPSSP 设备外观图



技术参数

Bypass OPSSP 的技术参数如表 2-8 所示。

表2-8 Bypass OPSSP 的技术参数

名称	参数
外形尺寸（宽×深×高）[a]	436mm×195mm×44mm
最大功率	40W
重量	满配置 4kg
直流输入额定电压	-48V～-60V
工作环境温度 [b]	0℃～40℃
存储环境温度	－40℃～70℃
环境湿度	10%～90%
支持的链路数	4

名称	参数
说明 a：“宽”为不带挂耳的尺寸。 b：温度和湿度，是指在机架前后没有保护板的情况下，距地板以上 1.5m 和距机架前方 0.4m 处测量的数值。	

2.1.5 交换机

在使用 SIG 系统前，您需要了解交换机的功能、外观和技术参数。需要注意，当选用 RH2288 V2 服务器作为后台服务器时，则不需要配置交换机。

功能

交换机推荐使用华为 S5328C-EI 交换机，主要用于 SIG 系统各设备间的互联。使用两台交换机可以实现前、后台链路双归属，提高系统可靠性。

说明
S5328C-EI 为推荐交换机型号。根据网络中所需要的交换机接口数量的不同，可以选用其他型号的交换机。

外观

S5328C-EI 机箱高度为 1U，可以安装在 N68E-22 或 19 英寸标准机柜中。设备外观如图 2-12 所示。

图2-12 S5328C-EI 设备外观图

接口说明：

- 设备：24 个 10/100/1000Base-T 以太网接口
- 前插卡：4 个 1000M Base-X 光接口（如图 2-12 右下角所示）

技术参数

S5328C-EI 交换机的技术参数如表 2-9 所示。

表2-9 S5328C-EI 交换机技术参数

名称		参数
外形尺寸（宽×深×高）[a]		442.0mm×420.0mm×43.6mm
最大功率		60W
重量	空机箱	≤5kg

名称		参数
	满配置	≤8.5kg
直流输入电压	额定电压	－48V～－60V DC
	最大电压范围	－36V～－72V DC
交流输入电压	额定电压	100V～240V AC
	最大电压范围	90V～264V AC
温度	工作温度	0℃～50℃
	存储温度	－40℃～70℃
相对湿度		10% RH～90% RH
海拔高度		0m～2000m
说明 a：“宽”为不带挂耳的尺寸。		

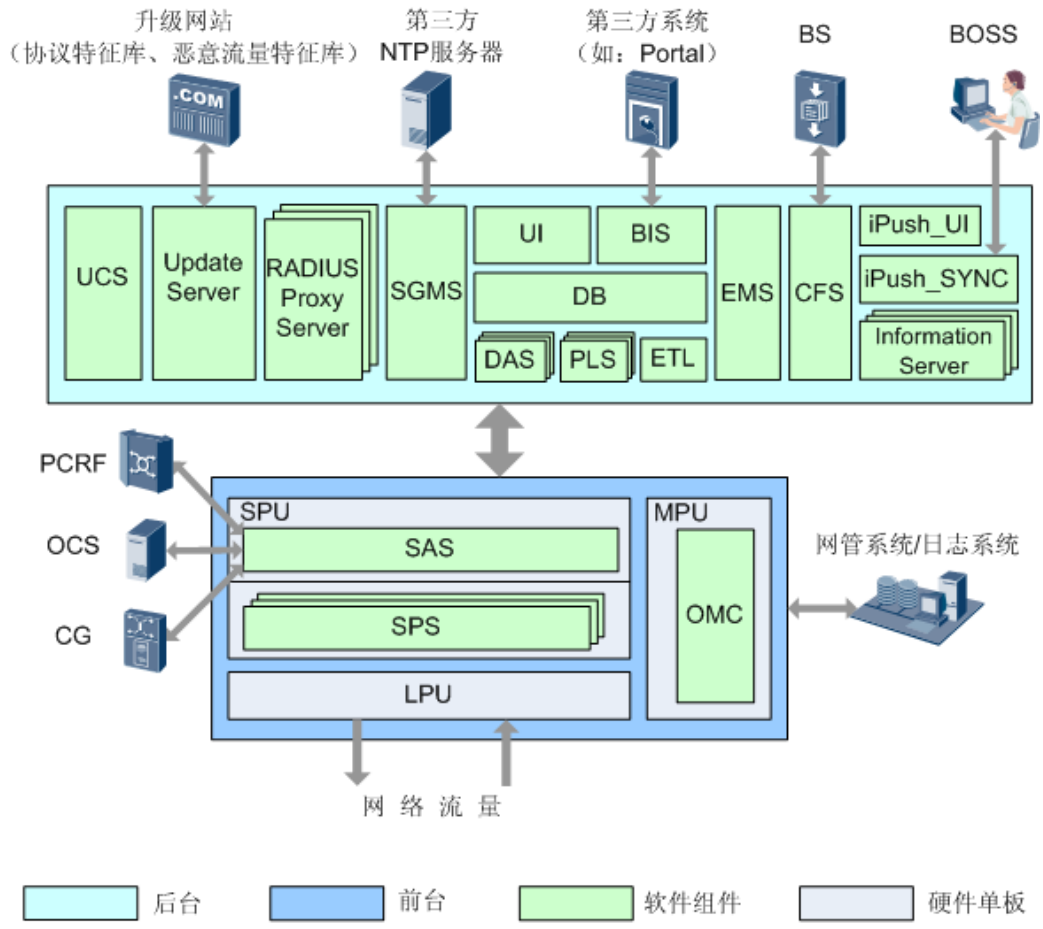
2.2 软件架构

介绍 SIG 系统的前台和后台软件架构、各个组件的主要功能，以及报文的基本处理流程。

系统软件架构

SIG 系统的软件架构及报文交互如图 2-13 所示。

图2-13 SIG 系统软件架构及报文处理流程图



BOSS（Business and Operation Support System ）业务运营支撑系统
PCRF（Policy and Charging Rule Function）策略与计费执行功能
OCS（Online Charging System）在线计费系统
CG（Charging Gateway）计费网关
BS（Billing System）计费系统

系统组件基本功能

图 2-13 中各组件的基本功能如表 2-10 所示。

表2-10 SIG 系统组件功能说明

组件		功能
前台	SPS（Service Probe System）	SPS 部署在业务板 SPU 上。SPS 完成对网络数据报文的解析和协议识别等初步分析，并将分析结果上传到相关的业务分析系统（SAS）或数据分析服务器（DAS）。同时接收 SAS 下发的策略并执行，实现流量控制、连接控制及 QoS 重标记等。另外，还执行流量镜像、分析 RADIUS 报文并发送给 RADIUS

组件		功能
		Proxy 等功能。
	SAS（Service Analysis System）	SAS 部署在业务板 SPU 上。SAS 将 SPS 上传的数据汇总并上报给 DAS，同时根据从 PLS 获取的配置策略进行决策。如果需要进行控制，则将控制策略下发到 SPS 上，SPS 根据 RADIUS Proxy 上报的用户 IP 对应关系，实现对用户账号的流量分析和控制。
	OMC（Operation Maintenance Center）	OMC 部署在主控板 MPU 上，主要负责设备管理、系统配置、日志告警生成。具体包括：设备注册和状态监控、分流策略的配置、业务调度、SIG 集群管理，并提供与网管系统和日志服务器的接口。
后台	RADIUS Proxy Server	RADIUS Proxy Server 获取并缓存用户上下线信息、用户账号与 IP 地址的映射关系、用户属性及其变更事件（例如：用户漫游），然后发送给 SAS。
	PLS（Policy Server）	PLS 根据 SAS 的策略请求，从 DB 中获取用户对应的策略信息，并向 SAS 下发策略。
	DAS（Data Analysis Server）	DAS 对多个 SAS 和 SPS 上报的数据汇总统计后写入数据库，为系统产生报表提供支撑。
	SGMS（System General Management Server）	即管理服务器。SGMS 监控 SIG 后台组件（除 UCS 外）的运行状态，同时为 SIG 系统提供时间同步服务。
	UI（User Interface）	为用户提供统一的图形界面管理接口，完成策略管理及报表查看。同时提供管理员认证、用户授权、系统审计等功能。
	Update Server	升级服务器提供协议特征库、恶意流量（Worm、Botnet 等）特征库的自动升级服务等。
	UCS（URL Category Server）	URL 分类服务器包括 UCSS（URL Category Searching Server）和 UCDB（URL Category Database）两部分，主要提供 URL 分类查询功能。
	BIS（Business Interface Server）	BIS 提供策略订阅、日志查询、用户管理的接口，供第三方系统调用。例如：客户 Portal。
	DSE（Dynamic Scan Engine）	DSE 可以对 HTTP 请求报文中的 URL 进行实时分析，检测用户访问的 URL 中是否存在恶意行为，包括恶意 URL 和恶意软件，并向 SPS 反馈检测结果。
	DB（Database）	DB 用于存储系统的配置、策略、数据统计等信息。
	ETL（Extractive Transition Loading）	数据二次加工处理服务器，处理多个 DAS 上报的数据，加工后将数据写入数据库。
	EMS（Element Management System）	EMS 为 SIG 内部网管，主要实现设备管理、系统管理等功能。

组件		功能
	Information Server	信息服务器，提供推送信息的具体内容，确认并记录信息推送结果。
	iPush_UI（iPush User Interface Server）	信息推送用户界面服务器，提供 iPush 系统的管理界面，管理员可以基于管理界面完成业务管理、报表查询、权限管理和系统管理。
	iPush_SYNC（iPush Data Synchronization Server）	信息推送数据同步服务器，用于从客户系统同步用户的账号、套餐或资费信息。

报文处理流程

SIG 系统处理网络数据报文的基本流程如下：

1. 网络数据报文从前台 SIG9800-X 的接口板进入 SIG 系统，接口板按照数据报文的源 IP 地址或目的 IP 地址将数据报文分流给不同的 SPS。
2. SPS 对报文进行初步分析并将分析结果提交给相关的 SAS 或 DAS。
3. SAS 将 SPS 上报的数据汇总并上报给 DAS，同时根据从 PLS 获取的配置策略决策执行不同的操作：
   - 如果决策结果是记录汇总的数据，则将汇总的数据发送到 DAS。
   - 如果决策结果需要对报文进行控制，则将控制策略下发到 SPS 执行。
4. DAS 对 SPS 和 SAS 上报的数据进行汇总统计后写入数据库，为系统产生报表提供支撑。
5. ETL 处理所有 DAS 上报的数据，加工后将数据写入数据库。

3 网络部署

3.1 按部署模式

SIG 系统支持直路和旁路两种部署模式（在旁路部署模式下，只支持流量可视化和流量镜像），客户可以根据所开展的业务和所要达到的监控效果选择部署模式。

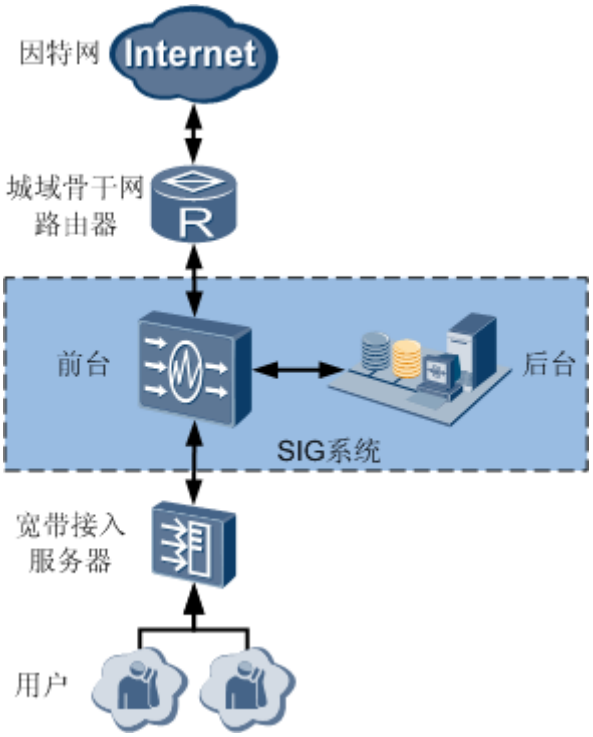
3.1.1 直路部署

在直路部署模式下，SIG 系统通过 Bypass 设备串接到网络链路中，以丢弃报文及干扰的方式对网络进行控制。当设备出现故障时，Bypass 设备自动将链路的数据直接转发，不影响业务运营。另外，结合网络具体情况以及对系统可靠性的要求，有两种特殊的直路部署方式：Hairpin 部署和级联部署。

