ISSN 1006－7167
CN 31－1707/T
实验室研究与探索
RESEARCH AND EXPLORATION IN LABORATORY
第37卷第4期 2018年4月
Vol. 37 No. 4 Apr. 2018

基于 eNSP 的安全园区网实验设计与构建

温 贺 平
(东莞职业技术学院 信息与教育技术中心，广东 东莞 523808)

摘 要：在网络设备国产化的政策背景下，提出了一种基于华为模拟软件 eNSP 的安全园区网的实验设计方案。通过 eNSP 部署防火墙、路由器及交换机等网络设备，划分出 Trust、Untrust 和 DMZ 3 个区域，利用 VLAN、路由、链路聚合、域间包过滤及 NAT 配置等技术，构建出了一个安全园区网的实验设计方案。给出了实验的关键配置方法，并通过 ping、Web、FTP 和 DNS 等进行功能验证。通过实验，学生不仅能理解安全组网的原理，而且可以掌握当今主流的华为网络设备的配置技术。

关键词：安全；校园网络；企业网络仿真平台；DMZ
中图分类号：TP 915 **文献标志码**：A
文章编号：1006－7167(2018)04－0126－04

Design and Construction of eNSP-based Security Campus Network Experiments

WEN Heping
(Department of Information and Technologe Center, Dongguan Polytechnic, Dongguan 523808, Guangdong, China)

Abstract: Under the national policy of network equipment localization, a secure campus network experimental design is proposed based on eNSP which is the simulation software of HUAWEI. The router and firewall, switch and other network equipment are deployed through eNSP, three areas including trust, untrust and DMZ are divided. By using VLAN, routing, link aggregation, packet filtering and NAT configuration technology, a security campus network experimental design is completed. The key configuration method of experiment is given and the results are verified by ping, web, ftp and DNS. Through the experiment, students can not only understand the principle of network security, but also grasp the current mainstream technology of HUAWEI network equipment configuration.

Key words: security; campus network; enterprise network simulation platform (eNSP); DMZ

0 引 言

在计算机网络、组网技术与网络管理等课程教学中，多采用 Cisco 的 Packet Tracer 模拟软件进行模拟上机实验[1]。自 2013 年斯诺登“棱镜门”事件以来，网络安全问题在国内各行业中引起了广泛的关注[2]。在国家信息安全相关政策的持续影响下，网络实验设备国产化势在必行[3]。然而，面对日新月异发展的网络技术，相关课程的教学实践面临一些新的问题，主要包括：① 受限于经费等条件约束，许多实验室难以采购昂贵的网络设备如防火墙为师生提供实验环境；② 实验设计方案多数是基于 Cisco packet tracer 平台，对外资设备具有依赖性；③ 基于国产网络设备的安全组网的实验设计较少，尤其是切合实际园区网环境的方案；④ 实验设计照抄陈年案例，缺乏创新性。因此，设计和构建基于国产网络设备模拟软件的安全组网实验方案[4-8]，此外，通过实验能够加深学生对安全组网原理的理解以及相关实践技能的掌握。

收稿日期：2017-06-15
基金项目：2014 年广东省科技计划项目(2014A040401079)；东莞职业技术学院科研基金(政 2017014)；东莞市职业技术教育发展研究会“十三五”规划课题(DZH1718012)
作者简介：温贺平(1984－)，男，广东梅州人，博士生，高级工程师，研究方向为网络技术与大数据安全。
Tel.：15818377943； E-mail: wenhp1019@163.com

1　安全园区网实验方案

1.1　实验目的

掌握安全园区网的关键配置方法,既包括组网中常见的虚拟局域网(Virtual Local Area Network, VLAN)、交换路由配置技术,还包括防火墙 Trust、Untrust 和 DMZ 区域划分、交换机链路聚合及 NAT 配置技术等。

1.2　模拟器(Enterprise Network Simulation Platform, eNSP)设备清单

实验在华为网络设备模拟器 eNSP 上实现。包括防火墙 USG5500 设备 1 台、路由器 1 台、华为 5700 三层交换机 1 台、3700 二层交换机 4 台、Server 服务器共 3 台、PC 共 3 台、Client 客户端共 4 个,直通线、交叉线和串口线若干。

