网康科技 NETENTSEC

中国企业信息化 500 强
上网行为管理设备指定提供商

打造文明健康安全高效的互联网

网康安全代理服务器NPS

产品白皮书

北京网康科技有限公司

2014年 11月

版权声明

信息更新

本文档仅用于为最终用户提供信息，并且随时可由网康科技更改或撤回。

适用版本

本文档适用于 NPS 4.1 系列版本。

免责条款

根据适用法律的许可范围，网康科技按“原样”提供本文档而不承担任何形式的担保，包括（但不限于）任何隐含的适销性、特殊目的适用性或无侵害性。在任何情况下，网康科技都不会对最终用户或任何第三方因使用本文档造成的任何直接或间接损失或损坏负责，即使网康科技明确得知这些损失或损坏，这些损坏包括（但不限于）利润损失、业务中断、信誉或数据丢失。

期望读者

期望了解本产品主要技术特性的用户、企业管理人员、系统管理员、网络管理员等。本文档假设您对下面的知识有一定的了解：

- Web 与 HTTP
- TCP/IP 协议
- 代理服务器基础知识
- 网络安全基础知识
- Windows 操作系统

目　　录

1 网康安全代理服务器简介

网康安全代理服务器（NPS）是专业的企业级硬件代理产品，能够为用户提供灵活高效的代理服务解决方案，实现业务安全连通、内容实时安全扫描和网络透明可控，从而全面提升用户网络的使用价值。用户能够基于应用层路由灵活规划网络逻辑结构，规划用户上网权限，同时对外隐藏内网用户信息，有效防御外网攻击。通过内置的专业杀毒引擎，在互联网出口处监控和防范病毒、木马、间谍软件、蠕虫等恶意行为。

2 功能介绍

2.1 业务代理

用户在互联网访问过程中，经常受到病毒、木马等安全威胁，因此如何有效抵抗网络威胁，在提供必要的外网访问服务的同时，能够保障企业网络的安全性，是所有用户需要面临的问题。

网康安全代理服务器为用户提供了丰富的业务代理功能，其作用相当于业务的中转站，能够替代用户获取网络资源，于此同时，又能够全方位屏蔽内网用户信息，对网络内容进行实时安全扫描，有效抵抗网络安全威胁，使用户在网络的连通性和可用性之间无需权衡与折中。对于潜在的恶意攻击者，通过连接只能找到代理服务器，由于代理服务器的安全性远高于普通的 PC 机，因此通过代理实现对内网安全的保护。

网康安全代理服务器支持的应用类型包括 HTTP、HTTPS、SOCKS 等应用，能够全方位满足用户的实际业务需要，同时支持灵活的端口配置和源/目的地址的代理配置，使业务的开启和服务能够根据实际需要灵活掌控。

网康安全代理服务器具备丰富的代理部署方式，可以在网关、透明网桥、单臂旁路的方式下提供代理服务。

2.2 内容安全分析

据国际计算机安全协会（ICSA）的统计，目前超过 90%的病毒是通过互联网进行传播的。网康安全代理服务器提供了实时内容安全扫描分析，可以有效的阻止病毒、木马、恶意软件、间谍软件、蠕虫、键盘记录软件等通过网关进入企业内部。

结合网络安全代理服务器的用户准入控制识别系统，可以快速确定威胁来源及谁触发了安全威胁。

2.3 网页过滤

Web 是互联网上内容最丰富、访问量最大的应用，然而网页内容良莠不齐，充斥许多反动、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，一方面躲避防火墙的封堵，一方面携带病毒、恶意软件，为内网用户带来安全风险，挤占网络带宽。网康安全代理服务器通过预分类过滤技术、URL 自动分类引擎以及灵活的策略设置，对违反国家法律、危害企业安全的内容进行过滤，避免用户有意无意访问包含非法内容的网页，净化网络，减少病毒进入局域网的几率，降低企业法律风险，创造文明健康的上网环境。