典型组网

SIG 系统的基本组网如图 3-1 所示。

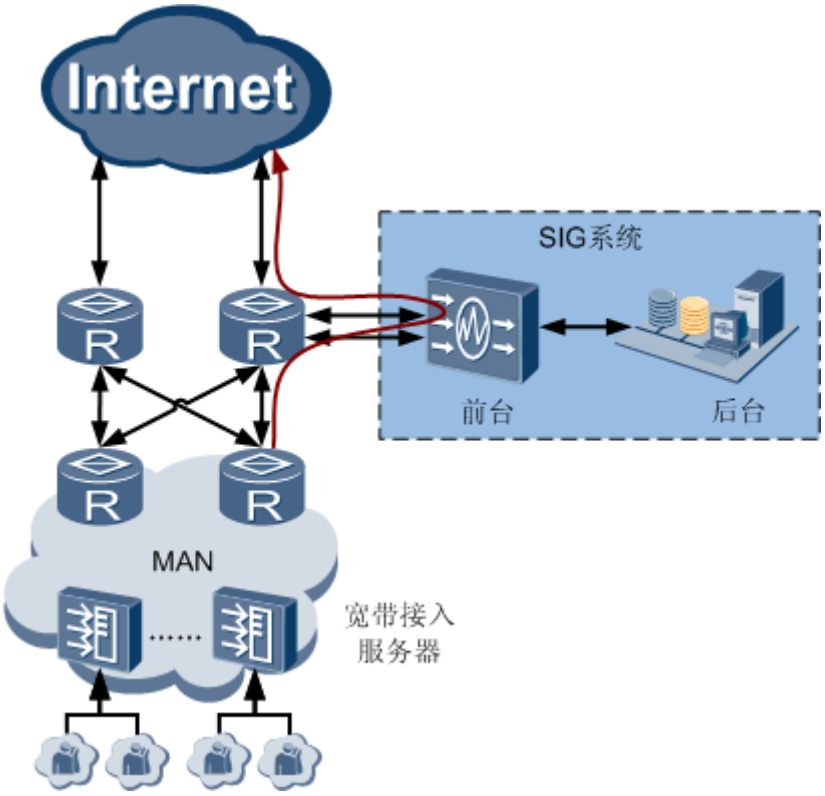
图3-1 SIG 系统直路部署



特殊的直路部署方式：Hairpin 部署

Hairpin 部署是一种特殊的直路部署组网方式，在这种部署方式下，SIG 系统的入口和出口都连接到同一台路由器或宽带接入服务器（BRAS）上，而且至少采用 2 条或 2 条的倍数以上的链路与路由器连接。路由器端口启用策略路由，将需要进行业务感知处理的流量转发到指定端口。在这种模式下，不需要使用 Bypass 设备。通过路由器自身的链路检测即可达到保护链路的目的。当 SIG 系统因断电等情况无法处理流量，路由器链路不可达，策略路由失效后，按正常路由进行数据转发。Hairpin 部署的基本组网如图 3-2 所示。

图3-2 SIG 系统 Hairpin 部署基本组网



解决非对称路由问题的部署方式：前台级联部署

由于部署的原因，网络流量存在路由不对称现象，即同一条流的上行和下行方向经过的链路不同。SIG 监控多条链路流量时，路由不对称会导致流量控制不准确，告警无法推送等问题。SIG 通过将相同内网 IP 地址的报文流归属到集群的同一个 SPS 分析和处理的方式（即满足同源同宿），解决非对称路由引发的问题。

说明

- 集群：由一台或多台 SIG 前台设备组成，集群中前台设备的角色以主、备和从进行标识。
- 内网：指 SIG 系统所监控的网络。

基于系统性能（单台设备处理能力有限）以及可靠性（单台设备部署存在单点故障可能性）的考虑，需要将两台 SIG 进行级联部署，以流量搬迁的形式将同一用户或相同用户组的业务流量分流给同一个 SPS 处理。两台 SIG 级联典型组网如图 3-3 所示。

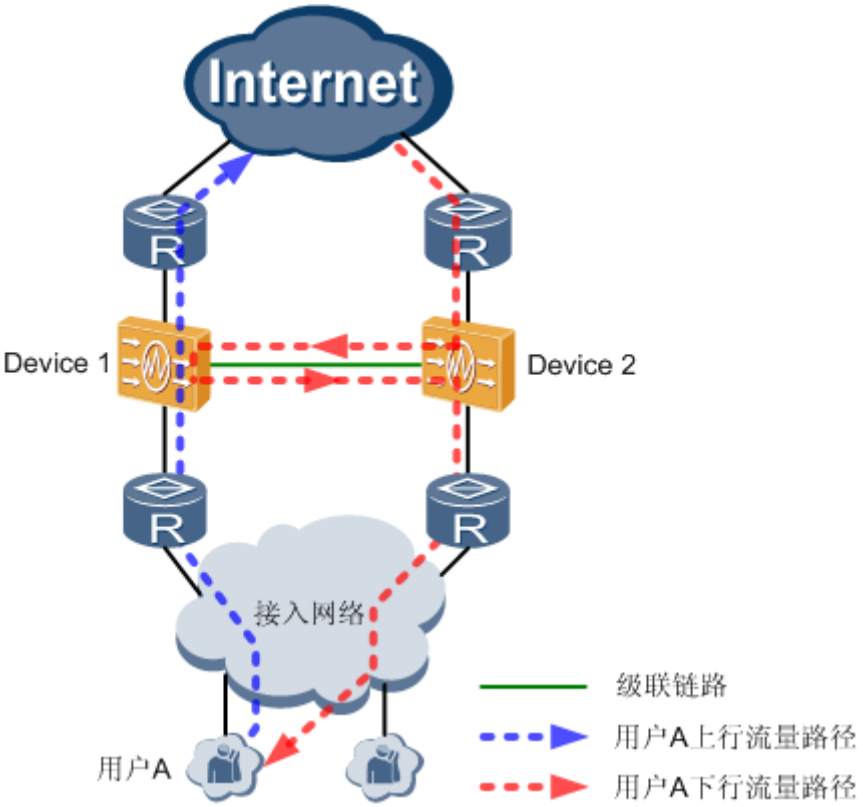
图 3-3 中，A 用户的上行业务流量流经 Device 1，而下行业务流量流经 Device 2，需要将用户 A 的下行业务流量通过级联链路搬迁到 Device 1 的 SPS 进行处理，处理后的业务流量再通过级联链路回迁到 Device 2 并由原业务链路转发。

说明

级联口：用于两个前台级联的接口。

级联链路：级联接口所在的链路。

图3-3 SIG 级联部署组网示意图



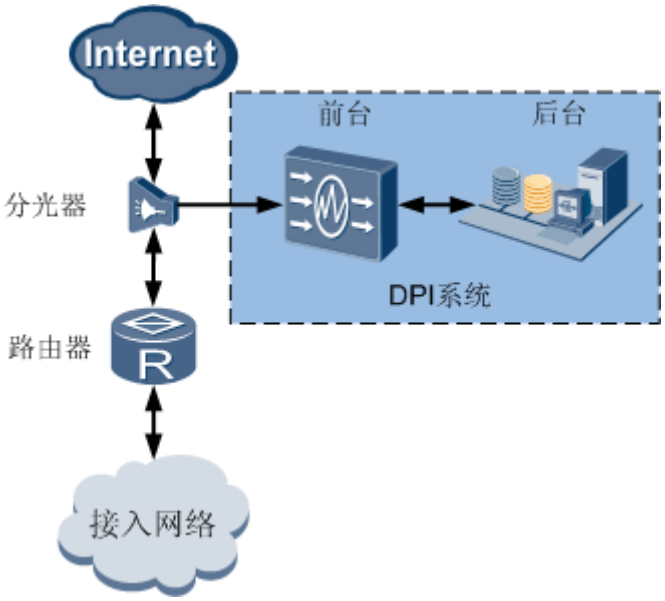
3.1.2 旁路部署

在旁路部署模式下，SIG 系统通过分光的方式获取网络流量，设备故障不会对网络流量产生影响。旁路部署时，SIG 系统可以实现流量可视化和流量镜像功能。

典型组网

SIG 系统的组网如图 3-4 所示。通过分光器以分光方式将网络流量的镜像从由器引入到 SIG 系统的前台。

图3-4 SIG 系统旁路部署图



3.2 按部署位置

SIG 系统可以部署在各种网络中，客户可以根据所要开展的业务和监控重点规划合适的部署位置。

SIG 系统支持的典型部署位置及特点如表 3-1 所示。

表3-1 SIG 系统支持的典型部署位置及说明

部署位置	详细描述
广电宽带网络	• 网络类型和需求与固网运营商的宽带网络类似，可以部署在广电宽带网络中从 BRAS 到互联网出口之间的 IP 网络中。
企业网络	• 可以部署在企业网络的核心位置，以监控互联网出口、数据中心出口或 WAN/VPN 互联口的流量。
公共事业/教育机构网络	• 可以部署在学校网络的核心位置，以监控互联网出口、数据中心出口或 WAN/VPN 互联口的流量。
政府机构网络	• 可以部署在政府机构网络的核心位置，以监控互联网出口、数据中心出口或 WAN/VPN 互联口的流量。

4 业务与功能

4.1 用户与网络管理

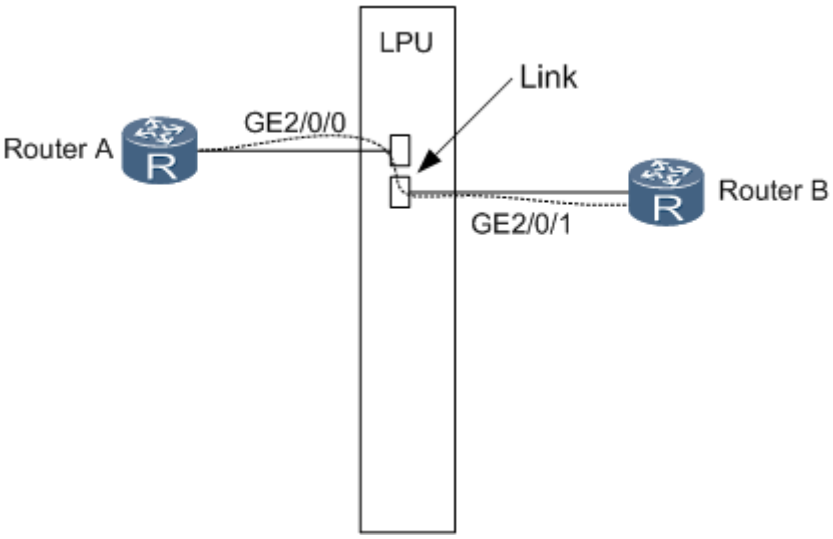
SIG 系统可以对公众客户、大客户、链路、虚通道、子网、流向等对象进行业务统计分析和管理，帮助客户从多角度掌握网络使用状况，并为策略配置提供依据。

SIG 系统可管理的业务对象包括以下类型：

- 链路（Link）

  指 SIG 系统前台所监控的物理链路。例如，在图 4-1 中，假设用户侧线缆接入 POS2/0/0 端口，网络侧线缆接入 POS2/0/1 端口，则 POS2/0/0 端口和 POS2/0/1 端口之间即为一条链路。

