WEB SECURITY CONFIGURATION EXPERIENCE

网络安全设备配置与管理实验

2021/6/25

www.kloudy.cn

Version 1.0

Preface

Kloudy Grasp: Web Security Configuration Experience
网络安全设备配置与管理实验

1. 说明

Kloudy Grasp: Web Security Configuration Experience 非官方资料，仅为个人学习笔记，不具有权威性。不做任何商业目的，仅供学习交流使用。

2. 版权声明

3. Kloudy Grasp 重要度标识

★ 非常重要
▲ 重要
一般
▽ 不重要
○ 不要求

4. 其他考试说明

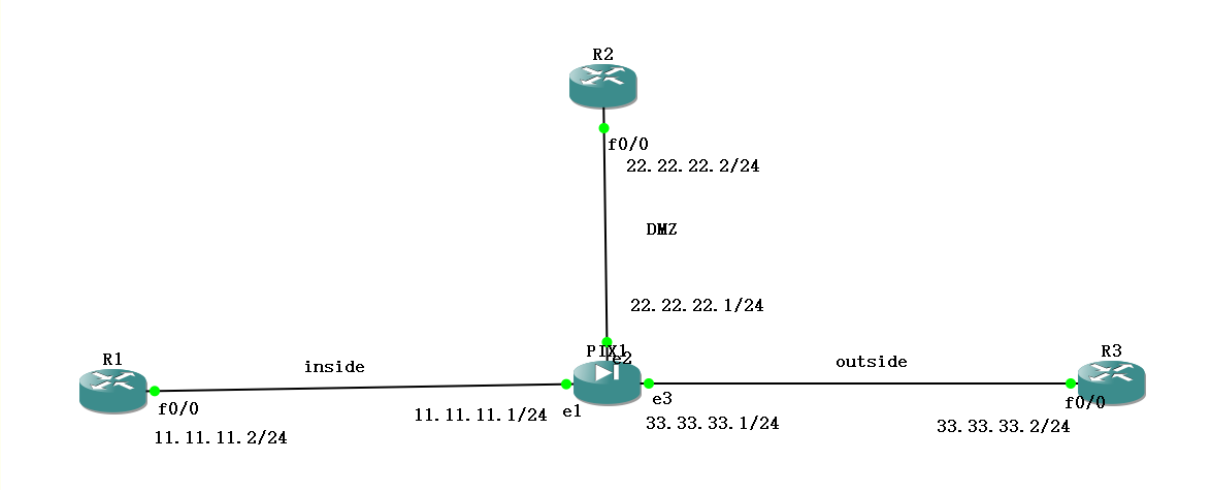
开卷考试，只有一道大型配置题，具体内容是五次实验的内容

Content

Web Security Configuration Experience

1 基本配置

5. 实验拓扑



6. 配置路由器 IP 地址和默认路由

进入配置模式

选择接口

R1(config)#int f0/0

为接口分配 IP 地址

R1(config-if)#ip add 11.11.11.2 255.255.255.0

打开接口

R1(config-if)#no sh

配置默认路由

R1(config)#ip route 0.0.0.0 0.0.0.0 11.11.11.1

在 R2、R3 重复上面步骤

R1

```
Connected to Dynamips VM "R1" (ID 4, type c3600) - Console port
Press ENTER to get the prompt.

R1#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int f0/0
R1(config-if)#ip add 11.11.11.2 255.255.255.0
R1(config-if)#no sh
R1(config-if)#exit
R1(config)#
00:00:48: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
00:00:49: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config)#exit
R1#w
00:00:52: %SYS-5-CONFIG_I: Configured from console by console
R1#wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R1#
```

```
R1(config)#ip route 0.0.0.0 0.0.0.0 11.11.11.1
```

