计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2018,27(10):291−295 [doi: 10.15888/j.cnki.csa.006566]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于黑洞路由和微信企业号的园区网访问控制系统①

夏凌云

(中国石油大学 (华东) 信息化建设处, 青岛 266580)
通讯作者: 夏凌云, E-mail: xialy@upc.edu.cn

摘　要: 黑客攻击和信息泄露对高校园区网造成了极大的网络和信息安全威胁, 在网络安全响应机制和流程中, 快速隔离和查封事故点可以极大的减小已发隐患对整个园区网络的负面影响. 基于此需求, 本文实现了一套软硬件结合的自动管理系统, 利用黑洞路由和 OSPF 路由分发机制, 以及配套的脚本服务器和身份认证系统, 实现了随时随地都能及时隔离和查封外部攻击源和内部故障点, 及时消除二次危害隐患. 同时通过 ACL 控制和 OAuth 身份认证控制, 保证了整体系统的安全性.

关键词: 黑洞路由; 微信企业号; 网管方案; 网信安全

引用格式: 夏凌云.基于黑洞路由和微信企业号的园区网访问控制系统.计算机系统应用,2018,27(10):291–295. http://www.c-s-a.org.cn/1003-3254/6566.html

Campus Network Access Control System Based on Black-Hole Routing and WeChat Enterprise Platform

XIA Ling-Yun

(Division of Information Construction, China University of Petroleum (East China), Qingdao 266580, China)

Abstract: Hackers and information disclosure have caused great network and information security threats to the campus network of colleges and universities. In the network security response mechanism and process, the rapid isolation and seizure of the accident point can greatly reduce the negative impact of the hidden risks on the entire campus network. Bearing this requirement in mind, this study has implemented a set of automatic management system by combining software and hardware. Using black-hole routing and OSPF routing distribution mechanism, and supporting script server and identity authentication system, we can isolate and seal external attack sources or internal failure point, thus promptly eliminate secondary hazards. At the same time, ACL control and OAuth authentication ensure the overall system security.

Key words: black-hole routing; WeChat enterprise platform; network management scheme; network and information security

1　前言

在“互联网+”建设和信息化建设高速发展的今天, 对网络安全管理的要求越来越高, 一方面, 国家层面日趋重视网络安全, 逐步认识到安全治理重要性, 加强了网络安全空间治理部署, 发布了《中华人民共和国网络安全法》, 并于 2017 年 6 月 1 日正式执行. 《中华人民共和国网络安全法》中对网络信息运行安全规范, 安全事件应急处理和相应法律责任做出了明确规定. 另一方面, 网络安全局势严峻, 全球化、信息化趋势下, 网络攻击事件层出不穷, 影响恶劣. 因此在网络安全事件响应机制的建立和实施方面, 为了适应新的法律要求和管理需求, 高校校园网的安全管理方面也面临着

① 收稿时间: 2018-02-25; 修改时间: 2018-03-19; 采用时间: 2018-03-21; csa 在线出版时间: 2018-09-28

新的挑战.

在高效的校园网络和信息安全管理机制中, 除了利用网络防火墙、入侵防御系统、应用防火墙等等主动防御技术外, 对安全事件的快速应急响应也是重要一环[1]. 虽然在技术上对信息系统做了重重防护, 但是还是有可能因为一些未发现的漏洞或者社会工程学等等原因造成网络或信息系统攻破并被恶意篡改, 此时如何第一时间隔离攻击源和封锁被篡改信息系统就成了安全响应的第一要务. 这种需求以往普通情况下是由网络管理员对网络防火墙进行操作来实现, 在响应要求越来越高的今天, 这种方式存在着一些问题:

1) 对管理员要求高: 一个是技术要求, 管理员需要对网络技术和当前网络架构有深入了解才能进行操作; 另外一个是岗位数量要求, 技术的高要求导致能执行响应任务的人员较少, 其他管理人员不能胜任响应任务需要;

2) 及时性难以满足: 安全事件要求 7×24 小时全天候响应, 而由于网络管理的安全性要求, 对网络的进行重新配置一般要求在网管机或者要经过多重安全机制后才能执行, 因此网络管理员接入网管系统面临着时间和空间的限制, 往往达不到快速响应的时间需求, 因此不得不随时随地现场值班, 大大加重工作负担.s

因此, 如何以最少的人员配置, 最低的技术要求达到快速安全响应的要求, 是我们一直面对和尚待解决的问题. 前期我们研究了利用路由协议和黑洞路由原理来实现快速响应安全事件, 隔离问题 IP 地址, 现在我们在此基础上, 搭建后台自动化管理系统, 解决了上述两个问题, 实现了一个简单化和快速化的安全响应方法.