- **URL 黑白名单**

通过 URL 黑白名单，可以设置 Web 访问中的特例：对于一些网站可能需要跳过已定义好的策略，而无条件地允许或阻塞，比如 Windows 自动更新服务，病毒库自动更新服务。被直接允许访问的网站列表称为 URL 白名单；相反地，被直接阻塞访问的网站列表称为 URL 黑名单。黑名单、白名单和策略的优先级从高到低为黑名单 -> 白名单 -> 策略。

2.4 用户管理

用户是网康安全代理服务器产品最核心的要素，任何一条策略都是针对一个用户或者部门设置的，因此对于用户的识别、认证与管理能力决定了管理的效果。网康安全代理服务器提供了丰富的用户认证方式以及符合企业实际的用户管理能力，很好地满足企业对于用户的管理要求。

2.4.1 按照企业组织结构建立用户组

当用户数目较多、组织结构比较复杂时，按照实际的组织结构管理用户是最有效的方式，易于管理员查询、定位和设置策略。网康安全代理服务器支持树型结构管理用户，能够完全按照企业的实际情况建立用户组。

2.4.2 IP 网段自动分组

任何互联网行为管控和审计策略最终都将赋予到用户或用户组上，对于以 IP 网段划分部门的机构，如果用户数目众多或者 IP 分配变化频繁（如大学的院系），针对每一个用户进行单独的设置是不现实的，这些机构关心的更多的是对某一类用户进行管理，而不是特定的用户。网康安全代理服务器可以按照网段进行分组并设置策略，属于某网段的 IP 会自动适用该网段的策略。代理服务器支持将新入网的未注册 IP 自动加入到所属的 IP 分组中，从而自动为该 IP 分配预定义的管控策略。对于那些临时来访的外来用户，管理员可以将其计算机设备统一划分在某一 IP 范围内，并对该 IP 网段分组制定相关限制性策略，大大增强了动态用户管理的灵活性。

此外，如果管理员没有预先设置 IP 网段，代理服务器可以将未注册的用户实时加入系统的未定义用户组中，管理员可以在合适的时机将其移动到已定义用户组中，从而逐步完善用户的定义。

2.4.3 丰富的用户认证方式

网康安全代理服务器提供多种用户认证和识别方式，为用户管理提供了灵活而完善的方案，包括基本的 IP/MAC 绑定、三层网络环境下的 IP/MAC 绑定、网关 Web 认证、AD 域透明认证、LDAP 认证、RADIUS 认证、POP3 认证、ESMTP 认证、SOCKS 认证、PPPoE 认证账号识别、第三方用户识别。此外，对于使用微软 ISA 系统的环境，代理服务器还支持 NTLM 认证和 BASIC 认证，实现与 ISA 的联动。对于每一种认证方式，代理服务器都支持分段/混合认证。通过规划并部署合适的认证方式，可以把互联网访问管理应用到具体用户，实现基于用户身份的访问管理。

在有些企业，实行规划合理并且严格执行的 IP 地址分配制度，那么通过 IP 地址和网卡 MAC 地址来确定用户身份是可靠的；但是在有些网络环境下，用 IP 或网卡 MAC 地址并不能确定一个人的身份，比如 DHCP 动态分配 IP、或多人共用一台设备的时候，就需要其它

方式确定用户身份，如网关本地 Web 认证或第三方认证。

在 WEB 认证方式下，管理员可以设定并分发统一的初始口令，并定义账号缓存的有效时间，保障用户身份的安全，使用户身份的确定与具体上网设备完全无关。要实现 WEB 认证，首先需要在网康安全代理服务器中建立用户信息。NS 代理服务器支持多种用户信息获取方式，可以通过 IP 网段地址扫描，自动获取内网用户的 IP 地址、计算机名、MAC 地址信息，也可以通过 LDAP 同步的方式定期更新用户目录服务器的用户信息，支持 RADIUS 认证，此外，还可以使用网康自定义用户导入功能，将微软 Excel 表格整理的用户信息快速导入。

建立用户信息后，按照管理需求，基于网段、权限、行政职能自定义用户组和成员，并且可以在不同用户组之间灵活调整成员用户，最终形成清晰直观的树型组织结构。这样就解决了“确定用户身份”的问题，并为基于用户或用户组制定策略和统计报表奠定了基础。

