桌面安全客户端部署的检测

周　霖[1]　何　源[2]　王阳洋[3]

1.中国石油集团工程设计有限责任公司西南分公司,四川　成都　610017

2.成都大学,四川　成都　610106　3.中国石油大学(北京),北京　102200

摘要:

桌面安全系统是企业网络安全体系的重要环节，桌面安全客户端是否全面部署是衡量桌面安全系统工程质量、企业安全体系完备性的重要依据,因此,企业网络接入计算机安全客户端的检测在评估企业信息化安全等级、企业网系统运行维护中都有着重要的意义。通过对 SEP 系统架构的研究,提出了一种自动化检测的方法,能实时检测客户端部署情况,可配合与网络设备联动自动关闭存在安全隐患的端口,使用标准、安全的方式访问网络设备,不影响桌面安全系统运行,检测带来的网络负载小,提高了企业网络的安全性。检测工具的应用部署投入小,快速检测客户端部署状态效果好,可在 SEP 项目验收、网络运维中广泛应用。

关键词:

SEP;桌面安全;Expect;ARP

文献标识码:B

文章编号:1006-5539(2011)05-0085-03

0　前言

目前,中国石油集团公司部署的基于 SEP 的桌面安全系统全面投入运行,为用户桌面安全提供安全保障。但是,SEP 客户端是否部署却难以管理,没有安装桌面安全客户端的计算机极有可能对其他用户造成病毒攻击。本文提供了一种通过 MAC 地址核查的方式以快速验证接入计算机的桌面安全部署情况,为桌面安全系统提供更加有效的管理控制措施。

1　问题的提出

随着企业信息化的不断推进,在提高企业核心竞争力的同时各种信息安全威胁也随之而来。以中石油企业网络为例,就存在网络结构混乱、网络病毒泛滥,网络安全攻击不时发生、网络缺乏统一管理等诸多安全问题。网络安全永远是企业信息化建设中重要内容,而网络安全的保证总是技术措施和管理手段的结合。防病毒网关、防火墙、入侵防护系统等网管型的安全产品能有效隔离网络威胁的跨网传播,但对网内的安全管理却缺乏控制,内网主机的安全问题一直是企业网络管理人员需要持续应对的技术难点。正是出于这样原因,中国石油集团公司从总体安排、统一部署的角度出发来推广桌面安全系统,正是为了较好的解决内网安全问题。

桌面安全系统结合了 802.1x、DHCP、RADIUS AAA 认证体系以及 PKI 等多项技术及规范,涵盖了赛门铁克、微软、思科、华三等多家软硬件厂商的产品,通过各个子系统的协同工作达到管理企业网内网络终端安全的目的。任何系统的部署实施是系统得以应用的基础，特别对于桌面安全这样的 Client/Server 模式的安全系统完整部署实施是系统能全面发挥作用的基

收稿日期:
2011-07-13

作者简介:
周　霖(1974-),男,四川成都人,助理工程师,主要从事信息化建设及计算机网络管理工作。

础。企业网中任何接入网络但未安装桌面安全的终端都可能成为整体系统的安全漏洞。因此桌面安全客户端的完整性就成为评估系统部署情况、检测系统应用效果、系统运行维护手段等工作的基础。企业网中桌面安全客户端的量非常大,仅仅一个二级单位的办公网络可能就达到上千个终端,手工检查几乎无法完成,更不可能做到实时检测。自动化、快速的检查客户端安装部署情况就成为桌面安全系统部署、应用、运维的首要问题和技术难点。