1.3　实验总体设计

安全园区网的总体设计如图 1 所示。实验网络分为 Trust、Untrust 和 DMZ 3 个区域。其中,Trust 区域为内网区,包含 1 台核心交换机、3 台接入交换机以及 PC 和终端若干。内网区采用当今主流的“扁平化”结构,即只有核心层和接入层,没有汇聚层。Untrust 区域包含一台外网路由器和测试终端。DMZ 区域是本实验的难点的重点,配置了 Web、FTP 及 DNS 3 台服务器。

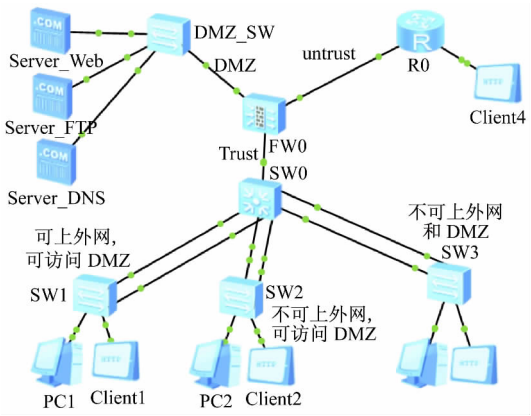

图 1　安全园区网的总体设计图

1.4　实验要求

对于 Trust 区域,在 SW0 下的交换机及各 PC 和终端可互连互通的基础上,有不同要求: ① SW1 区域可上外网,可访问 DMZ; ② SW2 区域不可上外网,可访问 dmz; ③ SW3 区域不可上外网,不可访问 DMZ; ④ SW0 与 SW1-SW3 3 台接入交换机配置链路聚合,实现负载均衡功能。

对于 Untrust 区域,有以下要求: ① 可以访问 Web 服务器,即公网地址的 80 端口对外开放; ② 可以访问 FTP 服务器,即公网地址的 21 端口对外开放; ③ DNS 服务器不对公网开放。即 Web 和 FTP 服务器采用 NAT 配置方法对外提供服务。

2　安全园区网实验设计与构建

2.1　实验网络逻辑规划

根据安全园区网实验总体设计及实验要求,防火墙 USG5500 的 3 个端口分别对应 Trust、Untrust 和 DMZ 3 个区域。在 Trust 区域规划 3 个 VLAN: vlan 10、vlan 20 和 vlan30 分别对应 SW1、SW2 和 SW3 3 台交换机。其中,vlan10 区域可上外网,可访问 DMZ; vlan20 区域不可上外网,可访问 DMZ; vlan30 区域不可上外网,不可访问 DMZ。在 SW0 上规划 vlan50 用于和 FW 进行通信。防火墙的 vlan100 对应 DMZ 区域的 3 台服务器。

实验中总共用到了 5 个公网的 IP 地址,202.1.1.1、202.1.1.2 分别用于出口防火墙 FW 和外网路由器 R0 的接口地址; 202.1.1.3-4 用于内网区 192.168.10.0/24 动态 NAT 的公网 IP 地址池; 202.1.1.5 用于 WEB 和 FTP 服务器的 NAT 端口地址映射。主要网络设备 IP 规划表及网络终端 IP 规划表如表 1、2 所示, NAT 映射表如表 3 所示。

表 1　主要网络设备 IP 规划表

设备	端口	IP 地址	业务描述
FW0	G0/0/2	192.168.50.2	Trust
	G0/0/3	172.16.1.1	DMZ
	S0/0/0	202.1.1.1	Untrust
R0	S0/0/0	202.1.1.2	Untrust
SW0	G0/0/0	192.168.50.1	Trust
	G0/0/11&21	192.168.10.1	链路聚合
	G0/0/12&22	192.168.20.1	链路聚合
	G0/0/13&23	192.168.30.1	链路聚合

