任天行网络安全管理系统
_SURF-RAG
产品白皮书

■ 文档编号	1.0	■ 密级	错误！未找到引用源。
■ 版本编号	V1.0	■ 日期	2012-06-09

■ **版本变更记录**

时间	版本	说明	修改人
2012-5-27		产品白皮书	陈翼、刘福林
2012-7-30		产品白皮书	刘磊

■ **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

随着信息技术的飞速发展和广泛应用，网络已经渗透到社会的各个领域，成为人们工作、学习、生活中不可或缺的一部分。互联网的商业和通讯业务也随之得到快速增长，在为组织带来更多商业机会、提升组织生产效率的同时，相应地也降低了组织运营、生产和沟通成本。目前，不论政府、学校、企事业单位或是个人与网络的联系越来越紧密，网络一旦出现故障，将严重影响到工作、学习、生活。

二. 产品概述

基于互联网的应用从最初的文件共享、文件传输（FTP）、静态网页浏览（HTML）以及 Telnet 等内容单一、静态的、简单、小规模的应用，逐步发展为包括 E-Mail、ERP、OA、CRM、新闻信息、文件共享、视频会议、VoIP、即时通讯、网络游戏、电子商务、电子政务等等在内的动态的、大规模的、复杂的应用。网络承载的内容日益丰富，变得更加复杂、多样化。当今，互联网进入了应用级网络时代，逐步成为一个虚拟的真实社会。P2P 传输、网络电视、网络游戏、在线聊天、Web 视频、股票软件、网上银行、数据库、物流供应链、各种论坛以及大量未知的内容和信息纷纷涌进网络。

传统的网络安全设备，如防火墙、入侵检测系统、防病毒软件、反垃圾邮件系统等，无法应对日新月异的网络应用给网络管理者们带来的严峻挑战。具体表现如下：

- **带宽资源浪费，关键业务得不到保障**

据 IDC 统计数据显示，2007 年 P2P 下载、网络视频等非关键业务的流量横行大肆吞噬了网络 67.5%的带宽资源，降低了企业 30%-40%的生产率。尽管带宽一扩再扩，却总是很快又拥挤不堪。这不仅造成带宽资源大量浪费，还使得网络关键业务（与用户生产经营、信息安全、关键用户息息相关的各类网络应用，包括 ERP、数据库、中间件、电子商务、视频会议等）的带宽无法保证，最终会造成直接的经济损失。

- **工作效率低下**

据一项调查显示，普通企业员工每天的互联网访问活动 40% 与工作无关，在线聊天、浏览新闻娱乐、网络视频、网络游戏、炒股等无时无刻不在占用正常的工作时间。

在降低工作效率的同时还侵占了大量带宽。在高度网络化的现代办公环境里，办公室可能成为“舒适的网吧”，人力资源在无形中浪费巨大。

- **敏感信息泄露**

电子邮件、MSN/QQ 以及 BBS 论坛等网络应用，已经成为提高工作效率的工具，但如果不加监管，也可能成为泄密的工具。对于政府机关、上市公司以及知识密集型企业，关键设计文档、软件源代码、市场销售计划等核心机密文档，可以通过电子邮件与在线聊天工具“轻易而快速”地传递到外部，给组织造成重大损失。

- **网络安全方面存在的隐忧**

网络技术的发展相应的也给网络安全带来了挑战。有数据表明超过 20% 的用户遭受了黑客的攻击，给网络运营和数据安全带来了困扰和损失。同时，令人忧虑的是，尽管网络安全问题造成的损失越来越大，仍然有大量的用户没有引起足够的重视或者说没有找到合适的方法有效提高网络的安全性。

因此在确保组织正常工作和关键业务的安全、高效运行的同时，如何从根本上解决上述问题，才能在显著提高企业的生产效率同时来保障 IT 投资的回报率，这是大部分组织目前在网络管理和运维中亟待解决的问题。

- **网络应用可见性差，存在法律风险**

一份来自于 IDC 的权威数据显示：80%以上的 IT 管理人员无法准确了解自己的网络。对网络管理来说，自己的网络就像一个黑盒子，里面都跑了些什么应用以及网络的状况根本不清楚，而管理员无法知道异常流量的类型、来源、具体流向、流量大小、持续的时间等，也无法有效规划网络资源的使用，导致网络管理处于无序状态。

为了加强对互联网的控制和管理，公安部颁发的 82 号令要求各机构要保存至少 3 个月的访问日志，以便协助公安调查取证。因此，如无有效的管理手段，企业内部对互联网资源的非法访问，比如访问色情、赌博、犯罪网站、发表反动言论、泄露重大机密等，都会触犯相关法律，给企业带来法律风险。

对网络的管控势在必行

员工的不当行为引发的问题无法通过传统的网络安全设备来实现，网络管理者必须要对网络使用基于内容进行管理，包括以下几点：

- 谁能上网 (哪个部门的哪个员工)
- 什么时间可以上网 (工作时间/周末、上班时间/休息时间、上午/下午)
- 允许访问哪些业务(浏览网页、收发邮件、下载文件、聊天、游戏)
- 具体允许访问什么内容(哪个网站、邮件内容、聊天内容)
- 允许占用的带宽、会话、流量是多大(每种应用占用了多大的带宽、多少会话数、流

量有多大)

三. 系统特点

3.1 智能的协议识别

提供对数据流的深度检测功能，对网络流量能准确的按协议类型识别，包括常规的应用、国内外的各种 P2P 软件、IM 软件、网络游戏、在线视频等。配合强大的带宽管理与行为管理功能，可有效提高带宽的利用率，规范用户的上网行为。

3.2 强大的流量控制功能

支持基于线路、基于内网和外网的 IP 地址/IP 地址范围/IP 子网/地址簿/用户组、基于四层服务和根据特征识别的七层服务、基于单个服务、服务组、多服务的任意组合等进行带宽控制和流量阻断；

支持基于流量优先级的流量控制策略；支持基于时间段的带宽控制和流量阻断策略；根据策略对某些用户或特定应用的最大带宽进行控制；通过策略或优先级，保证关键业务或者 VIP 客户应用的带宽；对特定应用或重点客户进行预留一定带宽。

能够根据 IP 地址/IP 地址范围/IP 子网/地址簿/用户组的配置来控制网络中单个用户的上行会并发会话数、下行并发会话数；针对流量异常的用户或者 IP 地址进行用户黑名单智能控制管理；根据每用户的“每日/每周/每月”使用的流量(上行/下行/双向)总和超过预设阀值，、根据每用户在连续一段时间的“上行速率/下行速率”超过预设阀值、根据每用户在连续一段时间的并发会话数(上行/下行)超过预设阀值、根据每用户在连续一段时间的新建会话数(上行/下行)超过预设阀值等，则自动进入黑名单。并能控制用户滥用 P2P、防止病毒等。

3.3 先进的上网行为管理

任天行网络安全管理系统_SURF-RAG系列设备提供了细致的上网行为管理方案，拥有着领先的网络行为识别能力。对用户的上网行为进行细致而灵活的管理，进而提高了员工的工作效率，避免了机密信息的泄漏。

URL过滤与记录：提供强大的 URL 过滤、全面的 URL 记录和 URL 排名功能。URL 库可达 1000万以上，如与 WebSense 联动，可达 2000 万以上。

网页内容过滤与记录：全面记录内网用户向公网 BBS、论坛、博客等发表的帖子内容及附件，还提供对帖子的内容进行关键字过滤。同时可对搜索引擎搜索的关键字进行过滤与记录；帮助企事业过滤不良网站。

文件传输过滤与记录：智能识别 HTTP 网页与 FTP 协议的文件上传和文件下载，并对文件的上传和下载进行过滤与记录。

邮件过滤与记录：支持对邮件内容和附件等进行监控、过滤和审计功能。既可以监控到任何一台计算机通过 Outlook 或 Foxmail 等邮件客户端软件 使用 SMTP 和 POP3 收发邮件，也可以监测到通过 Yahoo、Sohu、163、126、Hotmail、Tom、Sina、Gmail、QQmail 等 Webmail 提供商收发邮件的内容和附件。

即时通讯过滤与记录：支持对即时通讯协议进行阻断，及对文字聊天、语音聊天及文件传输进行过滤与内容记录。

3.4 高效的防火墙功能

任天行网络安全管理系统_SURF-RAG系列设备内置了专业的防火墙功能。灵活的安全规则以及多种防护机制保护了网络免受攻击，提升了整个网络的安全性。

NAT 支持：提供多对一的源地址转换、一对一的双向地址转换以及端口映射等三种类型的 NAT。并且支持多种应用协议 NAT 穿越，支持 H.323、SIP、FTP、TFTP、RSH、RTSP、SQL Net、HTTP、MS-RPC、PPTP/GRE、SUN-RPC 等协议的 ALG 功能。