2 桌面安全客户端部署情况的检测

要讨论客户端的检测首先应分析桌面安全的运行原理。我们认为桌面安全系统运行的基本原理包括如下三点[1]:

a)由桌面安全管理平台来定义、下发企业内部的安全策略,安装在接入网络的计算机的桌面安全客户端来实施计算机的安全策略;

b)由网络出口的 Enforcer 控制内网计算机的出口行为;

c)桌面安全客户端的完整性和安全策略的完备性保证内网安全。

一般来讲,安全策略的完备性在对企业网络及其应用的情况下一定可以规划出适合具体网络的、有效的安全策略规则。这些规则能通过桌面安全管理平台下发到客户端,实现安全规则,而安全客户端的完整性只能通过全面部署来实现。其实在桌面安全系统中已经包含了保证客户端安装的技术,即没有安装客户端或安装了客户端但安全标准不达标的计算机不能够通过网络出口 Enforcer。这样的安全技术实践起来简单、也比较有效,在实际应用中基本能够保证内网中使用的计算机达到安全标准。我们知道内网中只要有一台接入计算机没有安装客户端,就存在着安全漏洞,而网关型 Enforcer 并不能完全保证接入计算机安装客户端。这类计算机接入到企业网络但没有访问外部资源的需求,所以导致出口 Enforcer 不能够对其进行限制,典型的例子如用于打印和文件共享的计算机,接入企业内部无线热点(AP)计算机。因此,我们需要一种能实时检测企业内部网络接入计算机的技术手段和工具。这个系统应该满足如下要求:不影响现有桌面安全系统的运行;能快速检测全网接入计算机;能对未安装桌面安全客户端的计算机进行隔离。

要实现这样一个系统关键需要将桌面系统检测到的客户端和现在接入到网络中的客户端进行比较。我们可以通过桌面安全系统提供的 API 接口获取当前网络合法客户端的列表。而获取当前网络中接入计算机的列表可以通过两种方式:一是遍历并读取所有三层设备上的 ARP 列表;二是遍历并读取所有边缘交换机上的 MAC 列表。如果使用读取 ARP 列表的方式显然更快速,但由于 ARP 列表的记录有生存期,接入计算机列表可能不完整;而遍历边缘设备虽然可以获取完整的 MAC 列表但检测工作量比较大。我们可以采用多种方式相结合的检测方式,步骤如下:

a)通过桌面安全系统 API 获取合法用户 IP 及 MAC 列表;

b)获取三层设备上的 ARP 列表,并对 ARP 列表上的 IP 地址进行合法性检查,可获得有安全威胁的 IP 地址列表;

c)获取三层设备上的 MAC 地址列表,检测 MAC 地址的合法性,在 ARP 列表中查找有安全威胁的 MAC 地址的 IP。

这样我们可以获取一个有安全威胁的 IP-MAC 对列表,在这个表中是非法接入网络的计算机设备;同时可能获得一张 MAC 地址列表,这张列表中的 MAC 地址不在合法 MAC 列表中,但无法发现它的 IP 地址,这些 MAC 地址所对应的设备对网络存在着一定的安全威胁。

最后,我们可以通过 MAC 地址定位计算机设备的所在的交换机端口,然后根据系统配置进行下一步操作,比如关闭交换机端口、通知管理员等。

3 桌面安全客户端检测的实现

该检测系统的实现应该包括:SEP 用户读取接口程序、网络设备 ARP 及 MAC 列表获取模块、MAC 地址定位模块以及管理模块构成。SEP 用户读取接口程序可在 SEP 相关工程人员配合下应用 SEP API 实现。本文将重点讨论网络设备 ARP 及 MAC 列表获取和 MAC 地址定位。

3.1 网络拓扑结构的描述

不论是网络设备 ARP 及 MAC 列表获取还是 MAC 地址定位,先觉条件就是要清楚网络设备的拓扑结构。系统需要知道网内有那些三层设备,三层设备的每个端口下有那些边缘交换机。根据实际应用我们不需要一个完备的拓扑图描述,我们只需要如下信息,在系统运行前配置在系统中:三层设备的 IP 地址列表;每台三层设备的端口列表;每台三层设备的端口下联边缘交换机 IP 地址的对应表。

3.2 网络设备的访问方式

获取网络设备的运行参数可以通过 SNMP 方式

实现。SNMP 是一种通用标准但各个设备厂家在实现时都有细微的差别，特别是企业相关的 MIB 库结构更是千差万别，通常在使用 SNMP 的时候开发者不得不对每种设备开发不一样访问程序或配置脚本。既然 SNMP 标准并不能为程序的开发带来方便，而且软件开发时还受限 SNMP 协议本身和设备厂商 SNMP 实现方式及程度，故我们在实现网络设备访问时放弃了 SNMP，而改用模拟用户登陆的方式去访问网络设备[2~3]。