2 总体方案

本方案的核心是, 通过身份认证确认管理员身份后, 系统通过交互页面接收管理员命令, 并将其转换为黑洞路由条目, 下发至网络设备的路由表中实现流量管控的目的. 所谓静态黑洞路由, 是将该路由条目的下一条地址指向一个空接口, 由此将匹配这条路由条目的网络流量导向一个类似黑洞的接口, 使它们有来无回的, 达到阻止网络访问的目的[2]. 为了避免在核心生产设备上直接操作带来的风险, 我们选择利用前一个建设周期更换下来的旧路由器作为黑洞路由器, 通过在黑洞路由器上配置相关路由和 OSPF 协议[3], 以动态路由的方式将黑洞路由发布到出口路由器或核心交换机上, 以实现黑洞路由条目在校园网络生产设备上的配置生效, 实现在校园网内部或出口上对特定 IP 地址进行访问控制的目的. 总体方案设计如图 1.

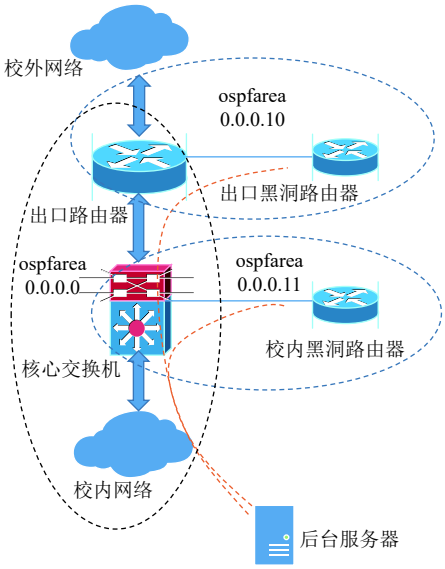

图 1 系统部署示意图

如图所示, 出口路由器为校园网络边缘路由器, 负责校园网内部和外部的路由交换, 在其上生效的黑洞路由条目可以阻止校园网络内外之间的通讯, 核心交换机为校园网内部三层交换机, 所有网络的网关可视为都在其内部, 在核心交换机上生效的黑洞路由条目可以阻断目标地址流量在企业网内部的通讯. 总体方案主要有以下特点:

1) 为了网络设施安全隔离考虑, 将整个系统分为 3 个 OSPF 区域, OSPF 0.0.0.0 区域为日常正常网络业务区, 区域内部为校园网络实际运行的正式路由表信息;

2) 出口黑洞路由器和出口路由器组成 OSPF 0.0.0.10 区域, 在出口黑洞路由器上配置的黑洞路由条目, 会被 OSPF 协议自动发布到同区域的正式出口路由器上生效, 将从外网访问目标 IP 的方位流量, 匹配发往出口黑洞路由器, 以实现隔离外网与目标地址的通讯连接;

3) 同理, OSPF 0.0.0.11 区域用于在校园网内部核心交换机的黑洞路由发布, 将所有对目标 IP 的访问流量导向校内黑洞路由器, 在核心交换机上实现对校内外所有地址对目标 IP 地址的通讯阻断.

4) 后台服务器负责下发黑洞路由配置到黑洞路由器, 并与微信企业号后台[4]对接, 实现身份认证和页面交互等等系统功能.

5) 由于黑洞路由的操作会影响整个校园网内部, 安全级别要求高, 因此两台黑洞路由器的 Telnet 服务, 均作基于源地址的 ACL 访问控制策略, 只允许后台服务器的 IP 地址登录, 以提高系统安全性, 防止非授权用户试探登录.

3 详细设计

3.1 OSPF 域配置

如整体设计所示, 除了正常校园网环境的 OSPF 0.0.0.0 区域外, 还需要分别加上 OSPF 0.0.0.10 和 0.0.0.11 区域作为黑洞路由自动分发域. 因此需要分别需要在上述四台路由器上分别配置接口地址和 OSPF 相关信息, 这里以 H3C SR6602 路由器为例介绍配置过程和命令.

