计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2018,27(1):235−238 [doi: 10.15888/j.cnki.csa.006087]

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

静态黑洞路由网络架构在校园网应用的配置方案①

龚文涛[1], 郎颖莹[2]

[1](中国石油大学 (华东) 信息化建设处, 青岛 266580)
[2](中国石油大学 (华东) 教育发展中心, 青岛 266580)

摘　要: 路由协议是 TCP/IP 协议族中重要成员之一, 包含内部网络协议和外部网络协议, 高校常见的网络协议是静态路由及 OSPF 路由. 本文分析和总结 OSPF 协议及静态路由相关概念, 针对高校网络安全管理工作需求, 引入静态黑洞路由来主动查封部分网络服务. 基于此, 本文将黑洞路由网络架构引入到校园网的安全管理中, 给出核心网络架构及具体的配置流程, 借助黑洞路由能第一时间快速查封事故点降低二次危害, 并降低其对整个校园网络的负面影响, 最终通过网络测试其黑洞路由配置的有效性.

关键词: 静态; 黑洞; 网络; 架构; 方案

引用格式: 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. http://www.c-s-a.org.cn/1003-3254/6087.html

Configuration Scheme of Static Black Hole Routing Network Architecture Applying in Campus Network

GONG Wen-Tao[1], LANG Ying-Ying[2]

[1](Information Construction Department, China University of Petroleum (East China), Qingdao 266580, China)
[2](Education Development Center, China University of Petroleum (East China), Qingdao 266580, China)

Abstract: The routing protocol is one of the important members of the TCP/IP protocol family, which contains the internal and external network protocol. The common network protocol in college is static routing and OSPF routing. This paper analyzes and summarizes the related theories of OSPF protocol and static routing, and initiatively closes down the network services by introducing the origin of the static black hole road according to the demand of campus network security management. Based on this, the paper introduces the black hole routing network architecture into the security management of campus network, and gives the network architecture of the core and the specific configuration process. With the aid of black hole, the routing can quickly close down the accident point to prevent more hazards, and reduces the negative impact on the entire campus network. Eventually, through the network the validity of the black hole routing configuration is tested.

Key words: static; black hole; network; architectures; scheme

路由协议是 TCP/IP 协议族中重要成员之一[1,2], 其选路过程实现的效率高低会直接影响到整个 Internet 网络的工作效率. 按照路由协议应用范围的不同, 路由协议主要分为两种: 内部网络协议 (interior gateway protocol) 和外部网关协议 (exterior gateway protocol).

常见的内部网络协议包括: RIP-1, RIP-2, IGRP, IS-IS 和 OSPF. 其中前 3 种路由协议均是采用距离向量算法, IS-IS 和 OSPF 采用的是链路状态算法; 外部网关协议是 EGP(Exterior Gateway Protocol), 是为一个简单的树形拓扑结构设计的, 适用于树状拓扑的网络[3,4].

① 收稿时间: 2017-02-24; 修改时间: 2017-03-16; 采用时间: 2017-03-29; csa 在线出版时间: 2017-12-22

路由协议通过在互联网中的路由器之间共享路由信息来支持可路由协[5,6]. 路由信息在互联网中相邻的路由器之间传递, 以此来保证所有路由器知道到其它路由器的路径信息, 依托路由协议来构建路由表, 以路由表描述网络拓扑结构; 路由协议与路由器协同工作, 执行路由选择和数据包转发功能. 路由协议主要运行于路由器上, 路由协议是用来确定到达路径的, 常见的路由协议包括 RIP, OSPF, IS-IS, BGP 等协议.

路由协议主要是为网络信息节点上网所用, 但是有一种情况是需要主动断开网络服务, 结合高校的网络信息安全工作来说, 出现下面两种情况, 需要主动断开网络信息服务: 一是网络攻击针对某个 IP 或者 IP 段, 会引发一定区域内的网络震荡, 导致网络瘫痪; 二是或者个别服务器被黑客攻击后, 需要及时断开其网络服务, 则需要通过主动干预方法来降低其二次网络安全事故带来的不利影响. 针对此, 需要在路由协议层面对其进行处理, 使得其不够上网, 而静态路由协议里面的黑洞路由可以用来处理非常时期的突发网络安全事件, 本文分析和总结静态路由和静态黑洞路由相关概念, 提出一种基于高校网络信息安全空间领域下的黑洞路由器配置, 给出核心网络架构及配置流程, 最终通过网络测试黑洞路由配置的有效性.

