**五邑大学**

**智能制造学部**



**网络安全课程设计**报告

**题 目：基于eNSP的网络安全环境设计与实现**

**专 业**：通信工程（计算机网络）

**班 级**：160805

**学 号**：3116001779

**姓 名**：陈淦

**指导教师**：　　　　　　　刘耀宗

**起止日期**：2019年4月23日 至2019年6月11日

递交的材料清单：

1. 源代码一份(小于10M)
2. 软件设计报告一份(word)

**指导教师审阅意见及成绩评定：**

指导老师签章：

日期：年 月 日

**基于eNSP的网络安全环境设计与实现**

1. **需求分析**

**1. 对处于不同两地的总公司和分公司利用公网进行安全通信**

**2. 内网用户可以访问公网数据**

**3. 使用相关安全机制保证公司内网网络安全**

1. **功能介绍**

**1. 使用IPSec 实现VPN功能，使得分隔两地的公司使用公网进行通信，另外IPSec也保证了数据在传输过程中的安全性**

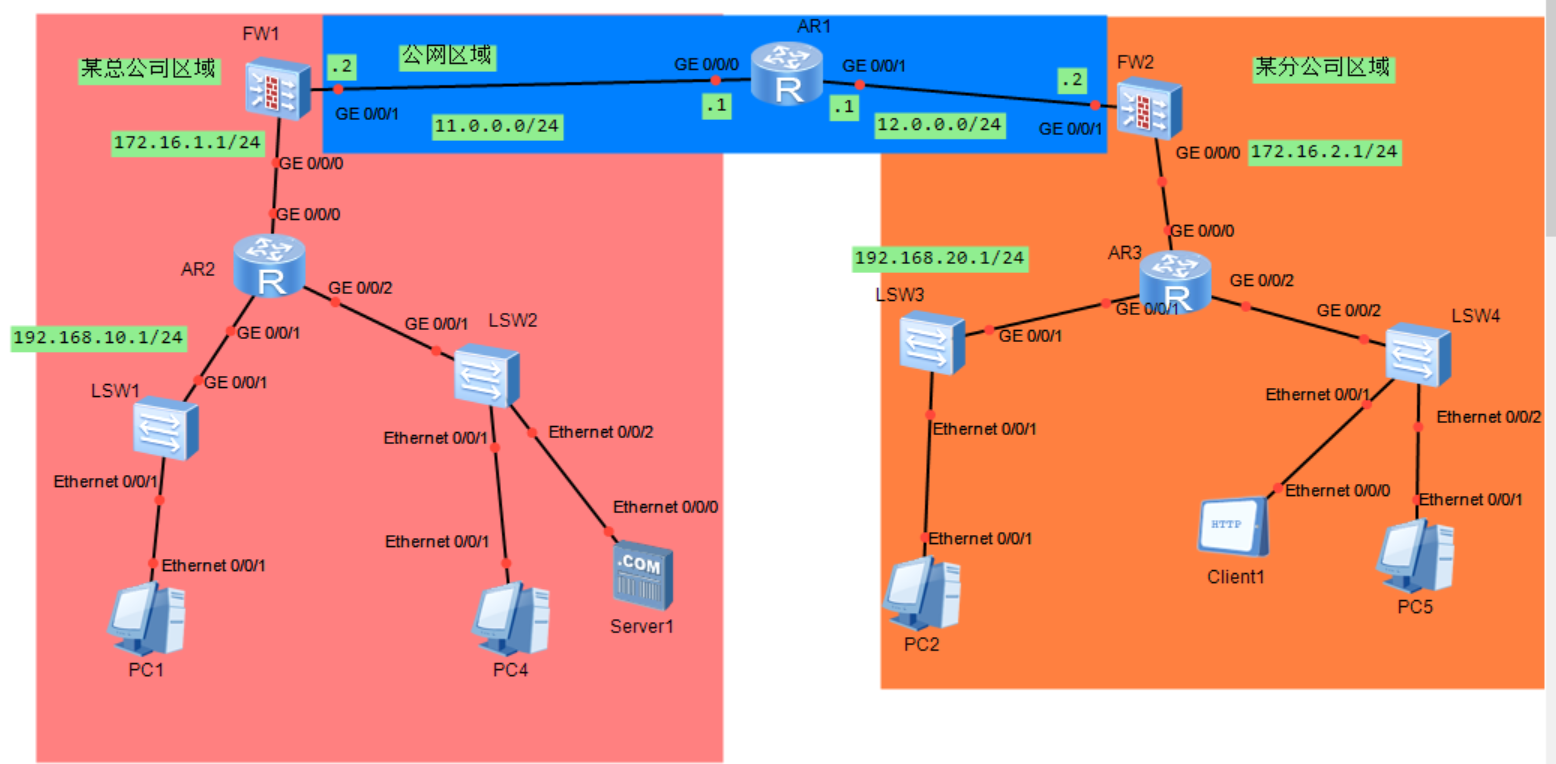
**2. 通过NAT技术实现了仅利用少量的公网IP就可以对公网进行访问传输数据的需求**