VPN 支持：支持 IPSec VPN、PPTP VPN 功能。

全面 DoS/DDoS 防护：提供全面的 DoS/DDoS 防护机制，支持 SYN Cookie，SYN 代理服务。防御各种网络攻击包括：IP 畸形包攻击、IP 假冒、TCP 劫持入侵、SYN flood、Smurf、Ping of Death、Teardrop、Land、Ping flood、UDP Flood 等。

3.5 丰富的用户认证方式

支持多种方式的用户认证功能，包括本地数据库认证、AD 认证、RADIUS 认证、LDAP 认证、POP3 认证。灵活的认证策略提供了安全的终端接入。同时提供单点登录认证方式，用户只需输入一次密码，降低密码泄露的风险。

3.6 酒店即插即用功能

由于酒店客人的电脑的 IP 地址与 DNS 的配置各不相同，经常需要酒店网管人员为其进行一番配置后才能正常上网。不管客人电脑的 IP 与 DNS 如何配置，开启酒店即插即用功能后，只要插上网线，客人即可上网。

3.7 HA 功能

系统支持一主一备，或一主多备的 HA 模式；也支持多个主设备(多主一备/多主多备)的 HA 模式，多个主设备间可实现负载均衡。

3.8 完整的统计及报表功能

任天行网络安全管理系统_SURF-RAG系列设备内置了强大的报表中心，可对全网的流量进行采集和统计、分析用户网络行为。报表中心提供丰富的统计数据，可按长期(周/月/年)、短期(分钟/小时/日)和实时(秒)的方式显示带宽使用状况，并根据用户需求产生报表。从而帮助管理者了解网络整体使用情况，轻松解决网络中存在的问题。

流量统计：提供全网流量统计信息，主要包括：用户/IP统计、用户组统计、服务/服务组统计、线路统计等，并可进一步查看 IP 地址、地址组和网络服务之间的关联。

全局行为分析：配合行为管理功能，可提供丰富的流量审计信息，可以记录用户 URL 日志、BBS/论坛发帖内容及附件、网页评论记录、收发邮件详细内容、即时通讯记录、FTP 日志等。

个人行为分析：根据组织结构中的逻辑树结构，可逐个展示用户，并将每个用户的上网行为分项统计并形象化显示。具体内容包括：个人网页统计、个人即时通讯记录、个人邮件记录、个人 FTP 记录。

会话记录：通过检查完整的会话日志，管理者可以跟踪网络中的任何操作。会话记录包括：源 IP、目的 IP、协议和端口、是否进行 NAT 转换(可显示转换后的 IP 和端口)、七层应用名称、会话产生的时间和会话持续时间。

报表生成：可生成转换为 PDF 、Excel 等格式的报表，大大简化了管理员手工制作报表。

3.9 集中管理平台

与任天行网络安全管理系统_SURF-RAG系列设备配套的集中管理平台(Central Management，简称 CM)部署于企业总部，可对各分支机构的任天行网络安全管理系统_SURF-RAG系列设备统一进行策略下发、定时备份配置文件、上网行为日志管理、全网设备

状态操控，同时还支持分支机构自行设置个性化管理策略，实现“个性化管理”与“集中管理”的完美结合。

四. 关键技术

4.1 定制操作系统

Linux 操作系统是一个安全的，高效的操作系统。任天行中的操作系统经过内核裁减，只保留了少数相关的服务与功能，系统内核达到最小化，使操作系统的额外开销与不稳定因素减至最小化。另外，采用特有的文件系统，使系统能抵御突然掉电等物理灾害造成的对系统的损害。

4.2 专用网络设备驱动

网卡的性能对于网络安全审计系统非常重要，因为它直接关系到数据采集（捕包）的速度。任天行通过硬件，软件两种方法来提高网卡的性能：一、任天行采用基于 INTEL 架构的网卡，速度快且稳定。二、开发专用的驱动程序，减少数据在网卡驱动不同模块间的传递环节，使数据通过 DMA 的方式直接传递给应用程序空间，减少 CPU 的参与，与及数据拷贝的次数，提高处理速度。

4.3 专有的数据捕获技术

通过深入的技术分析，我们在对 Linux 的系统内核进行充分剖析的基础上，对模块进行了修改和全面优化，并且对硬件的驱动程序进行了改造，使数据捕获性能有了质的提高，大大提高了系统的数据捕获和处理能力。数据捕获能力达到 100,000pps。

4.4 并行协议栈

对于网络信息安全审计产品来说，数据捕获、协议栈，协议分析等过程中的效率对系统的最后性能起着决定性的因素。

传统协议栈接收一个 UDP 数据包的流程是：以太网设备驱动程序首先响应中断，假定该中断表示一个正常的接收已完成，数据从设备读到一个缓冲链表中。这个链表除了记录数据内容、还保存一个指针指向接收数据的接口结构。然后把链表传给一个通用以太网输入例程，

它通过以太网帧中的类型字段来确定哪个协议层来接收此分组。在这个例子中，类型字段标识一个 IP 数据报，从而该链表被加入到 IP 输入队列中。接着产生一个软中断来执行 IP 输入例程。接着 IP 输入例程响应软中断，它验证 IP 首部检验和，处理 IP 选项，验证数据报被传递到正确的主机(通过比较数据报的目标 IP 地址与主机 IP 地址)，并当系统被配置为一个路由器，且数据报被表注为其他的 IP 地址时，转发此数据报。如果 IP 数据报到达它的最终目标，调用 IP 首部中标识的协议的输入例程：ICMP，IGMP，TCP 或 UDP。在这个例子中，调用 UDP 输入例程去处理 UDP 数据报。最后 UDP 输入例程验证 UDP 首部的各字段（长度和可选的校验和），然后确定是否一个进程应该接收此数据包。

很明显，传统协议栈采用类似函数链的串行处理方式，依次处理IP输入例程和UDP输入例程，这种软件结构不能充分利用现有SMP架构的性能，经常出现一个CPU的占用率达到100%，其他CPU还无事可作的情况。因此我们用并行协议栈取代传统协议栈，充分发挥SMP架构的性能，给多路CPU、多内核CPU、超线程CPU足够的施展空间。为了解决并行处理中不可避免的负载均衡的问题，选取硬件分流器中流行的IP+PORT分流策略，保证在大流量的情况下处理线程之间工作量均等，有效避免过载线程的出现。配合大流量数据捕获模块，取消传统协议栈软中断的开销，可以进一步地提高系统的性能。

4.5 多种算法的链路负载均衡技术

提供 ICMP、TCP、ARP、HTTP 等方式侦测机制，有效支持多个不同的、独立的链路接入；配合多出口链路，实现链路的负载均衡和备份链路自动切换，支持按照源IP轮询、会话轮询、线路负载、最佳路径等等多种链路自动均衡算法。

4.6 专业的流量管理技术

任天行网络安全管理系统_SURF-RAG系列设备以 8 Kbps 为粒度，提供精细网络带宽管理功能。可根据主机(单 IP、IP 组、用户组)、服务(服务组)、时间、URL、文件类型等参数，以及各个参数间的灵活组合来实现带宽的预留、保障和限制。对内网单个主机进行会话和带宽控制的同时，可对单个主机的多个特定服务(服务组)的带宽再进行控制。

任天行网络安全管理系统_SURF-RAG系列设备全面提升流量管理的灵活性、稳定性及安全性，发挥了网络整体资源的最佳利用，并满足复杂的商业需求，让网络资源更紧密的与业务发展整合，为企业带来最大效益。

五. 功能说明

对于网络资源的滥用，封堵还是放任，这是摆在网络管理者面前的难题，任天行网络安全管理系统_SURF-RAG 系列产品提供了灵活的管理策略，根据企业的需求，定制个性化的管理方案，帮助各企业建立安全、高效、健康、和谐的网络环境。

5.1 用户管理

用户是任天行网络安全管理系统_SURF-RAG 系列产品的基本要素，任何的行为管理策略都是以用户为核心。因此，对于用户的识别、认证与管理成了行为管理的前提要素，同时也决定了行为管理的效果。任天行网络安全管理系统_SURF-RAG 系列产品通过不断地深入实践与研发，提供了灵活而全面的用户管理方式，很好的满足了广大企业对用户管理的需求。

