ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.15, No.32, November. 2019

E-mail：jslt@dnzs.net.cn
http://www.dnzs.net.cn
Tel:+86-551-65690963 65690964

基于Packet Tracer的ASA防火墙实验设计

范君,蔡彬彬

(江苏工程职业技术学院,江苏 南通 226001)

摘要:防火墙实验是网络课程中安全实验的一个重要组成部分,从防火墙安全实验教学出发,以项目化教学案例为引导,设计实验需求、实验拓扑、实验数据,使用Packet Tracer仿真软件给出实验拓扑设计与配置流程,并对实验结果进行验证与分析。应用结果表明,该实验对学生提升的防火墙配置能力和协助教师教学开展取得良好效果。

关键词:ASA;防火墙;Packet Tracer;实验设计

中图分类号:TP391.9 **文献标识码:**A

文章编号:1009-3044(2019)32-0039-04

DOI:10.14004/j.cnki.ckt.2019.3784

开放科学(资源服务)标识码(OSID):

Design of Firewall Experimental Based on Packet Tracer

FAN Jun, CAI Bin-bin
(Jiangsu College of Engineering and Technology, Nantong 226001,China)

Abstract: Firewall experimentis an important part of thesecurityexperiments of network course. From the perspective of firewall security experiment teaching, the paper uses oriented project teaching case as guide, designs the requirements of lab ,lab topology and lab data of the experiment, uses the Packet Tracer simulation software to design topology and configure lab process, analyses and validates the experimental data. The results of experiment show that the experiment promotes students' abilities of firewall configuration, assists teachers in teaching process and achieves good teaching effect.

Key words: ASA; Firewall; Packet Tracer; experimental design

1 概述

随着互联网应用发展,对网络工程安全的要求日益提高,防火墙已经成为在网络工程建设中必不可少的设备,防火墙实验也成为网络技术课程中的重要实验内容之一。较常规实验课而言,防火墙的实验教学有较大的难度[1],首先,防火墙技术需以路由与交换技术为基础,防火墙的数据过滤机制和数据地址转换机制复杂,理论学习难度较高;其次,防火墙硬件产品价格高于其他网络产品,在学生实践过程中难以实现每名学生独立拥有物理防火墙实验条件,使得教学实践难以大规模开展和深入。

目前,Packet Tracer仿真环境已实现ASA5505防火墙的仿真,该类仿真环境是对思科ASA防火墙硬件的仿真,此类仿真较CBAC路由器级的防火墙实验[2]更接近真实的防火墙环境。因此设计基于ASA5505的仿真实验,作为防火墙教学实践的课程载体,借助实际案例展示工程实施流程和步骤[3],帮助学生掌握防火墙原理和知识,并进一步完善和深化学生在实验环节中配置防火墙的能力。

2 实验背景

工学结合的计算机网络工程的实验,应源于工程实践并适合实验类的教学开展。基于上述理念,实验设计以江苏某物流企业的广域网改造的项目作为实验设计的项目载体,根据企业的网络安全实际规划进行教学过程中的ASA防火墙实验设计。该企业无锡总部通过ASA5520防火墙外联至互联网,徐州分支机构则使用ASA5510防火墙外联至互联网,两台防火墙通过接入运营商ISP实现分支机构访问总部相关数据业务。

3 实验设计

3.1 拓扑设计

参考上述企业需求,实验拓扑设计如图1所示,总部和分支机构都使用ASA5500系列设备互联至ISP运营商,总部的ASA防火墙按照业务流量,划分为OutSide、InSide、DMZ三个不同的区域,其中OutSide区上联至ISP,InSide下联到内网的3560交换机,DMZ侧联至对外业务的Web服务器用于提供外部访问公司门户网站。分支机构的ASA防火墙按业务流量只划分为OutSide、InSide两个区域[4]。实验拓扑图如图1所示。

3.2 IP地址规划

根据设计,将工程中涉及的设备互联IP网段、终端设备业务网段IP进行统一规划[5],网络设备IP规划如表1所示,终端设备IP地址规划如表2所示。

收稿日期:2019-08-16
基金编号:江苏工程职业技术学院2015年教学改革立项项目(序号18)
作者简介:范君(1975—),男,江苏南通人,硕士,系统分析员,副教授,研究方向为机器学习和模式识别、网络工程与网络安全。

