第39卷 第2期 《新疆师范大学学报》(自然科学版) Vol.39,No.2
2020年12月 Journal of Xinjiang Normal University Dec.2020
(Natural Sciences Edition)

基于防火墙的园区网设计与仿真

杨 礼[1],刘 静[1],古丽孜热·艾尼外[2]
(1.喀什大学 计算机科学与技术学院,新疆 喀什 844000;2.伊犁师范大学 电子与信息工程学院,新疆 伊宁 835000)

摘 要:防火墙是构建园区网的重要设备之一,用于实现园区网的内外网的安全访问和隔离。借助华为eNSP模拟器搭建网络拓扑,我们设计了一种基于防火墙安全策略的园区网的实验方案。文章给出了实验配置过程,对实验进行测试,并给出了正确的测试结果。仿真结果表明该方案实现了防火墙在网络中的安全访问控制的要求,为园区网的设计提供相关参考。

关键词:防火墙;园区网;网络结构;eNSP
中图分类号:TP393 **文献标识码:**A **文章编号:**1008-9659(2020)02-0006-07
DOI:10.14100/j.cnki.1008-9659.2020.02.002

随着信息科学技术的发展,网络安全越来越被人们重视。在园区网建设过程中,防火墙设备在网络部署中发挥重要的作用,可以提高网络访问的安全性。网络结构关系到网络的可靠性、网络维护与管理等。关于防火墙在组网中的应用方面,唐灯平等人利用GNS3平台设计了在校园网的内网和外网之间部署防火墙的仿真实验[1];孟祥成给出了一个通过使用防火墙技术实现总公司与Internet的互联的工程案例[2];温贺平提出一种安全园区网模型,在接入层和核心层配置聚合链路实现内网负载均衡,通过对防火墙进行安全区域的划分实现内外网的安全访问[3]。在网络结构的设计上,谭志勇等人采用多生成树和虚拟路由冗余协议对园区网进行网络冗余设计[4];张梁斌等人给出了一种只有核心层和接入层的"扁平化"网络结构[5];唐灯平采用三层网络结构组建了一个大型单核心网络[6]。

企业网络仿真平台(Enterprise Network Simulation Platform,eNSP)是一款由华为提供的免费的网络仿真平台[7],支持图形化操作,具备高度仿真的特点。eNSP模拟器作为国产化网络设备的模拟软件,深受网络技术人员的喜爱。文章借助eNSP模拟器设计了一个基于三层结构的园区网实验,实现了内网的链路冗余和负载均衡,通过配置防火墙技术满足了内网与外网之间的安全隔离的要求。

1 组网技术

1.1 防火墙技术

防火墙技术是一种网络安全技术,用于把某个机构的安全和不安全的网络进行隔离[1]。防火墙是一个位于计算机和它所连接的网络之间的软件或硬件,是一种高级访问控制设备,用于不同网络安全域之间,通过相关的安全策略来控制进出网络的访问行为,目的是防止外部网络用户未经授权的访问[2]。防火墙具有访问控制、地址转换、网络环境支持、入侵检测和攻击防御等功能。

1.2 MSTP协议

多生成树协议[4](Multiple Spanning Tree Protocol,MSTP)把一个有环的网络进行修剪使之成为一个无环的树型结构的网络,避免报文在有环的网络中增生和无限次地循环。该协议不仅提供了数据转发的冗余链路,同时实现了在数据转发过程中的VLAN数据的负载均衡[8]。通过MSTP协议建立虚拟局域网(Virtual Lo-

[收稿日期] 2020-05-05
[基金项目] 新疆维吾尔自治区普通高校教育教学研究和改革项目(2018JGKD04)资助。
[作者简介] 杨 礼(1983-),男,山东日照人,硕士研究生,讲师,主要从事网络技术、高级计算机网络研究。

cal Area Network,VLAN)与生成树实例的映射关系,将多个VLAN捆绑到一个实例中,以节省通信开销和资源占用率。

1.3　VRRP协议

虚拟路由冗余协议[9](Virtual Router Redundancy Protocol,VRRP)也称为备份路由协议,是一种选择协议,它可以把一个虚拟路由器的责任动态分配到局域网中的一台VRRP路由器上。通常情况下,在VLAN中的每一台主机中会设置缺省路由,缺省路由器发生故障或端口关闭会导致内部主机将无法与外部通信。如果配置了VRRP协议,备份路由器将被启用,从而保持网络的连通。在组建网络时,通常把VRRP与MSTP两者结合起来使用。