图4-1 链路示意图



- 虚通道

  为识别并定义待管理网络流量，SIG 系统除提供公众客户、大客户、链路、AS 域组、子网等用户与网络对象外，还支持根据用户属性或流属性创建虚通道对象。

虚通道提供了一种对数据流进行分组的方法，能够将所有数据流根据一定的条件划分为多个虚通道，并将这些虚通道视为独立的链路进行管理。对数据流进行分组的条件包括：IP 五元组、ToS/DSCP、VLAN、MPLS、链路。同时，支持将一组用户的数据流划分为虚通道，可以根据用户区域、动态属性来划分用户组。

- 公众客户

  指普通客户，例如：以账号 ID 标识的 ADSL 拨号上网用户，以 IP 地址或 IP 地址段标识的固定 IP 用户。

- 大客户

  指由多个静态 IP 地址或 IP 地址段组成的客户，如企业用户。同一个 IP 地址只能属于同一个大客户。

- AS（Autonomous System）域组

  指一组 AS 的集合。在 SIG 中，AS 域组用于帮助客户灵活的统计 AS 域间的流量。

  AS 指拥有同一选路策略，在管理机构下运行的一组路由器。AS 号同 IP 地址一样，由国际组织统一分配。SIG 前台通常部署在私有 AS 域内，通过与邻居路由器建立 BGP 邻居关系，来学习网络中的 AS 信息。

- 子网

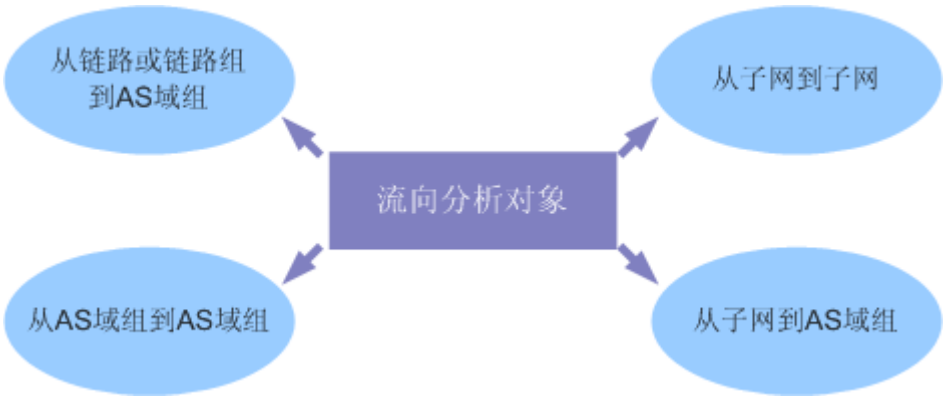
  子网指 IP 地址的集合，包含一个或多个 IP 地址段。

- 流向

  指具有特定源端和目的端的网络流量分析对象。

  SIG 支持的流向分析对象包括：从链路或链路组到 AS 域组、从 AS 域组到 AS 域组、从子网到 AS 域组、从子网到子网，如图 4-2 所示。

图4-2 流向分析对象



4.2 流量管理

通过 SIG 系统的流量管理功能，管理员可以灵活精准的控制网络流量并查看丰富多样的网络流量报表。

灵活精准的流量分析控制

通过 SIG 系统的流量控制管理功能，可以对指定类型或方向的流量进行控制，控制精度能满足流量遏制要求，另外可以控制低附加值业务流量。连接控制可以提高链路带宽利用率，提升高价值业务和关键客户业务的网络质量，并能降低在网络高峰期 P2P 等高资源性应用的流量占比。

SIG 系统流量管理的主要功能包括：

- **流量 QoS**

  流量 QoS 可以对链路、公众客户或大客户流量实施 QoS 控制，包括带宽控制、连接数控制等多种类型流量管理措施。主要提供以下功能：

  - 应用 QoS 策略包到链路

    实现对链路流量的流量限速（支持 PIR 和 CIR）、优先级标记、连接数控制、不控制、禁止标记策略控制。

  - 应用 QoS 策略包到虚通道

    实现对虚通道流量的流量限速（支持 PIR 和 CIR）、优先级标记、连接数控制、不控制、禁止标记策略控制。

  - 应用 QoS 策略包到公众客户

    按属性群组或用户组对公众客户，实现对公众客户流量的流量限速（支持 PIR 和 CIR）、优先级标记、连接数控制、不控制、禁止标记、整形、绝对优先级、加权公平队列策略控制。

  - 应用 QoS 策略包到大客户

    按属性群组或用户组对大客户，实现对大客户流量的流量限速（支持 PIR 和 CIR）、优先级标记、连接数控制、不控制、禁止标记策略控制。

  - 支持动态策略

    支持设置链路与虚通道的流量阈值，当指定链路或虚通道的流量超过阈值且持续一段时间后，系统自动执行针对链路、虚通道或公众客户的控制策略，解决客户网络的拥塞问题。

- **流向统计**

  通过流向统计可以查看流向报表，以便统计从链路到 AS 域组、从 AS 域组到 AS 域组、从子网到 AS 域组或从子网到子网的流量数据。SIG 系统能够统计的流向统计对象包括：

  - 链路（链路组）与 AS 域组之间

    对于链路与 AS 域组之间、链路组与 AS 域组之间的流向分析对象，系统提供流向趋势报表、流向占比报表和按流量 Top N 协议报表。

    另外，系统还提供针对出境流量、入境流量和过境流量趋势、占比等的报表统计。

  - AS 域组与 AS 域组之间

    对于 AS 域组与 AS 域组之间的流向分析对象，系统提供流向趋势报表、流向占比报表和按流量 Top N 协议报表。

  - 子网与 AS 域组之间

    对于子网与 AS 域组之间的流向分析对象，系统提供流向趋势报表、流向占比报表和按流量 Top N 协议报表。

- 子网与子网之间

  对于子网与子网之间的流向分析对象，系统提供流向趋势报表、流向占比报表和按流量 Top N 协议报表。

- **流向带宽控制**

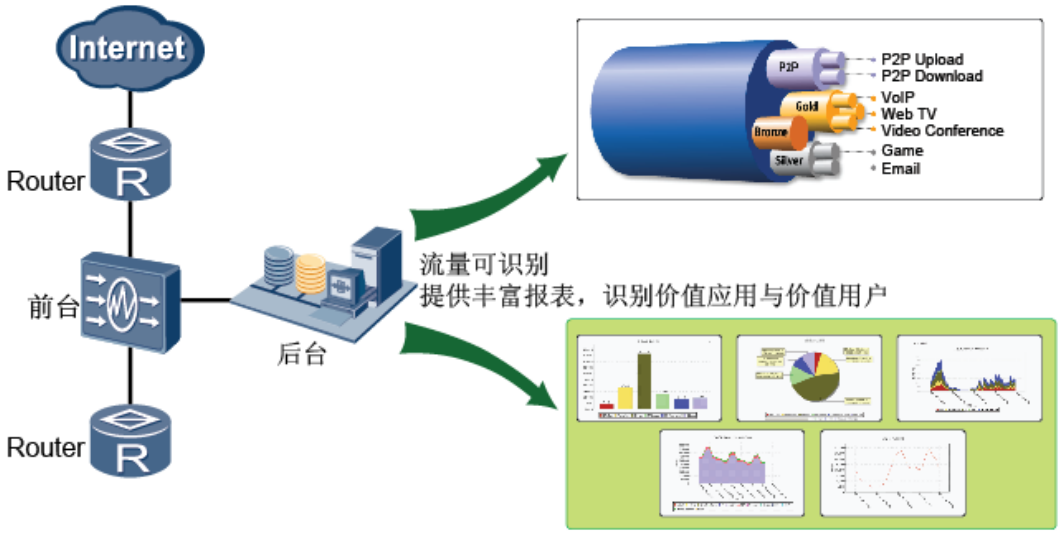
  流向带宽控制可以实现对从链路到 AS 域组、从 AS 域组到 AS 域组、从子网到 AS 域组或从子网到子网的流量实施带宽控制，主要包括：

  - 针对链路与 AS 域组之间的流向对象，支持按流分类实施流量限速（仅支持 PIR）和不控制策略控制。
  - 针对 AS 域组与 AS 域组之间的流向对象，支持按流分类实施流量限速（仅支持 PIR）和不控制策略控制。
  - 针对子网与 AS 域组之间、子网与子网之间的流向对象，支持按流分类实施流量限速（仅支持 PIR）和不控制策略控制。

全面丰富的报表

基于强大的协议分析技术，SIG 系统提供丰富多样的流量报表，实现对网络流量的识别和直观呈现，如图 4-3 所示。

图4-3 流量报表作用的示意图



按照分析对象的不同，流量报表包括如下几种类型：

- 链路与虚通道类流量报表

  指按链路与虚通道分析和统计网络中流量、连接数等的一系列报表，如链路实时流量、流量趋势、流量占比、连接数趋势、连接数占比等报表。

说明

查询连接数类报表时，可在查询条件中选择不同连接数类型，包括：

- 新建连接数

  指统计时间范围内累计新建的总连接数。

- **拆除连接数**

  指统计时间范围内累计拆除的总连接数。

- **平均连接数**

  指各采样时间点的瞬时连接数之和除以采样次数后得出的值。

  五分钟表中平均连接数的采样次数为 4 次～8 次。小时表、天表和月表中平均连接数由五分钟表数据逐步取平均后计算得出。

- 公众客户类流量报表

  指按公众客户分析和统计网络中流量、连接数等的一系列报表，如公众客户实时流量、流量趋势、流量占比、连接数趋势、连接数占比等报表。

- 大客户类流量报表

  指按大客户分析和统计网络中流量、连接数等的一系列报表，如大客户实时流量、流量趋势、流量占比、连接数趋势、连接数占比等报表。

- 综合类流量报表

  指不属于上述类型的其他一些综合类报表，如公众客户占总流量比、公众客户占总连接数比、公众客户占总流量比趋势等报表。

按照时间粒度的不同，流量报表包括如下几种类型：

- 五分钟表

说明

在查询报表时，如果不手动选择数据粒度，而只是输入查询时间范围，则系统将根据时间范围长短自动判定数据粒度。

由于不同数据粒度的数据汇总可查询时间点不同，因此，当查询后提示无数据时，请尝试更改查询条件。

查询条件中的“时间粒度”与查询结果中的报表数据粒度无一一对应关系，仅用于方便输入查询时间范围。

报表数据的存储周期可配置。要了解详细信息，请参见配置统计数据存储周期。

- 小时表

  当查询时间范围大于一天且小于等于一周，且开始时间和结束时间均为最近一周的时间时，将缺省查询小时表。报表示例如图 4-4 和图 4-5 所示。

  小时表是由五分钟表汇总而来，每小时的半点汇总前一小时的数据。例如：9:30 开始汇总 08:00～09:00 的数据。若此时时间为 09:20，则小时表此时查看不到 08:00 的记录。

- 天表

  天表是由小时表汇总而来，每天凌晨 1 点汇总前一天的数据。例如：1 月 2 号 01:00 开始汇总 1 月 1 号的数据。若此时时间为 1 月 2 号 00:30，则天表此时查看不到 1 月 1 号的记录。

- 月表

  月表数据最多保留 4 年。月表是由天表汇总而来，每月初的凌晨 3 点汇总前一月的数据。例如：2 月 1 号 03:00 开始汇总 1 月的数据。若此时时间为 2 月 1 号 01:00，则月表此时查看不到 1 月的记录。

