任天行网络安全管理系统 SA 系列

产品概述

■ **文档编号**	*(请输入文档编号)*	■ **密级**	内部使用
■ **版本编号**	V1.0	■ **日期**	2012-05-08

■ 版权声明

■ 版本变更记录

时间	版本	说明	修改人
2012-5-08	1.0	产品概述	陈翼

■ 适用性声明

本模板用于撰写任子行内外各种正式文件，包括技术手册、标书、白皮书、会议通知、公司制度等文档使用。

目录

一. 产品介绍

任天行网络安全管理系统 SA 系列是任子行网络技术股份有限公司为各行业机构高效解决网络信息安全管理难题而研发的核心产品之一，提供了信息安全管理的全面解决方案。产品通过各种业界领先的技术手段实现上网行为管理和合规细粒度审计，在加强上网机构内外部网络信息控制监管的同时，为避免相关信息外泄及事后的追溯取证提供了有效的技术支撑。产品能够详实记录网络内的各种网络活动；灵活地对网络用户的行为进行多种方式的分组策略控制与审计，实现基于用户的细化和量化的审计与管理，过滤各类不良访问行为；对日志进行深度挖掘，形成丰富多样化的统计报表；安装便捷快速；界面美观易用；主动有效的保护了用户关注的信息，使管理者能更有针对性地加强网络管理，为其规范网络管理、制定正确的管理决策提供有效依据，使用户能够安全、高效、合规地利用网络，最终带来生产力的提升。

该产品是基于硬件的高性能、高稳定性的上网行为管理和内容安全审计设备，一般安装于各种局域网络边缘出口线路上，可以根据实际情况选择以旁路监听或者透明网桥的方式工作，可以根据实际环境的规模选择单机、分布式及其他多种部署方式。产品在设计上采用了先进的模块化、层次化体系结构，集成了高性能数据捕获驱动、快速的并行协议分析引擎、实时内容分析引擎、基于状态的并行内容匹配技术、海量数据全文检索和数据挖掘等业界领先的自主核心技术，运行稳定、可靠，性能卓越。

该产品可广泛应用于政府、军工、教育、医疗、能源、制造、金融、运营商等各种行业单位，是目前国内上网行为管理及内容安全审计产品的首选。产品经过国内权威专家检测，多项指标处于国际先进水平。产品先后获得了公安部公共网络安全监察局签发的计算机信息系统安全专用产品销售许可证、中国人民解放军信息安全测评认证中心签发的军用信息安全产品认证证书、国家保密局涉密信息系统安全保密测评中心签发的涉密信息系统产品检测证书、中国信息安全认证中心签发的中国国家信息安全产品认证证书（3C 认证）等多个国内权威检测机构颁发的认证证书。

二. 核心价值

贯彻落实互联网管理法规

通过对任天行产品的部署应用，无论大到国家法规（如“公安部 82 号令”），还是小到单位自身的网络使用规定，都能够切实落实真正的“合规”管理。

有效提升生产力

基于用户的细化、量化的合理互联网行为控管，能够有效管理网络流量、提升内网可用性，达到有效地规范工作学习中对于互联网的使用，消除上网人员的惰性、侥幸心理，疏导结合，有效提升生产力，使单位网络资源得到最高效的利用，保障重要业务的优先正常运行，使基础设施投资回报最大化并降低管理成本等诸多目的。

规避风险与法律纠纷

通过阻止对各类不良信息的访问和传播，可有效规避由此带来的法律诉讼风险和纠纷；通过对 BBS、Email、WebMail、IM 即时通讯等形式的信息外发活动进行监管，并可实现追本溯源，有效防止信息外泄带来的利益风险。

为企业发展决策提供参考信息

任天行设备独有的十个内置智能报表和管理者界面以及内外网舆情功能为企业管理者提供进过设备智能分析后的各种数据，对企业网络使用现状进行透彻的分析。任天行通过企业网络使用情况，经过智能分析，得出的如员工工作效率、员工离职风险、焦点人物、事件等智能报表，可在管理者做出企业重要决策时做为重要的参考依据。

