文章编号：2095-2163(2019)02-0269-02　　中图分类号：TP393.08　　文献标志码：A

浅谈网络准入管理系统解决方案

冯　明，陈　倩
（天津易通易联科技有限公司，天津 300000）

摘　要：网络准入管理系统解决方案是以网络准入为核心，确保每一台接入终端的合法性及合规性的基础上，集成了 IP 地址管理、端口可视化管理、交换机运维等于一体的多维整体解决方案。

关键词：网络准入；解决方案；入网流程

Discussion on network access management system solution

FENG Ming，CHEN Qian
（Tianjin Yitong Yilian Technology Co. Ltd.，Tianjin 300000，China）

【Abstract】The network access management system solution is based on network access，which ensures the legitimacy and compliance of each access terminal，and incorporates a multidimensional overall solution that integrates IP address management，port visualization management and switch operation and maintenance.

【Key words】Internet access；solutions；network access process

1　系统的业务需求

随着信息化进程的不断深入，安全往往是由内而外、逐层递进，如何在成功建立了资产管理运行机制的基础上，全面实现终端接入的流程化、标准化和规范化，在从终端至入网之前就确保其安全性、扩容量与可信度，从而提升网络整体安全，即已成为企业亟待探讨攻关的重要问题。本文提供的设计方案将可为用户从根本上解决终端多、信息乱、接入随意、查找困难等管理问题，并为用户构建全网终端接入全生命周期的可视、可管、可查看的 5W 审计平台。

2　系统设计方案

2.1　产品部署

如图 1 所示，在架构复杂的网络环境下，本文采取的是双机热备部署方案，分别旁路部署在总部主备核心交换机，推荐与现有网络环境无缝接合的技术方案，完全遵循在不修改现有网络结构及配置的情况下完成部署。

2.2　入网流程

产品部署后，工作人员拟将遵循的入网流程即如图 2 所示。

2.3　系统设计

（1）自动化资产统计。纯旁路部署到客户网络后，在不开启任何准入策略的情况下，即可实现全网

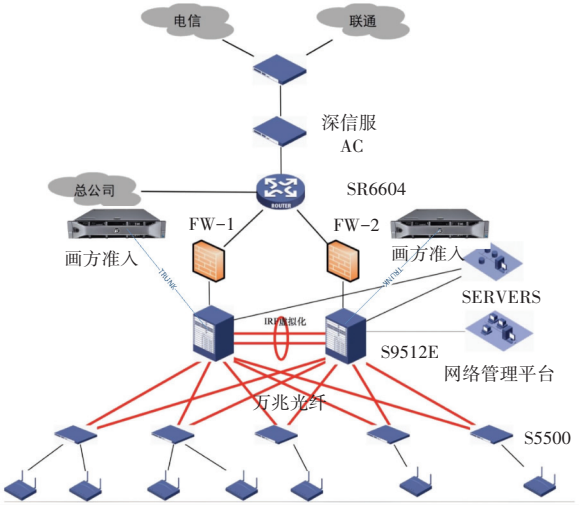

图 1　系统的整体设计架构

Fig. 1　Overall design architecture of the system

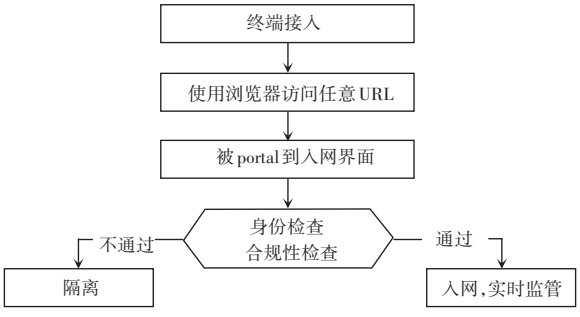

图 2　入网工作的的设计流程

Fig. 2　Design process for network access work

作者简介：冯　明（1971-），男，学士，讲师，主要研究方向：计算机设计、系统构建、大数据分析挖掘。

收稿日期：2018-11-05

资源的统计,统计信息包含:IP-MAC-VLAN-主机名-终端类型-交换机-端口-操作系统-浏览器-分辨率等等。协助用户建立全网资源统计平台,其次,协助用户自动分类网内资源的终端类型,建立全网泛终端的统一展示及管理平台。