2.4.4 支持混合认证

网康安全代理服务器支持多种认证方式的混合，可方便为不同的网段开启不同的认证方式，实现不同用户群的差异化管理；同一网段用户也可同时开启多种认证方式，方便用户在不同的应用环境下都可以认证入网。

2.4.5 支持邮件用户识别

对于拥有独立企业邮箱的网络环境，代理服务器支持 POP3 用户识别，用户入网无需认证，只要通过 POP3 协议接收一封邮件，代理服务器即可将邮件账号名记录下来，该用户所有互联网行为都可实名制记录下来，便于日后日志的查询、定位。

2.4.6 支持用户的权限组管理

网康安全代理服务器支持权限组的定义和管理。可在各级用户组织中建立“权限组”，可将任意用户添加入“权限组”中，一个用户可以同时隶属于多个权限组。这一功能提高了用户策略管理的灵活性，在不改变原用户的组织结构的情况下，可实现对一些分散在各组中的用户进行统一策略管理。

2.4.7 支持 AD 域权限组导入

网康安全代理服务器可将 AD 域服务器中用户权限组信息导入到用户组织列表中，并自

动创建相对应的权限组，可定义各权限组的互联网行为管控策略。

2.4.8 支持从多个 LDAP 服务器同时导入用户数据

对于那些拥有多 AD 子域服务器的网络环境，代理服务器可同时同步所有 AD 子域服务器中的用户信息数据，实现全网用户的统一管理。

2.4.9 支持用户对象的快速搜索选择

在用户数量庞大，用户组织结构复杂的网络环境中，管理员在制定策略或查询日志时，按组织关系逐层筛选用户这一操作会耗费大量的时间和精力。

网康安全代理服务器可以避免上述问题，在所有用户对象选择对话框中，支持用户搜索定位功能。只要在搜索框中输入要选择的用户组或用户名称，即可直接将该用户或用户组添加到用户对象中。

2.4.10 支持 IP/MAC 绑定

网康安全代理服务器支持二层网络环境和三层网络环境下的 IP/MAC 绑定。可自动阻塞那些非法占用他人 IP 地址的用户。

2.4.11 支持强制下线

网康安全代理服务器支持 WEB 认证、LDAP 认证、RADIUS 认证、邮件账号认证、IP 识别用户的强制下线。

使用者也可以随时将活跃用户列表中的 IP 加入“屏蔽 IP 列表”中。

2.4.12 支持认证账号有效期限制

对于一些需求临时入网的用户，管理员可通过该功能限制这些用户可以入网的时间范围，超出限定范围后，该用户无法再入网。一方面提高准入用户的安全性，另一方面可实现入网限时的功能。

2.4.13 支持认证账号唯一性控制

网康安全代理服务器支持认证账号唯一性控制。这一功能可以方便控制同一认证账号是

否允许在多台计算机上同时登陆。从而适应不同用户的认证需求。

2.4.14 支持认证账号黑名单

对于行为异常的认证账号，网康安全代理服务器支持将其加入到认证账号黑名单。未经管理员将其从黑名单中清除，该账号将无法通过认证。

2.4.15 支持第三方认证信息联动接口

网康安全代理服务器提供标准的第三方用户认证信息联动接口，可以接收来自第三方网络准入系统或上网计费系统的用户认证信息。从而将上网行为日志准确关联到具体的用户，并实现用户在多认证系统环境下的单点认证。

2.5 设备自身安全

为了最充分地管理控制用户上网行为，网康安全代理服务器部署在企业的网关位置，因此，设备自身的安全稳定将直接影响网络运行。网康安全代理服务器从软、硬件两方面针对性地增强了系统的稳定可靠，确保网络运行畅通。

2.5.1 专用的安全的软、硬件系统

网康安全代理服务器采用专用的操作系统 NSOS，它在成熟的操作系统基础上，针对网康安全代理服务器的特点，进行了大幅度的裁减，关闭非相关端口与服务，确保不受网络病毒的危害；重新编写 TCP/IP 协议栈，优化网络驱动，减少系统内核与用户空间的数据交换，大大提高了网络数据的处理能力。