**3. 在保证对公网访问的前提下，还要对尽心VPN连接的设备做特殊的NAT穿越配置，保证即使数据包在加密的情况下也能准确无误的送达目的地，实现总部PC1与分公司的PC2之间安全通信**

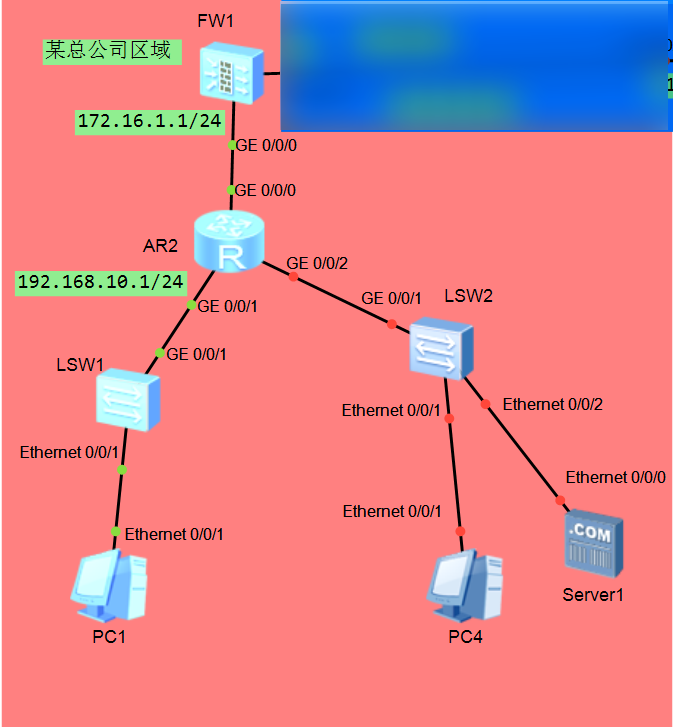
**4. 在边境路由的位置放置防火墙对内网环境进行保护**

1. **运行截图**

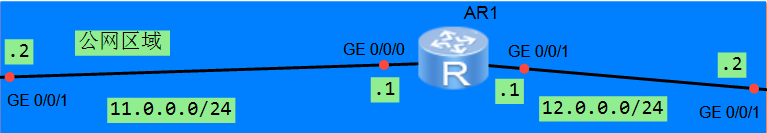
**总体拓扑图**



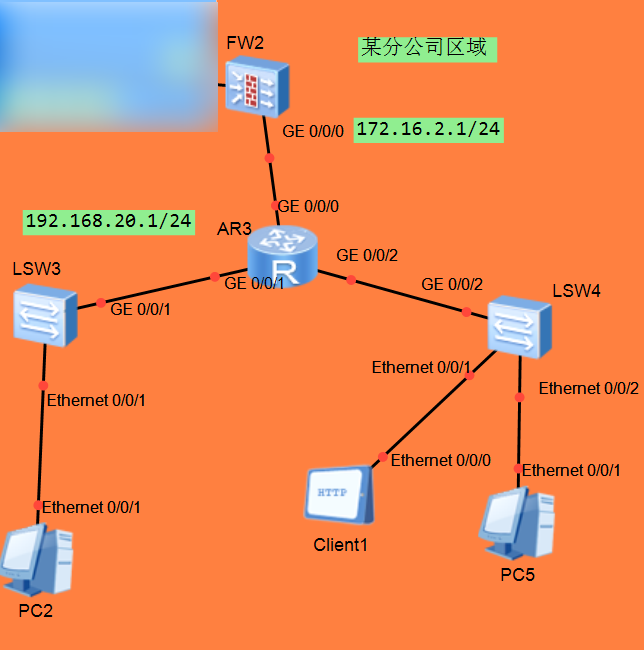
**总部区域详细图**



**公网环境详细图**



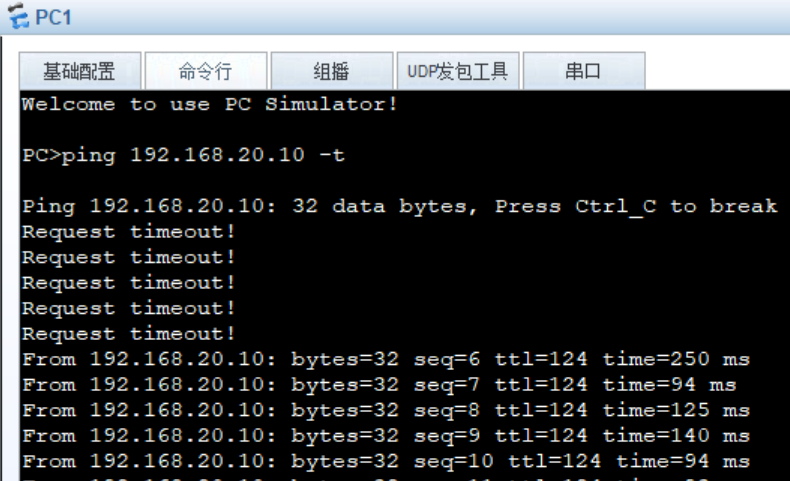
**分公司环境详细图**



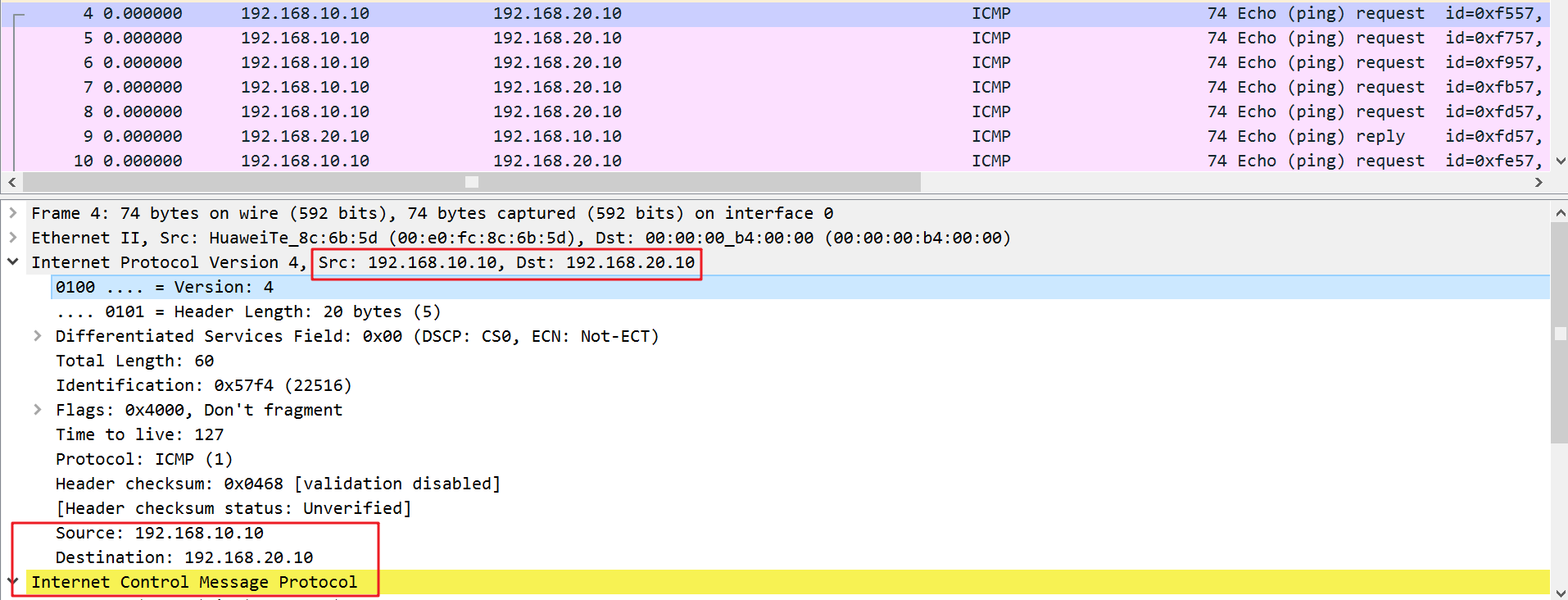
**实验模拟及抓包示意图**

**现在从PC1发出Ping命令，对防火墙FW2的GE 0/0/1接口和GE 0/0/0接口，防火墙FW1的GE 0/0/0接口进行抓包查看**

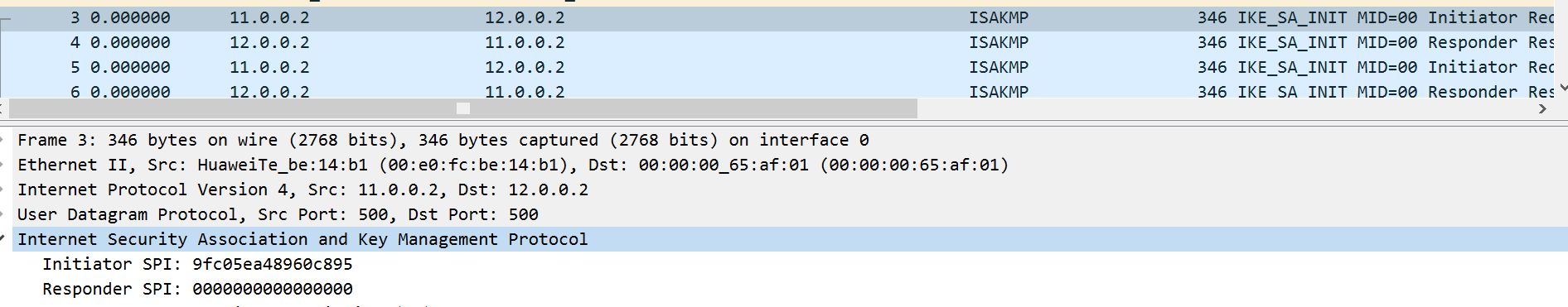
**PC1 发出Ping命令**

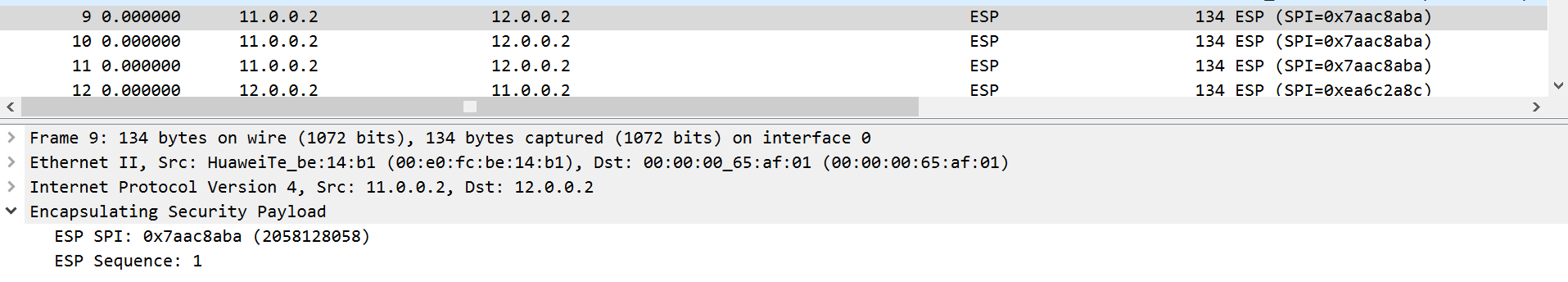


**FW1 G0/0/0接口抓包**

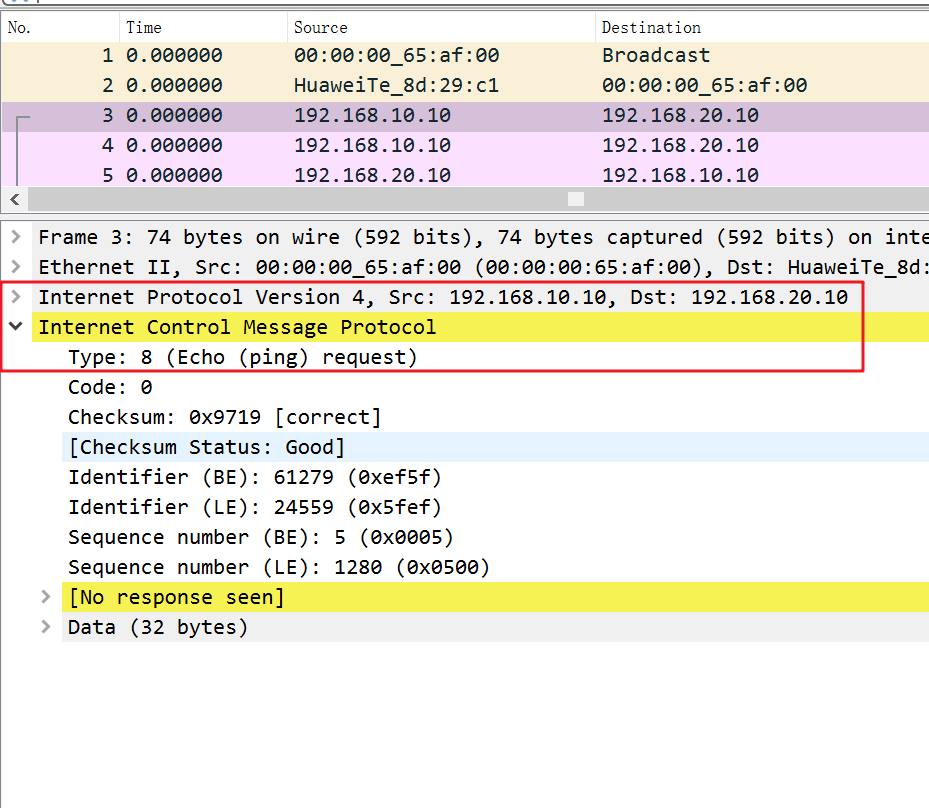


**FW2 GE0/0/1接口抓包**





**FW2 GE0/0/0接口抓包**



1. **完成情况**

**完成基本的连接以及安全要求**

1. **调试中遇到的问题及解决办法**

**在课程设计完成的过程中遇到了许多问题，比如对eNSP模拟器的不熟悉，对设备命令的不熟悉。只能通过一些互联网资料边学习边熟悉那些不懂的知识点**

1. **核心配置文件**

**FW1**

<FW1>dis current-configuration

16:56:36 2019/06/14

#

stp region-configuration

region-name c0a5b2154006

active region-configuration

#

acl number 3001

rule 5 permit ip source 192.168.10.0 0.0.0.255 destination 192.168.20.0 0.0.0.2

55

#

ike proposal 1

encryption-algorithm aes-cbc

dh group2

#

ike peer a

pre-shared-key %$%$fmvjS.fp(&Fmi5;<9Uk0Y[RI%$%$

