设计研究与应用

基于 Packet tracer 防火墙的基本配置仿真实验的设计与实现

彭如飞
（川北医学院，四川南充 637000）

摘　要：防火墙是最重要的网络安全设备，合理对防火墙的配置，是实现网络安全的有效保证。本文基于 Cisco Paket Tracer 6.0 网络虚拟仿真软件，搭建了以防火墙为中心的网络，并对其进行了基本配置，实现网络安全目标。通过防火墙的基本配置仿真实验，让学生加深对防火墙功能的理解，并掌握防火墙的基本配置能力。

关键词：Packet tracer；防火墙；仿真实验；DMZ；安全级别
中图分类号：TP393.08　　**文献标识码：**A　　**DOI：**10.3969/j.issn.1003-6970.2021.02.041
本文著录格式：彭如飞.基于Packet tracer防火墙的基本配置仿真实验的设计与实现[J].软件,2021,42(02):131-134

Design and Implementation of Basic Configuration Simulation Experiment Based on Packet Tracer Firewall

PENG Rufei
(North Sichuan Medical College, Nanchong Sichuan 637000)

【Abstract】：Firewall is the most important network security equipment, reasonable configuration of the firewall, is to realize the effective guarantee of network security. Based on the network virtual simulation software of Cisco PAKET TRACER 6.0, this paper builds a network with firewall as the center, and carries on the basic configuration to achieve the goal of network security. Through the basic configuration of the firewall simulation experiment, let the students deepen the understanding of the function of the firewall, and master the basic configuration of the firewall ability.

【Key words】：Packet tracer;firewall;simulation experiment;The DMZ;security level

网络的迅速发展，对网络安全的要求也越来越高，防火墙作为网络安全中非常重要的网络设备，其相关实验是网络课程教学的重要内容 [1]。对于防火墙这种昂贵的大型网络设备的配置实验，虚拟仿真实验明显优于传统实验。Packet Tracer 作为最广泛使用的网络虚拟仿真平台，本文以此作为防火墙基本配置实验的载体，帮助学生加深对防火墙相关知识的理解，掌握防火墙的基本配置。

1 Packet Tracer 网络仿真平台

Packet Tracer 是思科公司研发的一款辅助网络学习的虚拟仿真工具，其功能强大，操作简便，被广泛应用。在 Packet Tracer 中可完成网络的搭建，模拟网络并对其进行故障分析，完成交换机、路由器等网络设备的配置等实践操作 [2]。Packet Tracer 能够克服网络实验对实验场地的高要求，大幅度降低了实验成本，提高了实验效率及成功率，使教学效果得到大幅度提升。

2 防火墙

2.1 防火墙的概念和部署

防火墙放置于多个网络的边界处，通过执行设置的访问控制策略实现保护网络的设备。防火墙是保证内、外部网络通信安全的主要设备，其利用制定的访问策略对通过它的数据进行监控和审查，实现对网络存在威胁的数据包的过滤、屏蔽和阻拦，以保证内部网络不会受外部的非法访问和攻击。

防火墙要实现对多个网络的访问控制，保证网络安全，需布放在需要保护网络的边界处，部署结构如图 1

作者简介：彭如飞（1990—），男，四川资阳人，硕士，助教，研究方向：物联网医学信息化、教育信息化。

所示。

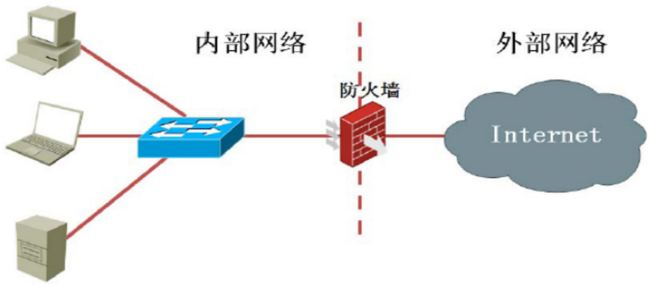

图1 防火墙的部署结构
Fig.1 Firewall deployment structure

2.2 防火墙的主要功能

防火墙主要功能包括：

（1）隔离内外部网络。将内外部网络隔离可以防止非法用户访问内部网络，并能有效防范邮件病毒和宏病毒等的攻击。

（2）形成集中监视点。防火墙位于多个网络交界处，通过强制所有数据包都要经过防火墙，并通过访问规则对所有数据包进行检查和过滤，这样就能集中对网络进行安全管理。

（3）强化安全策略。以防火墙为中心，能够将多种安全软件配置在防火墙上，比如口令和身份认证等，与传统的网络安全问题分散在多台主机上相比，这种集中管理方式操作更加简便并且节约成本 [3]。