表 2　网络终端 IP 规划表

设备	IP 地址	网关	vlan
PC1	192.168.10.2/24	192.168.10.1	10
Client1	192.168.10.3/24	192.168.10.1	10
PC2	192.168.20.2/24	192.168.20.1	20
Client2	192.168.20.3/24	192.168.20.1	20
PC3	192.168.30.2/24	192.168.30.1	30
Client3	192.168.30.3/24	192.168.30.1	30
Server_WEB	172.16.1.2/24	172.16.1.1	100
Server_FTP	172.16.1.3/24	172.16.1.1	100
Server_DNS	172.16.1.4/24	172.16.1.1	100
Client4	192.168.1.2/24	192.168.1.1	无

2.2　关键网络设备配置实现

防火墙的配置最关键,既是实验的重点也是难点。划分 Trust、Untrust 及 DMZ 区域以及 NAT 配置都是

表3 NAT映射表

公网IP	内网IP	备注
202.1.1.3-4	192.168.10.0/24	地址池
202.1.1.5:80	172.16.1.2:80	HTTP
202.1.1.5:21	172.16.1.3:21	FTP

在防火墙上进行配置。Trust区域的SW0实现局域网内的互连互通,外网路由器R0主要是模拟内网用户上网测试,及在外网测试NAT配置的可用性。

2.2.1 防火墙DMZ配置

划分Trust、Untrust和DMZ 3个区域,并将对应的接口加入相应的区域是实验配置中非常重要的一个步骤。主要配置代码如下:

```
[FW0-GigabitEthernet0/0/2] ip address 192.168.50.2 24
    //trust
[FW0-GigabitEthernet0/0/3] ip address 172.16.1.1 24
    //untrust
[FW0-Serial0/0/0] ip address 202.1.1.1 24 //dmz
[FW0] firewall zone trust
[FW0-zone-trust] add interface GigabitEthernet 0/0/2
[FW0] firewall zone dmz
[FW0-zone-dmz] add interface GigabitEthernet 0/0/3
[FW0] firewall zone untrust
[FW0-zone-untrust] add interface Serial0/0/0
```

接下来,配置域间包过滤,以满足网络安全访问的要求。值得指出的是防火墙的具有默认的包过滤配置。以USG5500为例,其默认包过滤规则为允许Local和Trust双向访问;允许Local访问DMZ及Untrust区域;其余访问默认均禁止。其中,Local是指防火墙本身的接口区域。因此,为了实现实验要求里的SW1区域可上外网,可访问DMZ;SW2区域不可上外网,可访问DMZ;SW3区域不可上外网,不可访问DMZ,关键配置代码如下:

```
//配置允许访问外网的IP段
policy interzone trust untrust outbound
policy 0
action permit
policy source 192.168.10.0 0.0.0.255
//配置允许访问dmz的IP段
policy interzone trust dmz outbound
policy 0
action permit
policy source 192.168.10.0 0.0.0.255
policy source 192.168.20.0 0.0.0.255
```

2.2.2 NAT配置

NAT配置包括内网IP访问公网和服务器对外开放端口两部分,均是在防火墙是进行配置实现。NAT配置关键代码及描述如下:

```
//创建NAT地址池1,地址范围为:202.1.1.3-202.1.1.4。
[FW0] nat address-group 1 202.1.1.3 202.1.1.4
//创建trust和untrust区域之间的NAT策略,确定进行NAT转换的源地址范围,并且将其与NAT地址池1进行绑定。
[FW0] nat-policy interzone trust untrust outbound
[FW0-nat-policy-interzone-trust-untrust-outbound] policy 0
[FW0-…-outbound-0] policy source 192.168.10.0 0.0.0.255
[FW0-…-outbound-0] action source-nat
[FW0-…-outbound-0] address-group 1
//创建两台内网服务器的公网IP与内网IP的映射关系。
[FW0] nat server protocol tcp global 202.1.1.5 www inside 172.16.1.2 80
[FW0] nat server protocol tcp global 202.1.1.5 ftp inside 172.16.1.3 21
```