1.4　DHCP技术

动态主机配置协议[10](Dynamic Host Configuration Protocol,DHCP)是一个局域网内的协议,为VLAN中的客户机提供IP地址、网关地址、DNS服务器的地址等信息,可有效地提升地址的使用率。客户机通过登录服务器自动获取IP地址和子网掩码。

1.5　NAT技术

网络地址转换[11](Network Address Translation,NAT)实现私有IP地址与公有IP地址之间的转换关系[12],该技术把内网主机的私有IP地址和端口号映射为公网IP地址和端口号,从而实现内网与外网的互通,同时还可以隐藏内部网络的结构,增强网络的安全性。

2　组网设计

在eNSP模拟器中经过设备的选择和连线,构建如图1所示的网络结构。实验以防火墙为中心,部署安全访问策略,在USG5500型防火墙上划分3个安全区域,分别为:Trust、Untrust和DMZ。其中内网接入Trust区域,包含的网络设备主要由SW1~SW5、PC1~PC4组成。外网接入Untrust区域,由AR1模拟外网;服务器接入DMZ区域,由SW6连接到服务器。在园区网的内部设计中,采用典型的三层网络结构,整合VRRP和MSTP协议实现网络冗余备份和负载均衡,使用DHCP方式使得内网用户动态获取IP地址,从而实现了内网终端用户的网络需求。

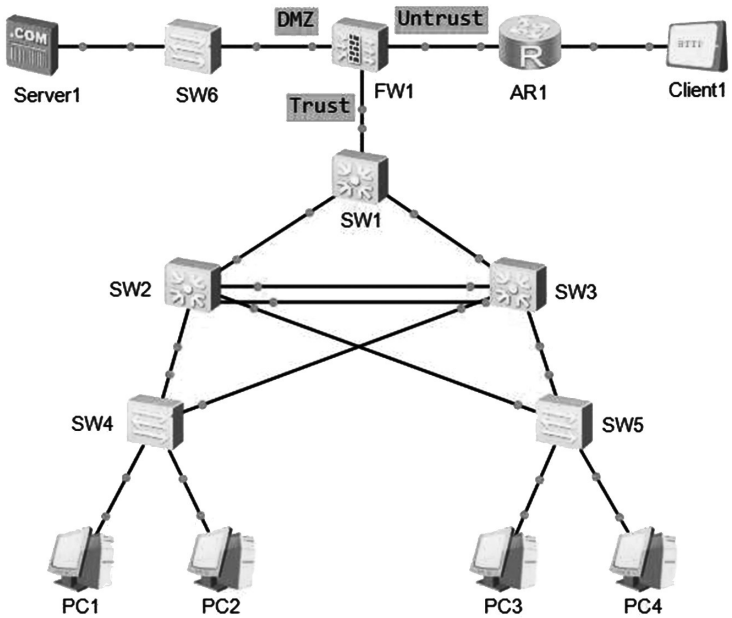

图1　园区网实验拓扑结构

3　实验环境构建

3.1　网络逻辑规划

根据实验的网络结构设计和实验要求,防火墙FW1的3个端口GE0/0/1~3分别接入Untrust、Trust和DMZ的安全区域。Trust区域为内网,在SW4和SW5上划分VLAN,内网可以访问Untrust区域和DMZ区域。SW2

与SW3之间的链路配置Eth-Trunk模式,SW2与SW4、SW5之间的链路配置Trunk模式。由于交换机接口不允许配置IP地址,SW1与SW2、SW3之间通过Vlanif接口的方式进行连接。在路由配置上,通过使用OSPF和默认路由连接不同的网段,实现网络连通。