图4-4 小时表图形

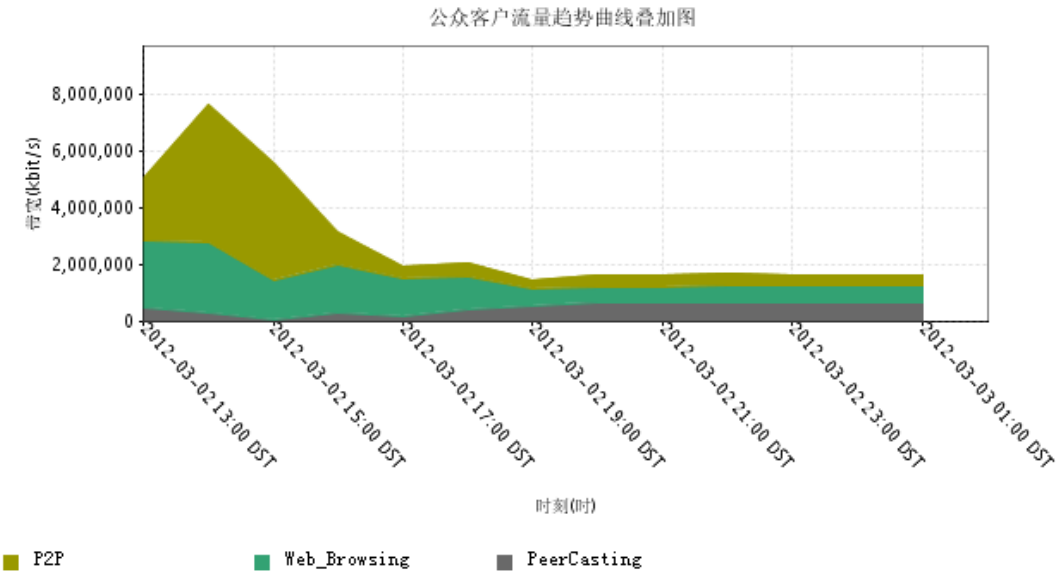


图4-5 小时表记录

序号	分析对象	流量类型	时间	上行流量(kbyte)	上行带宽(kbit/s)	上行包数(个)	上行包速率(pps)
1	root	P2P	2012-03-03 01:00:00 DST	175,748,566	390,552	627,642,728	174,345
2	root	P2P	2012-03-03 00:00:00 DST	173,839,764	386,310	637,142,656	176,984
3	root	P2P	2012-03-02 23:00:00 DST	173,498,443	385,552	635,991,404	176,664
4	root	P2P	2012-03-02 22:00:00 DST	170,897,573	379,772	618,964,376	171,934
5	root	P2P	2012-03-02 21:00:00 DST	169,385,702	376,412	625,377,372	173,715

4.3 URL 过滤

随着互联网的蓬勃发展，良莠不齐的网站层出不穷，不良网站的危害也日渐严重，如何有效地控制 URL（Uniform Resource Locator）已成了管理者不得不关注的问题。SIG 系统根据用户访问的 URL 所属分类（例如：新闻类、赌博类），对用户的 Web 访问行为进行实时检测和控制（控制方式包括：阻断、推送告警页面、不控制）。

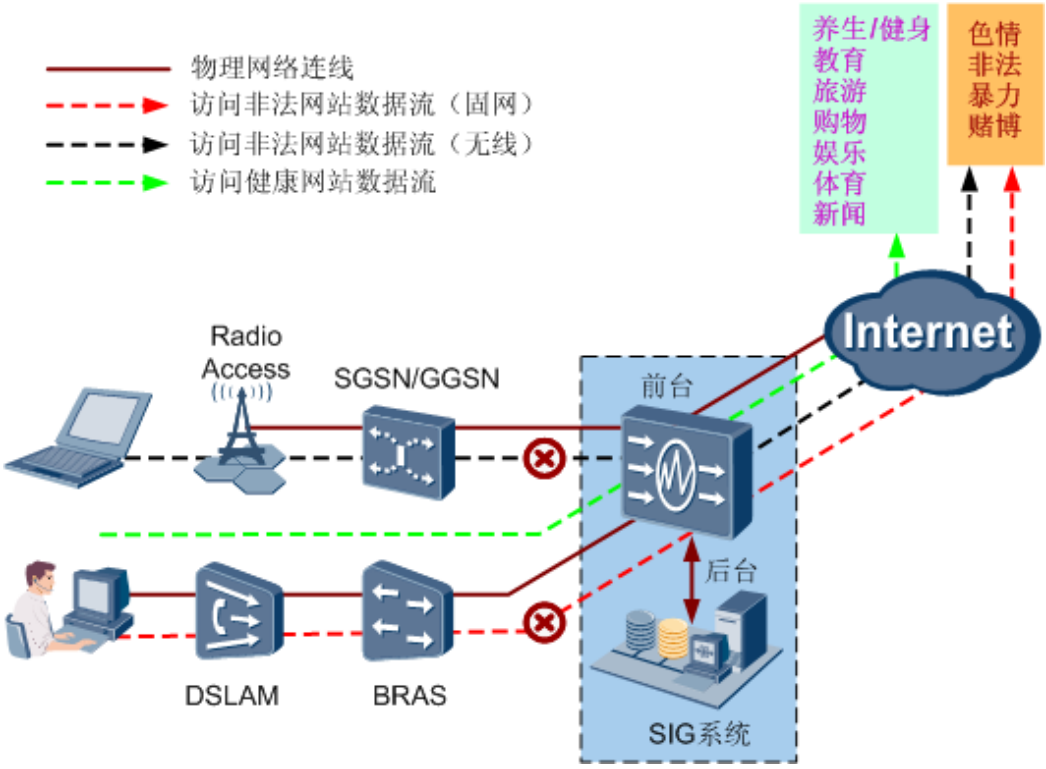
卓越的过滤功能

SIG 系统支持基于用户（包括：公众客户、大客户、用户组）和链路的 URL 策略，并能实现在不同时间段应用不同的 URL 策略。SIG 系统拥有强大的 URL 分类库，而且能够自动在线升级。同时，管理员也可以根据需要自定义 URL 和 URL 分类。通过 URL 过滤业务，可以实现如下功能：

- 控制低俗信息（如色情、暴力、犯罪和赌博等不健康网站）的泛滥。
- 屏蔽钓鱼网站，进而保护用户隐私安全。
- 屏蔽恶意网站，减少木马攻击。

URL 过滤业务的基本应用原理如图 4-6 所示。

图4-6 URL 过滤业务的应用



细致完善的报表

为提供全面、精确的 URL 访问行为分析，对于 SIG 监控流量中的 URL 访问流量，系统提供如下不同类型的分析报表：

- 按访问数 Top N 全局 URL

  可根据时间范围等条件，查看全局 URL 中前 N 个访问数最高的 URL 报表。
- 按访问数 Top N 分类 URL

  可根据时间范围等条件，查看某个或某些指定分类 URL 中前 N 个访问数最高的 URL 报表。
- 按访问数 Top N 客户

  可根据时间范围等条件，查看访问某个或某些指定热点 URL 的所有公众客户中前 N 个访问数最高的客户报表。
- 热点 URL 访问数趋势

  可根据时间范围等条件，查看某个或某些指定热点 URL 访问数趋势的曲线叠加图、曲线图。
- URL 分类访问数趋势

  可根据公众客户范围、时间范围等条件，查看某个或某些指定分类 URL 访问数趋势的曲线叠加图、百分比曲线图、曲线图。

- URL 分类访问数占比

  可根据公众客户范围、时间范围等条件，查看某个或某些指定分类 URL 访问数占比的饼图、柱状图。

- URL 分类访问数 Top N

  可根据公众客户范围、时间范围等条件，查看前 N 个访问数最高的 URL 分类报表。

- 按流量 Top N 全局 URL

  可根据时间范围等条件，查看全局 URL 中前 N 个访问流量最高的 URL 报表。

- 按流量 Top N 分类 URL

  可根据时间范围等条件，查看某个或某些指定分类 URL 中前 N 个访问流量最高的 URL 报表。

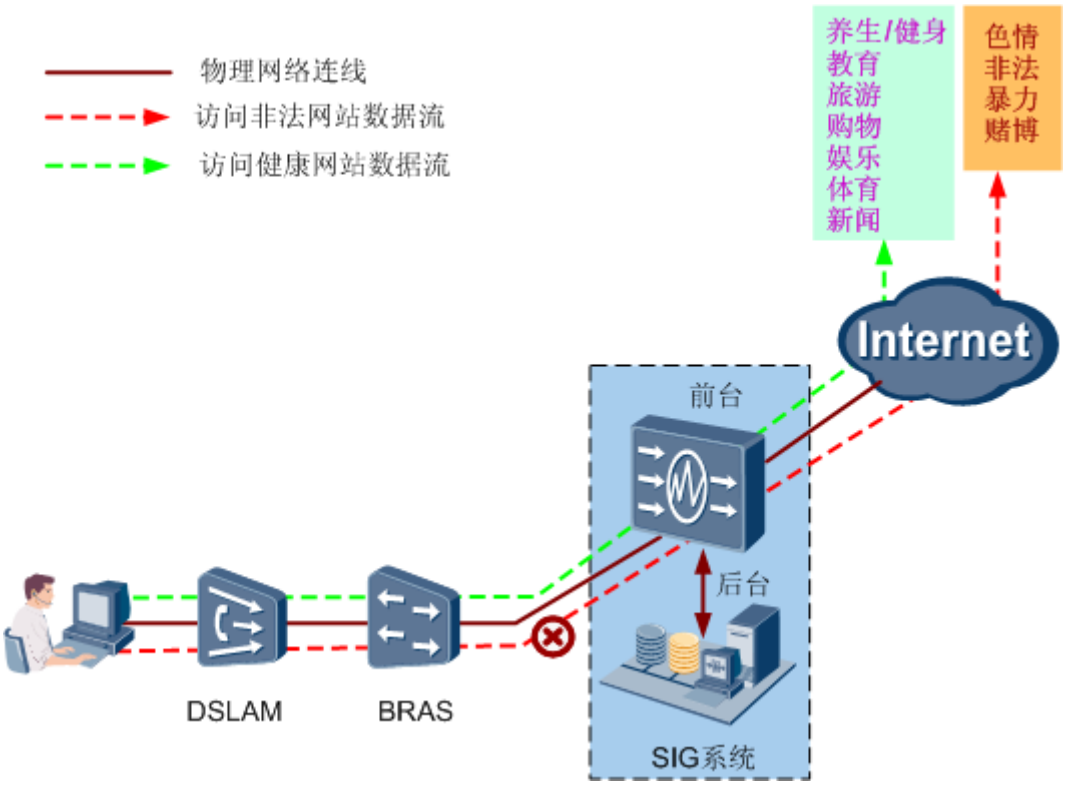
4.4 家庭上网安全

随着宽带网络的普及，色情、暴力、贩毒、网络游戏等有害网站的增多，由未成年人的网上活动（如网上聊天、网上交友）所引发的社会问题也日益突出。家庭上网安全业务是基于 URL 过滤和协议控制功能的运营业务，旨在帮助家长对孩子的上网行为进行管理。对于企业/机构用户，也可以通过此功能有效管理员工的上网行为，屏蔽和工作无关的网站和网络应用，使员工聚焦于工作。

切实有效的管控功能——父子账号

家庭上网安全业务的典型组网如图 4-7 所示。

图4-7 家庭上网安全业务典型组网

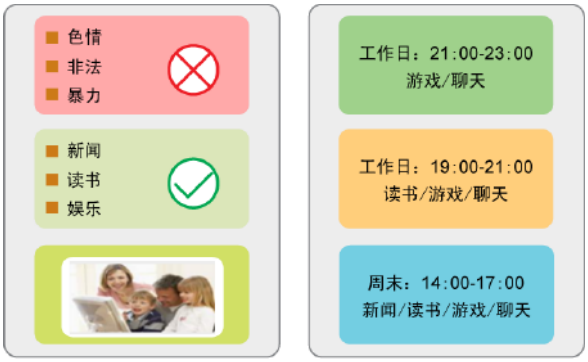


SIG 系统的家庭上网安全业务主要提供以下功能：

- 过滤色情、暴力、贩毒和成人网站等有害内容。
- 屏蔽有害的网络游戏、聊天和交友等网络工具。
- 根据需要（如节假日）设置用户的上网时长和上网时段。

以家长管理孩子上网为例，家庭上网安全的功能如图 4-8 所示，父账号限制子账号可以访问的网址、网络应用和上网时间。

图4-8 限制孩子可以访问的网址、网络应用和上网时间



具体而言，家庭上网安全业务实现的功能主要包括：

- 基于时间的 URL 库分类过滤

  为用户提供 URL 的访问控制服务，过滤不良网页，保护青少年健康成长。

  系统内置一百多类网站的分类列表，包括色情、赌博、购物、新闻、聊天等。在对用户的访问行为进行捕捉的同时，可判断其访问网站是否合法，并有效地阻断其对非法网站的访问。

- 基于用户的自定义的 URL 黑白名单过滤

  黑白名单服务的作用是过滤掉网上的各种有害信息，限制浏览范围。家长可以自定义 URL 的黑白名单，控制优先级由高到低依次为：URL 黑名单、URL 库分类、URL 白名单。通过 URL 的黑白名单，可以禁止子账号访问某些特殊网站，或只访问某些特殊网站。