1) 出口路由器相关配置如下:

interface GigabitEthernet2/0 #进入互联接口

ip address 10.10.10.1 255.255.255.252 #配置接口地址

ospf 1 #配置 ospf 进程 1

import-route static #自动导入静态路由

area 10.10.10.10 #配置 OSPF 区域

network 10.10.10.0 0.0.0.3 #指定引入 OSPF 的网络

2) 出口黑洞路由器相关配置如下:

interface GigabitEthernet0/0 #进入互联接口

ip address 10.10.10.2 255.255.255.252 #配置接口地址

ospf 1 #配置 ospf 进程 1

import-route static #自动导入静态路由

area 10.10.10.10 #配置 OSPF 区域

network 10.10.10.0 0.0.0.3 #指定引入 OSPF 的网络

3) 核心交换机相关配置如下:

interface GigabitEthernet2/0 #进入互联接口

ip address 10.10.11.1 255.255.255.252 #配置接口地址

ospf 1 #配置 ospf 进程 1

import-route static #自动导入静态路由

area 10.10.10.11 #配置 OSPF 区域

network 10.10.11.0 0.0.0.3 #指定引入 OSPF 的网络

4) 校内黑洞路由器相关配置如下:

interface GigabitEthernet0/0 #进入互联接口

ip address 10.10.11.2 255.255.255.252 #配置接口地址

ospf 1 #配置 ospf 进程 1

import-route static #自动导入静态路由

area 10.10.10.11 #配置 OSPF 区域

network 10.10.11.0 0.0.0.3 #指定引入 OSPF 的网络

按上述流程配置好各台路由器后, 在链路联通后 OSPF 区域会自动相互发现并组网, 此时可测试并发现, 在任意一台黑洞路由器配置的黑洞路由命令, “ip route-static 1.1.1.1 255.255.255.255 NULL0”, 会以 OSPF 路由的方式同步到对应的正常业务路由器的路由表中去, 在校园网运行环境中实现对某个 IP 的流量控制.

3.2 微信端认证和交互设计

在此方案中, 为在实现用户准入控制的同时提高安全性和便捷性, 我们将整个系统的认证和交互页面嵌入到微信企业号中实现, 通过在微信企业号中创建的独立子应用来自动确认用户合法性, 并让用户在微信企业号的 Html5 页面中实现交互功能. 认证和交互流程如图 2 所示.

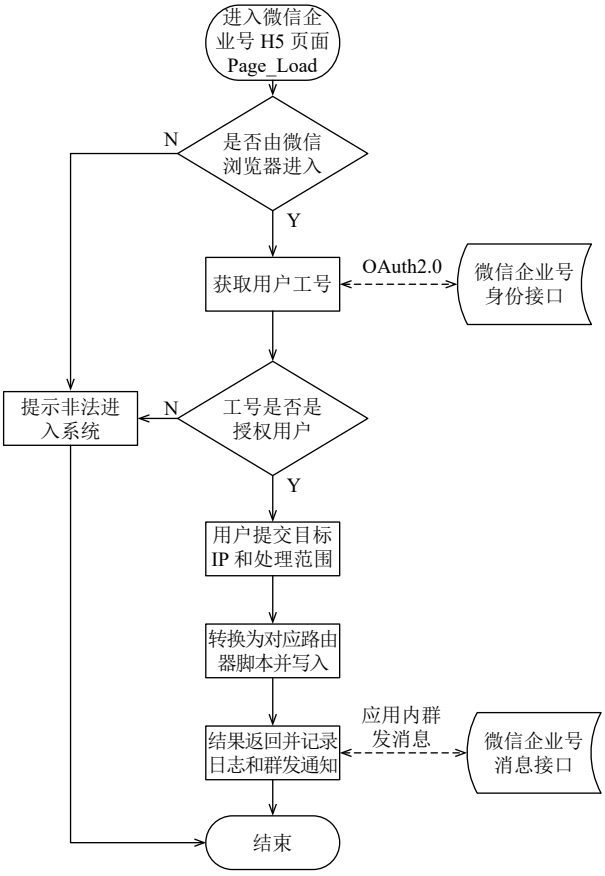

图 2 认证和交互流程

微信端交互设计主要包含以下内容和步骤:

1) 用户打开页面时, 在 Page_Load() 方法中, 自动通过调用 OAuth2.0 认证方法, 从微信企业号后台获取进入系统用户的学工号, 实现用户免密码的统一身份认证登录;

2) 根据学工号判断用户是否在已提前设置好的授权用户表中, 对非授权用户进行提示并强制退出页面等操作;

3) 授权用户在操作页面输入待控制的 IP 地址或域名, 选择封锁范围, 并进行二次确认, 以防止误操作;

4) 对用户输入进行分析、整理和判断, 并转化为需要下发的黑洞路由配置命令脚本, 下发到对应的黑洞路由器中;