2.2.3 链路聚合配置

3个接入交换机分别于SW0配置链路聚合功能,以提高网络的安全可靠性。以与SW1连接为例,SW0链路聚合配置如下:

```
interface Eth-Trunk1    //链路聚合标号1
port link-type trunk    //与SW1连接口属性一致
port trunk allow-pass vlan 10
interface GigabitEthernet0/0/11    //链路聚合捆绑g0/0/11
eth-trunk 1
interface GigabitEthernet0/0/21 //链路聚合捆绑g0/0/21
eth-trunk 1
```

其他两个交换机配置方法基本一致,只要修改对应的Eth-Trunk标号即可。

3 实验验证

3.1 链路聚合功能测试

网络测试一般采用“由近及远,由易到难”的测试步骤。因此,在基础配置完成的基础上,首先对链路聚合功能进行测试。通过测试SW0与SW1直接的互连互通性及查看SW0的链路聚合状态,如图2所示,容易验证配置的可行性。

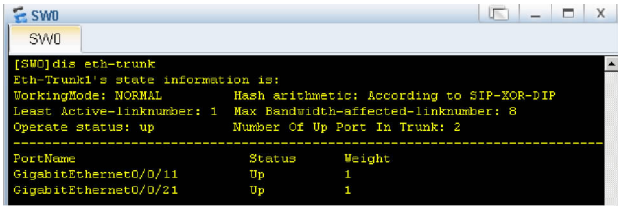

图2 SW0与SW1间链路聚合状态

3.2 内网访问外网和DMZ

用ping指令不难验证SW0下的3个交换机下的PC和终端不同的访问权限。此外,还可以通过PC和终端来验证DMZ中的服务器的功能。PC1访问外网的ping指令测试情况如图3所示。

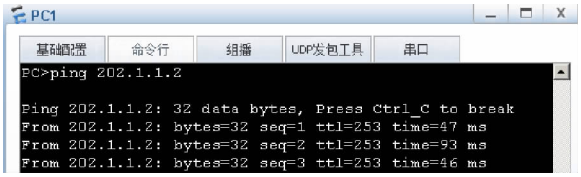

图 3　PC1 访问外网验证

根据实验要求,内网的 SW1 及 SW2 下的 PC 及终端应该能够访问 DMZ。利用 Client2 访问 FTP 的情况如图 4 所示。

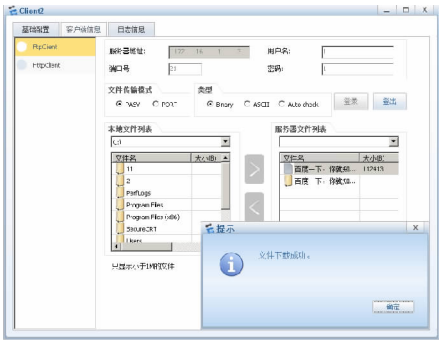

图 4　内网访问 FTP 验证

DNS 是 DMZ 中一个重要的服务。在 Server_DNS 上配置主机域名与 IP 地址对应的记录,然后在内网区的 PC 用 ping 主机域名,可验证能够正常解析 IP 地址。DNS 主机域名与 IP 地址配置信息及 Server_DNS 解析功能验证分别如图 5、6 所示。

图 5　DNS 主机域名与 IP 地址配置信息

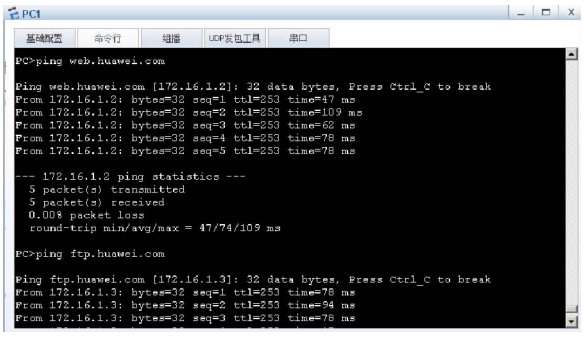

图 6　Server_DNS 解析功能验证

3.3　NAT 配置验证

服务器对外服务 NAT 映射验证可以通过在外网区域的 Client 终端进行功能测试的方法来完成。例如外网访问 Server_Web 的情况如图 7 所示,在外网 Client4 的浏览器中输入地址 http://202.1.1.5/default.htm 可以弹出对应的文件页面,验证了实验成功。