1 静态路由与黑洞路由概述

1.1 静态黑洞路由概念及功效分析

静态路由是由用户或者网络管理员人工配置的路由信息, 当网络局部的拓扑结构或者网络链路状态发生变更之后, 网络管理员则需要人工手动去修改路由表中的相关静态路由数据. 静态路由比较适应于小规模、架构简单的网络拓中, 网络管理员容易掌握网络拓扑架构, 较方便配置正确的静态路由策略.

静态黑洞路由是静态路由的一种, 所谓静态黑洞路由, 是将所有无关路由吸入其中, 使它们有来无回的路由. 黑洞路由, 其实就是一条特殊的静态路由, 下一跳指向 null0 口, 一个不存在的口, 结果就是将匹配这条路由的数据包丢弃. 提到黑洞路由就要提一下 null0 接口. null0 口是个永不 down 的口, 一般用于管理, admin 建立一个路由条目, 将接到的某个源地址转向 null0 接口, 这样对系统负载影响非常小.

黑洞路由功效: 如果同样的功能用 ACL(地址访问控制列表) 实现, 则流量增大时 CPU 利用率会明显增加. 所以, 设置黑洞路由一直是解决固定 DOS 攻击的最好办法. 相当于洪水来临时, 在洪水途经的路上附近挖一个不见底的巨大深坑, 然后将洪水引入其中. 黑洞路由最大的好处是充分利用了路由器的包转发能力, 对系统负载影响非常小.

1.2 常见路由协议优先级分析

常见的路由协议以 H3C 公司研发的网络架构下的路由优先级来说: Direct 直连路由的优先级是 0, 级别最高; ospf 路由的优先级是 10; is-is 路由的优先级是 15; static 静态路由优先级是 60; rip 路由优先级是 100, 需要对静态路由进行配置, 如果黑洞路由器上面的黑洞静态路由优先级是 60.

默认前提下, 如果是 OSPF 路由, 则其优先级静态路由要高, 则默认配置优先级别为 60 即可; 但是如果该目标 ip 地址在他区域也是配置的静态路, 则在黑洞路由器上配置的静态黑洞路由优先级要高于该 ip 地址的静态路由优先级, 否则其发布路由后, 会导致黑洞路由配置无效. 在静态黑洞路由配置完成后, 需要对其路由信息进行测试, 以确保黑洞路由确实起作用.

1.3 网络安全管理引入黑洞路由的意义和作用

伴随网络安全局势日益严峻, 国内外黑客对高校的攻击呈现出攻击范围广、攻击频率高的趋势, 如何有效阻隔和及时处理被黑客攻击成功之后的网络故障点对提升网络安全管理工作水平有着重要意义和作用.

当高校的网络安全事件发生或者要主动查封安全故障点的时, 通过黑洞路由的配置, 能够快速将故障点查封, 并减少对整个网络的负面影响, 当黑洞路由配置完毕之后, 当去往某一目的地的静态路由具有“blackhole”属性时, 无论配置的下一跳地址是什么, 该路由的出接口均为 NULL 0 接口, 任何去往该目的地的 IP 报文都将被丢弃, 并且不通知源主机.

综上所述, 从校园网络安全管理角度来看, 配置黑洞路由是一种非常有效的网络安全防御策略, 当网络管理员获悉网络遭受内外攻击之后, 查明攻击目的地址, 则可以通过配置黑洞路由的方法来丢弃去往目的地址的报文数据, 使得被配置黑洞路由的网络主机无法上网, 无法主动访问外网或者被动被外网访问, 达到一种网络安全防护目的.