5) 在日志数据库中, 对操作命令和结果进行记录, 同时通过微信企业号的群发消息功能, 实现与其它网络管理人员的消息交互;

3.3 黑洞路由下发流程实现

关于后台服务器如何连接路由器, 并下发配置命令的方式, 在 java 开发环境下[5,6], 我们选用了 apache commons-net 开源包, 使用其提供的 telnet 连接的工具类来实现脚本化的路由命令下发和保存. 同时利用 java.io.InputStreamReader 和 java.io.PrintStream 来发送脚本和接收路由器回复. 关键部分的初始化代码如下所示.

```
import org.apache.commons.net.telnet.TelnetClient;
import java.io.PrintStream;
import java.io.BufferedReader;
telnetClient = new TelnetClient(); //创建 Telnet 客户端
telnetClient.setDefaultTimeout(1000); //1 秒内未读取到服务器返回, 关闭连接
telnetClient.connect(switchIP, 23); //创建与路由器之间的 telnet 链接
//初始化发送脚本对象 printStream, 并绑定到 telnetClient 的输出;
PrintStream printStream = new PrintStream (telnetClient.getOutputStream());
//初始化接收回复对象 BufferedReader, 并绑定到 telnetClient 的输入;
BufferedReader bufferedreader = new BufferedReader (new InputStreamReader (telnetClient.getInputStream(), "UTF-8"));
```

初始化上述关键对象后, 即可通过 printStream.println() 方法向路由器逐行输出预订脚本, 通过 bufferedreader.read() 方法读取路由器返回信息, 用于判断脚本是否运行成功. 已我校现有的 H3C6602 路由器为例, 一般来说, 需要发送的路由器命令脚本如下:

```
RouterPassword #发送路由器密码
system-view #进入系统设置视图
ip route-static x.x.x.x 255.255.255.255 NULL0 #发布 IP(x.x.x.x) 的黑洞路由
save #保存系统设置
Y #确认保存系统设置
quit #退出
```

需要注意的是, 为了保证命令顺利执行, 避免意外情况发生, 系统应该在每条命令脚本执行后调用 bufferedreader.read() 方法来检查路由器回复是否与预期返回符合, 并做出相应的错误判断和重试. 成功执行完所有脚本后, 还需调用 telnetClient.disconnect() 方法断开服务器与黑洞路由器之间的连接.

4 结束语

按以上设计方案部署的系统已正式上线运行一段时间, 具有以下的优点: 1) 安全性高, 通过源地址访问限制、OAuth2.0 统一身份认证和企业号权限控制功能, 多层次保障了系统安全性; 2) 使用方便, 原来手工封锁 IP 的方式, 操作复杂, 仅熟悉路由器配置的专业网络管理员才具备操作能力, 而现在的系统提供了一种简便的交互方式, 使普通的值班人员也能进行有效操作; 3) 反应迅速, 以往的手工方式需要在网管机上登陆路由器, 再手动输入多条配置命令, 需要较长的响应时间, 现在的系统对人员所在位置没有要求, 只需使用进入微信, 点击进入我校的企业号应用, 设置好封锁 IP 地址, 确定运行即可, 大部分操作有后台自动完成, 使响应人员摆脱了时间和空间的束缚, 能够快速响应网络威胁. 下一步可以考虑将 Telnet 协议升级为 SSH 协议, 实现加密连接, 提高安全性, 并优化后台管理和日志记录功能, 并在使用中不断总结经验, 改善系统细节.

参考文献

1 黄瑞, 邹霞, 黄艳. 高校信息化建设进程中信息安全问题成

因及对策探析. 现代教育技术, 2014, 24(3): 57–63.
2 龚文涛, 郎颖莹. 静态黑洞路由网络架构在校园网应用的配置方案. 计算机系统应用, 2018, 27(1): 235–238.
3 潘楠, 王勇, 陶晓玲. 基于 OSPF 协议的网络拓扑发现算法. 计算机工程与设计, 2011, 32(5): 1550–1553, 1567.
4 杨树春, 辛云飞, 王义, 等. 基于微信企业号的高校移动平台设计与实现. 华中科技大学学报 (自然科学版), 2016, 44(S1): 158–161.
5 Java 虚拟机规范. http://java.sun.com/docs/books/jvms/second_edition/html/VMSpecTOC.doc.html.
6 欧锋, 邹敏, 李晓桢. Java 技术框架概述. 计算机系统应用, 2012, 21(8): 236–239.