三. 产品功能介绍

具体指标	功能描述
1. 部署模式	
网桥模式	支持以网桥模式部署，包括单桥和多桥的部署模式；支持 Bypass 功能。
路由模式	支持路由模式部署，可以作为出口网关，包括单出口和多出口的部署模式；并支持防火墙和 NAT 功能。
旁路模式	支持旁路模式部署。
2. 用户识别与管理	
本地认证	支持本地账号认证；
第三方认证	支持 AD 域、RTIUS、LDAP、POP3、刷卡认证等第三方认证；可与第三方认证计费系统结合，把终端认证账号作为实名信息；
实名联动审计	支持 PPPoE、RTius 协议的拨号帐号与上网日志关联；支持在网络环境中存在多种代理服务器时能够准确捕获还原网络日志数据，包括 ISA 代理、Socks4/5、Squid 等 HTTP Proxy；支持代理服务器与 AD 域控制器、LDAP 帐号的联动，自动获取

	代理帐号信息并与上网日志关联，以实现审计实名；
IP、MAC 认证	可以实现人员帐号与 IP 地址的绑定、IP 地址与 MAC 地址绑定、IP/MAC/帐号三方同时绑定，防止非法篡改 IP 地址；
新用户认证	支持默认认证方式，新用户将以默认认证方式接入，无授权不可访问网络；
混合认证	支持多种认证方式并存，不同用户使用不同的终端认证方式；
帐户导入	支持批量导入审计用户，支持系统自动搜索局域网内的所有用户并自动按组归类；
多级组织架构	对于机器管理和帐号管理，可以对自动或手动搜索生成的设备列表采用多层多组方式划分组别，最大层次要求 8 级以上，以实现有针对性的网络控制策略设置和日志查询统计，包括对全局、个别组、个别机器进行网络控制策略设置或查询统计，满足对网络使用情况的多种特殊控制和查询分析需要；
Ip/mac 绑定	可以实现人员帐号与 IP 地址的绑定、IP 地址与 MAC 地址绑定、IP/MAC/帐号三方同时绑定，防止非法篡改 IP 地址； 支持多个 IP 绑定一个 MAC 地址的功能，便于特殊电脑的漫游； 支持在三层交换网络环境下获取用户计算机真实 MAC 地址功能；
免审计 usb-key	支持免审计 key，持有该 key 的人员无论在哪台终端上都不做任何审计；
网址黑白名单	能够自定义网址黑名单、白名单； 支持机器、帐号的黑白名单定义，黑名单封堵，机器和账号白名单无条件放行，日志白名单既不封堵也不记录日志； 白名单支持免审计 USBKEY；
未认证通过用户权限管理	对未认证通过用户有全部封堵、只封堵 HTTP 应用两种权限控制
与计费系统联动	支持与计费系统联动，用计费系统的账号来实现实名审计
组织结构	用户分组支持无限级分组，子组可继承父组策略设置；
3. 应用行为识别	
URL 分类站点库	完备的 URL 分类站点库，总条目数超过 3000 万
协议总量	支持 1500 多种主流网络行为；
IM 识别	支持 QQ、MSN MESSENGER、UC、网易泡泡、飞信等主流 IM 软件
游戏识别	支持在线游戏，中国游戏中心，边锋网络游戏，密传，海天英雄传，凯旋，骑士，征服，天堂，三国演义 远航游戏中心，QQ 网络游戏，浩方网络游戏，茶苑，CS[反恐精英]，热血江湖，问道，星战前夜，圣战，天之炼狱 2，魔兽世界等；
流媒体识别	支持 MMS、RTSP、QQLive、PPLive、网页形式的视频播放等；
炒股识别	支持大智慧、通达信、大福星行情分析、钱龙、同花顺、分析家、龙卷风等主流炒股软件；
P2P 识别	支持迅雷、BT、EMULE 等 P2P 协议；
代理识别	支持在网络环境中存在多种代理服务器时能够准确捕获还原网络日志数据，包括 ISA 代理、Socks4/5、Squid 等 HTTP Proxy；
个性化定制	支持用户对协议进行个性化定制，不识别用户不关心的协议，提升设备性能；
4. 行为、内容审计	
URL 分类站点库	完备的 URL 分类站点库，总条目数超过 3000 万
协议总量	支持 1500 多种主流网络行为；
IM 识别	支持 QQ、MSN MESSENGER、UC、网易泡泡、飞信等主流 IM 软件

