教学过程中基于 Packet tracer 的防火墙仿真研究

段文龙（重庆工商大学融智学院，重庆 巴南 401320）

【摘　要】防火墙是信息安全技术教学中的重要知识点，新工科专业缺乏网络硬件平台无法去形象直观的感受和书本的理解理论，在教学中引入通过使用 Packet tracer 进行防火墙网络仿真，把抽象的理论知识可视化、形象化，让学生更深入的了解了防火墙工作原理及其体系结构，提高了学生网络综合构建的能力。

【关键词】Packet tracer；路由器；防火墙；DMZ
【中图分类号】TP393　　【文献标识码】A　　【文章编号】1006-4222（2020）04-0111-02

1　防火墙的简介

防火墙（firewall）是广泛使用的网络安全技术，用以保卫网络的安全，部署于可信任的内部网络（intranet）和不安全的外部网络（internet）之间。本文使用 Packet tracer 仿真部署一个非常典型的基于分组过滤技术的硬件组合体系结构三足防火墙。

2　防火墙网络的拓扑结构

防火墙网络可分为：不安全的外网（internet），可信任内网（intranet），非军事区 DMZ，由防火墙提供连接和防护，以及防火墙区域。

3　使用 Packet tracer 构建防火墙网络

3.1　防火墙设置

（1）首先将防火墙命名为 firewall

ciscoasa（config）#hostname firewall

（2）关闭cisco asa5505 防火墙模型在内网（intranet）方向的软件预设的 dhcp 服务。通过 showrun 命令可以发现 asa5505 防火墙模型在内网（intranet）方向的 dhcp 服务是打开的：

dhcpd address 192.168.1.5-192.168.1.35 inside

我们将其关闭：firewall（config）#no dhcpd address 192.168.1.5-192.168.1.35 inside

（3）定义 vlan，通过拓扑结构可知，防火墙连接了外网（internet）、内网（intranet）、和 DMZ，所以需要使用到 3 个 vlan：

firewall (config)#interface Vlan1//定义 vlan1

firewall (config)#nameif inside//内网（intranet）使用

firewall (config)#security-level 100 //安全级别最高

firewall (config)#ip address 192.168.1.1 255.255.255.0

firewall (config)#interface Vlan2//定义 vlan2

firewall (config)#nameif outside//外网(internet)使用

firewall (config)#security-level 0//安全级别最低

firewall (config)#ip address 10.10.10.1 255.255.255.0

firewall (config)#interface Vlan3//定义 vlan3

firewall (config)#no forward interface Vlan1 //不允许向vlan1转发

firewall (config)#nameif dmz //DMZ 使用

firewall (config)#security-level 70 //安全级中等

firewall (config)#ip address 192.168.2.1 255.255.255.0

（4）绑定 vlan 到相对应端口，asa5505 防火墙模型默认 vlan1 绑定到 Ethernet0/1 端口，可以不用再设置。

firewall (config) #interface Ethernet0/0

firewall(config-if) #switchport access vlan 2 //把 vlan2 绑定到 Ethernet0/0 端口

firewall (config) #interface Ethernet0/2

firewall (config-if) #switchport access vlan 3//把 vlan3 绑定到 Ethernet0/2 端口

（5）防火墙的安全策略和防火墙路由设置。

firewall (config)# class-map testMap

firewall (config)# match any

firewall (config)# policy-map testPolicy

firewall (config)# class testMap

家居的数据传输的安全性将是目前企业急需解决的问题，更是目前智能家居行业发展困境中的最为紧急的突破口。因此在智能家居未来的发展中，网络安全和信息安全将成为物联网行业发展的重中之重。未来在智能家居市场当中，如果抛开网络安全去发展智能家居，就像海市蜃楼，智能家居的发展走不了长远。

数据安全问题将是物联网时代的核心问题之一，但智能家居的安全不仅仅是一方的责任，亟待建立完善的治理机制。需要企业加大对智能家居信息安全及终端节点数据传输加密外等安全技术的投入研发，还需政府出台相关的政策法规，纳入诚信系统，与物联网的安全机制相结合，把强制性带入到物联网安全领域，建立有效的管控体系。智能家居的网络安全与智能化是一个整体属性，他们之间相互影响与促进，相互交流与配合，从而设计开发一个安全、可靠、全面的智能家居安全系统。

参考文献

[1]刘轶彤.物联网技术引领楼宇智能化工程技术专业发展[J].天津职业院校联合学报，2011(11).
[2]张益瑞.物联网智能家居安全性设计研究[J].通讯世界，2016(17).
[3]杨威，王宇建，吴永强.物联网设备身份认证安全性分[J].信息安全研究：2019(10).
[4]孙华.智能家居物联网安全性设计与实现[J].软件导刊，2015，14(7).
[5]段俊红，韩炼冰，房利国.智能家居系统的信息安全保密研究[J].通信技术，2016，49(10).