R2

```
Connected to Dynamips VM "R2" (ID 5, type c3600) - Console port
Press ENTER to get the prompt.

R2#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int f0/0
R2(config-if)#ip add 22.22.22.2 255.255.255.0
R2(config-if)#no sh
R2(config-if)#en
00:01:41: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
00:01:42: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R2(config-if)#end
R2#
00:01:44: %SYS-5-CONFIG_I: Configured from console by console
R2#wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R2#
```

```
R2(config)#ip route 0.0.0.0 0.0.0.0 22.22.22.1
```

R3

```
Connected to Dynamips VM "R3" (ID 6, type c3600) - Console port
Press ENTER to get the prompt.

R3#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int f0/0
R3(config-if)#ip add 33.33.33.2 255.255.255.0
R3(config-if)#no sh
R3(config-if)#
00:02:29: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
00:02:30: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R3(config-if)#end
R3#w
00:02:32: %SYS-5-CONFIG_I: Configured from console by console
R3#wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R3#
```

```
R3(config)#ip route 0.0.0.0 0.0.0.0 33.33.33.1
```

7. 配置路由器 telnet

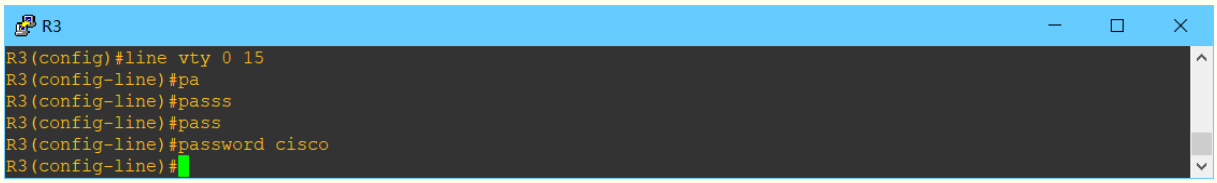
连接线路为 0 到 15

R2(config)#line vty 0 15

telnet 密码为 cisco

R2(config-line)#password cisco

在 R3 上重复上面步骤



8. 配置防火墙接口 IP 和名称

进入配置模式

选接口

pixfirewall(config)# int e1

为接口分配 IP 地址

pixfirewall(config-if)# ip add 11.11.11.1 255.255.255.0

打开接口

pixfirewall(config-if)# no sh

命名接口

pixfirewall(config-if)# nameif inside

为接口设置安全级别

pixfirewall(config-if)# security-level 100

PIX1

```
pixfirewall> en
Password:
pixfirewall# conf t
pixfirewall(config)# int e1
pixfirewall(config-if)# ip add 11.11.11.1 255.255.255.0
pixfirewall(config-if)# no sh
pixfirewall(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
pixfirewall(config-if)# se
pixfirewall(config-if)# sec
pixfirewall(config-if)# security-level 100
pixfirewall(config-if)# int e2
pixfirewall(config-if)# ip add 22.22.22.1 255.255.255.0
pixfirewall(config-if)# no sh
pixfirewall(config-if)# nam
pixfirewall(config-if)# namei
pixfirewall(config-if)# nameif
pixfirewall(config-if)# nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
pixfirewall(config-if)# sec
pixfirewall(config-if)# security-level 50
pixfirewall(config-if)# int e3
pixfirewall(config-if)# ip add 33.33.33.1 255.255.255.0
pixfirewall(config-if)# no sh
pixfirewall(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
pixfirewall(config-if)# sec
pixfirewall(config-if)# security-level 0
pixfirewall(config-if)# exit
pixfirewall(config)# exit
pixfirewall# we
             ^
ERROR: % Invalid input detected at '^' marker.
pixfirewall# wr
Building configuration...
Cryptochecksum: 339e8950 0511b072 97d3450c 4763e343

1278 bytes copied in 0.480 secs
[OK]
pixfirewall#
```

9. 配置防火墙默认路由

所有发送到外部的消息的下一跳都是 33.33.33.2

pixfirewall(config)# route outside 0 0 33.33.33.2

```
pixfirewall(config)# route outside 0 0 33.33.33.2
pixfirewall(config)#
```

