任天行网络安全管理系统 SA 系列

技术白皮书

■ 文档编号	*Pro-SA-003*	■ 密级	内部使用
■ 版本编号	V1.0	■ 日期	

■ 版权声明

■ 版本变更记录

时间	版本	说明	修改人

■ 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. 前言

近年来，随着宽带网络技术的不断发展以及网络基础设施的完善，Internet 的应用越来越广。政府机关、企事业单位、大专院校等各种组织机构都进行了信息化建设，利用互联网或虚拟专用网来进行协同管理，信息发布，借以降低成本，提高生产力。然而，信息系统的快速发展和网络安全管理问题的日益凸现，使二者成为一对如影随形的同步矛盾体，并行地呈现在网络管理人员的面前。

除了常见的上网人员利用工作时间娱乐、购物、聊天、进行 P2P 下载、在线游戏等无序上网行为外，由于网络访问的方便性与匿名性，加之电子信息复制的快捷简易，部分用户通过网络有意或无意地泄露了重要的机密信息，并且往往难于得到追查和取证。这些行为导致管理机构投资加大、风险提升、企业文化扭曲，而整体工作效率下降和企业信息管理混乱。因此，网络技术的广泛应用，尤其是不加监管的网络应用逐渐成为这些组织的效率杀手，甚至给这些组织带来一些不必要的麻烦。具体表现有以下几种：

- **上班时间浏览与工作无关信息**

  有关统计资料显示，企业员工平均每天有三分之一的上班时间是在网上浏览与工作无关信息；在员工从外部网络下载各种信息中，只有 25%的下载信息与其所从事的工作有关。企业缺乏有效的上网管理手段，将会导致企业的工作效率下降，这是与企业上网的初衷相违背的。

- **给企业带来法律纠纷**

  跟据国家相关法律的规定，在外部网络上发布淫秽信息与及迷信、反动、分裂等言论均为违法行为，有些企业员工滥用公司网络进行了上述行为，将把企业拖进复杂的、难以脱身的法律纠纷当中。

- **网络带宽的滥用阻碍了正常业务使用**

  在一些上网用户比较多的企业中，有些用户不停地下载大容量的文件或者在线听音乐、看视频电影，这些行为都会严重占用网络带宽，造成网络堵塞，上网速度下降，影响其他员工的正常上网行为，使重要的网络业务无法得到有效的保障。

- **通过网络使企业的机密信息外泄**

  由于对外网访问的方便性与匿名性，加上电子信息复制的快捷简易，使得企业内部用户通过外部网络有意或无意地泄露企业的机密信息，并且难于追查

和取证。这对企业参与公平竞争的威胁巨大。

- **互联网的滥用带来安全隐患**

  互联网中存在大量的恶意站点、黑客、木马工具、病毒程序等，不加限制地访问这些站点、使用这些工具，会给企业带来安全隐患，影响企业网络的正常使用。

如何规范网络使用，提高网络使用效率，同时避免互联网、虚拟专用网使用过程中的负面影响，关系到各机构的整体竞争力，是各机构在信息化建设过程中非常关键的一环。为了有效解决上述问题，部署专业的上网行为管理和审计产品势在必行。此类设备的安装和使用，能够帮助管理者针对上网人员、协议/应用、内容、流量、时间等几个关键维度进行灵活的审计和控制，对用户的网络应用信息进行跟踪式的记录和分析，从而及时发现网络应用中存在的问题，使其有方向性、有针对性地实施进一步有效的整合和管理。

二. 产品概述

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。

三. 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经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。任天行通过对企业网络使用情况的智能分析，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作为重要的参考依据。

四. 产品特点

4.1 识别上网应用

■ **行为识别**

面对互联网高速发展而产生的各种不断更新的版本、全新的乃至加密的应用，任天行产品研发团队一直专注跟踪随时出现的各种网络流行应用，并不断在升级过程中实现协议和应用分析的更新。产品在庞大的 URL 分类数据库和应用识别能力基础之上提供了全面的行为和内容安全审计功能。

■ **内容识别**

在对关键字的内容审计功能上，任天行系列产品采用基于状态机的多模匹配算法，极大地提高了匹配效率和关键字识别的准确性，为可靠的内容关键字审计功能提供了业界领先的技术保障。其中基于多编码的智能关键字匹配技术，更是独家率先解决了对国内部分地区特有语种（如维文、藏文等）的关键字匹配和内容审计问题。

■ **对象识别**

- 将上网人员与上网机器形成明确的对应关系，认清用户是谁，使用何种具体应用，采用独创的信息实名技术手段，对其实施准确、清晰的管理。
- 任天行系列产品支持包括 IP+MAC 地址绑定认证、本地 Web 认证、AD 域认证、LDAP 认证、USB KEY 身份认证、刷卡认证、三层交换环境 MAC 探测和白名单免监控管理等多种对象识别技术，可以实现对组织机构内部数量庞大的用户身份精准识别。

4.2 创新技术手段

■ **先进的系统体系结构**

系统设计上采用了先进的模块化、层次化体系结构，基于面向对象的思想和插件化的并行协议栈，具有高度灵活扩展性，充分体现了资源的共享，提高了运行效率和稳定性。

■ **高效的捕包引擎技术**

使用 Intel 高性能网卡、独创零拷贝技术驱动、DMA 直接内存存取技术，使得系统在高负载下捕包分析的不稳定性与不安全性减至最小，而性能和可靠性却得到了极大提升，处理效率比传统捕包引擎提高 1 倍以上。

■ **高性能海量数据检索**

独有的高性能海量数据检索引擎，在浩如烟海的审计数据查询与分析中表现出卓越的性能。

■ **核心技术 领航安全**

任天行多项技术突破了内容信息安全领域的难点和重点，填补了国内空白，具有独立的知识产权。作为国内信息安全领域的先行者，产品通过公安部检测中心、中国人民解放军信息安全认证测评中心及国家保密局评测中心的检测与认证,是国内网安市场推荐的优秀品牌。

4.3 有效管理网络

■ **全面的上网行为管理**

- 针对网络应用管理混乱所造成的不良影响，任天行产品提供了一系列贴近用户的 4W1H 五维智能化网络行为控管功能。
- 产品支持包括对网页/各种在线娱乐软件/P2P 下载工具/在线视音频/流媒体/炒股软件/各种文件传输工具/IM 即时聊天软件/Telnet 等多种方式的信息收发内容记录、关键字过滤、文件传档管控、报警。