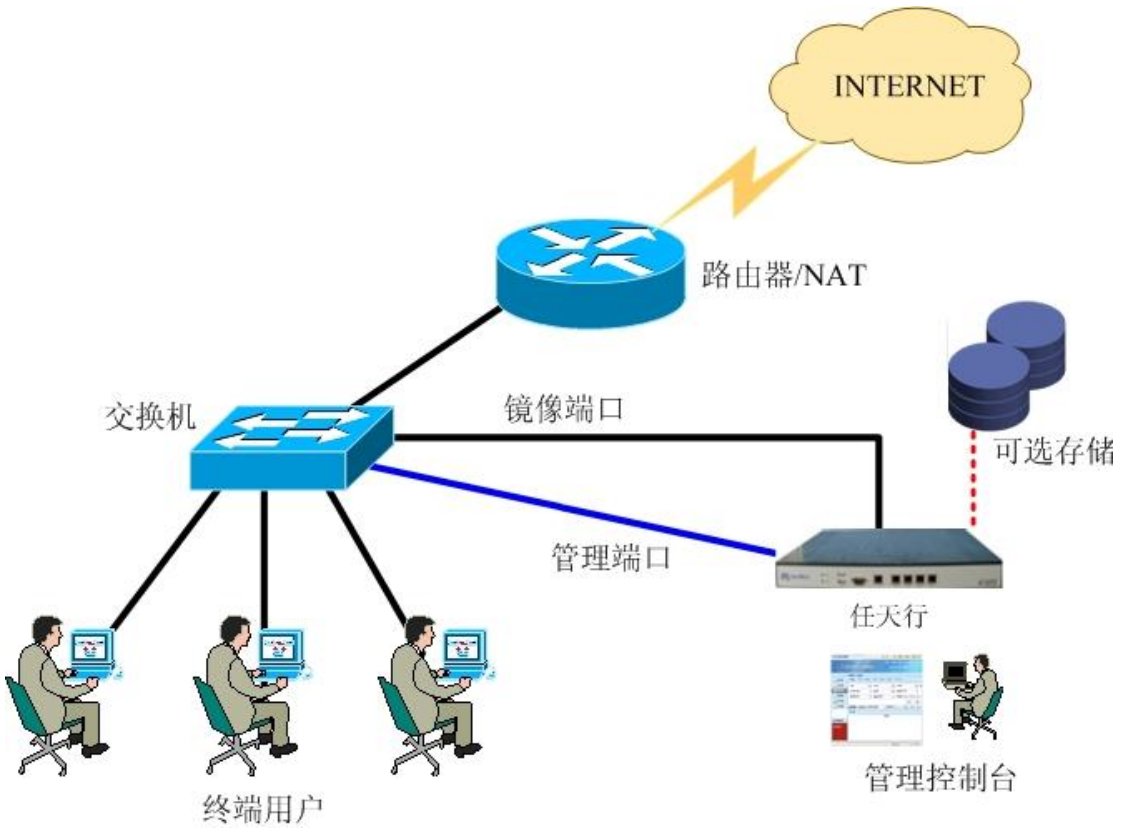
游戏识别	支持在线游戏，中国游戏中心，边锋网络游戏，密传，海天英雄传，凯旋，骑士，征服，天堂，三国演义 远航游戏中心，QQ 网络游戏，浩方网络游戏，茶苑，CS[反恐精英]，热血江湖，问道，星战前夜，圣战，天之炼狱 2，魔兽世界等；
流媒体识别	支持 MMS、RTSP、QQLive、PPLive、网页形式的视频播放等；
炒股识别	支持大智慧、通达信、大福星行情分析、钱龙、同花顺、分析家、龙卷风等主流炒股软件；
P2P 识别	支持迅雷、BT、EMULE 等 P2P 协议；
代理识别	支持在网络环境中存在多种代理服务器时能够准确捕获还原网络日志数据，包括 ISA 代理、Socks4/5、Squid 等 HTTP Proxy；
个性化定制	支持用户对协议进行个性化定制，不识别用户不关心的协议，提升设备性能；
网站审计	支持网站访问地址，标题的全文审计；支持网站关键字的审计及过滤；
网页论坛	支持各种论坛发帖的审计还原；可支持发帖关键字审计；
Webmail	支持 weimail 邮件标题，正文，附件的完全审计及还原；
电子邮件	支持基于 smtp,pop3 协议的邮件的正文，标题，附件的完全审计及还原；支持内容关键字，附件内容关键字的审计和还原；
5. 网页行为控制	
站点库	支持内置站点库分类及自定义站点文类；
关键字检索	支持地址，端口，访问标题的快速检索查询；
网页过滤	支持基于 URL，网页关键字的网页过滤；
6. 文件行为控制	
站点库	支持内置站点库分类及自定义站点文类；
关键字检索	支持地址，端口，访问标题的快速检索查询；
网页过滤	支持基于 URL，网页关键字的网页过滤；
7. 日志与报表	
数据统计报表	可根据自定义时间，对所有协议的上网情况进行统计，统计类型包括排名、趋势、应用结构、访问资源统计等，可生成列表、柱状图、饼图或圆环图等，以及各种上网情况的分布图。统计条件包括时间类型、报表类型、开始时间、结束时间、名次等。工作时间可方便自定义，以便进行各种分析和统计。可自定义不同级别的对象（机器/帐号、分组）、自定义统计数据列、自定义排序，生成自定义报表，自定义报表可灵活生成上述各种图形；
报表订阅	能够对各种报表设置自动订阅，周期性报表自动发送到指定邮箱；
日志查询	可以显示、查询所有用户的上网行为日志。查询条件包括源 IP/MAC、目的 IP、协议类型、开始时间、结束时间等，可以进行单个或多个组合查询，结果可以 Excel、HTML、TXT 等格式导出； 记录机器的上、下线操作，形成上下线日志供查询； 记录设备本身的所有操作，形成系统操作日志供查询； 记录设备发送邮件信息，形成系统邮件日志供查询；
多条件组合查询	对于内容审计结日志和报警数据，可按源 IP/MAC、目的 IP、协议类型等进行单个或多个组合查询，分别显示查询结果；查询的时间段，用户能够自己选择和定义。对于审计记录的查询要求条件丰富、使用方便，支持多条件查询；