在IP地址规划方面,FW1的GE 0/0/1端口的公网IP地址为200.100.1.1/24,同时作为内网访问外网的NAT地址池,DMZ区域的服务器的NAT地址映射的公网IP地址为200.100.1.3/24。Trust区域使用私有IP地址,其中VLAN2和VLAN3使用的网段分别为192.168.2.0/24和192.168.3.0/24,核心层与汇聚层使用的网段为10.1.18.0/30、10.1.19.0/30、10.1.20.0/30。DMZ区域使用的私有网段地址为172.16.1.0/24。文章的仿真实验中,三个关键设备的IP地址规划详见表1。

表1 设备端口IP地址规划表

设备	端口	IP地址
防火墙FW1	GE 0/0/1	200.100.1.1/24
	GE 0/0/2	10.1.20.2/30
	GE 0/0/3	172.16.1.1/24
核心交换机SW1	GE 0/0/1	10.1.19.2/30
	GE 0/0/2	10.1.18.2/30
	GE 0/0/3	10.1.20.1/30
	GE 0/0/24	10.1.19.1/30
汇聚交换机SW2	VLAN2	192.168.2.250/24
	VLAN3	192.168.3.251/24

3.2 实验仿真过程

3.2.1 VLAN配置

以SW4的配置为例,在接入层设备创建VLAN2、VLAN3,配置Access端口。配置边缘端口,有利于数据快速转发,配置如下:

```
vlan batch 2 3
interface GigabitEthernet0/0/1
port link-type access
port default vlan 2
stp edged-port enable
interface GigabitEthernet0/0/2
port link-type access
port default vlan 2
stp edged-port enable
```

3.2.2 MSTP配置

以SW2为例,配置MSTP协议消除网络中的环路。设置SW2是实例1中的主根桥,是实例2的备份根桥,实例1允许VLAN2通过,实例2允许VLAN3通过,配置如下:

```
stp mode mstp
stp instance 1 root primary
stp instance 2 root secondary
stp region-configuration
region-name RA
revision-level 1
instance 1 vlan 2
instance 2 vlan 3
active region-configuration
```

3.2.3　VRRP配置

以SW2为例配置VRRP协议,监测上行端口的拥塞情况,一旦拥塞优先级降低30,VRRP备份2组(vrid 2)作为Master设备,优先级设为120(默认为100),采取抢占方式,延时时间为20s;VRRP备份3组(vrid 3)作为Backup设备,以实现可靠性及流量的负载均衡,配置如下:

```
interface Vlanif2
ip address 192.168.2.250 255.255.255.0
vrrp vrid 2 virtual-ip 192.168.2.254
vrrp vrid 2 priority 120
vrrp vrid 2 preempt-mode timer delay 20
vrrp vrid 2 track interface GigabitEthernet0/0/24 reduced 30
interface Vlanif3
ip address 192.168.3.250 255.255.255.0
vrrp vrid 3 virtual-ip 192.168.3.254
```

3.2.4　DHCP配置

文章DHCP的配置采用基于全局地址池的配置方法。以SW2为例,设置地址池pool2,选取的接口是Vlanif2,实际接口地址为192.168.2.250,配置如下:

```
dhcp enable
ip pool pool2
gateway-list 192.168.2.254
network 192.168.2.0 mask 255.255.255.0
interface Vlanif2
dhcp select global
```

3.2.5　Eth-Trunk配置

在链路层设备之间的链路配置为Eth-Trunk模式,从而提高网络的可靠性。以SW2的链路聚合配置为例,配置如下:

```
interface Eth-Trunk 1
port link-type trunk
port trunk allow-pass vlan 2 to 3
trunkport GigabitEthernet 0/0/3 to 0/0/4
```

3.2.6　核心层Vlanif和OSPF配置

三层交换机作为核心层设备,用于高速的数据交换,运行ospf协议连接各个网段,因为交换机不能配置ip地址,通过VLAN方式连接,需要把ip地址配置在Vlanif接口上,核心层禁用stp协议,不需要配置生成树协议,配置如下:

```
stp disable
interface Vlanif5
ip address 10.1.19.2 255.255.255.252
interface GigabitEthernet0/0/1
port link-type access
port default vlan 5
ospf 1
area 0
network 10.1.18.2 0.0.0.0
network 10.1.19.2 0.0.0.0
network 10.1.20.1 0.0.0.0
```