2 静态黑洞路由校园网应用架构方案设计

2.1 基于静态黑洞路由的网络架构设计

基于静态黑洞路由的网络架构如图 1 所示, 在核心架构中, 主要包括学校核心路由器和黑洞路由器, 配

置的核心流程需要对其 Vlan 来配置端口绑定, 配置接口 IP 地址, 配置对接的 OSPF 协议, 配置路由信息等.

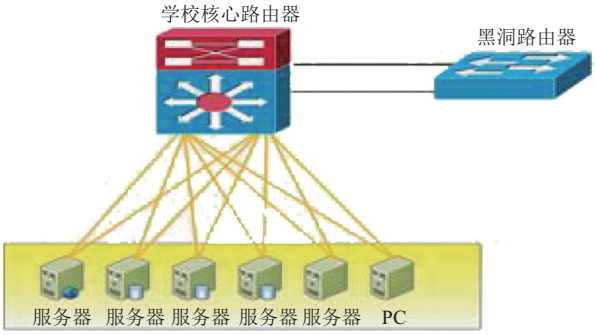

图 1 黑洞路由器架构图

基于静态路由网络架构需要配置黑洞路由器一台, 单模前兆光纤两对, 单模前兆模块 2 对. 需要配置的路由协议: 学校核心路由器配置路由协议是 OSPF, 而黑洞路由器, 则需要在接口 Vlan 配置 OSPF 协议基础上, 还需要配置其默认静态路由指向学校核心路由器.

2.2 静态核心路由器中校园网络核心配置计

学校核心路由器网络配置要点, 是要将核心路由器的网络与黑洞路由器网络互联互通, 并且能够及时将黑洞路由器上面的路由及时学习并且发布, 这样达到黑洞路由查封网络服务目的. 学校核心路由器与黑洞路由器接口地址要用自动学习能力性强, 不需要人工干预的 OSPF 路由, 并且将其添加到核心的 OSPF 域里, 接口链路要求捆绑, 达到链路冗余备份的要求.

需要配置核心的直连 Vlan, 配置接口 IP 地址, 并且将其添加到核心的 OSPF 域里, 为其 Vlan 配置专用的链路和接口, 在接口上面配置 Vlan 信息, 有时候, 需要配置强制前兆, 如果是对应的接口类型不一致, 需要通过强制千兆将光纤链路打通.

具体的配置如下所示, 构建编号为 2034 的专用 Vlan, 并且配置其接口地址.

学校核心路由器 Vlan 及 ip 地址配置如下:

```
interface Vlan-interface2034
 description ToSecRouter
 ip address 192.168.10.129 255.255.255.252
```

学校核心路由器链路捆绑配置如下:

```
interface Bridge-Aggregation90
 description ToSecRouter
 port access vlan 2034
```

学校核心路由器链路一号端口配置如下:

```
interface Ten-GigabitEthernet2/5/0/1
 port link-mode bridge
 description ToSecRouter
 port access vlan 2034
 speed 1000
 duplex full
 port link-aggregation group 90
```

学校核心路由器 OSPF 协议配置如下:

```
ospf 1
 default-route-advertise always
 import-route direct
 import-route static
 area 0.0.0.0
  network 192.168.10.128 0.0.0.3
```

2.3 黑洞路由器网络设计思路分析

在黑洞路由器配置核心流程是配置专用的 Vlan, 编号为 2034, 对应于核心路由器的专用 Vlan, 并且与之配置同一个网段的 IP 接口地址, 配置其专用的端口、专用链路, 配置默认静态路由, 指向学校核心路由器, 其他需要配置的则是将其 IP 地址、端口 Vlan 及链路信息进行配置, 对其黑洞路由进行配置, 出于网络安全管理需求, 还需要配置访问控制列表以确定其网络管理人员的登录管理, 黑洞路由器 Vlan 及 IP 地址配置如下:

```
interface Vlan-interface2034
 description ToSecRouter
 ip address 192.168.10.130 255.255.255.252
```