ike-proposal 1

remote-address 12.0.0.2

#

ipsec proposal tran1

esp authentication-algorithm sha1

esp encryption-algorithm aes

#

ipsec policy map1 10 isakmp

security acl 3001

ike-peer a

proposal tran1

#

interface GigabitEthernet0/0/0

alias GE0/MGMT

ip address 172.16.1.1 255.255.255.0

#

interface GigabitEthernet0/0/1

ip address 11.0.0.2 255.255.255.0

ipsec policy map1

#

interface GigabitEthernet0/0/2

#

interface GigabitEthernet0/0/3

#

interface GigabitEthernet0/0/4

#

interface GigabitEthernet0/0/5

#

interface GigabitEthernet0/0/6

#

interface GigabitEthernet0/0/7

#

interface GigabitEthernet0/0/8

#

interface NULL0

alias NULL0

#

firewall zone local

set priority 100

#

firewall zone trust

set priority 85

add interface GigabitEthernet0/0/0

#

firewall zone untrust

set priority 5

add interface GigabitEthernet0/0/1

#

firewall zone dmz

set priority 50

#

aaa

local-user admin password cipher %$%$XwO|${|^y\*tG-g&j.~)RX;2)%$%$

local-user admin service-type web terminal telnet

local-user admin level 15

authentication-scheme default

#

authorization-scheme default

#

accounting-scheme default

#

domain default

#

#

nqa-jitter tag-version 1

#

ip route-static 0.0.0.0 0.0.0.0 11.0.0.1