■ **深度细粒审计管理**

- 产品能够全面详实地记录网络内流经监听出口的各种网络行为，支持关于上网行为、内容、时间、用户等多种条件组合的信息审计策略和日志分析，全面监测各种网络行为，进行深度细粒审计。
- 内容审计既能进行无条件记录，又能通过策略指定访问者（IP 地址/帐号/分组）、时间范围、内容关键字等有针对条件的记录管理用户需要的访问内容。
- 不管是行为审计还是内容审计，都具备高度的灵活性、专业性和准确性，能够为管理机构进行事后追查、取证分析提供有力技术支撑。

■ **本地网络管理/异域分布统一管理**

任天行系统除了能够有效的管理本地网络外，也可以选择与任天行网络安全管理中心配合使用，实现异域分布统一管理，分散控制各地网络，达到

DCS 式的管控效果；总部可以统一配发策略，实现网络行为的多点集中控管和数据横向对比分析，从而形成集团全面网络状况报表。通过设定特殊网络策略，可自动获取相关日志或远程主动调取更详细日志，让管理者一目了然，省力省心。

- **别具匠心的管理者界面**

  任天行系统为企业管理层专门定制了一个管理者界面，该界面展现了员工使用的网络的整体情况，管理者可以从这个界面了解到员工的工作效率、心情动态、言论焦点；企业的信息泄露风险、法律风险等能为企业发展决策提供参考的信息。

4.4 多层面自身安全防护

- **系统级安全防护**

  在对操作系统内核进行充分剖析的基础上，在操作系统级对系统各支撑引擎进行了修改和全面优化定制，全面防止攻击与劫持，提升系统整体性能的同时保障自身系统级安全。

- **操作级安全防护**

  多权分离，针对各种不同性质的功能模块可灵活配置权限级别，并提供更强安全性的 USBKEY 自定义敏感权限控制，最大保障自身操作级安全。

- **数据级安全防护**

  采用自主的高效算法对关键审计数据的存储和传输进行加密防护，数据存储防篡改，数据传输防破解，多种加密防护措施保障自身数据级安全。

- **网络级安全防护**

  旁路部署保障对网络性能完全没有影响，保证网络无单点故障，优先保障用户网络级安全，是上网机构在内网和互联网安全监管和保密资格测评过程中最可信赖的安全工具。

4.5 多种灵活部署方案

- **丰富的线路部署方式**

基本的旁路部署，全面支持电口镜像与分路、光口的镜像与分光、电口桥接等多种线路部署方式，在复杂网络环境下的部署游刃有余，运用自如。

- **领先的多路并行捕包**

  业界领先的多路并行捕包技术，单台设备最多支持高达 4 路数据的并行捕获与分析，为在复杂环境下的灵活部署提供先进的技术保障。

- **扩展的多台分布部署**

  对于单台设备无法处理的超大流量环境，支持高扩展性的多台设备分布式部署方案，通过多台设备对超大的流量分而治之，又由统一的管理平台实现对整个网络的透明、统一的管理。

4.6 直观丰富的统计报表

- **支持合规细粒度审计**

  系统提供符合公安部 82 号令、SOX 法案、企业内控管理规范等多种合规审计报告，提供强大、多样化、面向用户需求的统计分析报表。

- **全面准确的统计结果**

  报表汇集流量统计与日志统计分析数据，支持统计排名分析，全面呈现全局运行状况；使管理者能够直观便捷的掌握网络使用情况，为其合理分配带宽资源，制定正确的管理决策提供有效依据。

- **多维清晰的分析形式**

  系统能够智能分析各种上网数据， 得到能够客观反映整个企业状态的报表。

- **智能便捷的输出形式**

  系统拥有数十种报表模板，支持报表自定义；报表可以以 EXCEL、PDF、WORD、HTML 等形式导出保存。根据不同管理层人员，可提供不同报表类型，报表能够通过系统后台自动发送或 Email 自动订阅。

五. 功能介绍

针对用户对网络内容安全管理的需求，任天行网络安全管理系统 SA 系列提供如下主要功能以实现对网络使用的高效管理。

5.1 网络行为审计

任天行系统能够全面详实地记录网络内流经监听出口的各种网络行为，并根据国家有关法规规定保存至少 60 天，以便进行事后的审计和分析。日志以加密的方式存放，只有管理者才能调阅读取。网络行为日志全面地记录了包括使用者、分组、访问时间、源 IP 地址、源端口、源 MAC 地址、目的 IP 地址、目的端口、访问类型、访问地址/标识等关键数据项。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；支持 GRE(通用路由协议封装）和 MPLS（Multi-Protocol Label Switching，多协议标签交换）两种协议及其应用环境下的网络数据审计还原。产品支持的协议和应用数量达到 260 多种，为国内领先。主要包括以下类型的协议和应用：

- **标准协议及其衍生应用**

  基于 HTTP 协议的网页浏览（GET）、网页提交（POST），其中 POST 应用可细分为 WEBMAIL、WEBBBS、WEBCHAT（聊天）、WEB 登录等上网行为，对基于 HTTPS 加密协议的网页浏览行为也将记录其关键数据；基于 TELNET 协议的远程登录；基于 FTP 协议的文件传输；基于 SMTP/POP3 的电子邮件收发、基于 Samba 协议的文件共享传输、基于 HTTP 的搜索引擎访问等。任天行系统将全面记录基于这些协议的行为日志和必要的帐号、文件名等关键信息。

- **即时通讯（IM）/网络电话应用**

  包括 QQ、MSN、ICQ、雅虎通、新浪 UC、网易泡泡、Google Talk、飞信、阿里旺旺、搜 Q、E 话通等 10 多种国内外流行的 IM 或网络电话应用软件，任天行系统将全面记录这些 IM/网络电话应用的行为日志和必要的帐号信息。

- **流媒体/网络视频直播**

  标准的 MMS、RTSP 流媒体播放协议和主流视频网站和视频直播软件所使用的视频直播应用协议（QQLIVE、PPLIVE、PPStream、优酷、酷六、六间房、新浪视频、搜狐视频、网易视频、央视高清等）。