黑洞路由器访问控制列表配置:

```
acl number 2000
 rule 0 permit source 192.168.20.0 0.0.0.7
 rule 1 permit source 10.10.10.0 0.0.0.31
```

黑洞路由器路由接口配置:

```
interface Route-Aggregation21
 description Connect-To-Core
 ip address 192.168.10.130 255.255.255.252
```

黑洞路由器一号及二号端口配置如下:

```
interface GigabitEthernet0/0
 combo enable fiber
 port link-aggregation group 21
```

黑洞路由器 OSPF 路由信息配置如下:

```
ospf 1
  import-route direct
  import-route static
  area 0.0.0.0
    network 192.168.10.128 0.0.0.3
```

黑洞路由器默认静态路由配置:

```
ip route-static 0.0.0.0 0.0.0.0 192.168.10.129
```

以需要配置黑洞路由的 IP 地址 172.19.253.197 为例, 配置静态路由脚本如下:

```
ip route-static 172.19.253.197 32 null0
```

2.4 黑洞路由处理网络事故案例

黑洞路由测试案例: 在正常情况下, 网络可达某台主机, 其 IP 地址为 172.19.253.197, 配置黑洞路由之前, tracert 测试如下:

```
C:\Python27> tracert 172.19.253.197
通过最多 30 个跃点跟踪到 172.19.253.197 的路由
  1    <1 毫秒    1 ms    <1 毫秒 211.87.191.30
  2    2 ms    2 ms    <1 毫秒 172.16.0.17
  3    <1 毫秒    <1 毫秒    <1 毫秒 172.19.253.197.
```

此时, 假设 172.19.253.197 被人攻击并产生极坏影响, 需要第一时间查封其网络, 则需要登录黑洞路由器里并配置黑洞路由策略如下:

```
ip route-static 172.19.253.197 32 null0
```

此时, 在普通的 pc 机器上 tracert 已经查询不到.

```
C:\Python27> tracert 172.19.253.197
通过最多 30 个跃点跟踪到 172.19.253.197 的路由
  1    <1 毫秒    <1 毫秒    <1 毫秒 211.87.191.30
  2    34 ms    <1 毫秒    <1 毫秒 172.16.0.17
  3    *    *    *    请求超时.
```

通过测试案例说明, 在黑洞路由查看路由信息, 已经指向 null0 接口, 并且无法访问到有网络安全隐患的 IP 地址, 说明黑洞路由已经起作用. 这也是验证了当有校园网络安全事故发生之后, 通过本文提出的静态黑洞路由网络架构黑洞路由及时处理, 第一时间能够查封故障点, 进而有效降低网络安全事故的二次危害.

3 总结

本文分析静态路由概念、重点就作为静态路由之一的黑洞路由的概念及作用做了研究与总结, 分析黑洞路由的起源和黑洞路由的配置运行机理, 分析和总结常见路由协议的优先级, 并且从网络安全管理角度分析高校网络管理中引入黑洞路由的意义和作用, 总结黑洞路由架构与学校核心路由器的架构设计, 给出核心路由器与黑洞路由器的核心流程与配置, 最终给出解决黑洞路由器与学校核心路由器的具体配置方案, 进行黑洞路由配置测试.

参考文献

1 Park J, Sandhu R. The UCONABC usage control model. ACM Transactions on Information and System Security, 2004, 7(1): 128–174. [doi: 10.1145/984334]

2 赵冶东, 张东亮, 李渊, 等. 路由交换技术. 北京: 清华大学出版社, 2012: 51–55.

3 唐伟, 郭伟. 无线传感器网络中的最大生命期基因路由算法. 软件学报, 2010, 21(7): 1646–1656.

4 Hill B. Cisco 完全手册. 肖国尊, 贾蕾, 译. 北京: 电子工业出版社, 2002: 33–37.

5 李诚, 李华伟. 网络处理器中处理单元的设计与实现. 计算机工程, 2007, 33(2): 252–254.

6 Comer DE. 网络处理器与网络系统设计. 张建忠, 陶智华译. 北京: 机械工业出版社, 2004: 5–15.