360 网络安全准入系统

技术白皮书

奇虎 360 科技有限公司

二 O 一 四年 十一 月

360 网络安全准入系统技术白皮书

更新历史

编写人	日期	版本号	备注
刘光辉	2014/11/11	1.2	补充 802.1x

目录

第一章 前言

网络信息化的飞速发展为用户内网管理带来新的问题和挑战，主要体现在以下几方面：

1) 外来终端随意地访问网络，不设防；

2) 内网中的用户可以随意地访问核心网络，下载核心文件；

3) 不合规终端也可以接入到公司核心服务，对整个网络安全带来隐患；

针对以上问题以及诸多安全隐患，360互联网安全中心凭借多年信息安全领域的技术积淀，推出了基于终端应用的准入系统（简称360NAC）。

360NAC是一套配合360天擎终端安全管理系统的安全准入解决方案，它基于用户核心服务保护模式，对非法访问用户核心服务的终端进行管控和限制，并对非法用户强推终端管控软件，从而实现了一套从网络到终端的立体准入系统。

第二章 产品概述

360NAC 是由 360 互联网安全中心开发的，具有自主知识产权的准入产品。该产品采用旁路部署方式，采用 360 自有技术，对企业内网数据流进行合法性检查并及时阻断非法连接。

2.1 产品构成

360NAC 是由硬件准系统配合天擎客户端组成的，硬件准入系统同时提供 B/S 架构的系统管理平台供用户对系统进行全方位配置与管理。

2.2 设计依据

- 《信息安全技术 信息系统安全等级保护技术要求》（GB/T 22239-2008）
- 《涉及国家秘密的信息系统分级保护技术要求》（BMB 17-2006）
- 《信息安全技术 终端计算机系统安全等级技术要求》（GA/T 671-2006）
- 《信息技术 安全技术 信息安全管理体系要求》（GB/T 22080-2008）
- 《信息技术 安全技术 信息安全管理实用规则》（GB/T 22081-2008）