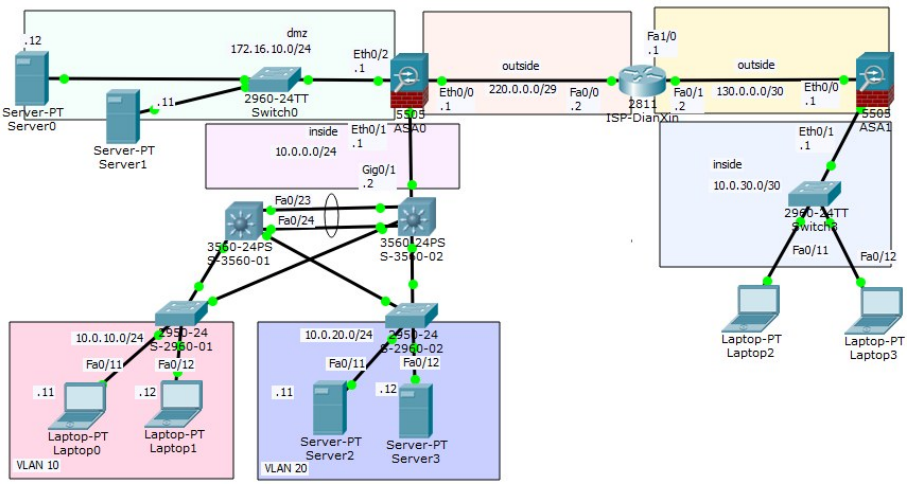

图1　实验拓扑设计

表1　网络设备IP地址规划

设备名称	端口号	IP 地址
ASA5505-01 总部防火墙	Eth0/0	220.0.0.1/29
	Eth0/1	10.0.0.1/24
	Eth0/2	172.16.10.1/24
ASA5505-02 分支机构防火墙	Eth0/0	130.0.0.1/30
	Eth0/1	10.0.30.1/24
2811 路由器 ISP 运营商	Fa0/0	220.0.0.2/29
	Fa0/1	130.0.0.2/30
3560-01	Gig0/1	10.0.0.2/24
	int vlan 10 物理	10.0.10.253
	int vlan 20 物理	10.0.20.253
	int vlan 10 浮动	10.0.10.254
3560-02	int vlan 10 物理	10.0.10.252
	int vlan 20 物理	10.0.20.252
	int vlan 20 浮动	10.0.20.254

表2　终端设备IP地址规划

设备名称	IP 地址	网关
Server-01	172.16.10.11/24	172.16.10.1/24
Server-01	172.16.10.12/24	172.16.10.1/24
Server-01	10.0.20.11/24	10.0.20.1/24
Server-01	10.0.20.12/24	10.0.20.1/24
PC-01	10.0.10.11/24	10.0.10.1/24
PC-02	10.0.10.12/24	10.0.10.1/24
PC-03	10.0.30.11/24	10.0.30.1/24
PC-04	10.0.30.12/24	10.0.30.1/24

3.3 防火墙安全设计

防火墙所联的各个网段对应不同的安全区域，这些安全区域中设置为不同的安全级别。数据流量通过防火墙时，防火墙将根据流量的方向、流经区域安全级别，应用在端口上所设置的不同的安全策略对数据流量进行过滤和限制[6]，故防火墙的端口安全级别需要在设计之初就规划好[7]。基于上述思路，对于拓扑图中防火墙的安全规划如表3所示，其中端口安全级别的数值范围为0~100，数值越大表示安全级别越高。

表3　防火墙IP地址与安全规划

设备名称	端口号	端口区域	VLAN号	安全级别
ASA5505-01 总部防火墙	Eth0/0	outside	10	0
	Eth0/1	inside	20	100
	Eth0/2	dmz	30	50
ASA5505-02 分支机构防火墙	Eth0/0	outside	10	0
	Eth0/1	inside	20	100

3.4 实验仿真设计

3.4.1 实验设备拓扑仿真

参考3.1小节拓扑设计、IP地址规划表和防火墙安全规划表，使用Packet Tracer6.3进行仿真拓扑设计。在Packet Tracer6.3中，选择两台ASA5505分别作为总部和分支的对外互联设备，在两台防火墙中间选择一台2811路由器模拟ISP电信运营商互联至防火墙。两台ASA5505的安全区域所对应的互联设备，依照安全区域的设计规划与表1数据，分别选择3560和2960交换机进行互联。所设计的实验拓扑仿真如图2所示。