- 基于时间的应用软件控制

  可以提供在线游戏、P2P、QQ、MSN 等大众化的应用软件控制。用户可直接选择屏蔽 QQ、MSN 等聊天软件，申请成功后，系统自动限制用户使用 QQ、MSN 等聊天软件对外通信。也可控制青少年访问登录网络游戏。

- 子账号上网时长的控制

  上网时长控制服务的作用是限制青少年上网的时长（系统不支持大客户上网时长控制）。

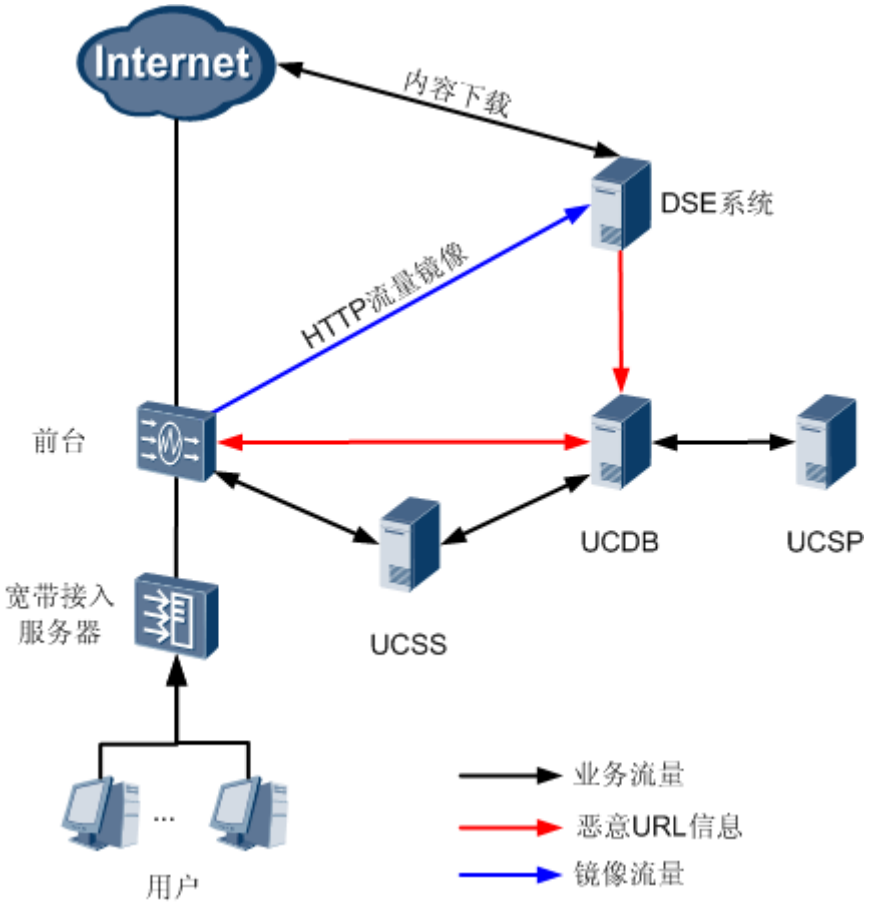
全面的恶意 URL 过滤功能

随着宽带网络的普及，恶意网站及恶意软件站点等有害网站的增多，网络安全越来越受到关注。订购了恶意 URL 过滤功能的公众客户和大客户访问恶意网站时，用户的访问直接被阻断或者被重定向到告警页面。

SIG 支持将 URL 地址划分到不同的分类，然后对某一分类的 URL 地址设置控制策略。“恶意网站”是 URL 分类中的一种。

恶意 URL 过滤功能的典型组网如图 4-9 所示。

图4-9 恶意 URL 过滤的典型组网



各组件的主要功能：

- UCSS（URL Category Searching Server）

  URL 分类查询服务器，负责对采集到的数据进行分类，同时向 SPS 提供 URL 分类查询的功能。

- UCDB（URL Category Database）

  URL 分类数据库，负责数据存储的模块，定期从 UCSP 获得升级数据，并将这些数据同步给所有的 UCSS。

- UCSP（URL Category Service Platform）

  URL 分类服务平台，为 URL 分类服务器提供系统预定义 URL 分类库的升级服务。

- DSE（Dynamic Scan Engine）

  若不部署 DSE 系统，UCDB 定期向 UCSP 更新 URL 分类信息；若部署 DSE 系统，可以实现恶意网站的实时监测。

  DSE 通过对用户访问的恶意网站和恶意软件下载这两类 URL 进行检测，将用户访问的恶意 URL 重定向到告警页面，防止用户感染病毒。DSE 能提取 HTTP 上行流量中关于 URL 的访问，对 URL 进行检测，识别出可能携带病毒或恶意代码的

URL；以及对下载链接的目标文件进行病毒检测，判断此下载链接是否为恶意下载链接。

详实直观的阻断报表

数据配置工程师可以在 SIG 查看用户的 URL 阻断和应用阻断报表，报表类型包括：

- 公众客户 URL 阻断日志

  可根据 URL 分类、时间范围等条件，查看某指定公众客户的 URL 阻断日志信息，包括 URL、URL 分类、阻断次数和时间等。
- 公众客户应用阻断日志

  可根据时间范围等条件，查看某指定公众客户的应用阻断日志信息，包括应用名称、时间、阻断次数等。
- 大客户 URL 阻断日志

  可根据 URL 分类、时间范围等条件，查看某指定大客户的 URL 阻断日志信息，包括 URL、URL 分类、阻断次数和时间等。
- 大客户应用阻断日志

  可根据时间范围等条件，查看某指定大客户的应用阻断日志信息，包括应用名称、时间、阻断次数等。

4.5 流量镜像

通过流量镜像业务可以将客户重点关注的流量（例如：HTTP、Email、VoIP 等）复制到第三方设备，即由 SIG 系统提供原始数据报文，第三方设备接收并处理这些数据报文，而原来的报文不受影响。

流量镜像

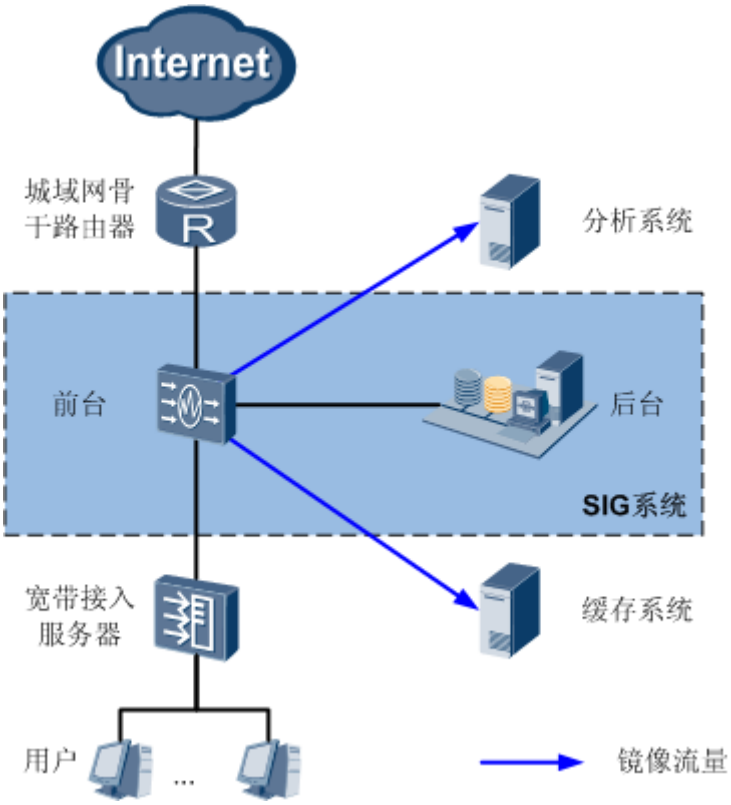
流量镜像就是 SIG 对网络上的流量进行识别，再根据需要将指定类型的报文进行复制并转发，将流量转发到指定的第三方系统（如 iCache 系统）上。由第三方系统对流量作进一步分析或缓存。选择镜像处理时原报文流向不受影响。

典型应用举例如下：

- 针对某指定链路的 SMTP（Simple Mail Transfer Protocol）流量、VoIP 流量配置镜像策略，第三方系统将流量存储备查，从而实现对 SMTP 邮件和 VoIP 业务的监控。
- 针对某指定链路的 HTTP 视频下载流量、P2P 下载流量配置镜像策略，将用户访问请求重定向到第三方缓存系统，从而实现网络下载加速。

流量镜像典型组网如图 4-10 所示。

图4-10 流量镜像典型组网



流量镜像功能实现

SIG 的流量镜像业务，可以提供如下主要功能：

- 支持对链路流量进行镜像。

  针对可疑地区，安全部门需要重点监控，对于其语音通信与邮件发送需要通过合法手段监控记录，将所有语音和邮件都保存一个副本到本地分析系统，在必要时审查。

  对链路而言，将流量镜像到本地缓存系统，可以将占用带宽较大的应用本地化，可以大大减少骨干网络的冗余流量。从而帮助客户提高带宽资源的利用率，同时也能提高最终用户的满意度。

- 支持对公众客户和大客户流量进行镜像，可以通过属性组或用户组进行策略应用。

  针对可疑用户或企业，安全部门需要重点监控，对于其语音通信与邮件发送需要通过合法手段监控记录，将所有语音和邮件都保存一个副本到本地分析系统，在必要时审查。

- 支持同时对链路流量和用户（公众客户和大客户）流量进行镜像。

  同时对链路流量和用户流量进行镜像时，用户流量镜像优先，同一份流量不会被镜像 2 次。

例如：用户 user1 的流量是通过链路 link1 进行传输的，管理员配置了针对用户 user1 的镜像策略 policy1 和针对链路 link1 的镜像策略 policy2。在这种情况下，用户 user1 的流量只会被 policy1 镜像而不会被 policy2 镜像。

- 支持传输层和应用层协议镜像、镜像组镜像、上下行报文镜像、远端 IP 镜像、端口号镜像和特征字镜像。
- 进入 SIG 的流量可以通过不同的匹配条件从多个镜像口转发给多个第三方系统。
- 支持转发接口定向配置，对于特定的流量可以转发给指定的目标系统。

SIG 前台在流量镜像业务中，主要实现以下功能：

1. 提取并复制匹配镜像组策略的流量。
2. 替换目的 MAC 地址。
3. 转发匹配策略的流量到第三方设备。

4.6 流量转向

通过流量转向业务将客户关注的流量（如 HTTP、Email、VoIP 等）转发到第三方设备，由第三方设备对流量作进一步分析和处理后再通过 SIG 将流量回注到网络中。

流量转向

流量转向就是 SIG 对网络上的流量进行识别，再根据需要将指定类型的报文直接转发至指定的第三方系统（以下均使用 VAS）。由 VAS（Value Added Server）对流量作进一步分析和处理并将处理后的报文回注到 SIG 前台，最后由 SIG 前台将报文发送到网络中。VAS 通常为缓存系统、杀毒系统等。