第三章 功能简介

3.1 网络准入

360NAC 网路准入控制系统通过安装天擎 – 入网、注册 – 入网、注册 – 安装天擎 - 入网，三种方式灵活实现企业需要的准入方式。

3.2 认证管理

3.2.1 保护服务器管理

支持将服务器 IP 添加至保护服务器管理，该服务器即刻被保护，未安装天擎的终端将不能访问被保护的服务器。

3.2.2 例外终端管理

支持将终端 IP 添加至例外终端管理，该终端将不受准入策略限制，无论是否安装天擎客户端都可访问被保护的服务器。

3.2.3 重定向设置

支持识别自定义 http 协议端口。

支持终端分发地址配置。

支持服务器管理地址配置。

3.2.3 认证服务器配置

支持本地 LDAP 连接。

支持第三方 LDAP 连接。

支持 Windows AD 域连接。

3.2.4 入网流程管理

支持安装天擎客户端后入网方式。

支持注册、LDAP 账号认证、WindowsAD 域账号认证后入网方式。

支持注册、LDAP 账号认证、WindowsAD 域账号认证并安装天擎客户端后入网方式。

3.2.5 访问控制列表

支持将网络划分为三个区域（保护区、可信区、非法区）灵活的限制区域间的数据的流动。

3.2.6 ARP 准入

支持 ARP 欺骗方式实现网络准入。

支持网络终端扫描功能。

新 3.2.7 802.1x

支持 360 自主研发的 PC 端 802.1x 客户端。

支持针对 PC 终端进行 802.1x 认证入网合规性检查。

支持合规性检查的策略自定义（普通检查项、关键检查项）。

支持根据管理员的策略自定义给予用户认证成功后的打分功能。

支持 PC 端 802.1X 认证后的日志记录功能，同时记录通过认证的交换机端口。

支持用户进行 802.1X 认证账户自主注册。

3.2.8 设备管理

支持展示交换机的基本状态信息，如接口列表、端口状态、端口类型、端口所属 VLAN、端口 dot1x 状态。

3.3 用户管理

3.3.1 认证用户管理

支持本地 LDAP 用户的添加删除修改。

支持第三方 LDAP 用户数据的查看。

3.3.2 注册用户管理

支持手动确认用户注册。

支持自动确认用户注册。

支持取消用户注册。

3.3.3 在线用户管理

支持在线用户名、用户 IP、用户 MAC 地址与用户最近检测时间查看。

3.3.4 用户终端扫描

支持跨路由器扫描在线 PC。

3.4 策略管理

3.4.1 策略配置

支持针对 PC 终端的远程桌面、文件共享、特定软件、特定进程等功能的状态（启用或禁用）进行准入控制。

3.5 系统管理

3.5.1 系统配置

支持密码修改。

支持系统时间查看修改。

3.5.2 接口管理

支持接口 IP、MAC、类型、启用状态、连接状态查看。

支持接口 IP 地址修改。

支持接口状态、类型修改。

3.5.3 路由管理

支持路由信息的添加与删除。

3.5.4 服务管理

支持系统服务器的停止、启动与重启

3.5.5 软件升级

支持页面操作方式升级 360 网络安全准入内核。

3.5.6 天擎联动

支持针对天擎联动，完成对用户终端的全方位保护。

3.6 系统日志

系统日志包括违规访问日志、心跳日志、认证日志三大类。

3.6.1 违规访问

支持违规访问的四元组信息、访问时间的查看、查询与删除。

3.6.2 心跳日志

支持心跳日志记录查询与删除

3.6.3 认证日志

支持本地 LDAP、第三方 LDAP、Windows AD 域认证记录查询与删除。

3.6.4 802.1x 认证日志

支持 802.1x 成功或失败认证记录的查询与删除。

第四章 产品优势与特点

- 基于标准旁路部署，对用户网络没有任何影响
- 基于自有旁路重定向技术，方便自动分发
- 支持第三方 LDAP 和 AD 域认证。
- 和 360 天擎无缝融合，提供天擎网络准入功能。
- 阻断策略配置灵活，可以满足多种场景。
- 支持无客户端准入方式。

第五章 产品性能指标

5.1 测试简介

测试目的在于对 360NAC 进行压力性能测试结果分析，评估出 360NAC 的整体性能。主要测试 360NAC 镜像接口的抓包能力，分别测试单接口以及整机的抓包性能

5.2 被测设备硬件配置

型号	360NAC-5130	360NAC-3130	360NAC-1130
主板	NSA5130(高)	NSA3130(中)	NSA1130(低)
CPU	I7 2600*1	G850*1	D525
内存	8G(DDR3 4G*2)	4G(DDR3 2G*2)	2G(DDR3 2G*1)
CF 卡	1G*1	1G*1	1G*1
硬盘	500GB	500GB	500GB
接口	4 光 6 电	2 光 6 电	5 电