(2)终端快速定位。通过 SNMP 简单可网管协议,建立与交换机网络设备的联动,自动创建终端与交换机端口对应关系,从而实现了终端快速定位平台。

(3)自动化用户信息搜集的管理手段。对于自动化提取的研究来说,需建立流程化、规范化、标准化的终端接入管控平台。准入是主要的技术手段,通过强制隔离,友好 portal 引导,建立实名制 ID 管理。PC(移动终端)新接入网络,默认无法与网内通信,打开 Web 页面自动 portal 引导页面,管理员可指定一次性入网登记、审批的流程,建立终端自动化台账管理,实现接入可信。其次,管理员也可定义入网终端输入用户名密码认证方式自动化接入流程,建立动态的终端接入档案,动态的人机对应关系。

(4)多元素绑定。在对信息进行自动统计的基础上,支持多元素绑定,如 IP-MAC-VLAN-主机名-交换机-端口-使用人等信息的绑定。当其中任意参数发生变化,则将其阻断,并采取强制隔离的技术手段,使得管理难度降低,并具有可视性。

(5)增值方案-网络边界威胁感知。在统计数据的基础上,可以协助用户构建网络边界威胁感知平台,自动发现、告警、定位和阻断网络内部未准入的小路由、wireless AP、便携式 WIFI 等。及时感知和定位网络内部的 IP 地址冲突、广播风暴等潜在的安全隐患,并于必要时进行主动报警。

(6)增值方案-IP 地址管理。除安全功能以外,还集成了运维方面的功能,即 IP 地址管理平台,协助用户建立 IP 地址自动统计、自动回收、自动下发的全自动平台,并且可以完全替换人工 Excel 表格的统计方式,结合准入功能,建立 IP-MAC-使用人-VLAN-交换机端口的自动登记平台,为用户提供追溯还原审计平台。

3 结束语

网络准入管理系统可为用户完美解决现有需求,为后期的发展趋势提供前瞻性解决方案。本系统采用纯旁路部署,可以在保持客户的原有网络架构以及原有配置的基础上,对系统网络不产生任何影响;具备灵活可混合式的准入技术,可以有效适应各种网络环境并且不完全依赖于网络环境;系统采用的是无客户端部署模式;拥有多级指纹绑定机制,智能鉴别仿冒终端;提供特色的终端类型识别功能,实现网络层准入管理,为用户打造智能、可视、易用的网络边界管理平台。

参考文献

[1] 史简,郭山清,谢立. 统一网络安全管理平台的研究与实现[J]. 计算机应用研究, 2006(9):92-94,97.
[2] 郭丽,杨振启. P2P 技术原理及安全性问题浅析[J]. 网络安全技术与应用, 2005(6):26-28.
[3] 谢东亮,程时端,阙喜戎. 对等网络的研究与进展[J]. 中兴通讯技术, 2005,11(2):58-60.
[4] 陈凯,银鹰,薛质. 基于"修补程序管理过程"的企业补丁管理方法[J]. 信息安全与通信保密, 2005(3):84-86.
[5] 王建忠,张忠能. 基于 802.1X 和 DHCP 控制网关的无线网络访问控制[J]. 计算机工程, 2004,30(S1):329-331.
[6] 董思良. 网络安全整体框架[J]. 信息安全与通信保密,2004(10):54-55.
[7] 胡华平,刘波,钟求喜,等. 网络安全脆弱性分析与处置系统的研究与实现[J]. 国防科技大学学报,2004,26(1):36-40.
[8] 单国栋,戴英侠,王航. 计算机漏洞分类研究[J]. 计算机工程,2002(10):3-6.