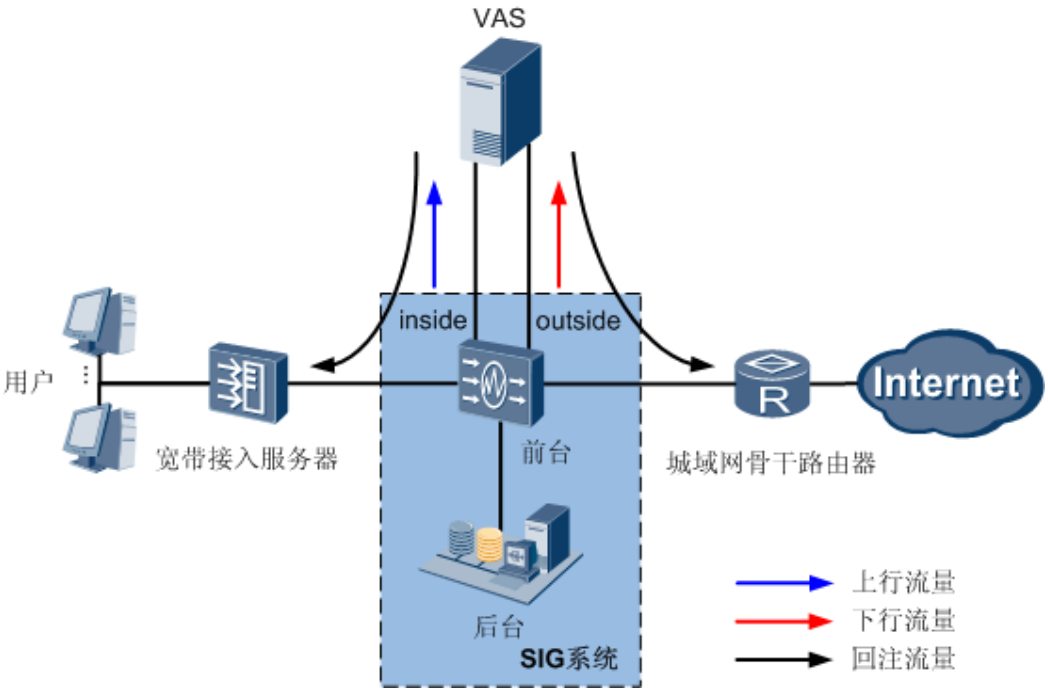
典型应用举例：针对某指定区域的 HTTP 视频下载流量、P2P 下载流量等配置转向策略，将用户访问请求重定向到 VAS（如 iCache 系统），从而实现网络下载加速。

流量转向典型应用场景如下：

- 单次转向

  VAS 处理后的流量再通过 SIG 前台回注到网络中。组网如图 4-11 所示。

图4-11 单次转向典型组网



单次转向的业务流程：

1. SIG 前台提取匹配转向策略的流量，修改报文的 VLAN ID 为 VAS 的 VLAN ID，修改报文的目的 MAC 地址为 VAS 的 MAC 地址。
2. 通过转向口，SIG 前台转发匹配策略的流量到 VAS。

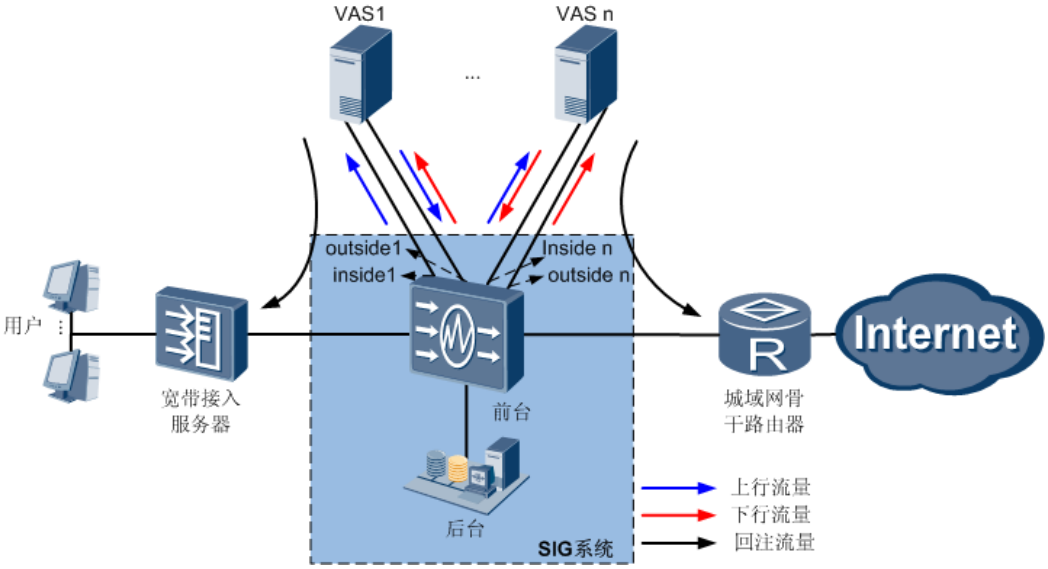
   上行流量通过 inside 口被转向到 VAS；下行流量通过 outside 口被转向到 VAS。
3. VAS 将处理后的流量回注到 SIG 前台。

   VAS 处理后的流量若是回注到内网，则通过 inside 口回注；若是回注到外网，则通过 outside 口回注。
4. SIG 前台还原报文的 VLAN ID 和目的 MAC 地址，并将报文发送到网络中。

- 多次转向

  流量依次经过多个 VAS，每经过一个 VAS 后，流量被回注到 SIG 前台。最后通过 SIG 前台将流量回注到网络中。

图4-12 多次转向典型组网



多次转向的业务流程：

1. SIG 前台提取匹配转向策略的流量，修改报文的 VLAN ID 为 VAS 的 VLAN ID，修改报文的目的 MAC 地址为 VAS 的 MAC 地址。
2. 通过转向口，SIG 前台转发匹配策略的流量到 VAS1。

   上行流量通过 inside1 口被转向到 VAS1；下行流量通过 outside1 口被转向到 VAS1。
3. VAS1 将处理后的流量回注到 SIG 前台。

   VAS1 处理后的流量若是回注到内网，则通过 inside1 口回注；若是回注到外网，则通过 outside1 口回注。
4. 通过 outside1 口回注到 SIG 前台的流量，SIG 前台修改报文的 VLAN ID 为 VAS2 的 VLAN ID，修改报文的目的 MAC 地址为 VAS2 的 MAC 地址。
5. 通过转向口，SIG 前台转发匹配策略的流量到 VAS2。

   上行流量通过 inside2 口被转向到 VAS2；下行流量通过 outside2 口被转向到 VAS2。
6. VAS2 将处理后的流量回注到 SIG 前台。

   VAS2 处理后的流量若是回注到内网，则通过 inside2 口回注；若是回注到外网，则通过 outside2 口回注。
7. 重复 4～6，将流量依次转向到多个 VAS。
8. SIG 前台还原报文的 VLAN ID 和目的 MAC 地址，并将报文发送到网络中。

说明

SIG 前台和 VAS 之间可以直接相连；也可以通过交换机与 VAS 相连，从而实现端口的复用。

流量转向功能实现

SIG 的流量转向业务，可以提供如下主要功能：

- 支持的 VAS 类型
  - VAS 为透明模式

    该种类型的 VAS 支持接收目的 MAC 地址不为本 VAS MAC 地址的报文。需要通过在 SIG 前台指定 VAS 的 VLAN ID，将流量转向至 VAS。
  - VAS 为非透明模式

    该种类型的 VAS 不支持接收目的 MAC 地址不为本 VAS MAC 地址的报文。需要通过在 SIG 前台指定 VAS 的 VLAN ID 并修改报文的目的 MAC 地址为 VAS MAC 地址，将流量转向至 VAS。
- 支持对公众客户、大客户和链路流量转向，对每个对象只有一个转向策略生效。
- 支持传输层和应用层协议转向、上下行报文转向、远端 IP 转向和端口号转向。
- 系统支持通过不同 VLAN 的 ID，将流量多次转向到不同的 VAS。
- 系统支持 8 对 inside 口和 outside 口，支持转向至 256 个 VAS。
- SIG 前台不能处理 VAS 新建的流，即 VAS 处理后报文的五元组不能被修改。否则 SIG 前台直接丢弃 VAS 新建的流。

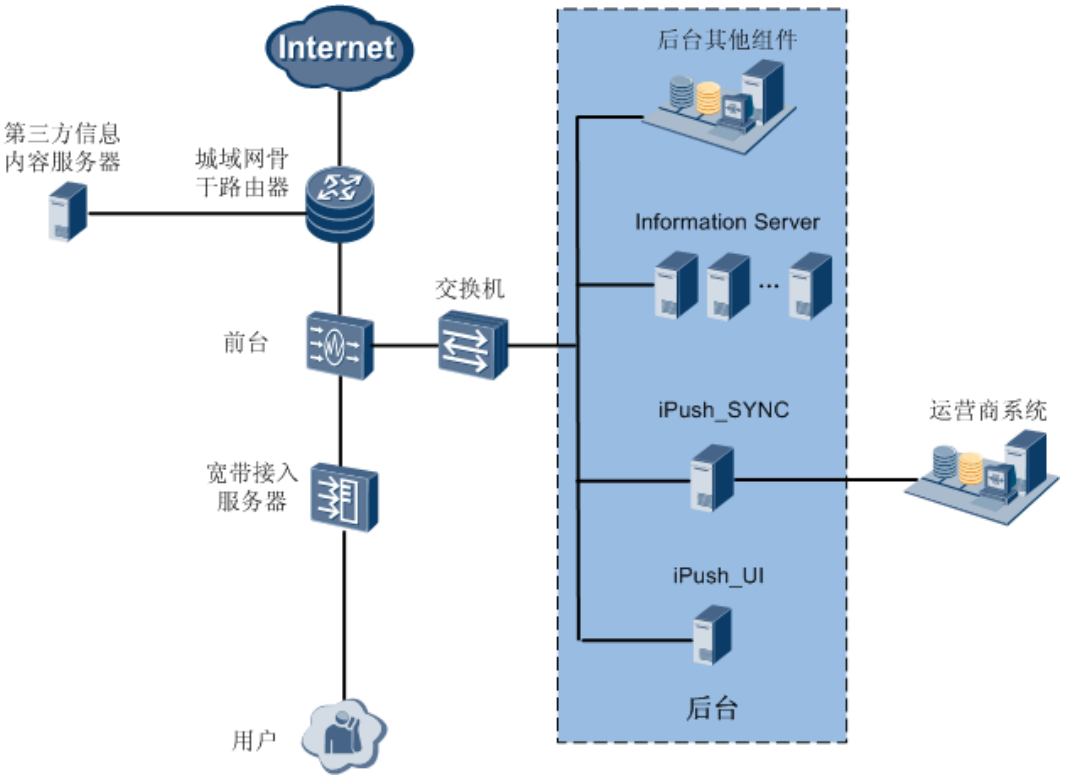
4.7 信息推送

iPush 信息推送系统可以向上网用户推送不同类型的信息（支持固网上网用户和无线数据卡上网用户，不支持手机终端上网用户），利用 iPush 系统客户可以充分利用现有网络资源开展增值业务。

系统组成

iPush 系统是 SIG 系统的子系统，由 iPush_UI（iPush User Interface Server）、Information Server、iPush_SYNC（iPush Data Synchronization Server）和第三方信息内容服务器组成，如图 4-13 所示。

图4-13 iPush 系统组成示意图



iPush 各组件的功能介绍如下：

- iPush_UI：信息推送用户界面服务器，提供 iPush 系统的管理界面，管理员可以基于管理界面完成业务管理、报表查询、权限管理和系统管理。
- Information Server：信息服务器，提供推送信息的具体内容，确认并记录信息推送结果。
- iPush_SYNC：信息推送数据同步服务器，用于从客户系统同步用户的账号、套餐或资费信息。
- 第三方信息内容服务器（可选）：提供推送信息的具体内容。