全文检索	支持全文检索功能，能够在指定日志摘要条件的同时对指定关键字进行内容查询。在硬盘空间足够大的情况下，允许在单台设备查询所有日志数据，不设置查询日志数据条数上限，支持多个内容关键字组成逻辑表达式的查询；
海量日志快速检索	通过全文检索的方式，查询日志量在 500G 以上数据，速度在 20S 以内；

四. 部署方式

天行系统通过可选的分布式部署与基本的旁路/串接部署方式灵活的结合起来，在不同网络环境下达到不同的管理和控制目的。在以下是几种典型的部署方式示意图。

4.1 单台旁路铜纤镜像

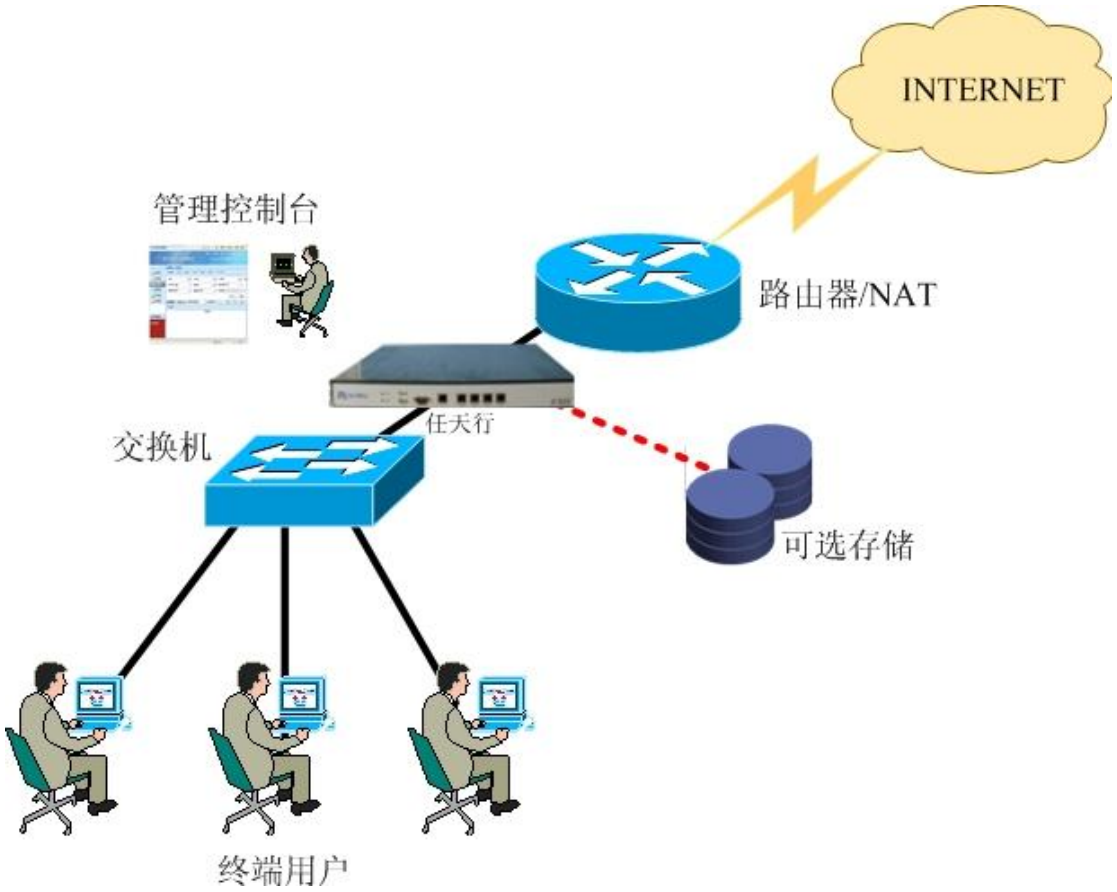


适用环境：用户交换机支持端口镜像，镜像端口连接介质为铜缆。