3.4.2 路由器配置

因防火墙内部流量IP为私有网段无须发布到外部路由器的路由表中，根据拓扑设计，ISP路由器只需完成如图2所示的端口配置即可。

```
interface FastEthernet0/0
ip address 220.0.0.2 255.255.255.252
!
interface FastEthernet0/1
ip address 130.0.0.2 255.255.255.252
```

图2　路由器端口配置

3.4.3 防火墙配置

根据实际工程实施流程，在实验设计中，将防火墙的配置划分为端口配置、路由配置、NAT地址映射配置、安全策略配置等几个步骤[8]，上述各个部分的配置过程是逐层递进的关系，为避免将当前配置过程中的错误引入到下一阶段，在配置过程中需要对阶段功能进行验证。

步骤1：防火墙端口配置

不同于ASA5510级别以上的ASA系列防火墙，ASA5505的物理接口实际是作为二层端口，该端口不能够直接配置三层IP地址，需要在交换虚拟接口SVI(Switch Virtual Interface)中先行配置Interface VLAN IP地址，之后将二层端口加入对应的VLAN后实现三层转发功能。以总部ASA5505为例，参照表3的数据，对端口的名称、安全级别、地址等信息进行配置，如图3所示。

```
interface Vlan10
nameif outside
security-level 0
ip address 220.0.0.1 255.255.255.252
!
interface Vlan20
nameif inside
```

```
security-level 100
ip address 10.0.0.1 255.255.255.0
!
interface Vlan30
no forward interface Vlan20  —(1)
nameif dmz
security-level 50
ip address 172.16.10.1 255.255.255.0
```

图3 防火墙SVI端口配置

ASA5505默认使用VLAN 1、VLAN 2作为IP配置，在实验配置中，为让学生体会在防火墙设计中VLAN的规划，在配置前需将VLAN 1和VLAN 2中默认配置的nameif区域名、IP地址配置信息去除，根据表3的规划自行建立VLAN 10、VLAN 20、VLAN 30。因仿真软件对ASA5505的限制，仿真环境中最多只能使用三个nameif区域，禁止多于两个区域以上的流量进入inside区域，即第三个VLAN端口的流量配置时有限制，故在配置dmz端口的时候，需要先行增加如图3中(1)的命令，限制dmz区域的流量进入inside区域之后，方可正常启用dmz端口功能[9]。

```
interface Ethernet0/0
switchport access vlan 10
!
interface Ethernet0/1
switchport access vlan 20
!
interface Ethernet0/2
switchport access vlan 30
```

图4 防火墙物理端口配置

配置完SVI，即可将ASA 5505防火墙的物理接口分配到SVI所相应的VLAN中，配置如图5所示。

步骤2：防火墙路由配置

ASA定义静态路由目的在于让防火墙对发往不同区域流量的目标IP进行识别并转发到相应的outside、inside或dmz区域。如图5所示，总部的ASA5505-01访问公网非直连网段130.0.0.0/30，需要首先指明流量路由到outside端口，然后设置目标网段、子网掩码和指向ISP路由器的220.0.0.2下一跳地址。

```
route outside 130.0.0.0 255.255.255.252 200.0.0.2 1
```

图5 防火墙路由配置

步骤3：NAT地址映射配置

服务器IP映射方式根据其业务分为两类，一类是静态NAT映射，实现一对一的映射，通过nat命令指定服务器内网ip映射到的公网地址供外部用户访问，如图7命令(1)所示。另一类是端口NAT映射，当内部多台服务器需要主动发起内网到外网的访问，可将此类服务器网段地址统一映射到防火墙outside外网口的IP，实现多对一的映射，如图6命令(2)所示[10]。

```
object network Dmz-WebServer1
host 172.16.10.11
nat (dmz,outside) static 220.0.0.3 —(1)
… ...
object network 172.16.10.0/24
subnet 172.16.10.0 255.255.255.0
nat (dmz,outside) dynamic interface —(2)
```

图6 防火墙nat地址映射配置

步骤4：安全策略配置

完成基本配置的防火墙，需要开启基本的安全策略防火墙才能开始工作[11]。默认情况下，ASA防火墙允许高安全区域的数据流量流向低安全区，而低安全区域流量流向高安全区时则需要通过设置安全策略命令放行，ASA安全策略特性如图7所示。