5.1.1 组织结构

对于用户数比较多的企业，有一个清晰的组织结构非常重要，便于管理员对用户的管理、查询和定位。任天行网络安全管理系统_SURF-RAG 系列设备支持树型结构的用户管理，并且不同的用户组之间可以灵活的调整成员用户，从而可建立与企业行政组织结构相同的网络组织结构，如下图所示：

5.1.2 自动分组

对于用户数比较多的网络环境，第一次构建组织结构时，如果让管理员手动的去建立每一个组和用户是很不现实的。在大多数情况下，管理员并不会对每一个用户单独的设定一个管理策略，而是针对某一类用户进行统一的管理。所以自动的创建用户组和自动的分配用户就显得非常重要。

任天行网络安全管理系统_SURF-RAG 系列设备支持将新入网还未在组织结构中的用户根据预设的 IP 网段进行自动分组并设定策略。新入网的用户可以根据其 IP 地址、MAC 地址、主机名、VLAN ID 等多种方式来定义用户名，可以达到各种网络环境的需求，如静态 IP 环境、DHCP 环境等等。每个用户还支持别名的功能，管理员可以为其添加别名，以更加直观的方式来呈现用户，为后续的行为审计、统计奠定了基础。

对于外来访问的临时用户，管理员可以为其分配一个特定网段，将其加入临时用户组，并预设一定的访问权限。同时可以设定用户离线多久就自动删除该用户，从而大大的简化了动态用户的管理，增强了用户管理的灵活性。

5.1.3 内网主机扫描

任天行网络安全管理系统_SURF-RAG 系列设备可通过 NetBIOS 协议扫描内网的主机信息，扫描结果将列出每个主机的 IP 地址、MAC 地址和主机名等，然后可以将其加入某个用户组中，逐步完善组织结构的管理。另外，在对用户进行 IP/MAC 绑定时，管理员只需要输入某个主机的 IP 或者 MAC 等信息，就可以扫描出对应的其它信息，从而大大简化了管理员的工作。

5.1.4 用户导入

除了自动分组和内网主机扫描以外，任天行网络安全管理系统_SURF-RAG 系列设备还支持批量导入用户的方式，以多种灵活的方式方便管理员建立组织结构：

- ✧ 自定义文件：可将管理员定义的包含批量用户的 Excel 文件导入系统，从而批量建立用户组和用户。
- ✧ LDAP/AD 用户导入：可将 LDAP/AD 服务器中的用户信息导入组织结构中，并自动创建默认的组权限，同时，任天行网络安全管理系统_SURF-RAG 系列设备还支持定期与 LDAP/AD 服务器同步用户信息，实现用户的定期更新。从而实现了与原有网络管理平台的结合，达到了全网用户统一管理的目的。

5.1.5 多种身份认证方式

用户身份认证有两种方式：客户端认证和免客户端认证。任天行网络安全管理系统_SURF-RAG 系列设备支持免客户端的 WEB 认证，即通过浏览器就可以完成全部的认证。任天行网络安全管理系统_SURF-RAG 系列设备除了支持本地的用户名/密码的认证外，还可以结合 LDAP、AD 域、Radius、POP3 等外部服务器实现用户的身份认证。

任天行网络安全管理系统_SURF-RAG 系列设备也支持多种认证方式的混合使用，可为不同的用户配置不同的认证方式，实现用户的差异化管理。比如，一部分用户使用本地服务器认证、一部分用户结合 LDAP 服务器认证，一部分用户不需要进行身份认证。

5.1.6 支持策略继承

任天行网络安全管理系统_SURF-RAG 系列设备提供了多种配置策略的方式。每个组都可以有自己独立的上网策略，子组也可以继承父组的策略，父组也可以强制子组继承自己的策略。

5.1.7 IP/MAC/VLAN 绑定

任天行网络安全管理系统_SURF-RAG 系列设备支持二层网络环境和三层网络环境的 IP、MAC、IP+MAC 和 VLAN ID 的绑定，可自动阻断哪些非法占用他人 IP 的用户上网。

5.1.8 认证账户有效期

对于一些临时的用户，通过有效期的限定可以控制这些用户的上网时间范围，当用户超出预设的时间有效期，就不能上网。很好的控制了外来用户上网的准入性和上网时长。同时可以设定用户离线多久就自动删除该用户，从而大大的简化了动态用户的管理，增强了用户管理的灵活性。

5.1.9 公用账户

任天行网络安全管理系统_SURF-RAG 系列设备的认证账户可支持多人同时登录，比如一个员工有 2 台电脑，那么可以用同一个账户认证，这样两台电脑的流量和行为都记录在同一个账户上，以便统一网络中的流量统计和行为审计与行为分析。

5.1.10 临时账户

支持临时用户自主申请临时账户，方便于外来的临时用户上网使用。支持自动审核和管理员手动审核的核定方法将临时账户加入到组织结构中，从而减少管理员对临时账户的频繁配置，同时统一了临时账户的上网权限和使用期限的管理。

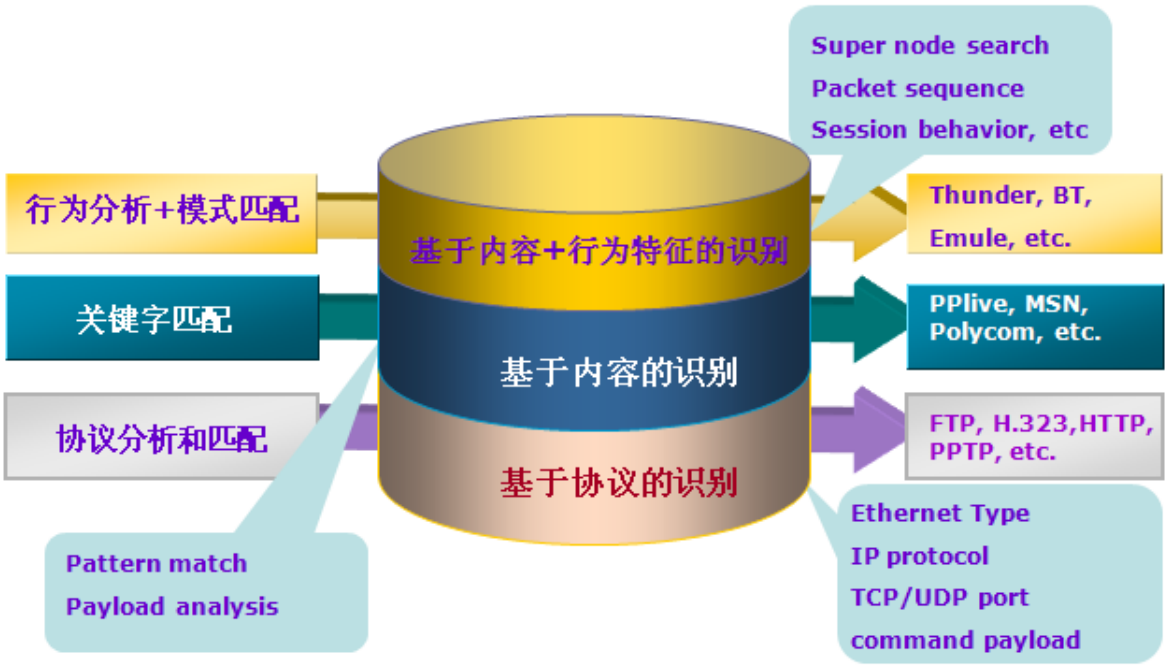
5.1.11 登录重定向

任天行网络安全管理系统_SURF-RAG 系列设备支持网页重定向的功能。当用户认证成功后，任天行网络安全管理系统_SURF-RAG 系列设备可以将其第一次的 WEB 访问重定向到预设的 URL 链接。此功能适合于政府机关、企业集团、大中小学等、或者酒店等网络环境，便于用户上网的时候直接导向最新的公告信息。

5.2 网络流量识别

要控制好各种应用，必须首先准确的识别。传统的安全设备通过 IP 或者端口封堵各种协议，但这只能局限于网络层和传输层的标准协议，如 HTTP、FTP 等。P2P、网络游戏、网络电视等一系列应用都是通过协商动态产生的端口，不再是固定的端口，而且诸如电驴、Skype 等协议还是加密的，面对这种应用传统的设备完全无能为力。

任天行网络安全管理系统_SURF-RAG 系列设备以 DPI（Deep Packet Inspect，深度包检测） 技术为核心，结合基于报文内容及基于行为特征的技术，实现网络中应用的自动识别和智能分类。任天行网络安全管理系统_SURF-RAG 系列设备可以探测和跟踪动态端口分配，通过比对协议的特征库，能够识别变动端口的流量，并能够对使用同一端口的不同协议进行自动识识别。下图就是任天行网络安全管理系统_SURF-RAG 系列设备识别各种应用采取的方法。