5.3 360NAC 抓包性能指标

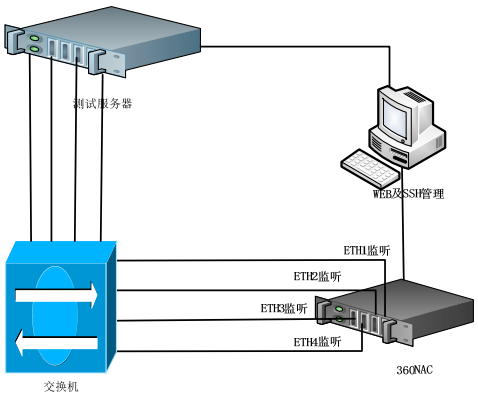


图 1 性能测试拓扑图

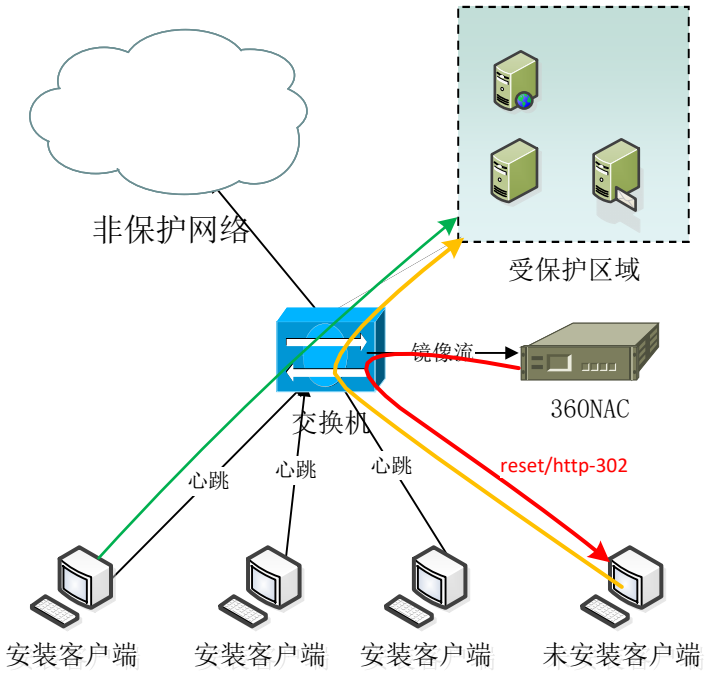
平台	抓包能力(bps)
5130	5G
3130	2G
1130	600M

第六章 产品应用部署

6.1 360NAC 解决方案

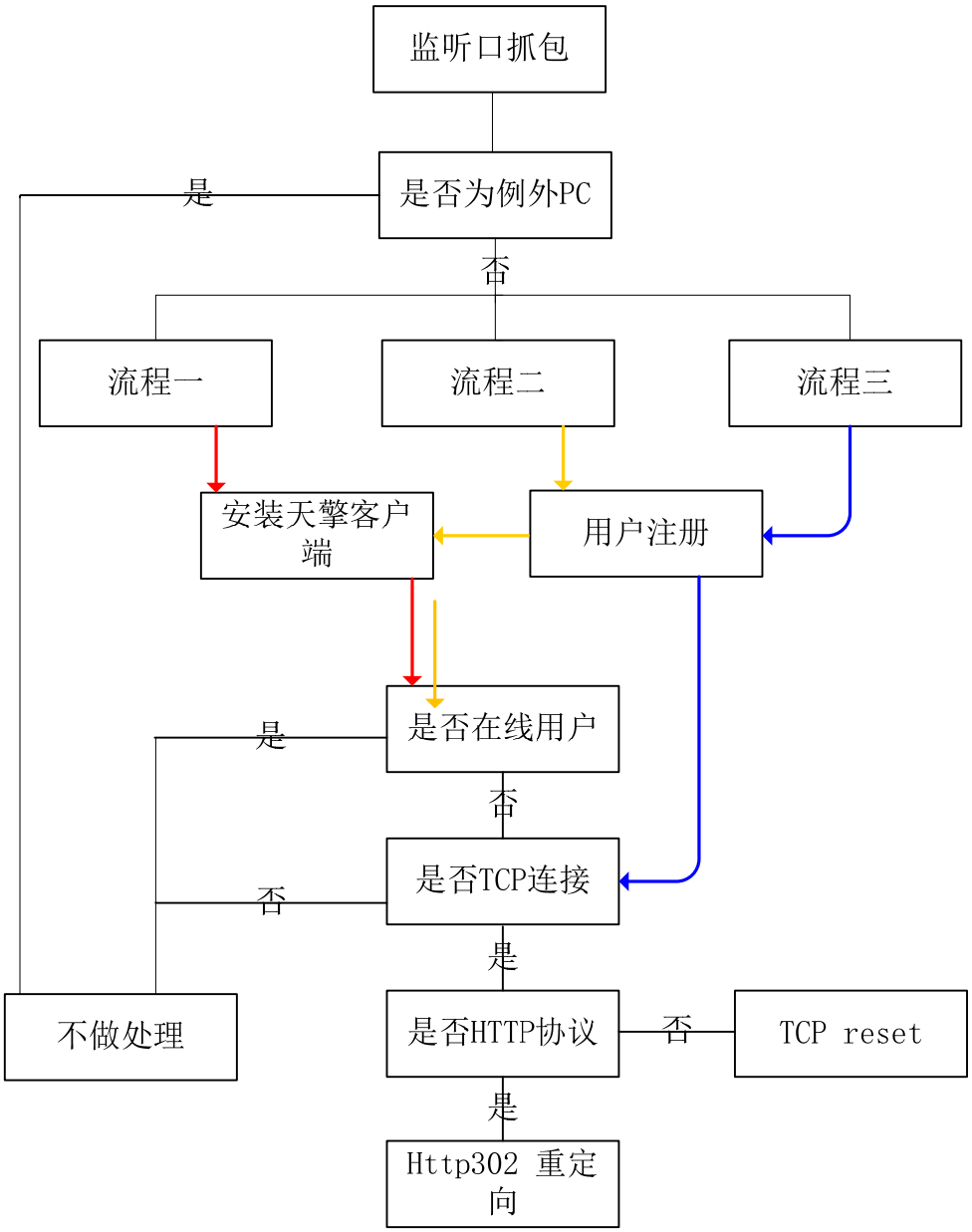
6.1.1 部署拓扑

当前解决方案是着眼于国税项目，使用阻断方式来干扰终端正常网络访问，来达到准入功能。其网络部署及数据流如下图：



6.2. 基本原理

6.2.1 360NAC 工作流程图



6.2.2 360NAC 工作流程图详述

6.2.2.1 360NAC 流程一部署

只有安装天擎客户端的 PC 才有权限访问受保护服务器。

1. 用户访问受保护服务器打开终端分发页面。
2. 点击链接，下载并安装天擎客户端，之后用户 PC 可正常访问受保护服务器。

6.2.2.2 360NAC 流程二部署

用户经过注册、管理员确认、下载并安装天擎客户端后才能访问受保护服务器。

1. 客户 PC 访问受保护服务器，打开注册页面，填写用户真实信息并提交。
2. 管理员确认用户注册。
3. 经管理员确认后，用户再次访问受保护服务器，打开下载天擎客户端页面，下载并安装，之后用户可正常访问受保护服务器。

6.2.2.3 360NAC 流程三部署

用注册并经管理员确认后，可直接访问受保护服务器。

1. 客户 PC 访问受保护服务器，打开注册页面，填写用户真实信息并提交。
2. 管理员确认用户组注册，之后用户可正常访问受保护服务器。