- **P2P 下载应用**

包括 BT、eMule 等国内外流行的 P2P 下载应用协议。

- **娱乐/游戏应用**

包括国内外流行的数种娱乐游戏平台和大型网络游戏，例如：联众、浩方、边锋、QQ 游戏、中国游戏中心、游戏茶苑、远航、CS、魔兽世界、武林外传、征服、跑跑卡丁车、劲舞团、大话西游、冒险岛等数十种网络游戏，任天行系统将全面记录这些娱乐/游戏应用的行为日志和必要的帐号信息。

- **财经证券类**

能够对国内流行的证券软件所使用的协议记录行为日志，主要包括以大智慧、钱龙、核新同花顺、通达信、大福星、龙卷风等研发厂商为核心的国内各大证券商数十种 OEM 版本，如安信证券、广发证券、国联证券、银河证券、招商证券、方正泰阳证券、湘财证券、国信证券等。

- **网上银行/网上支付**

能够识别通过客户端、网页登陆的网上银行、网上支付应用，支持的银行有：工商银行、招商银行、建设银行、农业银行、光大银行、交通银行、中国银行、民生银行、中信银行、上海浦东发展银行、华夏银行、深圳发展银行、广东发展银行、邮政储蓄银行、兴业银行、平安银行、渤海银行、杭州银行、重庆银行、浙商银行、成都银行、大连银行、齐鲁银行、东莞银行、东莞农村商业银行、广州银行、汉口银行、台州银行、河北银行、长沙银行、重庆农村商业银行、天津银行、上海农村商业银行、青岛银行、深圳农村商业银行、上海银行、包商银行、北京农村商业银行、北京银行、哈尔滨银行、徽商银行、江苏银行、宁波银行、南京银行、吉林银行；支持的网上支持有：支付宝、快钱、易宝支付、财付通、贝宝、我爱卡。

- **远程控制协议**

支持识别主流远程控制协议，包括 SSH、远程桌面、PCAnywhere、QQ 远程控制（2010、2011）

- **代理工具**

能够识别各种代理工具，如 socks4/5、HTTP-Tunnel、HTTP-Proxy、ISA（包括 ISA2000、ISA2004、ISA2006、ISA2010）等。

- **数据库访问**

支持对 MS-SQLSERVER、ORACLE 等主流关系型数据库的远程访问和操作信息审计记录。

系统还提供了一系列的日志管理功能，包括存储管理、备份、恢复等，使用上具备高度的灵活性和专业性。

5.2 网络内容审计

针对互联网上流行的可还原协议，任天行系统能够在记录网络内流经监听出口的各种网络行为产生的具体内容，包括正文、文件等信息，并根据国家有关法规规定保存至少 60 天，以便进行事后的审计和分析，我们称这个范畴的审计功能为内容审计。内容审计既能够无条件记录，又能通过策略指定访问者（IP 地址/帐号/分组）、时间范围、内容关键字等条件下进行有条件的记录管理用户需要的访问内容。主要包括以下类型的协议和应用：

- **标准电子邮件**

  标准电子邮件是指 POP3 /SMTP 两个使用最广泛的收发邮件协议。系统将详细记录访问者（IP 地址/机器名/帐号）、目标 IP 地址、邮件时间、发件人、收件人、正文、附件等信息，并提供附件下载备份功能。

- **网页浏览**

  网页浏览是指基于 HTTP 协议的 GET 请求产生的查看网页内容。系统将详细记录访问者（IP 地址/机器名/帐号）、目标 IP 地址、访问时间、网页 URL、网页详细内容等信息，并提供模拟访问的功能以达到还原后的仿真浏览。支持对 google, baidu, sogou, soso 等常见搜索引擎的搜索关键字记录，并具备良好的扩展能力，支持用户自定义其它搜索引擎。

- **远程登录**

  远程登录是指基于 TELNET 协议的远程登录访问。系统将详细记录访问者（IP 地址/机器名/帐号）、目标 IP 地址、访问时间、TELNET 帐号、TELNET 交互命令和执行回显等信息。

- **文件传输**

  文件传输是指基于 FTP 协议的文件传输、下载及其命令操作。系统将详细记录访问者（IP 地址/机器名/帐号）、目标 IP 地址、访问时间、FTP 帐号、FTP 交互命令和执行回显等信息，对 FTP 交互过程中发生的上传和下载文件操作，系统也将涉及的文件全部还原并提供下载备份功能。

- **即时聊天**

  目前能够捕获还原详细内容的即时聊天工具包括 MSN（Windows Live Messenger）、Yahoo Messenger、中国移动飞信等。系统将详细记录访问者（IP 地址/机器名/帐号）、目标 IP 地址、访问时间、聊天帐号、详细聊天内容等数据，并将聊天内容按次分组保存和展示。

- **加密即时聊天**

部分即时聊天工具对聊天内容进行了加密。一般手段很难获取到解密后的聊天内容，任天行网络安全管理系统 SA 系列通过特有的破解手段，能识别出如 QQ 等加密即时聊天工具的聊天内容。

- **网页外发数据**

网页外发数据是指基于 HTTP 协议的 POST 请求向外部的网站发布信息。由于 HTTP 的 POST 应用非常灵活，往往被用来实现多种应用，因此对网页外发数据的处理有其特殊性。任天行系统使用了独有的表单特征匹配技术框架，摒弃了传统的逐个 WEB 网站分析方式，突破了逐个分析方式带来的有效网站数量限制，可以准确分析出 100%的 POST 外发信息和文件，对 WEBMAIL、网页论坛等应用方式的识别率高达 95%以上。系统针对应用 HTTP-POST 最为广泛的 WEBMAIL、网页论坛、网页聊天、网页登录进行了应用方式识别并将其分类展示，对不能识别的其它 POST 应用则全部归类到“POST”中进行展示。系统记录的主要数据包括访问者（IP 地址/机器名/帐号）、目标 IP 地址、URL 地址、访问时间、外发文本内容、外发文件等数据，并提供外发文件的下载备份功能。

- **数据库访问**

支持对 MS-SQLSERVER、ORACLE、MySQL、DB2、Syabse、PostgreSQL、Informix 等 7 种主流关系型数据库的远程访问和操作信息审计记录，能够记录详细的操作内容，包括对数据库的增删改等敏感操作语句。

5.3 网络行为控制

对于多数企事业单位而言，如何通过有效的技术手段实现对单位职员上网行为进行规范的管理和控制是一个非常有意义的课题。任天行系统提供了丰富的网络行为控制功能，以协助管理者实现上述目标。