到目前为止，任天行网络安全管理系统_SURF-RAG 系列设备已经支持 400 多种协议的识别，如下所示：

- ✧ 常用协议：HTTP，HTTPS，FTP，Telnet，DNS，SMTP，POP3，Lotus_Notes，IMAP，NetBIOS，CVS，DHCP，NTP，NFS，ESP，AH，NNTP，SNMP，TFTP，BGP，VRRP，HSRP，VNC，UPNP，Syslog，SSL，SSH，SQL，MySQL，SOCKS，SCTP，RIP，OSPF，Remote_Desktop，PPTP，PING，PING_v6， LDAP，L2TP，IKE，IGMP 等。
- ✧ HTTP 应用：HTTP 代理，Web 下载，HTTP 多线程下载，伪 IE 下载，其他 HTTP 下载，Facebook，Plurk(噗浪)，QQ 农场，欢乐斗地主，开心网(kaixin001)，开心网(kaixin)，人人网，搜狐•白，163 邮箱、QQ 邮箱、126 邮箱、新浪邮箱、搜狐邮箱、21cn 邮箱、tom 邮箱、雅虎邮箱、yeah 邮箱、hotmail 邮箱、eyou 邮箱、live 邮箱、东方邮箱等。
- ✧ WEB 视频：六间房，土豆，新浪视频，腾讯宽频，我乐网，搜狐视频，酷六视频，葫芦网视频，优酷，CCTV，东方宽频，凤凰宽频，NBA 中国官方网视频，天线高清，飞速土豆，激动网，BBSee，i 酷，网易视频，金鹰网视频(芒果 TV)，第一财经网，新华网视频，YouTube，乐视网，17173 游戏视频，旅视网，爱播网视频，音悦台，国际在线视频，电影网视频等。
- ✧ P2P 下载：酷狗，百度下吧，PP 点点通，酷我音乐盒，迅雷，QQ 音乐，脱兔下载，QQ(超级)旋风下载，BT，Gnutella，电驴，网际快车(FlashGet)，360 下载，POCO，汉魅，RealLink，RaysouSURF-RAGe，顶悦视听盒，宝酷噢，foxy，LimeWire，ZCOM

杂志订阅器，搜娱，Soulseek，天网 Maze，屁屁狗，百宝，P8 数字娱乐传播平台，酷宝娱乐互动，网络蚂蚁，飞鱼娱乐，酷猴，WinMX，DirectConnect 等。

- ✧ 流媒体：pplive、ppstream、qqlive、uusee、sopcast、pstv、qvod(UDP)、netitv、MMS、RTSP、蚂蚁网络电视、风行网络电视、青娱乐、极速酷六、VGO 高清网络电视、乐鱼影音盒、暴风影音、皮皮影视(UDP)、PP 加速器、Dopool 直播、龙翔网络电视、球皇直播、九品极速影院、远古网络播放器、mysee、recool、vjbase、tvkoo 等。
- ✧ 即时通信：MSN， YahooMessger，QQ/TM，，WebQQ，网易泡泡，淘宝旺旺，新浪 UC，中国移动飞信，淘宝旺旺，雅虎通(Yahoo)，聪慧发发，校内通，阿里旺旺，Lava-Lava，iSpeak，AIM，彩虹(51 挂挂)，Paltalk，Raketu，百度 HI，GoogleTalk，中游 UU，联众好友在线，网易 CC 语音，都秀，酷宝，新浪 SHOW 等。
- ✧ 网络电话： Skype、ET263、UUCall、Netmeeting、阿里通网络电话、和悦网络电话、KC 网络电话、RedVip、SIP 等。
- ✧ 网络游戏：QQ 游戏系列，盛大游戏系列，网易游戏系列，完美时空系列，九城游戏系列，搜狐畅游系列，天晴数码系列，巨人游戏系列，久游游戏系列，金山游戏系列，蓝港在线系列，光宇游戏系列，天游游戏系列，小游戏(棋牌游戏)，RUNUP(云起)系列等。
- ✧ 股票交易：同花顺、大智慧(经典版、新一代版)、和讯股道、安信行情、齐鲁证券(同花顺版)、大福星、通达信、国信金太阳、钱龙系(旗舰版、经典版)、申银万国(金典版)、大有期货、证券之星(财富版)、广发证券(至强版)、168(888)行情系统、指南针、中信证券(至信版)、金融界、财龙投资、广大证券(超强版、大智慧、钱龙金典)、国泰君安大智慧、叩富网模拟炒股、操盘手、HY trader、中信建投(博易大师、大智慧)、诚浩钱龙合一版、华安证券投资赢家、仟家信黄金分析软件、斯道客、龙卷风、分析家 2006、飞天行情、易天富基金、行情眼等。
- ✧ 网上银行：中国建设银行、中国工商银行、中国农业银行、中国招商银行、中国人民银行、中国民生银行、交通银行、中国光大银行、兴业银行、上海浦东银行、深圳发展银行、台湾银行、台北富邦银行、台新银行、第一商业银行、兆丰国际银行、汇丰银行、中国信托商业银行、台湾企业银行、渣打银行、联邦银行、日盛网络银行、京城银行、元大商业银行、远东国际商业银行、高雄银行、庆丰银行、华泰银行、永丰银行等。

5.3 带宽资源管理

通过专业的带宽管理和分配算法，任天行网络安全管理系统_SURF-RAG 系列设备提供流量优先级、最大带宽限制、保障带宽、预留带宽、以及随机公平队列等一系列的应用优化和带宽管理控制功能。

5.3.1 流量优先级的划分

任天行网络安全管理系统_SURF-RAG 系列设备可基于业务应用的优先级，将业务应用划分为 高、中、低等共三个优先级，优先级越高的流量，优先传送。在实现流量控制时，可将核心业务应用、时延要求高的应用、以及重要人物的流量配置为高优先级，同时将 P2P、网络电视、WEB 视频等非核心的、占用带宽资源较高的应用配置为低优先级。从而可以实现在带宽资源紧张时，优先保证高优先级应用的传送，而在带宽资源使用宽松时，各级应用都可以正常使用。

5.4 强大的带宽管理功能

任天行网络安全管理系统_SURF-RAG 系列设备通过 DPI 为核心的深度包检测技术，结合各种应用的行为特点，能够精确到对每个会话的数据包的检测和控制。同时结合流量优先级、随机公平队列等，提供了最大带宽限制、保障带宽、预留带宽等一系列强大的带宽管理功能。

任天行网络安全管理系统_SURF-RAG 系列设备支持源会话数、目的会话数、上行、下行，以及双向总带宽的管理与控制，管理员可以基于线路、流量优先级、源 IP 地址(地址组、用户组或用户组)、目标 IP 地址(地址、地址组)、时间、会话、协议和应用等参数对网络流量进行划分，并确定如何有效的、合理的实现带宽的管理与控制。从而实现灵活的带宽控制和应用优化目的。

5.4.1 基于随机公平队列的流量整形和应用优化

基于任天行网络安全管理系统_SURF-RAG 系列设备特有的功能，随机公平队列可以保证在相同等级的每一个用户都具有相同的网络资源，避免少部分用户占用了大部分带宽资源的这种极端情况的出现。在相同用户等级的情况下，获得始终如一的服务，使所有用户都满意。

5.4.2 灵活的、强大的基于策略的带宽控制

任天行网络安全管理系统_SURF-RAG 系列设备基于流量优先级、随机公平队列、令牌桶算法、TCP 窗口控制算法等技术，提供最大带宽限制、保障带宽、预留带宽的功能，实现灵活、高效、可靠的带宽控制能力。基于策略的流量控制，可以根据线路、IP 地址(组)、用户(组)、协议(组)、URL、时间段等参数配置策略规则，然后再为这些规则分配优先级、带宽、会话数，从而实现对网络中的各种流量进行精细而灵活的控制。最大带宽、保障带宽和预留带宽的详细阐述如下：