我们知道标准的网络设备总是通过 telnet 或 ssh 登录到设备，再使用 CLI 命令进行操作。我们完全通过程序模拟这一过程，在 Linux/UNIX 下早有成熟的产品 Expect[4]。Expect 使用 Tcl 作为语言核心，可以将交互方式运行的过程变成非交互的方式运行，比如 CLI 中需要输入口令时 Expect 可以自动完成这一过程。在 Linux 下 Expect 可以很好的和其他语言比如 Python、Ruby 等整合成为程序的一个部分。比如我们希望获取某台三层设备 ARP 列表，可以使用配置好的 Expect 脚本自动的、非交互完成，而 ARP 列表的处理交由其他程序来处理。

3.3　MAC 地址的定位及报警

有了完整的网络拓扑结构和设备访问方式定位一个 MAC 地址就不再困难。MAC 地址总是来自与某台三层设备，首先可以定位该 MAC 来自于哪个端口，然后在该端口下联边缘交换机上逐一查找，最后在边缘交换机上定位该 MAC 地址来自于哪个端口。需要注意的是在边缘交换机端口查找中，应该将 Trunk 端口排除在外，因为 Trunk 端口上的 MAC 地址不一定来自于这台交换机。

在将非法接入定位到相应的交换机后可以对该交换机端口进行自动关闭，也可以通过邮件短信等方式通知管理人员[5]。

3.4　系统整体架构

检测系统架构图见图 1。

我们可以如图 1 实现整个检测系统，其他管理模块实现各个模块的协同工作和查找算法，而系统管理通过 Web 方式呈现给用户[6]。

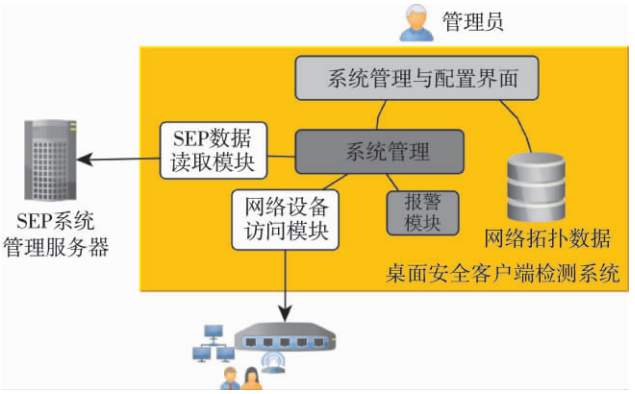

图 1　检测系统架构

4　结论

桌面安全客户端检测系统实施后不仅可以快速、主动地发现网络中非法接入的计算机和其他移动设备、第一时间给出报警信息，保护了企业的网络安全；而且还能定时检查客户机对网络及网络设备带来的负载影响，便于企业规划和分配资源。我们认为必须要采取相应的技术措施，而不是被动防护，桌面安全客户端检测系统就能较好的将安全问题第一时间检测出来，起到主动防护的效果。

参考文献：

[1] Symantec Corporation. Symantec Endpoint Protection：A unified，proactive approach to endpoint security[EB/OL]. https：//www4. symantec.com/Vrt/offer?a_id=42101，2010-09.

[2] 赫卡拜. CISCO 现场手册：Catalyst 交换机配置[M]. 北京：人民邮电出版社，2004，78-110.

[3] 王　达，杨学明. Cisco/H3C 交换机配置与管理完全手册[M]. 北京：中国水利水电出版社，2009，145-210.

[4] Don Libes. Exploring Expect：A Tcl-based Toolkit for Automating Interactive Programs[M]. Sebastopol，CA：O'Reilly Media.1994，87-106.

[5] 欧　勇. 用 Cactiez 实现对服务器和网络的监控[J]. 广西通信技术，2009，(1)：45-47.

[6] 傅和平，马　先，邓　坤. 可持续改进的信息化工作平台建设初探[J]. 天然气与石油，2010，28(6)：78-81.