3.2.7 防火墙区域配置

在防火墙上划分3个安全区域,把相应的接口划入Trust、Untrust和DMZ,配置如下:

```
firewall zone untrust
add interface GigabitEthernet0/0/1
firewall zone trust
add interface GigabitEthernet0/0/2
firewall zone dmz
add interface GigabitEthernet0/0/3
```

3.2.8 防火墙NAT与安全策略配置

(1)配置NAT地址池和NAT Server,创建Trust和Untrust的域间NAT策略,实现内网对公网的地址转换,配置如下:

```
nat address-group 1 200.100.1.1 200.100.1.1
nat-policy interzone trust untrust outbound
policy 1
action source-nat
policy source 192.168.2.0 mask 24
policy source 192.168.3.0 mask 24
address-group 1
```

(2)配置NAT Server,实现外网与DMZ之间的IP地址映射,以Web、FTP服务为例进行配置,配置如下:

```
nat server 1 protocol tcp global 200.100.1.3 8080 inside 172.16.1.80 www
nat server 1 protocol tcp global 200.100.1.3 21 inside 172.16.1.80 ftp
```

(3)配置Trust到Untrust的域间策略,允许内网访问外网,配置如下:

```
policy interzone trust untrust outbound
policy 1
action permit
policy source 192.168.2.0 mask 24
policy source 192.168.3.0 mask 24
```

(4)配置Trust到DMZ的域间策略,允许内网访问DMZ区域的服务器,配置如下:

```
policy interzone trust dmz outbound
policy 1
action permit
policy source 192.168.2.0 mask 24
policy source 192.168.3.0 mask 24
```

(5)配置Untrust到DMZ的域间策略,允许外网访问DMZ区域的服务器,配置如下:

```
policy interzone dmz untrust inbound
policy 1
action permit
policy service service-set http
policy service service-set ftp
policy destination 172.16.1.80 0
```

4 实验测试

文章通过查看配置命令的方式,使用Wireshark协议分析工具进行抓包,对实验进行了测试和验证。

4.1 DHCP功能测试

经过测试,内网的全部主机可以自动获取IP地址。打开PC机窗口,在“IPv4配置”中选择“DHCP”选项。以PC1的测试为例,在SW2的GE0/0/1端口进行抓包,图2显示了主机与DHCP服务器建立租约的四个过程。

No.	Source	Destination	Protocol	Info
22	0.0.0.0	255.255.255.2	DHCP	DHCP Discover - Transaction ID 0x1430
30	192.168.2.254	192.168.2.253	DHCP	DHCP Offer - Transaction ID 0x1430
32	0.0.0.0	255.255.255.2	DHCP	DHCP Request - Transaction ID 0x1430
33	192.168.2.254	192.168.2.253	DHCP	DHCP ACK - Transaction ID 0x1430

图2　PC机获取IP地址的过程

4.2　网关冗余测试

在SW2的端口(除了连接核心层交换机SW1的上行端口)上抓包,可以捕获VRRP协议的数据包。在SW2设备上查看VRRP协议,结果如图3所示,表明SW2作为VLAN2的Master设备,作为VLAN3的Backup设备。当SW2的上行端口链路端开后,SW3成为VLAN2的Master设备,结果如图4所示。

```
[SW2]display vrrp brief
VRID  State        Interface                Type     Virtual IP
------------------------------------------------------------------------------
2     Master       Vlanif2                  Normal   192.168.2.254
3     Backup       Vlanif3                  Normal   192.168.3.254
------------------------------------------------------------------------------
Total:2     Master:1     Backup:1     Non-active:0
```

图3　SW2上的VRRP信息

```
[SW3]display vrrp brief
VRID  State        Interface                Type     Virtual IP
------------------------------------------------------------------------------
2     Master       Vlanif2                  Normal   192.168.2.254
3     Master       Vlanif3                  Normal   192.168.3.254
------------------------------------------------------------------------------
Total:2     Master:2     Backup:0     Non-active:0
```