- ✧ 最大带宽：为某些用户或特定应用指定最大带宽。一方面，防止了某些用户疯狂抢占带宽，保证了网络使用的相对公平性。另一方面，限制了非关键应用毫无节制的消耗宝贵的带宽资源，保证了关键应用的服务质量。
- ✧ 保障带宽：结合最大带宽和流量优先级，根据需要为某些关键应用或者 VIP 客户保障一定带宽。当网络繁忙时，这些关键应用或者 VIP 客户至少可以得到预设的保障带宽，并还可以租借空闲的或低优先级流量的带宽；当网络空闲时，低优先级的流量亦可使用当前空闲带宽。从而保证了带宽的合理、高效的使用。
- ✧ 预留带宽：为某种特定应用或某些重点客户预留一定带宽，以保证用户在不同时间段、不同的网络使用环境中都能得到同样的带宽管理服务和网络使用感受。

5.4.3 基于单 IP/用户的带宽控制

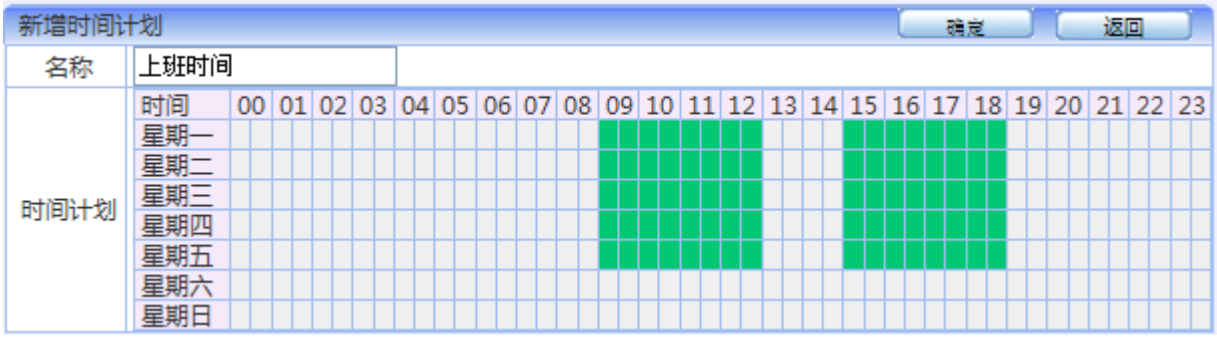
任天行网络安全管理系统_SURF-RAG 系列设备不仅提供由 IP 地址(组)、用户(组)、服务(组)、时间等组合而成的基于策略的带宽控制方式，同时对单 IP/用户使用网络资源也提供精细的控制方法。基于单 IP/用户的控制，可以将内网的用户分为多种等级，对同等级里的用户实现相同的控制策略。这种方式在对单个主机使用的会话和最大带宽(上行/下行)进行控制的同时，可再对每个主机的多个特定服务(组)的带宽进行精细的控制，再可以结合时间段，可满足不同网络的各种复杂的带宽控制需求。

5.4.4 对各种入侵攻击的安全保护措施

任天行网络安全管理系统_SURF-RAG 系列设备自带的防火墙功能，能够识别并阻断黑客的端口扫描以及普通的 DoS 攻击行为，保证内部网络的安全性。同时，系统也阻断了内网的垃圾数据包对防火墙资源的消耗，大大降低了防火墙工作的负担，提高了整体网络的安全性。

5.4.5 基于时间的管理

任天行网络安全管理系统_SURF-RAG 系列设备支持自定义时间对象，实现针对时间段进行带宽分配和上网行为的管理。比如，上班时间要对关键业务和重要人员的带宽进行保障，对 P2P 等非关键业务进行严格控制；下班时间可以对 P2P、网络电视等业务给与适当宽松的流量。再比如，上班时间不允许员工浏览与工作无关的网页，不允许某些员工使用 IM 软件等等。时间对象可以根据需要灵活选择，如下图所示：



5.5 上网行为管理

门户网站、社区论坛、交友网站、博客、个人网页，网络上五花八门、包罗万象的网页吸引着网民的眼球，诱惑网民拿起鼠标去体验网络世界的乐趣。在企业里，很多员工利用上班时间泡论坛、炒股、玩游戏、收发私人邮件、聊天等等，影响了工作氛围，降低了工作效率，浪费了企业资源，这是所有企业管理者都不希望发生的。

为避免企业为员工的这些不良行为买单，任天行网络安全管理系统_SURF-RAG 系列设备提供了细致的上网行为管理方案，对用户的上网行为进行细致而灵活的管理，进而提高员工的工作效率，避免机密信息的泄漏。

5.5.1 网页过滤

WEB 是互联网上内容最丰富、访问量最大的应用，然而许多网页充斥着反动、暴力、色情以及其它不健康的信息。此外，大量网络应用，如 P2P、IM、网络电视、游戏等等，也借助 HTTP 协议或者 80 端口，透过防火墙的封堵，抢占网络带宽，携带病毒、恶意软件，为内网用户带来安全风险。任天行网络安全管理系统_SURF-RAG 系列设备通过灵活的策略设置，对违反国家法律、危害社会、影响企业发展的内容进行过滤，避免用户有

意无意访问包含非法内容的网页，净化网络，降低企业法律风险，提高员工工作效率，提高人民素质，创造文明健康的上网环境。

5.5.1.1 URL 过滤

任天行网络安全管理系统_SURF-RAG 系列设备利用目前国际上最先进的方式，将 URL 按照一定的标准进行预分类，然后由网关设备对各种类别网页进行过滤。在 任天行网络安全管理系统_SURF-RAG 系列设备中内置了数百万的 URL 资料，分为新闻、音乐、视频、广告、财经、教育、科学、房地产、求职招聘等 URL 组。

此外，由于每个网络环境对互联网的访问特点差异很大，可能出现内置 URL 库没有包含的情况，任天行网络安全管理系统_SURF-RAG 系列设备支持自定义 URL 库的功能，客户可以根据自己的需要，将要被控制的 URL 灵活分组，从而使得客户 URL 访问范围得以全面覆盖。

在过滤 URL 记录的同时，可以对网络中所访问的 URL 进行记录和统计排名，以实现对 URL 访问的监控和控制。

有了任天行网络安全管理系统_SURF-RAG 系列设备，员工依然可以浏览网页，但其访问时间和内容可以受到管理和控制。比如，新闻、教育、科学以及同工作相关的页面是可以被允许访问的，而涉及到色情、暴力、恐怖等不良网站将被阻止。

5.5.1.2 搜索引擎关键字过滤

据调查显示，搜索引擎是网民访问量最大的网站类型之一，用户大多数的 WEB 站点访问行为都是从搜索引擎开始的。为了应对 WEB 访问使用所带来的效率、安全及责任风险等问题。任天行网络安全管理系统_SURF-RAG 系列设备提供了“搜索引擎关键字审计与过滤”，它可以记录用户通过搜索引擎类网站搜索的关键字内容，并基于搜索类别、关键字内容，过滤用户的非法搜索行为，全面解决不良搜索给用户带来的法律风险问题。“搜索引擎关键字审计与过滤”解决了网民通过搜索引擎访问色情、暴力等低俗网站的控制问题，体现了精细化管理的思路。

通过设置针对性策略，对搜索引擎关键字检索行为进行封堵，可以从源头上减少用户访问不良网站、获取不良信息。比如，某公司部署了 任天行网络安全管理系统_SURF-RAG 系列设备，并通过策略禁止公司员工通过搜索引擎访问“法轮功”；那么，员工搜索“法轮功”时，搜索结果将为空，查不到任何相关的内容。此时，系统自动对搜索到的网址页面进行屏蔽，帮助企事业单位用户将涉及低俗的、带有病毒的网站彻底封堵掉。

5.5.1.3 发帖关键字过滤

泡论坛、顶帖子等已经成为诸多员工互联网休闲方式之一。但如果将总裁办公室里的八卦、对工资的不满、对组织的抱怨等，或者涉嫌非法关键字、政治词汇、色情词汇等发布到各种贴吧、论坛上，必将给组织带来不良影响。

为加强论坛管理，禁止发布不良信息！任天行网络安全管理系统_SURF-RAG 系列设备提供对发帖的内容启用关键词过滤，对含有攻击国家领导人、分裂国家言论、下流词汇，或者伤害公司利益的帖子进行审计和过滤处理，并能对所有成功上传的内容进行详细记录以便事后查验。从而帮助员工养成远离低俗内容的上网习惯，协助推动“互联网低俗内容整治”，帮助企事业单位建立健康、规范、有序的上网环境。

5.5.1.4 文件下载过滤

WEB 的上传下载也存在一系列安全问题。如何过滤在网页中嵌入的恶意软件、病毒、木马控件…… ？如何防止员工上传文件？是当前网络管理者急需得到答案。

任天行网络安全管理系统_SURF-RAG 系列设备可以制定灵活的控制策略，针对不同的文件类型，对 IE/FTP 的上传或下载进行跟踪、阻断或者限速。帮助企事业单位防止员工泄密，净化网络流量，提高内网的安全性。