- **应用封堵策略**

对局域网内所有机器生效的外网访问权限控制。可根据人员帐号、机器、机器组对不同的时间段设置，可设置的应用封堵类型包括：

- 网页类：可根据 URL 关键字、下载类型、搜索关键字、IP 网站、网页内容关键字、POST 网址、HTTPS 加密网页、自定义站点等组合条件进行设置。
- 邮件类：对于 SMTP/POP3/IMAP 标准电子邮件协议，可根据服务器、邮箱地址、邮件标题、邮件正文、附件名、附件内容等多中关键字组合条件进行设置。
- 即时通讯：针对流行的 10 多种即时通讯应用，可根据应用类型和内容关键字进行设置，针对 MSN、QQ 文件传输、雅虎通、飞信等明文传输的即时通

讯应用可根据内容关键字封堵。

- 网络游戏：支持近百种流行网络游戏的封堵设置。
- P2P 下载：支持流行的 BT、eMule 等典型 P2P 下载进行设置。
- 文件传输：主要针对 FTP 文件传输，可根据服务器、文件类型、帐号、传输内容等关键字进行设置。
- 远程登录：主要针对 TELNET，可根据服务器与账号进行封堵设置。
- 音视频：支持流行的近 20 种网络音视频应用进行设置。
- 财经股票：支持流行的 20 多种财经股票行情与交易应用进行封堵设置。
- 网上银行：支持封堵国内各个银行的客户端和网页登录。
- 远程控制：支持封堵如 SSH、远程桌面、PCAnywhere 等远程控制工具。
- 代理工具：可封堵 socks4/5、HTTP-Tunnel、HTTP-Proxy、ISA 等代理上网工具。
- 自定义协议：可以自己根据需要基于特殊 IP、端口的自定义协议设置封堵。
- 分类站点：系统内置 3000 多万 URL 分类站点库，可根据这些分类设置封堵。
- 数据库：支持针对 SQL Server、Oracle、Mysql、DB2、Sybase、PostgreSQL、Informix Online 数据库的帐号、服务器 IP 地址、sql 关键字进行封堵。

■ **流量控制**

流量控制可实现用户在某一个时间段的带宽限制和保证。用户可自由设定在这个时间段能拥有的上下行最大带宽，以及在网络资源紧张的情况下，用户对象最少能拥有的上下行保障带宽。并且可对同一用户的不同的源、目的端口，目的 IP、不同应用的流量设置不同的流量控制和带宽保障。

■ **流量限制**

可对任意用户对象或团体设置每日、每周、每月的上下行流量或总流量进行上限设置，超出设置的上限之后将禁止上网。

■ **IP/MAC 绑定**

可以灵活设置多种形式的 IP/MAC 绑定，用于限制非法修改 IP 地址与移动办公的应用场景，包括单一绑定、一个 IP 绑定多个 MAC、多个 IP 绑定一个 MAC 等方式。

■ **黑白名单**

- 机器黑白名单：可基于 IP 或 MAC 设置，对于被设为黑名单的机器，系统将无条件禁止其与外网的一切通讯。对于被设为白名单的机器，则其的网络访问不受全局或局部策略的影响，在任何条件下都不对其进行封堵，其网络日志可灵活设置为是否记录。
- 站点黑白名单：可基于目标 IP 或网址设置，对于被设为黑名单的站点，则网络内的所有机器（白名单机器除外）都不能访问此站点。对于被设为白名单的站点，则网络内的所有机器（黑名单机器除外）都可以访问此站点。
- 帐号黑白名单：在帐号控制模式下应用，对于被设为黑名单的帐号，系统将无条件禁止其与外部网络的一切通讯。对于被设为白名单的帐号，则其的网络访问不受全局或局部策略的影响，在任何条件下都不对其进行封堵，但其网络日志仍将被记录。基于帐号的控制可有效避免动态 IP 地址环境或 IP 人为变更造成的网络控制漏洞。
- 免审计 KEY：给特殊用户配置上网时豁免审计与控制的 USBKEY。

5.4 上网用户管理

局域网内的上网用户管理，在任天行系统中是重要的一个环节。它不仅为管理者提供了方便的管理功能，而且在配合网络行为控制与审计策略的配置实施过程中起到基础性的关键作用。对于上网用户的组织架构，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，最大层次可达 16 级。用户管理部分的主要功能包括：

■ **组织管理自动分组**

用户可根据实际的网络规划，对系统管理的 IP 地址段、IP 段分组规划进行事先设置。根据事先设定的搜索范围，任天行系统将自动获取指定范围内的机器信息资料，包括机器名、分组、IP 地址、MAC 地址等，也可进行手工搜索，在机器管理功能中可对这些信息进行增、删、改、导入、导出、设置控制方式等操作。随着系统总的识别方式的设置不同，机器管理也将以 IP 地址或 MAC 地址字段作为机器的唯一标识。

在认证识别方式下，系统还提供帐号管理功能，可对上网认证的帐号进行增、删、改、注销上网、本地文件导入、帐号分组管理等各种操作；对基于 USB 锁的上网认证器则提供对应的上网认证器的配置、密钥导入等管理功能。

■ **用户识别方式**

- 企事业单位接入外部网络的方式各不相同，其内部局域网的组网方式、设备等环境也千差万别。任天行系统能够针对各种不同的网络环境，结合用户的组网规划和对网络控制的不同需求，采取灵活的上网控制方式设置，应对各种差异化需求。

- 任天行系统支持的上网识别方式包括认证识别和透明识别。认证识别是指用户上网之前必须经过上网认证操作才能接入互联网；透明识别是指不需经过认证，系统可适应复杂多变的网络环境，根据 IP、MAC、各种外部认证帐号等多种方式自动识别用户特征，实现上网实名审计。
- 透明识别方式包括：AD 域帐号识别、HTTP 代理用户识别、IP 识别、MAC 识别、POP3 账号识别、PPPoE 帐号识别等。
- 认证识别方式包括：客户端认证、本地 WEB 认证、远程 AD 认证、远程 ESMTP 认证、远程 LDAP 认证、远程 POP3 认证、远程 RADIUS 认证等。
- 针对各种不同的用户环境设置灵活多样的控制方式，使任天行系统最大限度地与用户现有的认证环境相结合，保护已有投资。