图4　SW2的上行链路断开后的VRRP信息

4.3　内网访问Untrust区域的外网测试

以PC1为例,在FW1的GE0/0/1端口进行抓包,捕获了10条ICMP数据包,结果如图5所示。通过图5的第2、5、8、10、12号报文,可以看出内网主机PC1的IP地址被转换为公网IP地址,实现了NAT功能。

No.	Source	Destination	Protocol	Info
2	200.100.1.1	202.102.2.2	ICMP	Echo (ping) request id=0x080a, seq=1/256, ttl=125
3	202.102.2.2	200.100.1.1	ICMP	Echo (ping) reply id=0x080a, seq=1/256, ttl=254
5	200.100.1.1	202.102.2.2	ICMP	Echo (ping) request id=0x080b, seq=2/512, ttl=125
6	202.102.2.2	200.100.1.1	ICMP	Echo (ping) reply id=0x080b, seq=2/512, ttl=254
8	200.100.1.1	202.102.2.2	ICMP	Echo (ping) request id=0x080c, seq=3/768, ttl=125
9	202.102.2.2	200.100.1.1	ICMP	Echo (ping) reply id=0x080c, seq=3/768, ttl=254
10	200.100.1.1	202.102.2.2	ICMP	Echo (ping) request id=0x080d, seq=4/1024, ttl=125
11	202.102.2.2	200.100.1.1	ICMP	Echo (ping) reply id=0x080d, seq=4/1024, ttl=254
12	200.100.1.1	202.102.2.2	ICMP	Echo (ping) request id=0x080e, seq=5/1280, ttl=125
13	202.102.2.2	200.100.1.1	ICMP	Echo (ping) reply id=0x080e, seq=5/1280, ttl=254

图5　捕获的IMCP数据包

4.4　内网访问DMZ区域的服务器测试

No.	Source	Destination	Protocol	Info
4	192.168.2.252	172.16.1.80	ICMP	Echo (ping) request id=0x10d0, seq=1/256, ttl=125
5	172.16.1.80	192.168.2.252	ICMP	Echo (ping) reply id=0x10d0, seq=1/256, ttl=255
7	192.168.2.252	172.16.1.80	ICMP	Echo (ping) request id=0x11d0, seq=2/512, ttl=125
8	172.16.1.80	192.168.2.252	ICMP	Echo (ping) reply id=0x11d0, seq=2/512, ttl=255
9	192.168.2.252	172.16.1.80	ICMP	Echo (ping) request id=0x13d0, seq=3/768, ttl=125
10	172.16.1.80	192.168.2.252	ICMP	Echo (ping) reply id=0x13d0, seq=3/768, ttl=255
12	192.168.2.252	172.16.1.80	ICMP	Echo (ping) request id=0x14d0, seq=4/1024, ttl=125
13	172.16.1.80	192.168.2.252	ICMP	Echo (ping) reply id=0x14d0, seq=4/1024, ttl=255
14	192.168.2.252	172.16.1.80	ICMP	Echo (ping) request id=0x15d0, seq=5/1280, ttl=125
15	172.16.1.80	192.168.2.252	ICMP	Echo (ping) reply id=0x15d0, seq=5/1280, ttl=255

图6　PC1访问服务器区的抓包结果

以PC1与DMZ区域的服务器通信为例,通过在防火墙的GE0/0/3端口进行抓包,捕获到ICMP数据包如图6所示。对于5条ICMP请求报文,序号seq分别为1-5,其源地址为PC1的IP地址,目的地址为Sever服务器的IP地址;同理对于5条ICMP应答报文,序号seq分别为1-5,源地址为Sever服务器的IP地址,目的地址

为PC1的IP地址,表明实验取得预期效果。

4.5 外网访问DMZ区域的服务器测试

打开Client1窗口,在地址栏中输入DMZ区域的服务器对外开放的公网映射地址:200.100.1.3:8080,显示访问成功的页面。通过在防火墙FW1的GE0/0/3端口捕获数据包,结果如图7所示。从图7可以分析,第1条数据包显示源地址为外网Client1客户端的IP地址,目的地址为DMZ区域的Server服务器的IP地址映射的公网地址,表明外网的客户端成功访问DMZ区域的服务器。