方案说明：此方案为任天行设备旁路接入最典型的代表方案，用于中小型企业、学校等简单的二/三层网络，任天行设备通过交换机的镜像端口获取原始数据进行协议还原。

方案特点：对原网络性能无影响，布署简单方便，易维护。

4.2 单台透明网桥

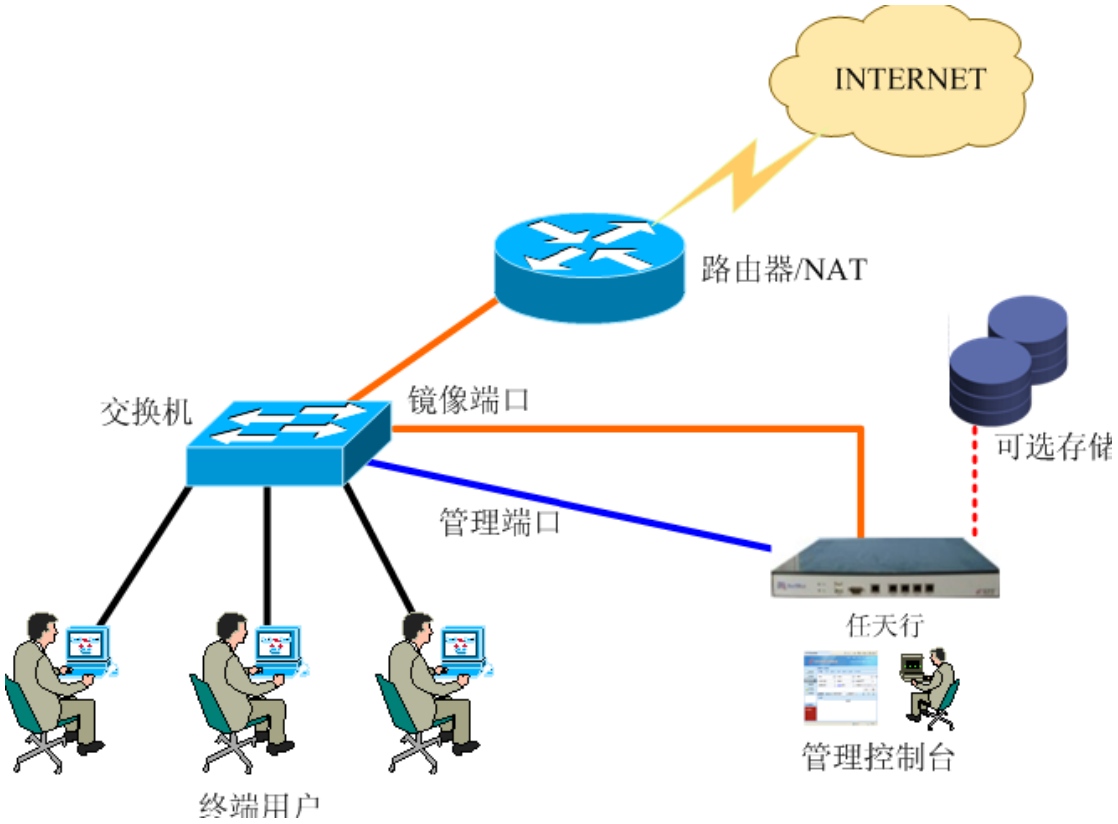


适用环境：对网络行为控制有较高要求的用户，端口连接介质为铜缆。

方案说明：此方案为任天行设备串接接入最典型的代表方案，用于中小型企业、学校等简单的二/三层网络，任天行设备通过网桥端口获取原始数据进行协议还原。

方案特点：对各种上网行为有强大的控制能力，同时保留了旁路方式的审计功能。

4.3 单台旁路光纤镜像

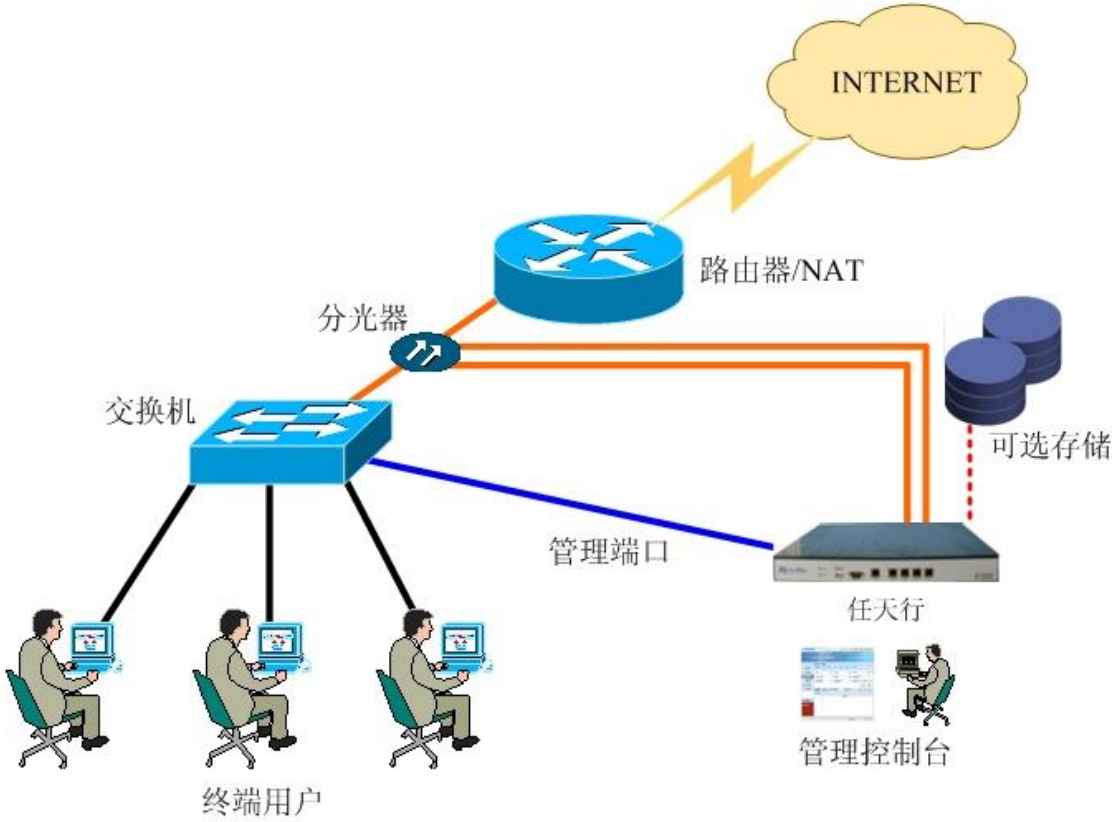