5.5 统计分析与智能报表

根据历史上网日志数据统计产生丰富详细的报表，包括分组上网排名、人员上网排名、网络应用统计、访问资源统计、趋势分析、自定义报表等。可按年度、月度或者指定时间范围生成周期性报表。报表种类包括柱状图，饼图，曲线图，折线图等。报表可以以 EXCEL、PDF、WORD、HTML 等形式导出保存。并支持自定义的周期性报表自动生成和订阅。任天行支持的统计分析功能包括：

■ **智能报表**

任天行将审计到的数据经过智能分析，形成各种智能报表，目前内置有离职风险报表、工作效率报表、行为违规报表、安全风险报表、泄密风险报表、法律风险报表、焦点人物报表、焦点事件报表、带宽资源评估报表、互联网指数报表。并且用户可自定义其他类型报表。

■ **统计报表**

可根据用户、行为、流量、上下机、搜索引擎、时间、外发文件等多个维度对各种网络活动在自定义的时间周期内输出表格形式的统计数据。

■ **用户分析**

以上网用户为统计主体，对其各种网络行为在自定义的时间范围、自定义的团体范围内进行基于日志数量的上网活动分析，输出柱状统计图表。

■ **行为分析**

以某一种具体的网络行为为统计主体，在自定义的时间范围、团体范围内进行基于日志数量上网排名分析，输出柱状统计图表。

■ **流量分析**

以上网用户为统计主体，在自定义的时间范围、团体范围内进行基于流量的上网排名分析，输出柱状统计图表。

■ **上机分析**

以上网用户为统计主体，在自定义的时间范围、团体范围内进行基于上机次数的排名分析，输出柱状统计图表。

- **搜索分析**

  以搜索引擎关键字为统计主体，在自定义的时间范围、团体范围内进行基于关键字的排名分析，输出柱状统计图表。

- **趋势分析**

  以上网用户为统计主体，在自定义的时间周期、团体范围内进行基于各种上网行为次数的时间趋势分析，输出折线统计图表。

- **外发文件分析**

  以上网用户为统计主体，在自定义的时间周期、团体范围内进行基于外发文件次数的排名分析，输出柱状统计图表。

- **报表订阅**

  对于上述各种统计报表，可实现自定义条件的周期性报表订阅，订阅后系统将按照预先定义条件自动生成统计报告并自动发送到用户指定的邮箱。

- **订阅历史**

  可以在系统中查询以往订阅的历史报表。

5.6 系统管理与配置

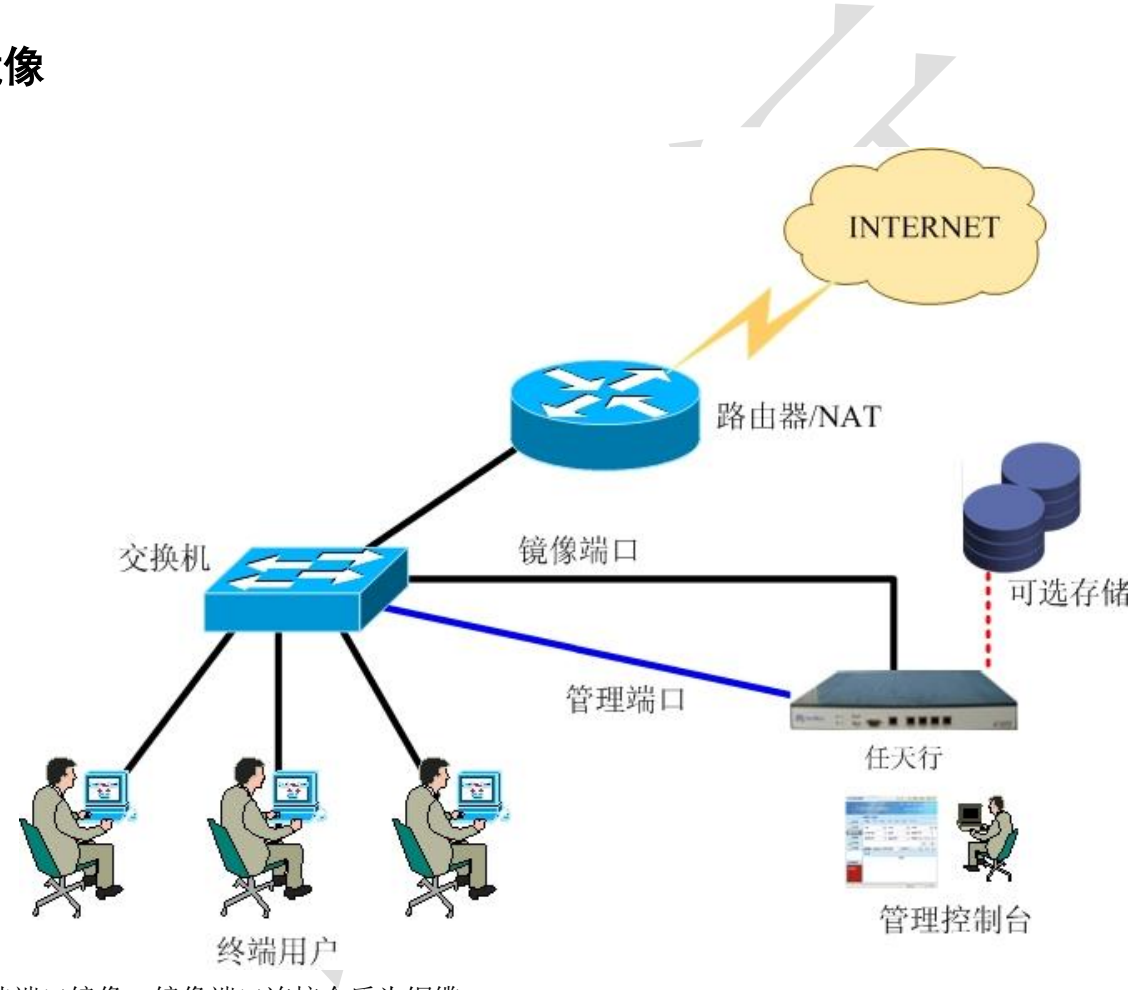
为了保障系统正常、稳定、有效、安全地运行，任天行系统本身的管理设置和附加功能必不可少。其主要作用在于为系统提供符合网络环境要求的基础性参数设置、为系统提供足够的访问管理权限安全保障、为一些故障判断提供辅助工具等。包括但不限于：IP 地址位置查询、网络诊断工具、自定义站点分类、角色与权限管理、连接管理中心参数设置、产品升级、远程维护开关等。