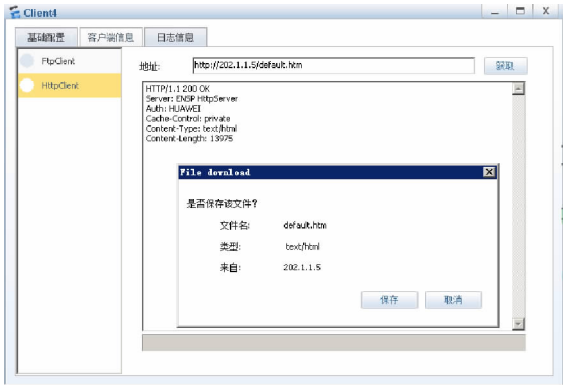

图 7　外网访问 Server_WEB 验证

4　结　语

基于华为模拟软件的 eNSP 的安全园区网实验设计综合运用了网络路由、链路聚合、域间包过滤及 NAT 配置等技术,对于辅助学生掌握安全网络的构建和配置方面具有较好的指导作用。同时,对提高学生在华为 HCNA、HCNP、HCIE 及信息安全工程师等新兴的认证考试的通过率方面能起到积极的作用。在此实验方案基础上,还可以进一步延伸和拓展实验内容。比如,可以结合 SecureCRT、VMWare、GNS3 等常用的网络软件构建更为综合的实验平台,根据不同场景定制设计更多丰富的实验方案,从而达到更好的教学效果。

参考文献(References):

[1] 田安红,付承彪. 静态路由协议在模拟仿真器中的设计与实现[J]. 实验技术与管理,2014(2):100-103.
[2] 陈左宁,王广益,胡苏太,等. 大数据安全与自主可控[J]. 科学通报,2015,(Z1):427-432.
[3] 黄建忠,张沪寅,裴嘉欣. 网络安全虚拟仿真实验教学体系设计[J]. 实验室研究与探索,2016(10):170-174.
[4] 陈　潮,靳慧云,黄安安. VLAN 间路由实验在仿真器中的设计与实现[J]. 实验技术与管理,2016(8):129-132.
[5] 孟祥成. 基于 eNSP 的防火墙仿真实验[J]. 实验室研究与探索,2016(4):95-100.
[6] 鲁先志,胡海波. 基于开源架构的虚拟网络安全实验平台[J]. 实验技术与管理,2015(7):120-123,155.
[7] 李　永. 基于 Packet Tracer 的路由综合实验设计与实现[J]. 实验室研究与探索,2015(9):111-114.
[8] 温贺平,曹文梁,刘　庆. 一种模拟校园网的综合组网实验设计[J]. 实验室研究与探索,2017(2):141-144.
[9] 施　游. 网络规划设计师考试全程指导[M]. 北京: 清华大学出版社,2009.
[10] 褚建立. 中小型网络组建[M]. 北京: 中国铁道出版社,2010.
[11] 李林林. 单机环境下路由交换技术综合实验设计[J]. 实验室研究与探索,2015(8):115-118.

(下转第 169 页)

进行,以便能够对完整的课程进行评价。但实验课没有考试,要求学生在期末考试紧张的阶段再次来到教室完成问卷调查是不现实的。在理论课上完成问卷的方式也不可取,首先会影响理论课教学,其次理论课教学实际上不能保证出勤率,反而是实验课可以全部出勤。因此实验课的问卷调查在最后一次实验课上进行,这也使得问卷回收率较高,达到 96%。但这种方式也有一定的问题。① 由于最后一次安排的是选做实验,同时进行的实验种类较多,教师的工作比较紧张忙乱,无法集中督促回收问卷,这是回收率不能达到 100% 的原因之一。② 学生选择的实验难度不同,有的实验难度较高,过程比较紧张,学生没有时间认真填写问卷,这会影响调查的质量。