硬件方面，网康安全代理服务器充分考虑用户机房网络环境，在设备的通风、电磁、降噪、信息显示以及手工管控等方面进行了大量的革新，确保设备的高效运行与安全操作。

2.5.2 软硬件旁路功能避免出现单点故障

网康安全代理服务器提供硬件 bypass 与软件 bypass 双重保护，确保发生异常时网络依然畅通。

硬件 bypass：由于意外原因发生设备掉电时，网康安全代理服务器将自动启动硬件 bypass 功能，设备在物理上成为一条连通的网线，不会对已有的网络连接产生任何影响。此外，网康独有的一键 bypass 功能，在设备有电的情况下，可以“主动”将设备切换为 bypass

状态，卸载网络流量。

软件 bypass：当网络负载超过设定的安全阀值时，系统自动启动软件 bypass 功能，选择性停止对各种网络数据的分析处理，以设备最大带宽“放行”数据包。当网络负载恢复到安全阀值以下时，系统自动恢复各种处理功能。

2.5.3 控制内网病毒攻击导致的异常流量

网康安全代理服务器通常部署在防火墙的内部，与防火墙互为补充，可以针对来自内部的攻击进行识别与防范。如果内网发生 ARP 攻击事件，引起网络流量异常增加，代理服务器可以在第一时间识别感染 ARP 病毒的主机，并发送告警邮件给管理员，提示及时防范。此外，当发生异常流量时，通过设置来源 IP 访问的上传包速率、上传速率、新建连接速率、小包发送速率等多个阀值，对突发流量进行带宽整形，对危险主机进行带宽“抑制”，同时保障代理服务器自身的请求响应能力。对于超出阀值的流量，除了带宽限制，还可以完全阻塞、或者只阻塞超出阀值部分的流量，对于异常流量的 IP，可以设置加入黑名单进行屏蔽。

2.5.4 限制可访问代理服务器的 IP 地址范围

为确保代理服务器自身的安全，网康安全代理服务器提供管理界面访问限制功能，可定义允许登录代理服务器管理界面的 IP 地址范围，非法用户即使获取了用户名和口令，也无法登陆代理服务器的管理界面。

3 特点与优势

作为一款优秀的代理服务器产品，网康安全代理服务器全面引领国内行业潮流，并在多个方面达到国际水平。

3.1 全面的代理服务支持

全面支持 HTTP、HTTPS、SOCKS 等代理服务，全面覆盖用户主流业务，通过代理为用户网络提供更高的安全保障，使用户在网络连通性和安全性方面无需折中。

3.2 高效内容分析引擎

- **零拷贝技术，极大提高网络包处理速度**

零拷贝（zero-copy）基本思想是：数据包从网络设备到用户程序空间传递的过程中，减少数据拷贝次数，减少系统调用，提高 CPU 与内存的使用效率。实现零拷贝的最主要技术是 DMA 数据传输和内存区域映射技术。网康安全代理服务器采用零拷贝抓包技术，极大减少了 CPU 的中断调用，显著提高了包处理效率。

- **择时组包，智能流分析**

在 IP 网络中，内容数据被分拆封装在多个数据包中传输，为了获得完整的内容，必须把连续的多个包“拆封”重新组合起来。网康安全代理服务器专有的择时组包技术，能够智能判断哪些包可以放过，哪些包需要暂留重组，减少了包处理的数量，从而提高数据流的分析效率。

3.3 人性化界面设计，易于操作管理

- **标签页管理界面**

网康安全代理服务器管理界面使用标签页打开每一个配置页面，可以自由切换，极大便利配置和查看。

- **管理界面简洁清晰，美观大方**

网康安全代理服务器管理界面采用最新的 web 技术，结合传统 C/S 的操作风格，大大加强了 Web 操作的交互能力。界面结构清晰，美观大方，从整体布局到细小按钮