六. 典型部署

任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。以下是几种典型的部署

方式示意图。

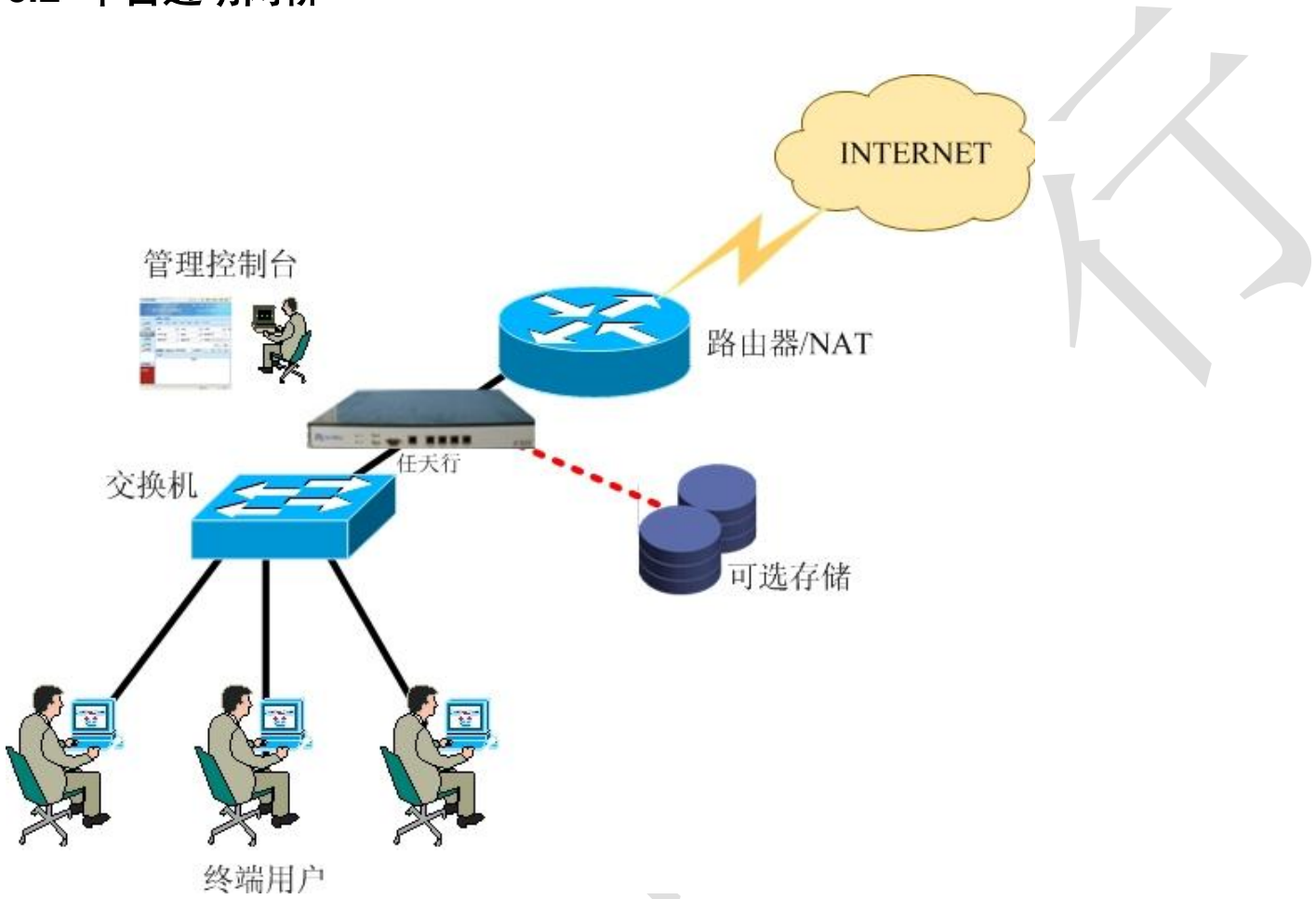
6.1 单台旁路铜纤镜像



- 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。

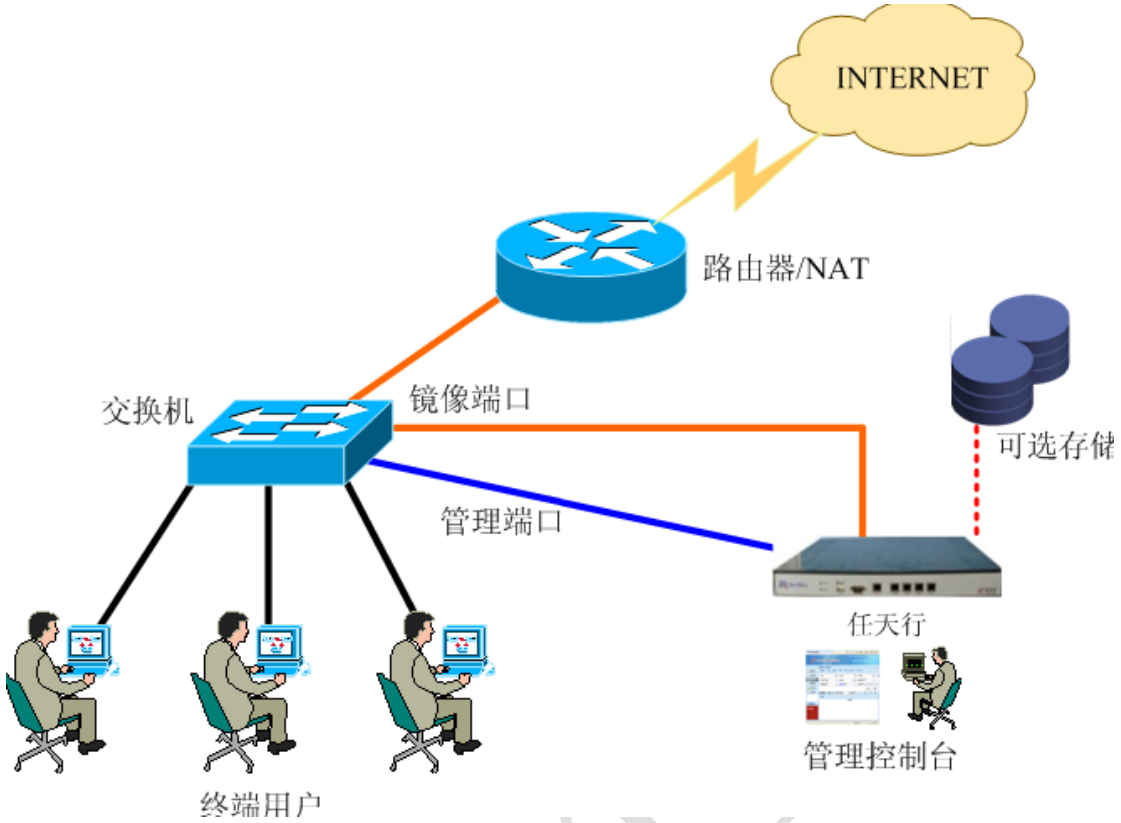
6.2 单台透明网桥