NATURAL GAS AND OIL (BIMONTHLY)
Vol. 29 No. 5 Oct. 2011

KEYWORDS: Waste water treatment; Water quality; Problem analysis; Process improvement

Calculation of Convection Heat Transfer in Tubular Heating Furnace Radiation Chamber

Zhang Jin, *Dong Jun* (China Petroleum Engineering Co., Ltd. Southwest Company, Chengdu, Sichuan, 610017, China)
Guo Xiaoyan (China University of Petroleum, Qingdao, Shandong, 266555, China) **NGO, 2011, 29(5): 77–80**

ABSTRACT: Numerical simulation is conducted on convection heat transfer in cylindrical tube type furnace radiation chamber. Adopted is a jet flow model to divide the radiation chamber into such three areas as the same quality area, jet flow area and backflow area according to different conditions of smoke movement, adopted are different boundary conditions for limiting the areas, mathematically described are the three areas respectively and realized is the calculation process by using VB language programming. Taking a normal pressure furnace for example, simulation calculation is conducted on outer wall temperature of furnace tubes in the radiation chamber and adopted is the Monte-Carlo method for radiation heat transfer calculation. Outer wall temperature distribution of furnace tubes calculated through comprehensively considering radiation heat transfer and convection heat transfer is compared with that calculated through only considering radiation heat transfer, the former is more identical with theoretically inferential value.

KEYWORDS: Heating furnace; Radiation chamber; Convection heat transfer; Jet flow model

Construction of Explosion-proof Wall around Oil Depot

Xu Xiaoqin, *Zhang Jichun* (Domestic Trade Engineering Design Institute, Beijing, 100069, China)
Qin Xuan (Southwest Petroleum University, Chengdu, Sichuan, 610500, China) **NGO, 2011, 29 (5): 81–84**

ABSTRACT: It is found during oil depot expansion reconstruction that there is serious nonconformance of safe clearance between railway trunk line and the existing oil depots with relative requirements specified in Regulation on Railway Transportation Safety Protection (Decree No. 430 issued by the State Council of the People's Republic of China on December 27, 2004) and it is especially imperative to develop some corresponding effective measures in order to ensure railway transportation safety and necessary expansion reconstruction of oil depots in both sides of railway trunk lines. Researched are pool fires and explosive steam clouds formerly occurring in a certain oil depot tank lorry or oil tank farm and quantitative analysis is conducted on their risks. The analysis results show that fire and explosive accidents in oil depot tank lorry or oil tank farm will result in serious hazards on local railway transportation safety in the absence of any protective measures. Construction of an explosion-proof wall around oil depot can effectively reduce risks of such accidents on railway transportation safety. Calculation results show that a specially structured explosion-proof wall with a horizontal equivalent load of 4t/m^2 will have optimum efficacy for railway transportation safety protection, which can provide important reference for solving similar issues in future.

KEYWORDS: Oil depot; Explosion-proof wall; Risk; Solution

COMPUTER AND COMMUNICATION

Testing on Desktop Safety System Layout

Zhou Lin (China Petroleum Engineering Co., Ltd. Southwest Company, Chengdu, Sichuan, 610017, China)
He Yuan (Chengdu University, Chengdu, Sichuan, 610106, China)
Wang Yangyang (China Petroleum University, Beijing, 102200, China) **NGO, 2011, 29(5): 85–87**

ABSTRACT: Desktop safety system is an important part of enterprise network safety system and its completeness degree is an important basis of its engineering quality and enterprise safety system completeness. Therefore, testing on interlinkage of computer terminals with enterprise network system is of great significance in enterprise information safety level assessment and enterprise network system operation and maintenance. Researched is the SEP system architecture and put forward is an automatically testing method, which can real-time detect arrangement of computer terminals and automatically shut down computer terminals with potential safety hazard in cooperation and linkage of network equipment. Network equipment can be accessed by using a standard and safe way and operation of desktop safety system will not be affected, network load resulted from testing is low and enterprise network safety is improved greatly. The testing tool has such advantages as low investment and good testing efficiency and can be widely applied in SEP project acceptance check and network operation and maintenance.

KEYWORDS: SEP; Desktop safety; Expect; ARP