ip route-static 192.168.10.0 255.255.255.0 172.16.1.2

#

banner enable

#

user-interface con 0

authentication-mode none

user-interface vty 0 4

authentication-mode none

protocol inbound all

#

slb

#

right-manager server-group

#

sysname FW1

#

l2tp domain suffix-separator @

#

firewall packet-filter default permit interzone local trust direction inbound

firewall packet-filter default permit interzone local trust direction outbound

firewall packet-filter default permit interzone local untrust direction outboun

d

firewall packet-filter default permit interzone local dmz direction outbound

#

ip df-unreachables enable

#

firewall ipv6 session link-state check

firewall ipv6 statistic system enable

#

dns resolve

#

firewall statistic system enable

#

pki ocsp response cache refresh interval 0

pki ocsp response cache number 0

#

undo dns proxy

#

license-server domain lic.huawei.com

#

web-manager enable

#

policy interzone local untrust inbound

policy 0

action permit

policy source 12.0.0.2 0

#

policy interzone trust untrust inbound

policy 1

action permit

policy source 192.168.20.0 mask 24

policy destination 192.168.10.0 mask 24

#

policy interzone trust untrust outbound

policy 1

action permit

policy source 192.168.10.0 mask 24

#

nat-policy interzone trust untrust outbound

policy 0

action no-nat

policy destination 192.168.20.0 mask 24

policy 1

action source-nat

policy source 192.168.10.0 mask 24

easy-ip GigabitEthernet0/0/1

#

Return

FW2

<FW2>dis current-configuration

16:57:54 2019/06/14

#

stp region-configuration

region-name 90144e151075

active region-configuration

#

acl number 3001

rule 5 permit ip source 192.168.20.0 0.0.0.255 destination 192.168.10.0 0.0.0.2

55

#

ike proposal 1

encryption-algorithm aes-cbc

dh group2

#

ike peer a

pre-shared-key %$%$wzJ"T~~d3Sf#S\*UxW[ZSY!ul%$%$

remote-address 11.0.0.2

#

ipsec proposal tranl

esp authentication-algorithm sha1

esp encryption-algorithm aes

#

ipsec policy map1 10 isakmp

security acl 3001

ike-peer a

proposal tranl

#

interface GigabitEthernet0/0/0

alias GE0/MGMT

ip address 172.16.2.1 255.255.255.0

#

interface GigabitEthernet0/0/1

ip address 12.0.0.2 255.255.255.0

ipsec policy map1

#

interface GigabitEthernet0/0/2

#

interface GigabitEthernet0/0/3

#

interface GigabitEthernet0/0/4

#

interface GigabitEthernet0/0/5

#

interface GigabitEthernet0/0/6

#

interface GigabitEthernet0/0/7