- 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。

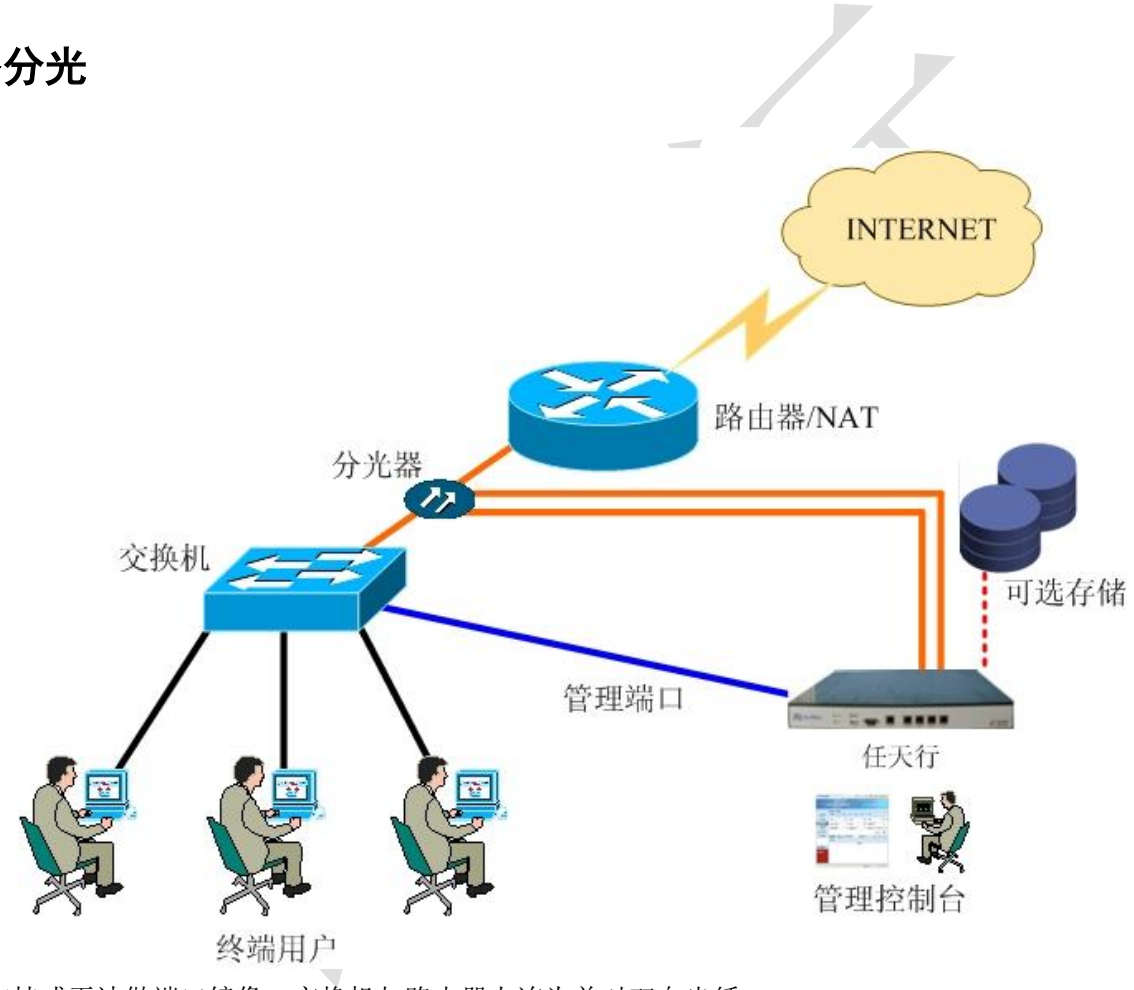
6.3 单台旁路光纤镜像



- 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光纤镜像最典型的代表方案，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，部署简单方便，易维护。