（4）能够有效审计和记录内外网络之间的通信活动。因为内外网络之间所有的数据包都要流经防火墙，因此防火墙能对所有的数据包进行记录，并写进日志系统。当发现异常行为时，防火墙能够发出报警，并提供导致异常行为的原因，比如系统被检测或被攻击等。

2.3 防火墙的 DMZ 区及安全级别

DMZ 是独立于内部网络和外部网络之间的一个缓冲区，此区域主要存放一些必须对外部网络开放的一些服务器等设备，比如 FTP 服务器和 Web 服务器等。网络中有些设备需要对外网的一些设备提供服务，如果这些设备和内网设备放在一起，则会给内网带来巨大的安全风险。DMZ 区的作用则能将这些需要对外开放的设备和内部网络的设备进行隔离，根据情况采取针对性的隔离措施，使得这些设备既能对外提供服务，同时也能较好地对内部网络进行保护 [4]。DMZ 区根据网络实际需要能够划分多个，进而实现安全目标。DMZ 防火墙组成示例如图 2 所示。

思科防火墙把将接口设置为不同的安全等级，等级以数字 0 至 100 的整数表示，默认时高等级区域可以访问低等级区域，而低等级区域不能访问高等级区域。若等级低等级区域需要访问高等级区域，可以通过 ACL 或 conduit(管道) 明确进行配置。安全级别 100 是 PIX(或 asa) 防火墙内部接口的最高级别，安全级别 0 是 PIX(或 asa) 防火墙外部接口的最低级别，它们都是是默认设置，且不能改变 [5]。

3 防火墙的基本配置仿真实验的设计与实现

3.1 实验需求及网络拓扑结构设计

本次实验目标是让学生了解防火墙的概念，熟悉防火墙关键技术，掌握防火墙的安全级别，以及熟悉思科防火墙的基本配置。为实现预设实验目标要求将网络划分为 inside（内网）、outside（外网）、dmz（服务器区）