#

interface GigabitEthernet0/0/8

#

interface NULL0

alias NULL0

#

firewall zone local

set priority 100

#

firewall zone trust

set priority 85

add interface GigabitEthernet0/0/0

#

firewall zone untrust

set priority 5

add interface GigabitEthernet0/0/1

#

firewall zone dmz

set priority 50

#

aaa

local-user admin password cipher %$%$4.-rHmyxT5EG&4$VoCu\*XVMD%$%$

local-user admin service-type web terminal telnet

local-user admin level 15

authentication-scheme default

#

authorization-scheme default

#

accounting-scheme default

#

domain default

#

#

nqa-jitter tag-version 1

#

ip route-static 0.0.0.0 0.0.0.0 12.0.0.1

ip route-static 192.168.20.0 255.255.255.0 172.16.2.2

#

banner enable

#

user-interface con 0

authentication-mode none

user-interface vty 0 4

authentication-mode none

protocol inbound all

#

slb

#

right-manager server-group

#

sysname FW2

#

l2tp domain suffix-separator @

#

firewall packet-filter default permit interzone local trust direction inbound

firewall packet-filter default permit interzone local trust direction outbound

firewall packet-filter default permit interzone local untrust direction outboun

d

firewall packet-filter default permit interzone local dmz direction outbound

