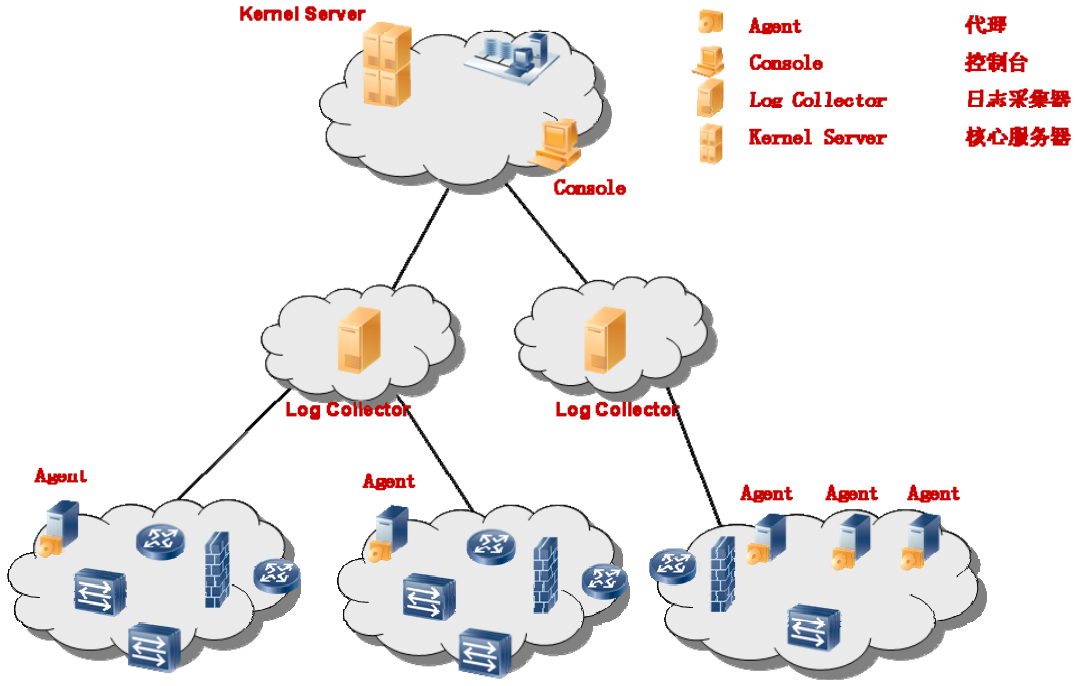
SIMS 日志审计系统产品规格

日志审计产品的组成如图所示，其组成部分包括：

- 控制台
- 日志采集服务器
- 核心服务器
- 代理



日志审计系统结构图

- **控制台**

控制台安装在 Windows 操作系统上，为用户提供图形化的日志管理和系统管理界面。

- **日志采集服务器**

日志采集服务器保存代理及安全设备上报的日志，对日志格式进行转换，并上报到核心服务器。同时，通过日志采集服务器可以对日志进行查询。

- **核心服务器**

核心服务器日志进行管理，并把控制台的操作命令传送至日志采集服务器和代理。

核心服务器包括以下功能：

- 向控制台实时传递日志信息。
- 将控制台发出的指令传递给日志采集服务器及代理。
- 对安全资产进行管理。
- 报表功能

  提供了基于Web的报表生成、分发、管理的一整套灵活方便的报表应用服务。

报表组件不仅支持手工报表和周期报表，还拥有完善的报表分发机制。

主要包括以下功能：

- 手工报表生成
- 周期报表管理
- 报表存储管理
- 报表分发

手工报表生成

手工生成报表是报表操作员根据业务需求，通过手工操作而较为实时的生成所需报表的活动，适用于突发和灵活的小型报表生成。

可以直接用报表模板手工立即生成HTML或Excel手工报表。生成手工报表后，可根据需要保存报表，选择将报表发送到用户报表邮箱、Email邮箱，或以公共报表方式发布、打印报表等。