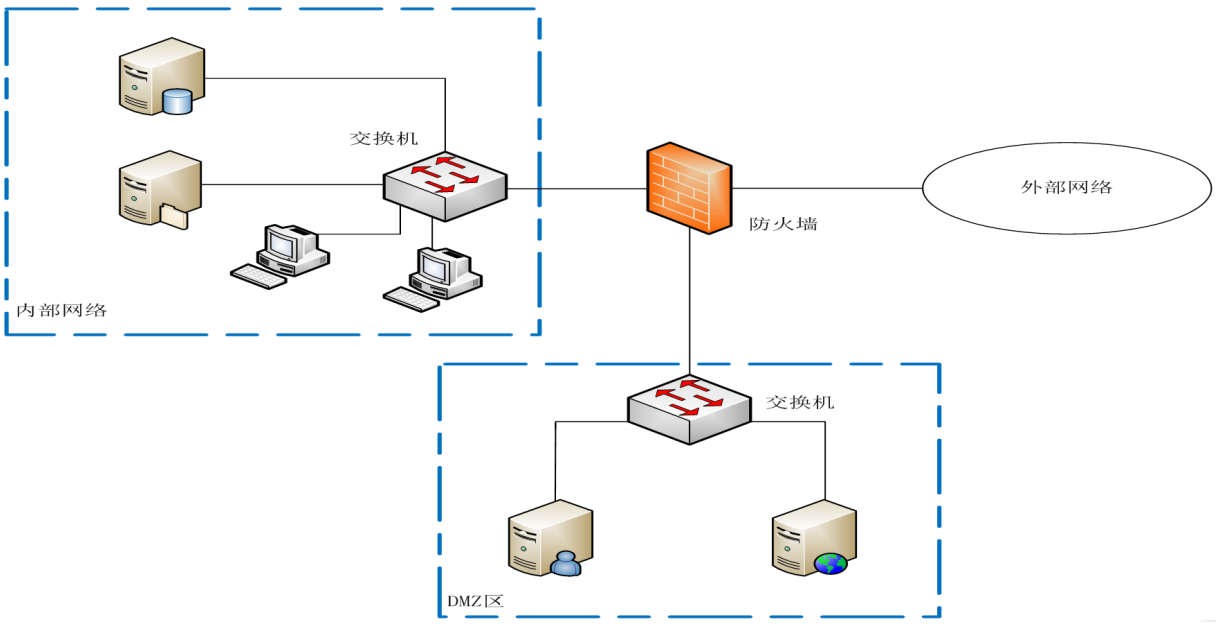

图2 DMZ防火墙组成拓扑
Fig.2 DMZ firewall composition topology

三个区域，并对防火墙进行配置，使得内网和 DMZ 区的设备可以访问外网的设备，内网设备可以访问 DMZ 区设备，但是 DMZ 区设备不能访问内网设备，外网设备可以访问 DMZ 区的设备。根据实验目标和需求设计网络拓扑如图 3 所示：

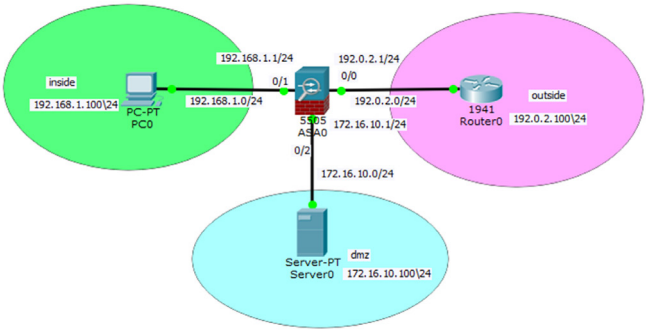

图3 防火墙基本配置实验网络拓扑图
Fig.3 Network topology diagram of firewall basic configuration experiment

对网络拓扑图各设备 IP 地址规划如表 1 所示。

3.2 实验具体步骤

（1）根据设计的网络拓扑图，在 Cisco Packet Tracer 中搭建网络。

（2）配置主机、服务器和路由器的接口的 IP 地址。

通过 IP Configuration 分别配置主机（Inside User）和服务器（Web Server）的 IP 地址。

通过命令配置路由器接口的 IP 地址：

Router>enable

Router#configure terminal

Router(config)#interface GigabitEthernet 0/0

Router(config-if)#ip address 192.0.2.100 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#ip route 0.0.0.0 0.0.0.0 192.0.2.1

命令说明：命令：ip route <ip_address> <mask> <gateway> [<preference>]，no ip route <ip_address> <mask> <gateway> [<preference>]。功能：配置静态路由；本命令的 no 操作为删除静态路由。参数：<ip_address> 和 <mask> 分别是目的设备的点分十进制格式的 IP 地址和子网掩码，<gateway> 则为下一跳设备的 IP 地址，<preference> 表示路由优先级，在 1 至 255 间取值，其值越小表明优先级越高 [6]。其中 0.0.0.0 不是一个真正意义上的 IP 地址，而是表示本地主机路由表中没有具体写明的目的主机或网络的这样一个集合。

（3）开启路由器的 telnet 服务。

Router(config)#line vty 0 15

Router(config-line)#password cisco

Router(config-line)#login

（4）更改 ASA 防火墙名称。

ciscoasa>enable

Password:（密码默认为空）

ciscoasa#configure terminal

ciscoasa(config)#hostname PKT-ASA

（5）配置 VLAN 1 的 IP 地址和名称。

PKT-ASA#configure terminal

PKT-ASA(config)#interface vlan 1

PKT-ASA(config-if)#ip address 192.168.1.1 255.255.255.0

PKT-ASA(config-if)#nameif inside

PKT-ASA(config-if)#security-level 100

说明：Packet Tracer 中的 ASA 5505 已经默认配置好了两个 VLAN：

VLAN1：Inside VLAN（interfaces E0/1->E0/7）

VLAN2：Outside VLAN(interfaces E0/0)

（6）配置 VLAN 2 的 IP 地址和名称。

PKT-ASA#configure terminal

表1 设备IP地址规划表
Tab.1 Device IP address planning table

网络设备	端口	IP 地址	子网掩码	默认网关
PC	F/0	192.168.1.100	255.255.255.0	192.168.1.1
路由器	G/0	192.0.2.100	255.255.255.0	192.0.2.1
server	F/0	172.16.10.100	255.255.255.0	172.16.10.1
防火墙	0/0	192.0.2.1	255.255.255.0	192.0.2.100
	0/1	192.168.1.1	255.255.255.0	192.168.1.100
	0/2	172.16.10.1	255.255.255.0	172.16.10.100