都经过精心设计，充分贴合用户的思维、操作习惯。

- **树型控制元素，实现便捷操作**

代理服务器的 URL 分类、用户组织结构、应用协议结构等多种控制元素都以树型结构展示，一目了然，便于操作和管理。

- **在线帮助系统提供智能定位，精确解答操作疑问**
- **向导式配置，轻松完成网络配置**
- **Dashboard 方式集中显示系统宏观信息**

代理服务器采用 Dashboard（仪表盘）方式集中显示设备的运行状况与关键网络活动，使管理员可以迅速了解最重要的信息。

- **界面元素灵活设置，预留充分的数据显示空间**

代理服务器的界面元素如菜单、按钮、区域窗口都可以按需伸缩，列表窗口的字段宽度也可以自由拖动交换，为数据的显示留出足够的空间，便于用户管理策略和查看审计结果。

3.4 运行稳定可靠，确保网络畅通

- 全系列设备支持硬件 bypass，避免电源失效导致的网络中断；
- 独有的一键式 bypass 设计，支持管理员主动调整网络负载；
- 独有的软件死锁与高负载跳转功能，根据预设阀值自动分流高负载流量；

3.5 灵活的部署方式

- 支持透明模式、网关模式、单臂模式、WCCP 模式
- 网桥透明接入既有网络环境，不影响原有网络配置；
- 串接方式接入，过滤所有报文，实现完整过滤、审计；
- WCCP 方式确保网络无单点故障，不对网络性能产生任何影响。

3.6 完善的代理功能

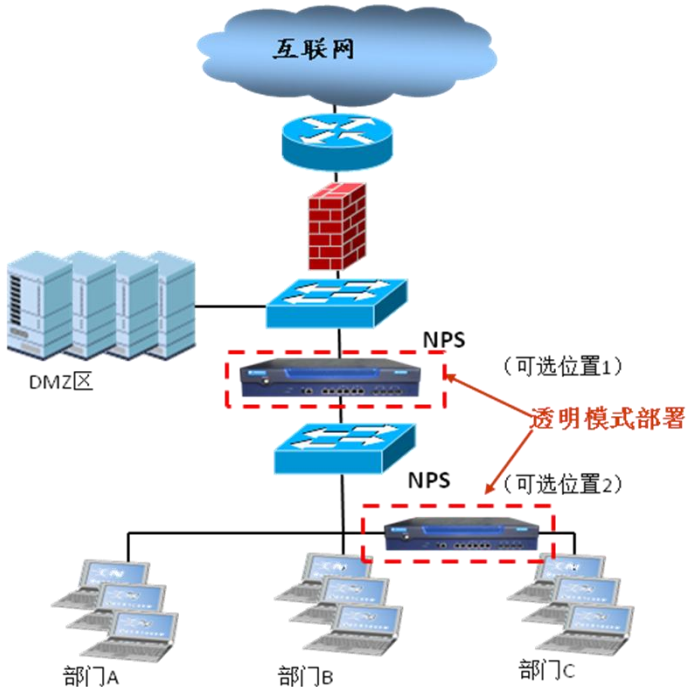
- 支持 HTTP、HTTPS、SOCKS 代理；
- 支持 SOCKS 代理认证。