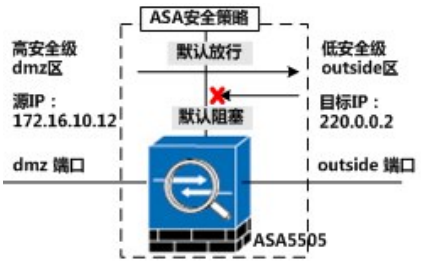

图7 ASA防火墙默认安全策略特性

ASA安全策略分析，以dmz区的服务器ping包访问outside区的ISP路由器地址为例，数据流量从dmz区进入ASA防火墙后，ASA判断目标IP对应outside区域，且该区域的安全级别低于源IP的dmz区域，则ASA放行此部分流量，并在离开outside端口前应用NAT将dmz的服务器地址转换为公网IP。当上述流量返回，ASA安全策略判别源IP、目标IP安全级别相同，ASA防火墙从outside端口接受流量后将目标IP地址通过NAT转换为dmz区域的IP地址，此时防火墙进一步检查安全策略，防火墙判别目标IP地址安全级别高于源IP地址，在未设置安全策略时则默认将此部分流量丢弃。

为放行outside上联isp的220.0.0.0/29网段访问dmz服务器172.16.10.0/24网段的流量，定义如图9所示的安全策略并应用到端口中。根据流量的源IP和目标IP所对应的网段，首先定义网段IP对应的地址对象，如图9命令(1)所示。然后定义ACL安全策略，允许在icmp协议背景下，上述isp网段访问dmz网段，如图9命令(2)所示。最后将定义的安全策略应用到dmz端口的out方向上，如图9命令(3)所示。

inside与outside区域之间的流量安全策略定义与部署与图8命令类似，除地址对象和ACL不一样外，应在inside端口out方向上应用安全策略。

```
object network 220.0.0.0/29
subnet 220.0.0.0 255.255.255.248  —(1)
……
access-list isp-to-dmz extended permit icmp object 220.0.0.0/29object 172.16.10.0/24—(2)
access-group dmz-to-isp out interface dmz —(3)
```

图8 安全策略定义与应用

3.4.4 交换机配置

总部的3560交换机下联的多个VLAN的网关终结在3560上，与ASA5505采用三层连接。仿真环境中设计中，我们发现ASA5505防火墙仿真环境中，对于直连的inside区域的流量是可以直接通过防火墙NAT进行地址转换后访问外网，而3560以下的VLAN业务流量到达ASA5505时，尽管有相关NAT和策略放行配置命令，但ASA5505并不支持对此部分非直连的inside区域IP网段实现NAT功能。

为解决上述问题，在实验设计中，利用3560具备三层路由和NAT功能，将源地址为非直连的内网业务IP网段，在3560-02设备上先行NAT转换为3560-02与ASA5505互联网段的IP网段，最终通过两级NAT实现防火墙放行inside区域所有IP网

段访问外网。

```
ip routing————————(1)
!
interface GigabitEthernet0/1
no switchport————————(2)
ip address 10.0.0.2 255.255.255.0
ip nat outside————————(3)
.....
interface Vlan10
ip address 10.0.10.254 255.255.255.0
ip nat inside————————(4)
!
interface Vlan20
ip address 10.0.20.254 255.255.255.0
ip nat inside————————(5)
!
ip nat inside source list 10 interface GigabitEthernet0/1 overload——(6)
!
ip route 0.0.0.0 0.0.0.0 10.0.0.1 ——(7)
!
access-list 10 permit 10.0.10.0 0.0.0.255
access-list 10 permit 10.0.20.0 0.0.0.255
```

图9　3560-02交换机NAT配置

默认情况下，3560交换机处于二层工作模式，需要使用如图9所示的命令(1)进入三层工作模式。进行NAT的outside端口则直接定义在物理接口Gig0/1上，且该接口也配置了物理IP，如命令(2)、(3)所示，而NAT的inside端口则在VLAN 10和VLAN 20的SVI接口下配置，如命令(4)、(5)所示。对于上述两个VLAN的地址网段通过定义ACL，配置基于Gig0/1端口的NAT[12]端口映射，如命令(6)所示，将上述网段的IP均转换为10.0.0.2的IP地址，并配置3560缺省路由指向ASA5505的inside端口IP，如图命令(7)所示，最终实现所有内网流量能够访问到ISP路由器。篇幅所限，3560的HSRP等配置此处不再叙述。