另一个问题是问卷的统计工作量较大,需要教师阅读每一张问卷并记录结果。这个过程除了花费时间外,还有可能造成错误,而一旦发生某个数据统计错误的情况,很难找到发生的位置,或者再花费时间重新统计,或者寄希望于一两个错误不至于影响结论。此外,问卷属于课堂外的内容,虽然可以给学生一个对课程“吐槽”的机会,但是并没有实质的益处,而是对今后选课的同学有益。对于参加这类义务活动,应该给予一定程度的奖励。但目前的问卷使用匿名方式,不能知道哪位同学参加,只能整体加分进行鼓励。这实际上对于认真填写问卷的同学并不公平。

解决问题的一个思路是将最后一次课改为讨论,这样能够避免课上内容不同造成的紧张度差异,但并不能解决更多问题。更好的解决方案是使用网络进行问卷调查。当前互联网技术飞速发展,而通过网络进行问卷调查的思路早就有过报道[5-6]。现在已经可以找到免费进行问卷调查的网站,这种方式可以解决上述问题。首先能够在任意时刻任意位置进行,不必局限于课上,可以确保不影响正常学习。其次结果能够方便的统计,并且保证准确性,统计方式的种类也远多于人工操作。最后可以给每个参加的学生生成特征码,以此获得加分等奖励,既可以保证匿名,又可以准确鼓励,是非常适用的方式。从 2017 年开始,问卷调查将采用网络方式进行,我们会总结经验教训,进一步完善问卷调查的方式,更好的服务于教学工作。

4　结　语

我校生理学实验课进行的长期问卷调查表明,这是一种有效的收集课程反馈信息的方式。不同于学生评教,这种问卷调查能够更精细的了解上课过程的不足和优势,可以进一步扬长避短,准确的改进缺点。实践过程也证明了确实可以找到需要改进的位置,而有效的改变也确实能够在今后的调查中得到正面的回应。这是一个有益的正反馈过程,可以为教学改革指出正确的方向,并提供强大的动力。因此,应该继续坚持进行并完善问卷调查,在教学活动中发挥更大的作用。

参考文献(References):

[1] 张海英,谢丽媛,薛　洁. 学生对教师课堂教学质量的调查问卷分析 [J]. 中国中医药现代远程教育,2010,8(16) : 10-11.

[2] 练彩霞,辜夕容,刘亚敏,等. 本科课堂教学质量学生满意度实证研究——以重庆市某全国重点综合性大学为例 [J]. 教育教学论坛,2015(3) : 54-56.

[3] 吕　欣,张晓妮. 从调查问卷看分子生物学课程教学 [J]. 高教论坛,2013(3) : 69-72.

[4] 孙玉红,蓝　天. 基于调查问卷的国际经济学课程教学现状分宜与对策——以东北财经大学为例 [J]. 对外经贸,2012 (2) : 136-139.

[5] 米子川. 网络调查问卷的生成与数据反馈 [J]. 山西财经大学学报,2001,23(1) : 99-100.

[6] 黄　璐,王爱云,杨　梅. 关于网络调查问卷设计的分析 [J]. 山东师范大学学报(自然科学版) ,2011,26(1) : 13-16.

(上接第 129 页)

[12] 吴　迪,薛政,潘　嵘. 基于 XEN 云平台的网络安全实验教学 [J]. 实验室研究与探索,2013(7) : 62-66.

[13] 徐功文, 刘文学, 张志军,等. 基于 GNS3 模拟器的 BGP 仿真实验的设计与实现 [J]. 实验室科学, 2012, 15(6) : 108-111.

[14] 杨　敏. 基于 Packet Tracer 的 OSPF 仿真实验 [J]. 网络安全技术与应用,2016(2) : 83-84.

[15] 谭　娟,黄　永. 利用 gns3 + ensp 组建高校网络仿真实验室 [J]. 硅谷,2013,6(20) : 154,159.

·名人名言·

教师之为教,不在全盘授予,而在相机诱导。

——叶圣陶