#

ip df-unreachables enable

#

firewall ipv6 session link-state check

firewall ipv6 statistic system enable

#

dns resolve

#

firewall statistic system enable

#

pki ocsp response cache refresh interval 0

pki ocsp response cache number 0

#

undo dns proxy

#

license-server domain lic.huawei.com

#

web-manager enable

#

policy interzone local untrust inbound

policy 1

action permit

policy source 11.0.0.2 0

#

policy interzone trust untrust inbound

policy 1

action permit

policy source 192.168.10.0 mask 24

policy destination 192.168.20.0 mask 24

#

policy interzone trust untrust outbound

policy 1

action permit

policy source 192.168.20.0 mask 24

1. **课程学习体会**

历时一个多月的网络安全课程结束了,在这一个多月中,通过多个不同的实验项目,对信息安全的实践操作和重要性又有了深一步的了解。当今社会是一个高科技的信息化社会,信息的传播方式在不断的改进,由人工传递到有线网络的传递,由有线网络到无线网络的传递,随着网络日益成为各行各业快速发展的必要手段和工具,网络的安全重要性是毋庸置疑的。

网络作为当前社会传输信息的一种重要工具和手段。其网络的安全性从本质上来讲,就是网络上的信息安全,就是指网络系统中流动和保存的数据,不受到偶然的或者恶意的破坏、泄露、系统连续正常的工作,网络服务不中断,让信息正确、完整、通畅的传输到指定的位置。从广义上来说,凡是涉及到网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全所要研究的领域,因此,通过实验来让我们了解信息安全的过程是尤为重要的。

在这次的课程设计中,我们的实验循序渐进。从信息安全的基础操作开始,先了解了信息安全中的密码算法,包括对对称密码算法,非对称密码算法, HASH算法,数字签名算法,信息隐藏算法的认知和其原理的掌握,这些都是信息安全的基础,对做好信息安全意义重大。