5.5.2 邮件过滤

为防止机密信息泄露，任天行网络安全管理系统_SURF-RAG 系列设备可以对 SMTP、POP3、Web-Mail 等进行监控审计，能够对用户收发邮件的时间、标题、内容以及附件等等元素进行过滤和完整的内容记录，避免企业、机关敏感信息泄露。

- 邮件过滤条件
  - 发件人地址
  - 邮件主题关键字
  - 邮件正文关键字
  - 邮件附件类型
- 邮件审计内容
  - 用户名/IP 地址/用户组
  - 发件人地址

- ✧ 收件人地址
- ✧ 邮件主题
- ✧ 邮件正文
- ✧ 邮件附件名称及文件
- ✧ 收发邮件的时间
- ✧ 邮件的类型（收/发、允许/过滤）
- ✧ 详细的会话信息

➢ Web-Mail 邮件

163 邮箱、QQ 邮箱、126 邮箱、新浪邮箱、搜狐邮箱、21cn 邮箱、Tom 邮箱、雅虎邮箱、yeah 邮箱、Hotmail 邮箱、Eyou 邮箱、Live 邮箱、东方邮箱。

5.5.3 即时通讯管理

即时通信工具因其沟通的便利性、即时性，如今几乎成为人手必备的工具。但由于即时通讯工具自身偏重娱乐性，在企业应用中，缺乏自律的员工往往将其作为上班期间的私人聊天工具。员工对即时通讯工具的滥用已经成为影响效率乃至运营成本的极大隐患。

不仅如此，其日益暴露出的企业信息安全问题则让企业老板越发无法忍耐。因为缺乏有效的管理机制与安全保障，由即时通讯工具引发的企业机密信息流失、被盗取和滥用的情况屡见不鲜，已经对企业信息安全构成严重威胁。

此外，近年来通过即时通讯工具传播的病毒、蠕虫、间谍软件以及混合攻击层出不穷，如某些蠕虫病毒通过即时通信软件，向用户的“联系人”发送恶意代码以获取用户信息。

针对以上问题，一些管理员试图通过关闭防火墙上 即时通讯流量的端口来禁止，即时通讯应用能够通过智能检测机制，自动转到其它端口，例如 80、443。任天行网络安全管理系统_SURF-RAG 系列设备以 DPI（Deep Packet Inspect，深度包检测） 技术为核心，结合行为分析技术，准确识别各种即时通讯软件。任天行网络安全管理系统_SURF-RAG 系列设备对即时通讯软件提出了如下解决方案：

✧ 阻断

对于在工作时间不需要和外部频繁交流的某些部门，可以阻断他们对即时通讯工具的使用，或者限制其使用即时通讯软件的部分功能，比如只允许使用文字聊天，不允许语音聊天或者传输文件。

✧ 监控

对于必须使用即时通讯工具作为工作手段的部门和员工，一方面企业领导者希望员工可以利用即时通讯工具进行更有效的商务活动，但对于一些通过即时通讯工具泄露组织机密的行为也是不愿意让其发生的。因此，对于普通人群，我们可以通过 任天行网络安全管理系统_SURF-RAG 系列设备允许其使用即时通讯工具，但对其使用过程和内容进行监控和记录；但对于特殊人群，比如领导，可以完全不做控制和监控。

通过对即时通讯的行为记录和聊天内容的监督，让员工有所警惕，达到间接控制员工的不规范行为。

5.5.4 黑名单控制

为了防止网络资源的滥用和方便管理员管理用户，任天行网络安全管理系统_SURF-RAG 系列设备支持将用户加入黑名单的功能。对进入黑名单的用户可以采取惩罚机制，惩罚期限到了之后，该用户又可以正常使用网络。用户一旦进入黑名单，当再次上网时，网页回弹出已经进入黑名单、是什么原因进入黑名单的。灵活的黑名单功能可以帮助管理员快速、准确的定位出谁肆意占有网络资源。

黑名单可以同时基于以下几种参数来控制：

- ✧ 流量配额：控制用户每日、每周、每月使用的流量(上行/下行/双向)总和，防止用户肆意占用带宽。
- ✧ 速率控制：控制用户速率(上行/下行) 在一段时间不能超过一定阀值。可以防止蠕虫等病毒的突发性、或者防止某个时段某个用户占有大量带宽。
- ✧ 并发 Session 控制：控制用户并发会话数(上行/下行) 在一段时间不能超过一定阀值。控制用户滥用 P2P、防止病毒等。
- ✧ 新建会话控制：控制用户新建会话数(上行/下行) 在一段时间不能超过一定阀值。控制用户滥用 P2P、防止病毒等。

当用户上网参数的超过以上阀值时，即可将用户加入黑名单进行惩罚一定时长（N 分钟/小时/天），惩罚方式有以下几种：

- ✧ 强制下线：将用户强制下线，即用户不能上网。
- ✧ 修改带宽：将用户上网速率修改到一个较小的值。
- ✧ 修改会话：将用户的并发会话数修改到一个较小的值。

对黑名单的控制，有一个生效时间，在生效时间内才进行黑名单的控制。在生效时间外，不对用户的速率和会话进行限制，用户产生的流量也不记入黑名单的流量配额内。

5.5.5 白名单管理

对于公司领导或者重要的用户，他们的上网不希望受到各种控制策略的限制，也不希望上网的内容被记录。设备的白名单功能可以很好的满足这些需求。符合白名单规则的流量，将不受“防火墙规则、流控规则、认证策略规则、上网策略对象规则、黑名单规则”的控制；同时上网的流量和上网行为的内容（如发送的邮件、发送的帖子、访问的网页、即时通讯记录等）将全部不记录。

白名单功能包括 IP 地址白名单、URL 白名单、即时通讯白名单。IP 地址白名单和 URL 白名单表示：对内网中某些用户访问的 IP 地址或 URL 地址不做控制和记录。即时通讯白名单表示：对即时通讯软件的某些账户不做控制和记录。

5.5.6 酒店管理-即插即用

由于酒店客人的电脑的 IP 地址配置各不相同，经常需要酒店网管人员为其进行一番配置后才能正常上网。既费时费力，又降低了客人的满意度。开启酒店即插即用功能，不论其电脑的 IP 地址、网关，DNS 服务器怎样配置，都能实现客人的电脑插上网线即可正常上网。大大方便了客人的使用，又降低了酒店的运作成本。

任天行网络安全管理系统_SURF-RAG 系列设备还可以管理、监控、查询、过滤酒店客人的上网行为，规范上网行为，预防网络违法犯罪，避免法律风险，保障网络信息安全。通过绑定房间号来绑定账户，由于房间号和账户一一对应，这样查找上网记录时就可以定位到人。

5.6 统计与报表系统

一个能够允许用户访问互联网的系统也必须及时关注用户对网络资源的使用情况。任天行网络安全管理系统_SURF-RAG 系列设备的报表中心提供了完整的互联网访问记录，根据 IP/用户、应用、时间、线路等参数对上网流量及行为进行全方位的记录，内容涵盖网络流量、带宽速率、新建会话、活跃会话、Web 访问、邮件收发、IM 聊天、论坛发帖、P2P 下载等各种网络行为。

由于将所有网络流量和行为记录完全整合到网关设备中会影响设备的性能，尤其是对于大量的统计和查询会占用较高的设备资源。另外，由于公安部颁发的 82 号令要求各机构要保存至少 3 个月的访问日志，以便协助公安调查取证。一般情况，网络设备的内置存储空间有限，无法记录 3 个月的访问日志。所以 任天行网络安全管理系统_SURF-RAG 系列设

备除了内置的报表中心，还支持在服务器上安装外置的报表中心。只要你的硬盘空间足够大，你能存储的日志内容将无限多。

报表中心提供丰富的统计数据，可按长期(周/月/年)、短期(分钟/小时/日)和实时(秒)的方式显示网络使用状况，并根据用户需求产生报表。从而帮助管理者了解网络整体使用情况，防止出现滥用、误用、盗用的行为。具体统计项目如下：