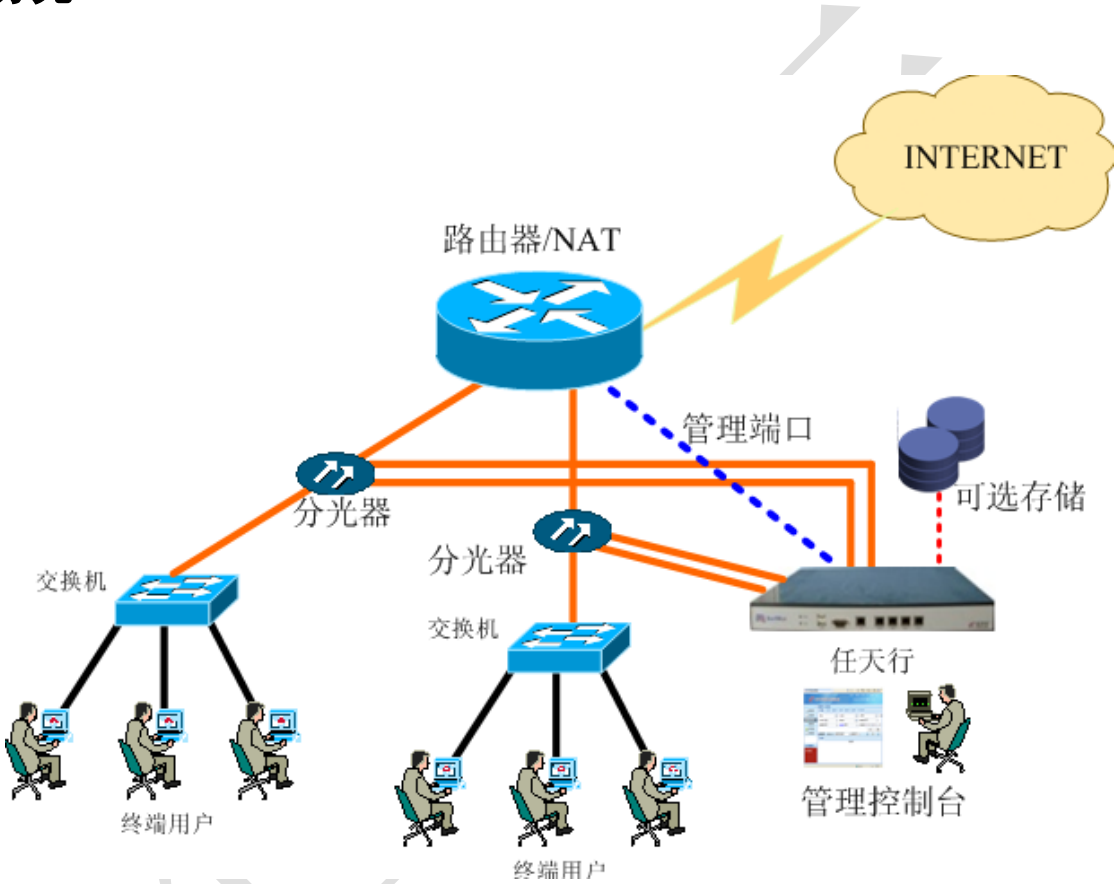
6.4 光纤网络单链路分光



- 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部署任天行的方案。

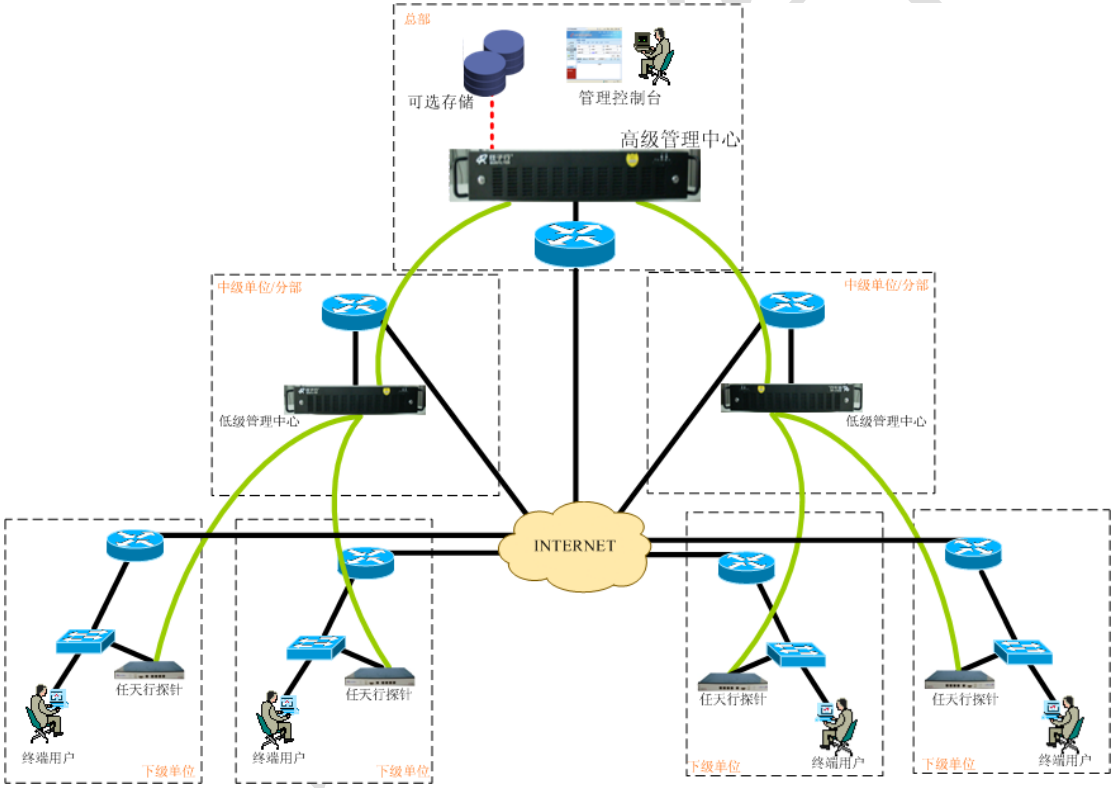
6.5 光纤网络双链路分光



- 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部署任天行的方案。

6.6 多点分布式



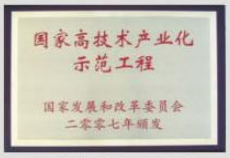
- 适用环境：用户有多个独立出口物理网络，每个物理网络的核心位置分布于多个地点。对于大型企业集团、政府机构、教育机构、网络访问的出口分布在各个分支机构或下级单位中，但是总部往往又需要对整个组织部署的各套任天行设备进行统一的管理。
- 方案说明：该方案由多台任天行探针组成，每台探针完成单个网络数据的获取及部分协议还原，探针与任天行管理中心相连，可由任天行管理中心统一设定下发审计与控制策略，管理信息由任天行管理中心发出，通过网络将管理数据发送到每个独立探针，各探针的审计数据可以选择性汇集到中心服务器，实现中心的集中控管与数据查询。
- 方案特点：每个不同流量的物理网络可以选择不同性能的任天行探针，由管理中心统一管理，解决多个物理网络管理
- 复杂的现状。

七. 资质荣誉

公司和产品相关的主要资质和荣誉如下：

公安部销售许可证

涉及国家秘密计算机信息系统集成资质证书

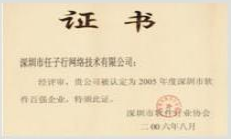


国家高技术产业化示范工程


国家计算机信息内容安全重点实验室

自主创新行业龙头企业

计算机信息系统集成资质三级证书



深圳市软件百强企业

中国内网安全市场“优秀推荐品牌奖”

中国国际软件博览会“创新奖”


科学技术进步奖一等奖

第十届中国国际软件博览会金奖

软件企业认定证书

高交会优秀软件产品奖

深圳市2006年科技创新奖

守合同重信用企业

广东省计算机信息系统安全服务等级一级资质

2008年度优秀软件产品

国家级火炬计划项目证书

ISO9001：2008质量管理体系认证

国家级网络安全应急服务支持单位

广东省科技进步三等奖

深圳市重点软件企业

高新技术企业认定证书


最具成长性企业

高新技术企业认定证书