适用环境：用户交换机支持端口镜像，镜像端口连接介质为光纤。

方案说明：此方案为任天行设备最典型的代表方案，用于中小型企业、学校等简单的二/三层网络，任天行设备通过交换机的镜像端口获取原始数据进行协议还原分析。

方案特点：对原网络性能无影响，布署简单方便，易维护。

4.4 光纤网络单链路分光

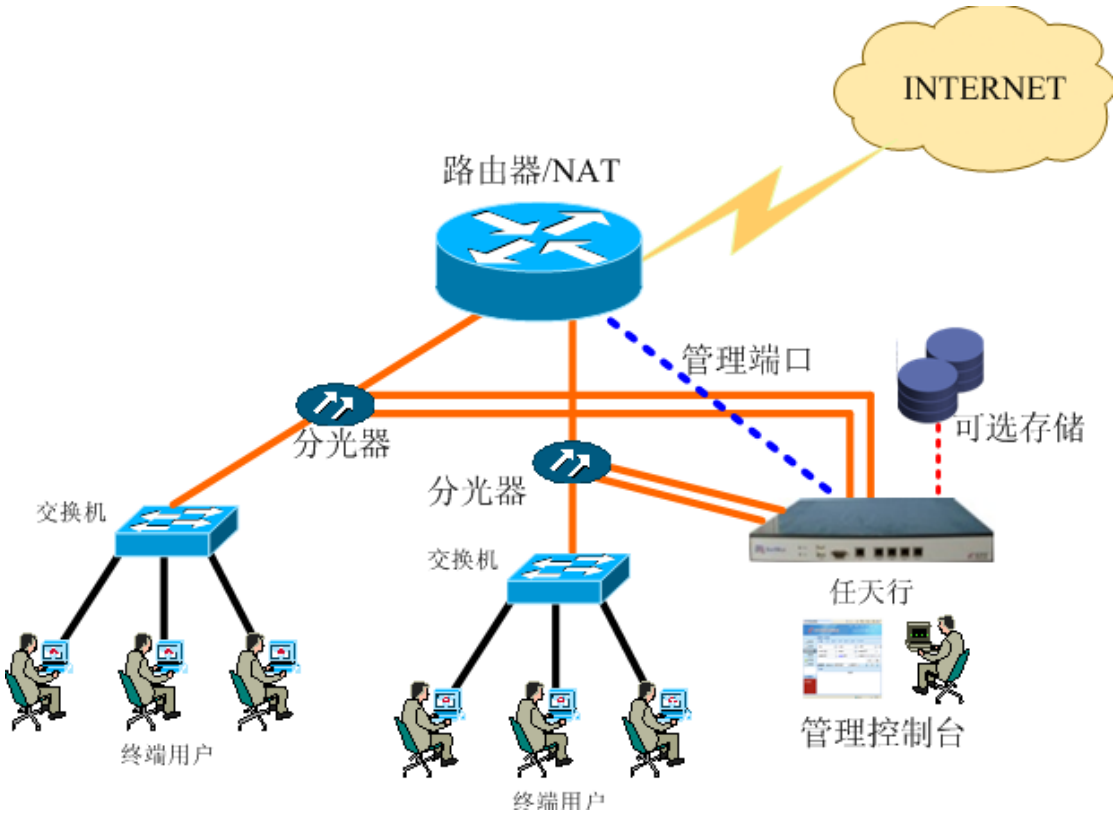


适用环境：用户交换机不支持或无法做端口镜像，交换机与路由器上连为单对双向光纤。

方案说明：此方案为解决千兆线路情况下，交换机无法做镜像时采用分光的一种方案。分光器对双向链路分别进行分光，之后通过设备的 2 个光口捕获数据还原分析。