周期报表管理

周期任务可以周期运行生成HTML或Excel周期报表，它是在报表模板基础上通过定制生成条件、生成信息和分发信息来生成。

生成信息包括：

- 周期类型
- 生成时间
- 命名规则
- 存放位置

周期任务有以下几种类型：

- 生成一次
- 按天生成
- 按周生成
- 按月生成
- 按年生成

创建周期任务后，在用户指定周期时间，系统会自动生成指定格式的报表，并按指定命名规则命名报表，然后按照设定的分发信息发送报表给用户。

周期报表管理支持：

- 创建、查看、查找、修改、移动、恢复/暂停、删除周期任务。
- 手工生成周期报表，查看、保存、发送、删除周期报表。
- 用户可以根据需求创建、重命名和删除周期任务文件夹。

报表存储管理

报表存储管理是对存储区的报表文件夹中的报表进行管理。报表文件夹中报表来自用户的以下操作：

- 将邮件中报表另存到报表文件夹中。
- 将公共报表存到报表文件夹中。
- 将手工报表保存到报表文件夹中。
- 将周期报表存放到报表文件夹中。

报表存储管理支持发送、发布、移动、复制、删除、查找报表。

另外，用户可以根据需要创建、重命名和删除报表文件夹。

报表分发

报表系统拥有独有、方便易用的报表分发机制，提供了如下三种报表分发方式：

- 将报表发送到用户的报表邮箱。
- 将报表发送到用户的外部 Email 邮箱。
- 将报表为公共报表发布。

作为公共报表发布时，所有的报表操作员和查看员都能查看公共报表。

报表操作员和报表查看员可以对报表邮箱中的报表和公共报表可进行查看、保存、转发等管理活动。

● 代理

日志采集代理负责应用类安全对象的日志采集，通常包括各种操作系统（包括Windows、AIX、Solaris、SuSE Linux等）、数据库和WEB SERVER等。

用户通过将代理软件安装到目标安全对象中进行日志数据的采集。当目标安全对象的操作系统启动后，代理软件自动启动守护进程进行日志采集。

路由器、交换机、防火墙等网络设备无需安装代理，只需用户对其进行配置就能采集日志。

日志审计系统支持的日志采集对象

日志采集对象	
操作系统	Windows 2000, WINDOWS XP, WINDOWS 2003 Solaris AIX SUSE Linux
数据库	Oracle Sybase SQL Server Informix
应用系统	Apache IIS

日志采集对象	
	Symantec AntiVirus
防火墙	Huawei Eudemon Firewall CISCO PIX Firewall Netscreen Firewall Checkpoint Firewall ISONE Linktrust Firewall
IDS	Huawei NIP IDS ISS Real Secure IDS ISONE Linktrust IDS
路由器	Huawei Quidway R2621, R2631 CISCO 7206, 7507, 3725, 12016, 2691, 3662, 3640
交换机	Huawei Quidway S3526, S3026, S3050, S3552, S6506 CISCO Catalyst 2950-24, 2950T-48, 6509, 4003, 4506, 4006, 2950G-48, 2924XLv

日志审计系统运行环境

项目	硬件环境参数	软件环境参数
控制台	CPU：Intel Pentium 4 1.3GHz 以上 内存：512MB 或以上 硬盘：40GB 或以上	Windows 2000/ Windows XP 操作系统
核心服务器	平台：SUN Fire V240 或以上 CPU：2x 1.28GHz 或以上 内存：4GB 或以上 硬盘：2 x 73GB 或以上	操作系统：SUN Solaris 8 数据库：Sybase 12.0
日志采集服务器	平台：SUN Fire V240 或以上 CPU：2x 1.28GHz 或以上 内存：4GB 或以上	操作系统：SUN Solaris 8 数据库：Sybase 12.0

	硬盘：2 x 73GB 或以上	

日志审计系统参数指标

项目	硬件环境参数
采集协议	SYSLOG, SNMP TRAP, OPSEC
处理能力	> 500 EPS (Events Per Second)
日志存储	在线存储：2*73G以上，支持磁盘阵列
	离线存储：支持磁带机存储