No.	Source	Destination	Protocol	Info
1	202.102.2.2	200.100.1.3	TCP	clearvisn > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460
2	200.100.1.3	202.102.2.2	TCP	http > clearvisn [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3	202.102.2.2	200.100.1.3	TCP	clearvisn > http [ACK] Seq=1 Ack=1 Win=8192 Len=0
4	202.102.2.2	200.100.1.3	HTTP	GET / HTTP/1.1 Continuation or non-HTTP traffic
5	200.100.1.3	202.102.2.2	HTTP	HTTP/1.1 200 OK (text/html)
6	202.102.2.2	200.100.1.3	TCP	clearvisn > http [ACK] Seq=158 Ack=308 Win=7885 Len=0

图7 捕获的TCP和HTTP数据包

5 结语

文章通过eNSP模拟器设计了一个基于防火墙的高性能园区网的实验方案,对实验进行了网络设计与规划、设备配置和实验结果的测试,仿真结果表明实验具有可行性和扩展性,取得了预期的实验效果。文章设计的网络模型满足园区网的基本需求,实现了防火墙在网络中的安全访问和隔离作用,内网的设计满足了网络的可靠性和负载均衡的要求。

参考文献:

[1] 唐灯平,朱艳琴,杨哲,等.计算机网络管理仿真平台防火墙实验设计[J].实验技术与管理,2015,32(4):156-160.
[2] 孟祥成.基于eNSP的防火墙仿真实验[J].实验室研究与探索,2016,35(4):95-100.
[3] 温贺平.基于eNSP的安全园区网实验设计与构建[J].实验室研究与探索,2018,37(4):126-129,169.
[4] 谭志勇,李进生.基于MSTP+VRRP的高可靠性园区网络设计与实现[J].计算机时代,2018,10(2):35-39.
[5] 张梁斌,高昆,梁世斌.基于Packet Tracer的小型企业网络应用架构的仿真实验[J].实验室研究与探索,2012,31(10):372-376.
[6] 唐灯平.利用Packet Tracer模拟组建大型单核心网络的研究[J].实验室研究与探索,2011,30(1):186-189.
[7] 时晨,赵洪钢,余瑞丰,等.基于eNSP的高可靠性企业园区网设计与仿真[J].实验室研究与探索,2020,39(2):112-117.
[8] 郭能华.基于MSTP+VRRP双核心技术的企业网络冗余设计与实现[J].中国管理信息化,2016,19(12):54-55.
[9] 孙光懿.基于VRRP和MSTP协议实现校园网高可靠性[J].中央民族大学学报(自然科学版),2018,27(2):37-45.
[10] 李澍,姚磊.实验室搭建复杂网络环境下的DHCP服务及安全防护[J].实验室研究与探索,2014,33(1):143-148.
[11] 田安红,付承彪.NAT原理实验在仿真器中的设计与实现[J].实验技术与管理,2014,31(9):135-138.
[12] 谢娇娇.基于空间通信协议的图像传输安全机制研究[D].哈尔滨工业大学,2017.

Design and Simulation of Campus Network Based on Firewall

YANG Li[1], LIU Jing[1], GULIZIRE·Ainiwai[2]

(*1.College of Computer Science and Technology, Kashi University, Kashi, Xinjiang, 844000, China;*
2.College of Electronic and Information Engineering, Yili Normal University, Yining, Xinjiang, 835000, China)

Abstract: The firewall is one of the important devices for building a campus network, which is used to implement secure access and isolation of internal and external networks. With the help of Huawei eNSP simulator to build network topology, an experimental scheme of campus network is designed, which is based on firewall security policy. In the paper, the configuration process of the experiment is given, the experiment is tested, and the correct test results are given. The simulation results show that the scheme realizes the security access control of firewall in the network, and provides relevant reference for the design of campus network.

Keywords: Firewall; Campus network; Network architecture; eNSP