收稿日期：2020-02-14

作者简介：陈胜华（1979-），男，汉族，玉林人，高级工程师，本科，主要从事教育教学工作。

面向云计算的数据中心网络体系结构设计分析

黄 旭（中国电信股份有限公司天津分公司，天津 300385）

【摘 要】随着我国信息化领域的不断发展，云计算技术在新的时代背景下获得了长足的进步，此项技术已经广泛应用于社会的各个领域当中，并为计算机行业带来了巨大的发展突破。本文对现阶段的云计算技术的方式进行分析和总结，旨在帮助计算机行业的工作人员能够构建更加完善的数据中心。

【关键词】云计算 数据中心 网络体系
【中图分类号】TP308 【文献标识码】A 【文章编号】1006-4222（2020）04-0112-02

在 20 世纪当中，网络由多种服务器与客户端组建形成，数据中心存在的价值便在于将诸多在服务器当中产生的数据储存起来，随后再给予客户端相应的服务信息。但是，在近些年当中，由于互联网技术的快速的更新换代，全球都在致力于研究如何构建更加完善且智能化的数据中心。在这种科技浪潮的不断影响之下，各种新型的网络功能诞生了，人们可以实现利用网络执行各种经济方面的交易，还可以通过网络客户端了解到各种新闻信息等等。网络能够给人们更多形式的服务。由于云计算技术的不断革新和普及，互联网行业发展的速度更加迅猛，数据中心建设的工作也进展得更为顺利。

1 云计算技术的核心内涵

现阶段，在云计算技术的不断支持下，互联网能够根据用户的实际需要为其提供更加快捷便利的服务，服务的类型也趋于多样化。这种运营方式突破了传统单一信息的提供模式。数据中心在整个互联网体系中都占据着重要的地位，能够为云计算工作提供最为基本的运行条件。当前形势下，云计算技术能够实现的服务种类已经愈发丰富，人们通过网路获取信息的渠道更加多元化，读取信息的类型也趋于精细化。针对这种发展情况，数据中心便必须进行相应的调整，利用更加先进的手段来重新构建网络体系，将云计算技术的核心内涵加以更加深入的研究，挖掘其中更多的价值，尤其是信息传递功能需要加以更多的关注和完善，这是最基本的功能同时也是各种服务功能顺利应用的重要组成部分。只有将最基本的功能加以优化，各种更为复杂的服务技术才能实施得更加顺利。

2 利用云计算技术实现数据中心网络体系优化的主要原则

2.1 可扩展性

数字中心领域的网络体系的再次构建需要具有鲜明的可扩展性。从数据方面的角度来说，其中存在的扩展性能够在数据处理方式中得到充分体现，数据可以依靠这种特性得到具有保障的维护，也能够实现数据的更新。这样，云计算技术在为各种客户端提供各项服务的过程中便可实现对数据信息的更改。从网络系统的角度上来说，这种拓展性主要表现在维护

firewall (config)# inspect icmp
firewall (config)# service-policy testPolicy interface inside
firewall (config)#route outside 0.0.0.0 0.0.0.0 10.10.10.2 1

3.2 边界路由器 Router0 设置

（1）边界路由器 Router0 的两个端口及静态路由表设置。

```
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 10.10.10.2 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip address 201.1.1.1 255.255.255.0
Router(config-if)#exit
Router(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.1
```

（2）路由器动态 NAT 设置，针对来自内网（intranet）的 ip，路由器提供了 201.1.1.3-201.1.1.9 一共 7 个 IP 地址进行动态地址转换，将路由器 FastEthernet0/0 的端口定义为内网（intranet）端；interfaceFastEthernet1/0 定义为内网（intranet）端。

```
Router(config)#interface FastEthernet0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)#ip nat pool mypoolname 201.1.1.3 201.1.1.9 netmask 255.255.225.0
Router(config)#ip nat inside source list 1 pool mypoolname
```

4 验证与结论

完成上述设置后。可以操作 Pc0、Web serve、Server1 进行防火墙功能验证，结果为 Pc0 可访问 Web serve、Server1 的 web 服务，并且 ping 到这两服务器，反之则不可以。

参考文献

[1]张雪峰.信息安全概论[M].北京：人民邮电出版社，2014：129-131.
[2]汪双顶，武春岭，王津.网络互连技术理论篇[M].北京：人民邮电出版社，2017：267-268.

收稿日期：2020-03-09
作者简介：段文龙（1979-），男，汉族，四川金堂人，讲师，硕士研究生，研究方向为计算机网络、信息安全技术。