

网康科技上网行为管理案例

(能源行业)



国家电网河南省电力公司

项目背景:

河南省电力公司是国家电网公司的全资子公司，国有特大型企业，主要承担河南省内电力资源优化配置，为河南经济社会发展和人民生活提供可靠优质电力保障的责任。公司承担着全省 18 个市、2000 多个乡、9800 多万人口的供电服务，代管 108 个县供电企业，其中改制控股 20 多个县供电公司。河南省电力公司采用网康设备实现对全集团的上网行为管理。

用户面临的问题与挑战:

1、国家法规及信息安全达标的要求

国家 82 号令要求上网企业至少保留 60 天的上网记录，国资委要求关系国计民生的重点企业，其信息化建设必须满足对应的等级保护要求；

2、非法网站的访问带来了较多的法律风险

反政府，反社会，反道德，反法律的网站的主动或被动浏览，给企业带来了巨大的法律风险；

3、关键业务流量无法保证

网络中存在着大量的 P2P 类应用（如 BT、迅雷、网络电视等），严重侵蚀带宽，导致一些依托于互联网的业务系统和视频会议无法正常工作；

4、异常流量无法有效定位，办公系统无法正常运转

网络中充斥着大量病毒、攻击，伪造 IP 等，对外不断发起连接并大量发包（尤其是小字节数据包），造成的网络中断事故时有发生；

5、业务数据的保密性无法得到保障

无法通过企业网外发信息进行审计（包括 POST 审计和邮件审计），来保证企业内部信息外发的安全。

网康科技解决方案:

网康为河南省电力公司总公司以及每个子公司分别部署一台网康 NSICG 设备，进行分布管理，有效地帮助用户管理上网行为，具体管控策略如下：

1、通过总部的集中管理服务器和日志服务器，可以管理各地部署的所有设备。监测各分支设备运行状态，强制性策略分级下发、以保障公司所有单位均满足国家政策法规的上网管理要求。

2、通过 NSICG 的 URL 预分类库、关键字过滤技术，过滤病毒、违反法律等非法信息。对于

外发非法内容，基于关键字拦截，增强内部控制机制。

3、通过应用流量管理、屏蔽非法应用（主要为 P2P 和 P2P streaming 类协议）增大带宽有效利用率，提高访问速度，提高员工工作效率；定义并保障关键业务流的带宽；保障视频会议等业务应用的顺畅。

4、开启网络防护报警功能，对异常的流量进行自动管控，以实现网络无人值守时的自我防护，保障互联网出口带宽的畅通。

5、对部分出口带宽较小的分支机构，开启 Web 缓存功能，加速 Web 访问速度。

用户效果

1、开启审计策略后：大量的内容信息从此拥有了全面的日志。

2、对大量的高风险类网站和娱乐类网站进行封堵。

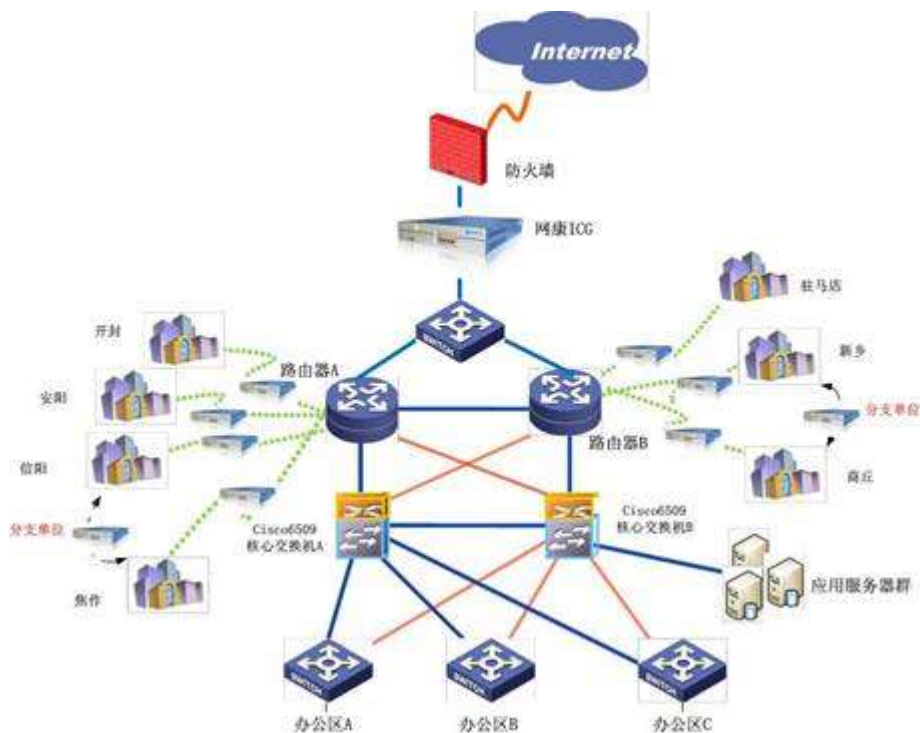
3、迅雷、bt、电驴、在线视频等流量被控制住了，降到了 41%左右。视频会议再没出现过带宽吃紧的现象。http 的应用得到了保证，从 10%提高到 32.7%。我们能够明显看出总带宽流量在平滑，优化，网页图片打开速度明显变快。

4、开启防护后，可以通过获取经验值，设定内网防护的基准，同时可以将超出基准的流量阻塞，以保证内网安全，防止病毒或攻击行为的产生。

5、网康设备的长期运行，能够记录用户的所有上网行为，并能基于此记录，统计分析出内网的总体现状，用户、应用的行为模型一目了然。

6、递进式统计查找功能，方便快速定位问题。

网络拓扑图



河南省电力公司总部及以下 18 个地市分支机构共部署 19 台网康设备

河南电力公司	平顶山分公司	驻马店分公司	鹤壁分公司
三门峡分公司	焦作分公司	信阳分公司????	安阳分公司
洛阳分公司	郑州分公司	周口分公司	濮阳分公司
南阳分公司	许昌分公司	开封分公司	商丘分公司
济源分公司	漯河分公司	新乡分公司	