PKT-ASA(config)#interface vlan 2

PKT-ASA(config-if)#ip address 192.0.2.1 255.255.255.0

PKT-ASA(config-if)#nameif outside

PKT-ASA(config-if)#security-level 0

（7）配置 VLAN 3 的 IP 地址和名称。

PKT-ASA#configure terminal

PKT-ASA(config)#interface vlan 3

PKT-ASA(config-if)#no forward interface vlan 1

PKT-ASA(config-if)#nameif dmz

PKT-ASA(config-if)#security-level 50

PKT-ASA(config-if)#ip address 172.16.10.1 255.255.255.0

（8）分配 ASA 防火墙的接口到不同的 VLAN（其中 VLAN1 和 VLAN2 已经默认划分，不需要再配置）。

PKT-ASA#configure terminal

PKT-ASA(config)#iinterface Ethernet 0/2

PKT-ASA(config-if)#switchport access vlan 3

3.3 结果验证

（1）验证 ASA 防火墙和主机、服务器、路由器的连通情况：

从 ASA 防火墙分别 ping 主机、服务器和路由器。结果表明全部能够 ping 通。

（2）验证从 inside 和 dmz 区域连通到 outside 区域情况：

使用 ping 命令进行验证，结果表明能够从 inside 和 dmz 区域连通到 outside 区域，因为 inside 和 dmz 区的安全级别高于 outside 区域。

（3）通过 ACL 开启防火墙的 icmp 通路：

模拟网络运行，通过数据包动态传输图，结果表明 icmp 数据包可以从高安全级别的 inside 区域通过防火墙到低安全区域的 outside，反之则不行，这正是防火墙的作用。如果需要使得 icmp 数据包可以从低安全级别的 outside 区域通过防火墙到高安全区域的 inside，则需要手动通过 ACL 进行配置。

PKT-ASA#configure terminal

PKT-ASA(config)#access-list icmp extended permit icmp any any

PKT-ASA(config)#access-group icmp in interface outside

命令说明：在 ASA 上配置 ACL 有两个作用，一是允许入站连接；二是控制出站连接的流量。目前有两种主要的 ACL: 标准 ACL 和扩展 ACL，标准 ACL 只对数据包中的源地址进行检查，而扩展 ACL 既要对数据包的源地址进行检查，也要对数据包的目的地址进行检查，并且能够检查数据包的端口号、特定协议类型等 [7]。

标准 ACL：

asa（config）#access-list acl-name [standrad] {permit | deny } ip_addr mask

扩展 ACL：

Asa（config）#access-list acl_name [extended] {permit | deny } protocol src_ip_addr src_mask dst_ip_addr dst_mask [operator port]

将 ACL 应用到接口：

asa（config）#access-group acl_name {in | out} interface interface_name

4 结语

使用 Cisco Paket Tracer 6.0 进行防火墙基本配置实验，构建了具有内部网络、外部网络、DMZ 区的防火墙实验的虚拟仿真场景。学生通过对防火墙的基本配置，有助于理解防火墙的功能，DMZ 区的作用，以及防火墙如何实现对网络的保护，与此同时也锻炼了学生们配置防火墙的动手能力。

参考文献

[1] 范君,蔡彬彬.基于Packet Tracer的ASA防火墙实验设计[J].电脑知识与技术,2019,15(32):39-42.

[2] 景朋森,王飞.网络工程实践教学中Packet Tracer的应用研究[J].电子商务,2010(12):55-57.

[3] 魏荣华,崔凌云.防护计算机网络信息安全之我见[J].电脑知识与技术,2008,4(S2):191.

[4] 吉诚. 企业级网络设计方案的规划与测试[D].上海:上海交通大学,2008.

[5] 陈兰兰.网络地址转换NAT技术及在CISCO PIX防火墙中应用[J].甘肃科技纵横,2007(6):19-20.

[6] 张洪涛.虚拟路由器冗余协议在网络中的应用[J].中国新通信,2018,20(21):121-122.

[7] 李大周.利用路由器ACL功能保障局域网安全[J].电脑知识与技术,2010,6(12):2892-2894.