4 产品的部署

网康安全代理服务器支持多种接入方式，以适应不同用户的网络环境和管理需求。

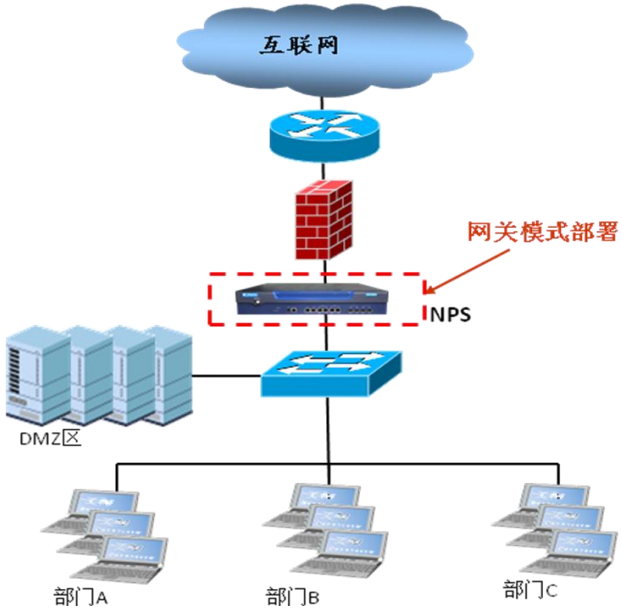
4.1 透明模式

以透明网桥方式部署在企业或部门网络出口位置。无需改动用户网络结构和配置，仅需配置一个网桥 IP 地址。客户端也无需指向代理，流经设备的 Web 请求会自动重定向到代理服务。这种部署方式的好处是配置简单，维护量小，对用户透明，设备自身安全性较高。



4.2 网关模式

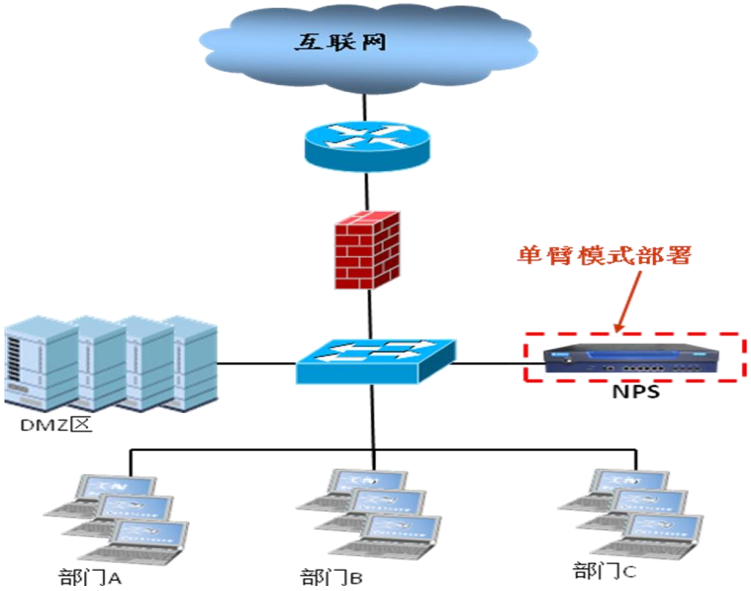
也称为路由模式，将设备串接到网关处，起到隔离内外网和 NAT / 路由的作用。需要为设备配置内网和外网 IP 地址。除了内外网口需要配置不同 IP 外，其它配置与网桥模式相同。这种模式下，客户端浏览器可以指向 NPS 内网口的代理服务端口。



4.3 单臂模式

对于业务网和办公网逻辑分离的环境，NPS 能够采用单臂部署模式。单臂部署模式下，客户端必须在浏览器设置代理服务器地址和服务端口，使访问互联网的请求直接发送到代理服务器。而访问业务网的请求则不会流向代理服务器，因此不受到任何影响。

WCCP 也适应于单臂模式。



5 关于网康科技

网康科技有限公司是是中国技术最领先的网络应用管理设备提供商，专注于网络应用管理领域，为用户提供先进的网络应用管理产品、解决方案及服务，旨在帮助用户实现“上好网 用好网”的目标。

网康科技拥有业界最领先的“互联网应用及内容研究实验室”，研发了“第三代网络应用识别（XAI）技术”、“实时网页过滤（RACE）技术”等世界顶尖水平的网络应用管理技术，并缔造了“全球最大的中文网页数据库”和“中国最大的网络应用协议库”。

网康科技拥有业界最领先的上网行为管理、智能流量管理、安全代理服务器、移动互联网业务管理系统等系列产品，并广泛应用于政府、金融、能源、教育、通信、企业等众多行业，其中不乏世界 500 强、中国 500 强企业，拥有大量成熟的行业解决方案和典型成功案例，是中国高端用户最多的网络应用管理设备提供商。

联系方式

公司地址：北京市海淀区中关村东路 66 号 世纪科贸大厦 A 座 3 层

邮政编码：100190

联系电话：010 – 62670909

传真号码：010 – 62670958

服务热线：400-678-3600

电子邮件：marketing@netentsec.com

公司网址：www.netentsec.com