5 实验验证

上述数据配置完成后，进行实验数据检验与分析。首先通过在防火墙节点执行show route命令[13]，检测ASA设备的路由表中的静态路由、缺省路由等信息是否完整，转发方向和端口是否对应。

对于ASA功能配置验证，以DMZ区域的两台服务器为例，使用Server1服务器访问ASA外网侧的路由器，执行ping命令结果如图10所示。

```
SERVER>ping 200.0.0.2

Pinging 200.0.0.2 with 32 bytes of data:

Reply from 200.0.0.2: bytes=32 time=1ms TTL=254
Reply from 200.0.0.2: bytes=32 time=2ms TTL=254
Reply from 200.0.0.2: bytes=32 time=0ms TTL=254
Reply from 200.0.0.2: bytes=32 time=0ms TTL=254

Ping statistics for 200.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

图10 服务器从ASA内部访问公网

检查防火墙的流量转换情况，可通过show nat命令观察和验证[14][15]。如图11所示，观察到内网VLAN 10和VLAN 20访问ISP路由器时，可以看到内网流量NAT转换都正常，同时dmz区的服务器也有NAT成功的流量记录。即NAT配置和安全策略使用正常。

```
HQ-WuXi-ASA5505-01#show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic 10.0.0.0/24 interface
    translate_hits = 6, untranslate_hits = 5

3 (dmz) to (outside) source dynamic 172.16.10.0/24 interface
    translate_hits = 9, untranslate_hits = 5
4 (dmz) to (outside) source static 172.16.10.11/32 220.0.0.3
    translate_hits = 0, untranslate_hits = 0
```

图11　从内网发起访问验证ASA的NAT配置

6 总结

通过设计ASA防火墙的综合性实验，能够让学生较为完整的理解防火墙在工程项目中的设计和应用，提高了学生的防火墙设计、实施、故障排除能力，同时有效了提升学生在网络系统集成过程中安全设计能力。实验设计中在3560上启用NAT功能，结合ASA防火墙NAT功能，实现两级NAT地址转换，有效促进学生在设计过程中对NAT的理解和应用。

参考文献：

[1] 周敏. 计算机网络安全实验教学改革[J]. 实验技术与管理，2013(6):113-117.

[2] 姜恩华,李素文,赵庆平,等. 基于PacketTracer软件的防火墙技术实验教学设计[J]. 通化师范学院学报,2013(8):45-47.

[3] 任晓鹏,李伟华. 基于Packet Tracer构建虚拟网络实训平台[J]. 中国职业技术教育,2006(9):44-46.

[4] Alexandre M.S.P. Moraes. Cisco防火墙[M] .Cisco Press, 2014.

[5] 贺惠萍,荣彦,张兰. 虚拟机软件在网络安全教学中的应用[J]. 实验技术与管理,2011(12):112-115.

[6] 李永,甘新玲. 基于PacketTracer的路由综合实验设计与实现[J]. 实验室研究与探索,2015(11):111-114.

[7] 冯丹,游胜玉. 基于PacketTracer的区域策略防火墙技术仿真实验平台的设计与实现[J]. 科技广场,2015(12):116-120.

[8] 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(4):156-160.

[9] 邹航,李梁,王柯柯,等. 整合ACL和NAT的网络安全实验设计[J]. 实验室研究与探索,2011(11):61- 65.

[10] Dave Hucaby.Cisco ASA、PIX与FWSM火墙手册[M] .2版. 北京：人民邮电出版社, 2010.

[11] JazibFrahim, Omar Santos. Cisco ASA设备使用指南 [M]. 北京：人民邮电出版社, 2010.

[12] David Hucaby, Dave Garneau, Anthony Sequeira. CCNP安全防火墙642-618认证考试指南[M]. 人民邮电出版社, 2013.

[13] YusufBhaiji. 网络安全技术与解决方案[M]. 北京：人民邮电出版社, 2009.

[14] MerikeKaeo. 网络安全设计[M]. 2版. 北京：人民邮电出版社, 2005.

[15] Priscilla Oppenheimer. 自顶向下网络设计[M]. 2版. 北京：人民邮电出版社, 2005.

[通联编辑：王力]