说明
如果部署第三方信息内容服务器，则第三方信息内容服务器负责提供推送信息的具体内容，信息服务器负责确认并记录信息推送结果。

信息受众

信息受众也即推送对象，是指一个或多个用户的集合。

在 iPush 系统中，用户是指在 SIG 系统中配置的公众客户，也即普通客户，如 ADSL 拨号上网用户和无线用户。

iPush 系统支持向特定类型的信息受众推送信息：

- 向指定区域的所有用户推送信息。
- 向指定区域的指定终端用户组推送信息。

终端用户组在 iPush 系统中配置，其中可以添加一个或多个用户。

- 向指定同步用户组推送信息。

  同步用户组是指 iPush 系统从 SIG 系统中同步的公众客户用户组。公众客户用户组在 SIG 系统中配置，其中可以添加一个或多个用户。

- 向指定属性组推送信息。

  属性组是指一个或多个属性的组合，所有属性值都匹配的用户在推送范围内。属性是 iPush 系统从 SIG 系统中同步的公众客户分组属性。公众客户分组属性在 SIG 系统中配置，分组属性按照属性值可以将公众客户区分为有限的组，如：性别、基站、小区等。

iPush 系统还支持对特定类型的信息受众不推送信息：

- 对免推送用户组不推送信息。

  免推送用户组在 iPush 系统中配置，其中可以添加一个或多个用户。对于不想收到 iPush 系统推送的信息的用户，可以将其加入免推送用户组。

- 访问免推送网址时不推送信息。

  免推送网址在 iPush 系统中配置，可以添加一个或多个网址。如果需要在用户访问某些网址时不向用户推送任何信息，可以将这些网址配置为免推送网址。

信息分类

iPush 系统支持信息分类和信息子类，以便于管理推送信息。iPush 系统还支持设置信息分类优先级，用于定义多条信息的推送顺序。系统预定义信息分类包括以下 2 种：

- 公告

  用于向终端用户发布新闻、系统升级公告等信息。

- 资费信息

  用于向终端用户发布用户账户余额信息或套餐到期信息，提醒用户及时充值以免影响业务的正常使用。

除以上 2 种系统预定义的信息分类外，系统管理员还可以自定义信息分类和信息子类。

信息管理

iPush 系统提供灵活多样的手段进行信息管理：

- 多种信息样式

  iPush 系统预定义了多种样式，支持指定信息内容并使用预定义样式展现信息。iPush 系统还支持直接使用带有信息样式的外部 URL 信息或本地信息文件，展现形式由信息文件自定义。

- 分时段推送

  设置信息的有效期，并可以在有效期内按周、小时分时段向终端用户推送信息。iPush 系统支持灵活的推送时间间隔，可以针对单用户或区域内所有用户设置推送时间间隔。

- 信息优先级

对于一个用户同时有多个策略生效时，按照信息分类的优先级和策略的优先级进行推送，信息分类的优先级高于信息策略的优先级。

- 推送次数可配置
  - 对于不限次数推送的信息，不设置推送总次数，只要在策略有效期内，满足推送时间间隔就一直推送。
  - 对于指定推送次数的信息，在策略有效期内满足推送条件时推送，达到推送次数后停止推送。
- 信息状态

  支持通过信息状态管理信息创建、审核、发布、结束的完整流程，信息状态分为 5 种：初始化、待审核、已发布、更新、结束。

5 操作与维护

5.1 网络管理

SIG 系统支持多种管理方式；可以与支持 SNMP 标准的网管系统对接；同时系统能够提供完善的告警和日志，帮助管理员迅速定位并解决系统问题。

支持多种系统管理方式

SIG 系统支持网络管理功能，支持的管理方式包括：

- 通过基于 B/S 架构的 Web UI 进行业务和用户管理。
- 分布式部署集中管理。
- 多级分权分域管理（不同级别的管理员在不同的管理域上有不同的权限）。
- 命令行（支持 SSH）。

支持与 SNMP 网管系统对接，同时提供 SIG 系统内嵌的网管系统

SIG 系统能够与支持 SNMP 标准的网络管理系统对接（例如：华为 U2000、M2000），并将硬件和业务异常告警记录并上报网管系统，同时支持 MIB 信息。

如果您没有购买与 SIG 配套的第三方网管系统（例如：华为 U2000、M2000），或第三方网管与 SIG 系统间出现故障，或第三方网管发生单点故障时，可以使用 SIG 提供的网元管理系统 EMS（Element Management System）实现 SIG 系统的自监控、自管理，具体功能包括：网元管理、系统管理、故障定位等。

SIG 系统支持的网管协议包括：

- SNMP V1
- SNMP V2c
- SNMP V3

提供完善的告警和日志

SIG 系统能够提供完善的前、后台告警信息，帮助管理员迅速定位并解决系统问题。告警信息类型主要包括以下几种：

- 通讯告警

这类告警与信息传送的处理进程有关，包括网元之间、网元与操作系统之间或者操作系统之间的通信失败时产生的相关告警。

- 业务质量告警

  这类告警是由于业务质量退化问题而引起的，包括发生拥塞、性能下降、资源占用率高、带宽减小等业务质量降低时产生的告警。

- 处理出错告警

  这类告警是由于软件或处理过程错误而引起的，包括软件错误、内存溢出、版本不匹配、程序异常中止等业务处理时产生的告警。

- 设备告警

  这类告警是由于物理资源故障而引起的，包括电源、风扇、处理器、时钟、输入/输出接口等硬件设备产生的告警。

- 环境告警

  这类告警是由设备所在地相关的问题而引起的，包括设备所处环境的温度、湿度、通风等不符合设备正常工作要求时产生的告警。

SIG 系统提供丰富的日志信息，主要包括：

- 操作日志

  操作日志记录各用户在 SIG 的 web 客户端发起的各种操作。当系统出现故障时可通过操作日志查看特定时间段的操作情况，帮助维护工程师定位故障。同时，审计人员可通过 web 导出和查看操作日志，定期审计操作维护人员所作的操作，及时发现不当或恶意操作。

  操作日志主要包括以下内容：

  - 账户登录相关事件。例如：登录、退出等操作。
  - 账户管理相关事件。例如：账户的增、删、改，口令更改，权限变更。
  - 系统管理相关事件。例如：对系统各参数值的增、删、改。

- 运行日志

  运行日志主要记录系统和服务器运行情况相关的信息，由系统的各个业务模块产生。维护工程师可通过查看运行日志了解并分析系统的运行状况，及时发现并处理异常和故障。运行日志主要包括以下内容：

  - 系统运行过程中的异常状态和异常动作。例如：配置失败。
  - 系统运行过程中的关键事件。例如：系统启动、系统关闭。
  - 系统管理相关事件。例如：系统各参数值的增、删、改。

- 操作系统日志

  SIG 后台使用 SUSE Linux 11 操作系统，由操作系统记录其日志，SUSE Linux 操作系统支持以下类型的系统日志：

  - 操作系统内核日志。
  - 操作系统启动日志。
  - 用户操作记录。
  - 进程信息。
  - 内存信息。
  - 硬件信息。

- 文件句柄信息。
- 网口流量信息。
- 系统中断信息。

- 数据库日志

  SIG 后台使用 Oracle 数据库，Oracle 日志包括以下内容：
  - 数据库运行日志：记录数据库运行状态的日志。
  - 审计日志：记录数据操作的日志。

5.2 权限管理

权限管理完成 SIG 系统本身的权限控制，主要通过权限管理（包括：业务权限、数据权限）和安全接入实现。

权限管理

- **相关名词**

  系统权限管理涉及的名词主要包括：
  - 管理员

    使用 SIG 后台管理系统的人员。
  - 操作

    使用业务需要完成的动作。例如：配置策略、查看审计日志、导入用户等。
  - 角色

    根据职能对管理员进行分类的方式。例如：“审计日志管理员”角色可以查看审计日志；“用户管理员”角色可以导入用户。

  说明
  - 一个角色对应一组操作。
  - 一个管理员可以同时拥有多个角色。

- **业务权限管理**
  - 基本概念

    业务权限是执行某操作的权限。管理员如果要执行某操作，必须先拥有该操作对应的业务权限。

    例如：“重置其他管理员的密码”是一个业务权限，“二级区域管理员”是个角色。可以把“重置其他管理员的密码”这个业务权限分派给“二级区域管理员”角色。相应地，所有的“二级区域管理员”即可执行“重置其他管理员的密码”操作。
  - 使用场景

    业务权限的使用基于以下场景：
  - 不同的管理员有不同的角色。
  - 不同的角色执行不同的操作，完成不同的任务。
  - 存在一些操作，只能由某些管理员，而不是全部管理员可以执行。

例如：需要“修改其他管理员密码”操作，同时要求只有“一级区域管理员”才可以执行此操作。为了确保只有部分管理员可以“修改其他管理员的密码”，需要给这个操作增加业务权限。

- **数据权限管理**
  - 基本概念

    数据权限是针对某个数据对象执行某类操作的权限。对某个数据对象的操作分为 3 类：
  - 读：可以查看、查询此对象。
  - 写：可以修改、删除此对象。
  - 授权：可以将此对象的数据权限赋予其他管理员。

    相应地，对某个数据对象的数据权限也分为 3 类：读、写、授权。
  - 使用场景

    数据权限的使用基于以下场景：
  - 要对一类数据进行操作，管理员首先应具有该操作对应的业务权限。
  - 对这类数据中的某些具体的数据对象，不同的管理员需要有不同的操作权。

    例如：对于“查看财务报表”操作来说，财务处长和财务会计都有权执行。但是处长可以看到“年度财务报表”，而普通的会计只能看见“月度财务报表”。即不同的管理员针对同一个数据对象有不同的操作权。处长对“年度财务报表”有“读”权限，而普通的会计则对“年度财务报表”没有任何操作权。
  - 管理员的多级管理，分权分域，不同的管理员只能管理相应区域的业务。

    例如：有 2 个管理员都拥有“二级区域管理员”角色，分别是“1 区管理员 a”和“2 区管理员 b”。前者只能针对 1 区的用户配置策略、查看报表；而后者则只能针对 2 区的用户执行该操作。
  - 大客户管理部。

    例如：大客户管理员 A 和 B，管理员 A 只可以管理“1 公司”；管理员 B 则只可以管理“2 公司”。

安全接入

- SIG 系统前台支持 SSH V2.0 协议，可以从远端安全地登录设备进行管理。同时，支持权限分级，可以针对指定 IP 地址进行访问控制。
- 通过 HTTPS（Secure HTTP）方式登录 SIG 系统 Web 服务器，有效保护系统安全。
- SIG 系统支持设置允许访问后台的 IP 地址范围。若试图登录的 IP 地址不在该 IP 地址范围内，将无法访问系统。
- 同一管理账号连续 3 次登录不成功时，锁定该账号（默认锁定 15 分钟），同时会话终止并记录日志。
- 登录 SIG 后台 Linux 操作系统的会话在超过 30 分钟没有活动的情况下将超时，需重新登录。

6 可靠性与安全性

6.1 可靠性

6.1.1 系统级可靠性

支持 Bypass

系统直路部署时，通过 Bypass 设备确保高可靠性。当 SIG 接口板出现故障或整机断电时，系统能够自动切换到 Bypass 保护通路，将业务流量直接转发，切换时间 10ms 以内。同时，在系统升级等维护情况下，支持手动切换 Bypass。

6.1.2 系统组件可靠性

SIG 系统的前后台关键组件（包括：SPS、SAS、RADIUS Proxy、OMC、PLS、DAS、DB、DSE 等）在设计上通过备份实现可靠性。

SPS 可靠性

SPS 每个框内采用 N+M 冷备。每个 SPS 与 OMC 通过心跳检测存活，当某个 SPS 出现故障后，OMC 启动备份的 SPS，同时通知接口板变更分流策略，将分配到原来故障 SPS 的数据分配到备份 SPS。

SAS 可靠性

SAS 采用 N+M 冷备，物理部署时每个业务处理板上部署一个 SAS（只有 CPU0 可以部署 SAS）。系统集群多框部署时，多个前台的 SAS 共同实现 N+M 冷备，如果单个 SAS 出现故障，OMC 通知 SPS，SPS 将原来发往故障 SAS 的数据直接发给备份 SAS。

OMC 可靠性

OMC 部署在 MPU（Main Processing Unit）板上，MPU 板采用 1+1 热备份。OMC 利用 MPU 板的备份机制，对用户的配置策略及设备注册信息在主备 MPU 板之间进行备份。