方案特点：此方案用于解决传输介质为光纤且无法对数据进行进镜像的网络环境，该方案为典型的光纤以太网布署任天行的方案。

4.5 光纤网络双链路分光

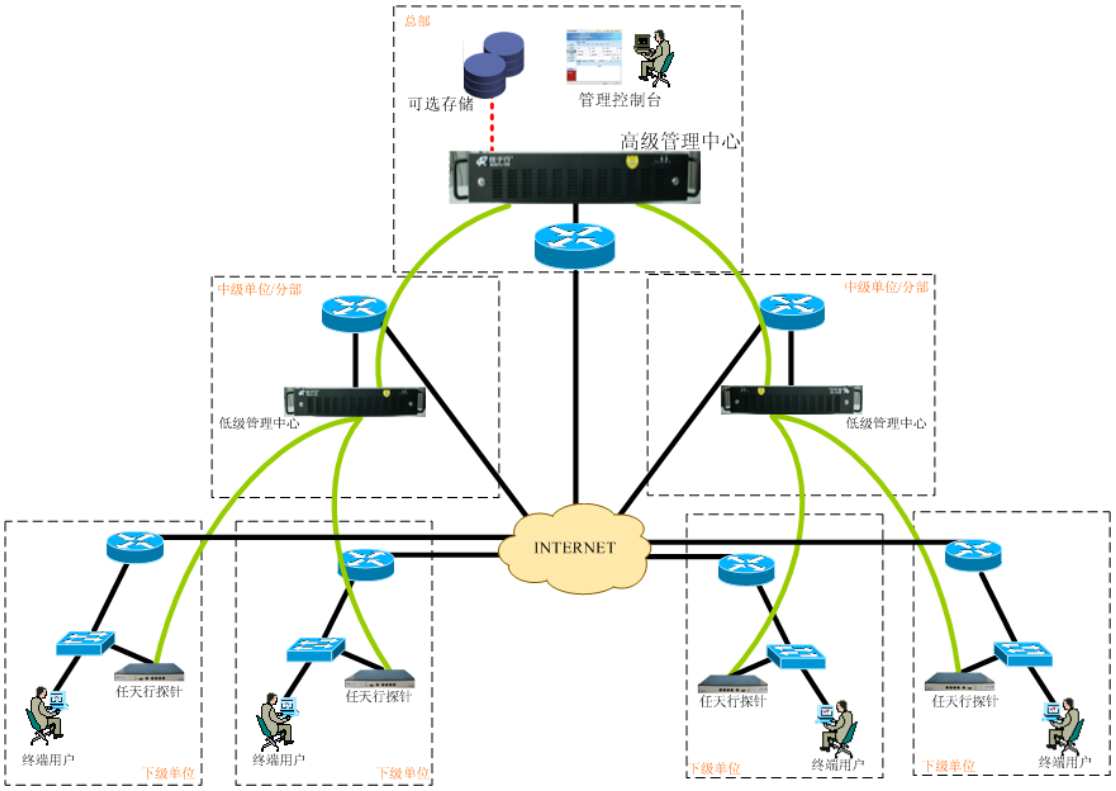


适用环境：用户交换机无法做端口镜像，用户同时具有 2 个独立的物理网络，或一个逻辑网络由两台核心交换机组成一个热备/均衡的网络。

方案说明：此方案为解决千兆线路情况下，交换机无法做镜像时采用分光的一种方案，也用于两台核心交换机组成均衡/热备的网络。分光器对两组双向链路分别进行分光，之后通过设备的 4 个光口捕获数据还原分析。

方案特点：此方案用于解决千兆网络环境下，传输介质为光纤且无法对数据进行进镜像的网络环境，可用一台任天行设备同时对两个网络或一个冗余网络进行数据捕获，该方案为典型的光纤以太网布署任天行的方案。

4.6 多点分布式



适用环境：用户有多个独立出口物理网络，每个物理网络的核心位置分布于多个地点。对于大型企业集团，政府机构，教育机构，网络访问的出口分布在各个分支机构或下级单位中，但是总部往往又需要对整个组织部署的各套任天行设备进行统一的管理。

方案说明：该方案由多台任天行探针组成，每台探针完成单个网络数据的获取及部分协议还原，探针与任天行管理中心相连，可由任天行管理中心统一设定下发审计与控制策略，管理信息由任天行管理中心发出，通过网络将管理数据发送到每个独立探针，各探针的审计数据可以选择性汇集到中心服务器，实现中心的集中控管与数据查询。

方案特点：每个不同流量的物理网络可以选择不同性能的任天行探针，由管理中心统一管理，解决多个物理网络管理复杂的现状。