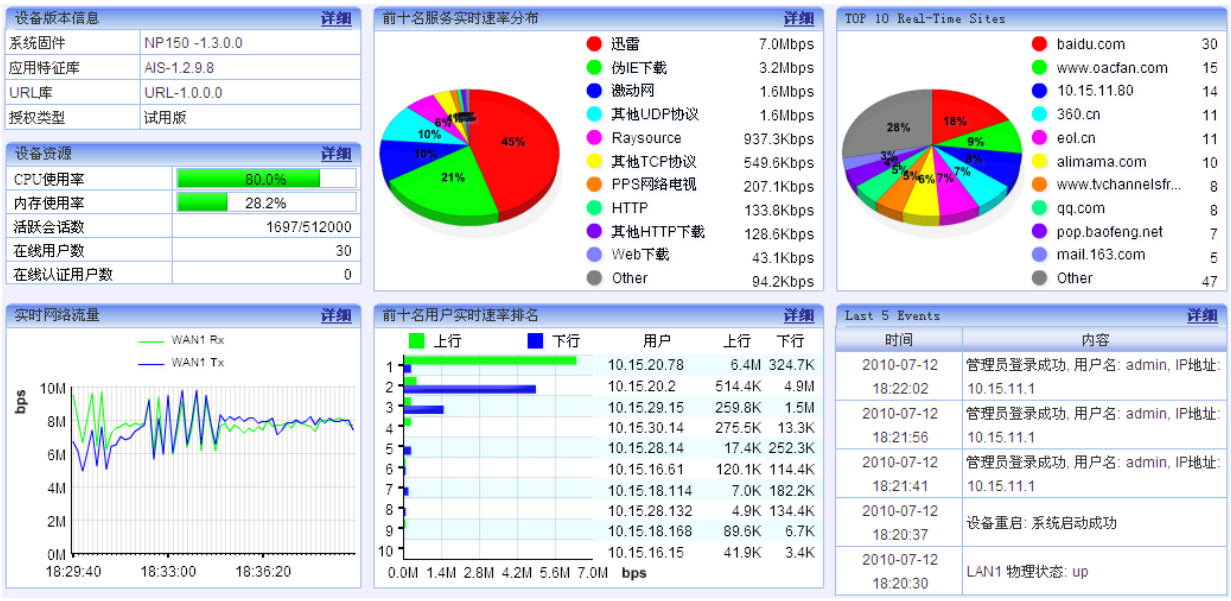
- ✧ 实时在线网络监控
- ✧ 上网行为分析
- ✧ 流量与会话统计分析
- ✧ 报表系统

5.6.1 实时在线网络监控

任天行网络安全管理系统_SURF-RAG 系列设备及其报表中心都支持管理员实时地监控设备运行状况与当前网络情况，可确保管理员在第一时间内掌握网络运行情况，帮助管理员对网络异常进行定位分析。

- ✧ 系统资源使用状况，如 CPU、内存等使用信息；
- ✧ 物理端口的实时流量以及最近 1 小时网络流量变化情况；
- ✧ 当前网络前 10 名服务最近一小时流量趋势图
- ✧ 服务组最近一小时流量堆叠趋势图
- ✧ 当前活跃服务/所有服务的当前速率、最近一小时总流量、最近一小时平均速率；
- ✧ 当前网络前 50 名用户实时流量、上下行速率、新建会话速率、活跃会话数；

下图显示了设备当前的运行情况、端口状态和流量情况，以及前 10 名服务带宽分布情况、前 10 名 IP 带宽占用情况：



5.6.2 上网行为监控

通过互联网传递信息已经成为企业的关键应用，然而信息的机密性、健康性、政治性等问题也随之而来。通过 任天行网络安全管理系统_SURF-RAG 系列设备，您可以制定精细化的信息收发监控策略，有效控制信息的传播范围，控制敏感信息的泄露，避免可能引起的法律风险。任天行网络安全管理系统_SURF-RAG 系列设备能够对以下信息发送进行监控与控制：

- **WEB访问记录**
  - ✧ URL 统计与排名
  - ✧ 网页标题统计
  - ✧ 搜索引擎上搜索的关键字统计
  - ✧ 文件上传下载记录
- **论坛发帖**
  - ✧ 发帖正文监控
  - ✧ 发帖附件监控
  - ✧ 发帖关键字阻断
  - ✧ 网页评论记录
- **电子邮件**

- ✧ SMTP 发送邮件
- ✧ WebMail 邮件
- ✧ POP3 接收邮件
- ✧ 审计内容包括收件/发件邮箱、邮件标题、邮件正文、邮件附件、邮件日期

➢ **即时通讯软件**

- ✧ 聊天内容监控
- ✧ 聊天账户监控

➢ **FTP 记录**

- ✧ 登录信息
- ✧ 文件上传记录
- ✧ 文件下载记录

➢ **Telnet 记录**

- ✧ 登录信息
- ✧ 命令记录

5.6.3 递进式的流量统计分析

任天行网络安全管理系统_SURF-RAG 系列设备的报表中心通过流量统计分析模块详细的记录了全网的流量信息。同时，报表中心采用递进的方式，把统计数据从宏观到微观、从总体到局部、层次分明地展现给用户，帮助管理员快速在全局与细节上把握网络活动的状况。

举例来说，如果管理员想了解全网流量的情况，那么，他可以按照服务进行第一层的分类统计。首先，可以看到在不同时间段内网络中有哪些服务，每种服务所占用的流量大小、带宽速率、会话数，并可以根据这些参数进行排名，并分别以饼图、柱图、现行趋势图、及表格呈现。然后，可以再进一步查看每种服务有哪些 IP/用户在使用，每个 IP/用户占用的流量大小、带宽速率、会话数，以及每个 IP/用户对应这些参数的趋势图等；当有多条线路时，还可以看到每种服务在不同线路的流量分配情况。反过来，如果首先基于 IP 地址分类统计和排名显示，那么可得知哪个 IP 传输的流量最大、占用的带宽最高，然后可进一步查看到每个 IP 所使用的服务等等详细信息。

同样，对于全网的流量还可以按照 IP 地址组、用户、用户组、线路等元素进行第一层的分类统计，然后可再一层一层往下进行递进查询分析。

5.6.4 会话记录

任天行网络安全管理系统_SURF-RAG 系列设备可记录全部的会话日志。通过检查完整的会话日志，管理者可以跟踪网络中的任何操作，尤其可帮助公安部发稽查案件。目前，在大多数的网络中，内部用户上互联网都需要做 NAT 转换。如果谁在网上散步了一些关于恐怖、拐卖、色情等等违法的言论，往往只能追查到网络出口的 IP 地址，很难追查到原始用户的 IP 地址，对案件的进展非常不利。

任天行网络安全管理系统_SURF-RAG 系列设备的会话记录包括：源 IP、目的 IP、协议类型、七层应用名称、源端口、目的端口、是否进行 NAT 转换(可显示转换后的 IP 和端口)、会话产生的时间和会话持续时间。当管理员发现异常的流量和行为记录时，可以再去追查到这个行为的会话信息，即便是有 NAT 转换的网络环境，也可以很快的定位到发布信息的原始用户。

5.6.5 阻断记录

任天行网络安全管理系统_SURF-RAG 系列设备可记录被防火墙策略、流量管理策略、行为管理策略阻断的报文的日志。阻断日志包括：源 IP、源端口、目的 IP、目的端口、协议类型、服务名称、报文长度等。当网络有异常时，阻断日志可以协助管理员查找网络问题，可以清楚的知道哪些报文被策略阻断。

5.6.6 个人行为分项统计

全局的行为统计，是将网络中所有的用户的记录综合在一起进行统计。而个人行为分享统计，是根据组织结构中的逻辑结构树，逐个展示用户，并将每个用户的上网行为进行分项统计。同时也可以将个人行为的数据导出为报表。个人行为分项统计可使管理员简明清晰的了解每个用户的上网行为，极大的帮助管理员跟踪网络行为的动向。

个人行为分项统计包括以下几项：

- 网页统计：将每个用户的网页标题记录、论坛发帖记录、网页评论记录、搜索引擎上搜索的关键字记录、网页文件上传记录、URL访问记录分项统计并显示。
- 即时通讯记录：将每个用户的 MSN、QQ、Yahoo、ICQ 等即时通讯工具的登录记录、聊天记录、或文件传输记录分项统计并显示。聊天记录的显示完全模拟即时通讯软件的聊天记录框的样式。
- 邮件记录：将每个用户收发的邮件详细记录并显示。邮件信息包括：邮件收发者、

主题、正文、附件及大小、日期等信息。若用户使用了多个邮件账户，每个账户将分别显示其收发邮件的信息，完全模拟了FoxMail 客户端的显示方式。

- FTP 记录：将每个用户使用 FTP 的登录信息、文件上传记录、文件下载记录分项统计并显示。
- Telnet 记录：将每个用户使用 Telnet 的登录信息、命令记录分项统计并显示。