另外，SIG 系统支持双主 OMC。备用 OMC 备份主 OMC 的集群配置以及实时运行信息，当主 OMC 故障时，备用 OMC 切换为主 OMC，保持集群继续运转。

6.1.3 硬件可靠性

SIG9800-X 设备在单板、风扇、电源等硬件方面进行了可靠性设计。

单板的冗余设计

SIG9800-X 重要单板的冗余设计可有效保证设备的可靠性，具体情况如下：

- 交换网板
  - SIG9800-X16 的交换网板支持 3+1 备份。
  - SIG9800-X8 的交换网板支持 2+1 备份。
- 主控板

  SIG9800-X 各设备的主控板均支持 1+1 备份。
- 业务板

  SIG9800-X 各设备的业务板均支持 N+1 备份。

风扇的冗余设计

SIG9800-X 设备的风扇均为冗余设计，当其中一个风扇故障时，不影响整个系统的正常散热。具体情况如下：

- SIG9800-X16 有 4 个风扇框，每框有 1 个风扇，共 4 个风扇，为 3+1 备份。
- SIG9800-X8 有 2 个风扇框，每框有 1 个风扇，共 2 个风扇，为 1+1 备份。
- SIG9800-X3 有 1 个风扇框，含 2 个风扇，为 1+1 备份。

电源的冗余设计

通过电源的冗余设计，增强了 SIG9800-X 设备供电的可靠性。具体情况如下：

- SIG9800-X3 设备的电源支持 1+1 备份，一个电源模块故障不影响系统正常工作。
- SIG9800-X16 设备的电源为分区供电，支持 4+4 备份。
- SIG9800-X8 设备的电源为分区供电，支持 2+2 备份。

单板支持热插拔

SIG9800-X 设备的主控板、交换网板、业务板、接口板均支持热插拔。即允许带电插拔，且不影响系统及其他单板（子卡）的业务正常运行。

6.2 安全性

组网安全

SIG 系统部署在客户网络内部，与接入网络之间没有协议栈，不对外暴露 IP 地址。因此，外部无法通过 IP 地址对 SIG 系统进行攻击，保证了系统的安全。除此之外，SIG 系统包括两种典型安全组网。

- 前台、后台同地部署

  SIG 前台和后台部署在同一站点的同一个安全域内。前台管理网口和后台均为私网地址，即公网 IP 地址的终端用户无法访问 SIG 系统，以保证系统安全。

- 前台、后台异地部署

  在 SIG 前台与后台异地部署（即部署在物理相隔的两个站点），或者 SIG 后台之间的异地部署（如：后台异地容灾）场景下，业务数据会经 Internet 传输。此时需要在两个区域之间部署 VPN，使用 IPSec 加密传输数据，并且在区域与 Internet 之间架设防火墙，确保数据传输的安全。

个人数据安全

- 个人数据使用目的

  SIG 系统基于保障网络运营和提供增值业务的目的，保存了公众客户的基础数据。

- 个人数据内容

  SIG 系统保存的公众客户基础数据包括：

  - 账号、IP 地址。
  - 所属区域、所属小区基站。
  - 用户姓名、性别和住址（非必须内容，客户根据需求选填）。

- 个人数据应用场景

  SIG 系统使用个人数据的场景包括：

  - 维护公众客户基础数据。包括：增加、修改、删除、查询公众客户信息。
  - 查询或导出公众客户相关的报表。

- 个人数据保护机制

  SIG 系统通过以下技术措施确保个人数据安全：

  - 安全组网

    用户管理需使用的后台 GUI 不提供公网访问地址，一般用户无法访问。管理员远程访问 SIG 时，管理员和 SIG 分别部署在安全域内，此时在两个安全域间部署 VPN，使用 IPSec 加密传输的通信数据。

  - 安全通信协议

    要求通过 HTTPS、SSH V2.0 协议登录系统。

  - 登录认证保护

    登录后台 GUI 要求使用用户名、密码和验证码，登录后台服务器或数据库均要求使用用户名和密码。

  - 角色和权限控制

    根据角色划分账户权限内容，只赋予账户所需操作必备的最小权限。

  - 个人数据匿名化处理

    对于传给不在信任网络域的第三方的个人数据，支持将个人数据匿名化处理。

- 个人数据保存时间

  SIG 保留公众客户数据是基于保障网络运营和提供增值业务的目的，不永久保留公众客户的行为数据。数据过期后，系统自动删除过期数据。

- 公众客户流量数据：可根据用户需求设置
- 5 分钟粒度数据：保留 1 天
- 1 小时粒度数据：保留 7 天
- 1 天数据：保留 6 个月
- 1 月数据：保留 4 年
- 公众客户访问 URL
- 1 小时粒度数据：保留 7 天
- 1 天数据：保留 6 个月
- 1 月数据：保留 4 年
- VoIP 详细话单：保留 6 个月

操作系统安全

- 操作系统软件安装
  - 只安装业务需要的软件包与服务组件，减少系统漏洞，降低系统遭受攻击的风险。
  - 使用最新或最稳定的操作系统，并及时更新操作系统的安装补丁。
  - 系统安装时对操作系统进行安全加固，禁止 root 远程登录，对操作系统的系统服务进行安全设置。
- 最小化网络服务和端口开启
  - 端口开放必须基于服务，无用的端口默认关闭。
  - 网络服务只能绑定到提供该服务的网路接口（例如：SSH 服务只能绑定在管理接口）。
- 最小化启动服务
  - 不启动路由选择守护进程，防止被攻击者或者渗透测试者使用。
  - 不启动日志接收功能，简单防止 DoS 攻击。
  - 禁止通过 X11 协议的转发，防止信息泄露。
  - 设置最大并发连接数，简单防止 DoS 攻击。
- 内核调整

  安全加固时，关闭或禁用可能造成系统安全问题的内核参数和服务，如关闭 TCP_timestamps 支持、关闭 ARP 代理，禁止发送网关的 ICMP 重向。
- 系统日志
  - 记录所有与认证相关的事件。
  - 记录守护进程产生的 Debug 日志。
- 审计日志
  - 记录所有与认证相关的事件，包括登录错误、**su** 命令和其他鉴权事件，帮助分析用户登录情况。
  - 记录定时任务产生的日志。
  - 系统的审计日志有专门的日志服务器，支持远程日志功能。
- 系统接入、认证和授权

  - 用户只分配完成任务的最小权限，只允许应用账号执行应用操作。
  - 使用 PAM 进行权限认证。
  - 不使用快捷键重启系统。
  - 登录 Linux 的会话设置超时时间，默认 30 分钟。
- 账号与操作环境
  - 账号的密码符合口令基本复杂度要求。
  - 支持对反复尝试登录的账号的锁定。

数据库安全

- 数据库软件安装
  - 数据库安装时，只安装必须使用的服务和协议。
  - 不允许在数据库的文件中配置未加密的密码。
  - 安装脚本在保留 7 天之后即自动删除。
- 数据库访问
  - 可执行文件只给必要的用户赋予执行权限。
  - 数据库的配置文件只给必要的用户赋予读写权限。
- 账号管理和密码策略
  - 所有账号都有明确的用途，区分应用账号和管理账号。
  - 数据库厂商提供的默认账号只保留必须使用的，不使用的默认账户锁定或删除，且默认账户只能用于特定任务，不用于日常维护。
  - 用户账号的密码符合口令的复杂度要求。
  - 不设置个人账户、研发账户和测试账户。
  - 支持对账户进行定期审计。
  - 数据库密码至少记录 8 个历史密码，历史密码不能被设置。
- 权限控制
  - 账号只能具备执行任务的最小权限。
  - 应用账号不赋予授权权限。
- 网络接入
  - 所有管理性接口均实现了加密和认证控制（例如：VPN、SSH、HTTPS）。
  - 关闭非专门的和面向 Internet 的管理性接口。
  - 数据库连接（即：用户名/密码@连接串）不在程序中硬编码。
  - Oracle 异地部署的客户端、应用服务器、数据库服务器之间使用 IPSec 加密数据流。

数据传输安全

SIG 使用一系列安全的协议和应用，保证数据传输安全：

- web 应用默认使用 HTTPS 协议。
- 操作系统连接访问默认使用 SSH V2.0 协议。

- 网络通信加密支持 SSL（Secure Socket Layer）和 IPSec（Internet Protocol Security）协议。
- 网管支持 SNMP V3 协议。
- 文件传输默认使用 SFTP 协议。

操作维护安全

SIG 系统从用户、应用、日志等多个层面提供安全机制，构建操作维护的安全性：

- 分组、分级别和分权限的访问机制

  系统采用分组、分级别和分权限的访问机制，管理员登录系统必须提供用户名和密码，登录后只能进行其权限内的操作。

- 安全日志功能

  系统对于重要操作，包括登录、退出等都提供了安全日志功能，可以供后续系统安全审计使用。

- 应用软件安全机

  提供密码和身份认证，采用高强度的数据加密算法对敏感的用户信息数据进行加密保存。系统为每个用户分配一个密码，在为用户提供各种服务时，系统对用户密码进行校验，以保护用户信息的安全性。

- 操作界面自锁定机制

  当管理员中断操作一定时间，界面将自动锁定，防止非法用户的操作。

7 可靠性指标

通过可靠性指标，您可以了解系统可用度、平均故障间隔时间、平均故障修复时间、系统启动时间、Bypass 切换时间等指标。

SIG 系统的可靠性指标如表 7-1 所示。

表7-1 SIG 系统可靠性指标

参数		指标
系统可用度		≥99.999%
平均故障间隔时间（MTBF）		10 万小时
平均故障修复时间（MTTR）		≤5 分钟
系统启动时间		<15 分钟（为空配置情况下的启动时间。配置越多，启动时间越长。）
外置 Bypass 从工作通路到保护通路切换时间	主动切换 Bypass 时间	≤2ms
	Bypass 检测被动切换时间	≤8ms

8 遵循的标准及通过的认证

8.1 产品遵循的标准

SIG 系统遵循的标准如表 8-1 所示。

表8-1 SIG 系统遵循的标准

标准名	标准内容
IEEE 802.3	IEEE standard for local and metropolitan area networks: Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications (includes 802.3ab， 802.3ac and 802.3ad)
RFC0768	User Datagram Protocol
RFC0791	Internet Protocol
RFC0792	Internet Control Message Protocol
RFC0793	Transmission Control Protocol
RFC0826	An Ethernet Address Resolution Protocol (ARP)
RFC0894	A standard for the transmission of IP Datagram over Ethernet networks
RFC1155	Structure and Identification of Management Information for TCP/IP-based Internets, Network Working Group, May 1990
RFC1157	Simple Network Management Protocol (SNMP)
RFC1213	Management Information Base for Network Management of TCP/IP-based internets: MIB-II 2.Draft Standards
RFC1293	Inverse Address Resolution Protocol
RFC1661	Point to Point Protocol(PPP)
RFC1889	RTP: A Transport Protocol for Real-Time Applications
RFC2748	The COPS (Common Open Policy Service) Protocol

标准名	标准内容
RFC2865	Remote Authentication Dial In User Service (RADIUS)
RFC2866	RADIUS Accounting
RFC3087	Control of Service Context using SIP Request-URI

8.2 产品通过的认证

SIG9800-X 通过的认证如表 8-2 所示。

表8-2 SIG9800-X 通过的认证

认证	描述
RoHS	欧盟 RoHS（Restriction of the Use of Certain Hazardous Substances）认证
REACH	欧盟 REACH（Registration, Evaluation, Authorization and Restriction of Chemicals）认证
WEEE	欧盟 WEEE（Waste Electrical and Electronic Equipment）认证
MET	美国 MET（Maryland Electrical Testing）认证
CB	国际通用认证 CB（Certification Bodies' scheme）
CE-CERT	欧盟 CE（Conformité Européene）认证
FCC-DOC	美国 FCC（Federal Communications Commission）认证
VCCI	日本 VCCI（Voluntary Control Council for Interference by Information Technology Equipment）认证
IC	加拿大 IC（Industry Canada）认证
C-Tick	澳大利亚 C-Tick 认证