5.6.7 报表分析

为了有效地展示大量分析数据，任天行网络安全管理系统_SURF-RAG 系列设备的报表中心提供丰富的、图文并茂的报表，包含曲线图、饼状图、柱状图以及数据统计报表等多种样式和内容，以小时、天、周、月、年，或自定义的时间段为时间单位的系列报表。此外，为了方便信息的沟通，每种报表都可以通过电子邮件发送，并支持定期订阅功能。报表中心提供的报表包括：

- **统计报表**

  用于以用户、用户组、服务、服务组、线路等为对象，统计某段时间的流量信息和行为次数，并按统计对象进行排名，便于管理员了解网络的使用情况以及内网用户的上网行为。

- **趋势报表**

  用于以用户、用户组、服务、服务组、线路等为对象，统计某段时间内各个时间点的流量信息和行为次数，便于管理员掌握某个时间段内网络的运行状态、流量和行为的趋势信息。

5.6.8 无为而治的管理方式

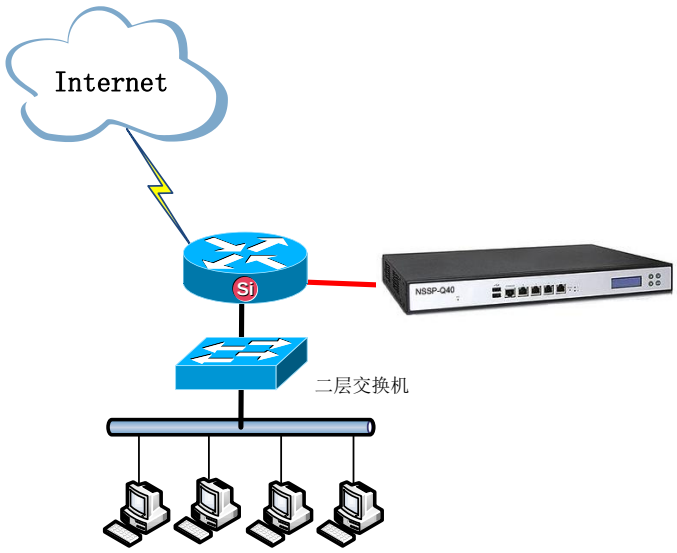
强大的监控手段往往涉及到个人隐私，建议您在监控网络流量和网络行为前，向相关的人员发出正式通知，让每一个员工知道他们在工作时间发生的网络行为是可以被监视的。当员工意识到上班时间的网络行为有可能被监控，便会主动减少上班时间做与工作无关的事情，自觉地提高工作效率，使网络管理者对网络的管理达到无为而治的效果。

六. 典型部署

任天行网络安全管理系统_SURF-RAG 系列设备采用串接方式接入网络，支持网桥模式、路由模式和旁路模式。

6.1 旁路模式

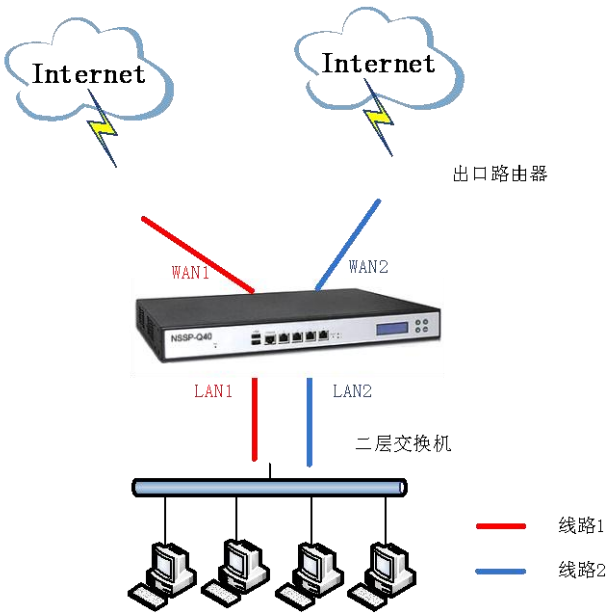
以透旁路方式接入网络，可对网络的流量进行前面的监控和记录，无需改动用户网络结构和配置。



6.2 网桥模式

以透明网桥方式接入网络，可以部署到网络的网关位置或各部门的出口位置。无需改动用户网络结构和配置，即插即用，支持单网桥、多网桥的部署方式。

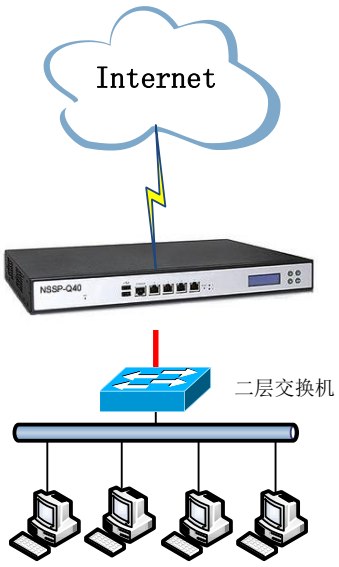
单桥模式



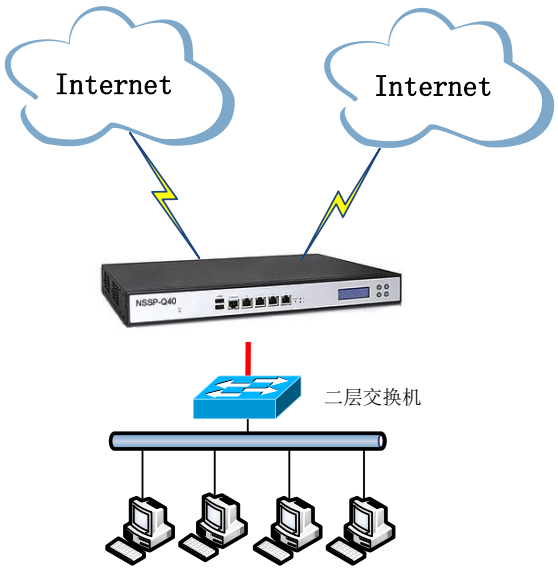
双桥模式

6.3 路由模式

将设备串接网络中，可以放于内网的任意子网边界，或与核心交换机相连。可以代替防火墙或路由器，需要为设备配置内网和外网接口的 IP 地址。



单链路路由模式



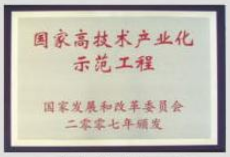
双链路路由模式

六. 荣誉资质

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

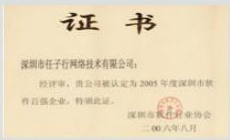


国家高技术产业化示范工程


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

七. 关于任子行

任子行网络技术股份有限公司创立于 2000 年 5 月，是专业从事计算机网络信息安全技术产品研发的高科技企业。公司现已获得深圳市高新技术企业和软件企业资格认证，并通过了 ISO9001：2000 国际标准质量管理体系、国家信息产业部计算机信息系统集成三级资质、国家保密局涉及国家秘密的信息系统集成单项资质、国家商用密码产品定点生产单位资质认证及广东省安全服务二级资质认证。

公司现有员工约 500 人，人员以本科和硕士以上学历为主。专注于网络信息安全领域产品和技术的研发，现已拥有任天行网络安全管理系统、NET110 网络安全审计系列、任子行 IDC 信息安全审计管理系统、任子行公共信息网络视音频节目管理系统、任子行网络安全管理软件、网页防篡改系统等多条安全产品线，产品目前全部通过国家权威机构的认证，能够在政府、军工、教育、能源、运营商、广电部门、企事业单位等各个行业均得到了广泛、成功的应用，竭诚为广大用户提供全面、优质的计算机网络及信息安全解决方案。

公司作为国家计算机信息内容安全重点实验室的深圳实验室，承担了国家计委信息安全专项产业化示范项目及其他多项国家重点网络安全研究和工程项目。公司的研发项目被科技部列为国家级火炬计划项目和国家、省重点新产品计划。公司产品荣获“科学技术进步一等奖”、“深圳市优秀软件产品奖” 、“广东省科学技术奖三等奖”、“中国国际软件博览会创新奖”、“中国内网安全市场优秀推荐品牌奖”。

秉承“诚信、敬业、协同、创新”的企业精神，任子行公司将致力于“绿色、高效和安全网络”技术和产品的研发,通过不断加强自主知识产权核心技术的研究，持续的产品质量改进以及全方位的产品技术服务，为客户提供一流的网络安全产品和服务，全方位地提升用户网络使用效率，让网络为用户创造更大的价值。