10. 验证配置：防火墙可以 ping 通三个直连接口

```
pixfirewall# ping 11.11.11.2
Sending 5, 100-byte ICMP Echos to 11.11.11.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/16/40 ms
pixfirewall# ping 22.22.22.2
Sending 5, 100-byte ICMP Echos to 22.22.22.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/22/50 ms
pixfirewall# ping 33.33.33.2
Sending 5, 100-byte ICMP Echos to 33.33.33.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/20/50 ms
```

11. 配置防火墙本地主机和全局地址池

允许所有的内部主机（R1）向外进行连接访问

pixfirewall(config)# nat (inside) 1 0 0

定义源地址将要翻译成的地址或地址范围（R2、R3）

pixfirewall(config)# global (outside) 1 33.33.33.10-33.33.33.20 netmask 255.255.255.0

pixfirewall(config)# global (DMZ) 1 22.22.22.10-22.22.22.20 netmask 255.255.255.0

```
pixfirewall(config)# nat (inside) 1 0 0
```

```
pixfirewall(config)# global (outside) 1 33.33.33.10-33.33.33.20 ne
pixfirewall(config)# global (outside) 1 33.33.33.10-33.33.33.20 netmask 255.25$
pixfirewall(config)# global (DMZ) 1 22.22.22.10-22.22.22.20 net
pixfirewall(config)# global (DMZ) 1 22.22.22.10-22.22.22.20 netmask 255.255.25$
pixfirewall(config)#
```

12. 验证配置：R1（内网）可以 telnet 到 R3（外网）、R2（DMZ）

R1

```
R1#telnet 33.33.33.2
Trying 33.33.33.2 ... Open


User Access Verification

Password:
R3>
```

R1

```
R1#telnet 22.22.22.2
Trying 22.22.22.2 ... Open


User Access Verification

Password:
R2>
```

13. 查看防火墙翻译 show xlate

PIX1

```
pixfirewall# show xlate
2 in use, 2 most used
Global 22.22.22.10 Local 11.11.11.2
Global 33.33.33.10 Local 11.11.11.2
pixfirewall#
```

14. 配置 R2 从 DMZ 到外网的静态地址翻译

pixfirewall(config)# static (DMZ,outside) 33.33.33.3 22.22.22.2 netmask **255.255.255.255**

PIX1

```
pixfirewall(config)# static (DMZ,outside) 33.33.33.3 22.22.22.2 netmask 255.25$
pixfirewall(config)#
```

15. 配置访问控制列表

创建访问控制列表 110，允许任何源到任何目的的 icmp 和 tcp 报文

pixfirewall(config)# access-list 110 permit icmp any any

pixfirewall(config)# access-list 110 permit tcp any any

将访问控制列表应用于接口

pixfirewall(config)# access-group 110 in interface outside

pixfirewall(config)# access-group 110 in interface DMZ

PIX1

```
pixfirewall(config)#
pixfirewall(config)# acc
pixfirewall(config)# access-l
pixfirewall(config)# access-list 110 per
pixfirewall(config)# access-list 110 permit icm
pixfirewall(config)# access-list 110 permit icmp any any
pixfirewall(config)# acc
pixfirewall(config)# access-l
pixfirewall(config)# access-list 110 per
pixfirewall(config)# access-list 110 permit tc
pixfirewall(config)# access-list 110 permit tcp any any
pixfirewall(config)# acc
pixfirewall(config)# access-g
pixfirewall(config)# access-group 110 in
pixfirewall(config)# access-group 110 in in
pixfirewall(config)# access-group 110 in interface outside
pixfirewall(config)# access-group 110 in interface DMZ
pixfirewall(config)#
```

16. 验证配置：从 R3（外网）可以 telnet 到 R2（DMZ）（使用翻译过的外网 IP 地址）

R3

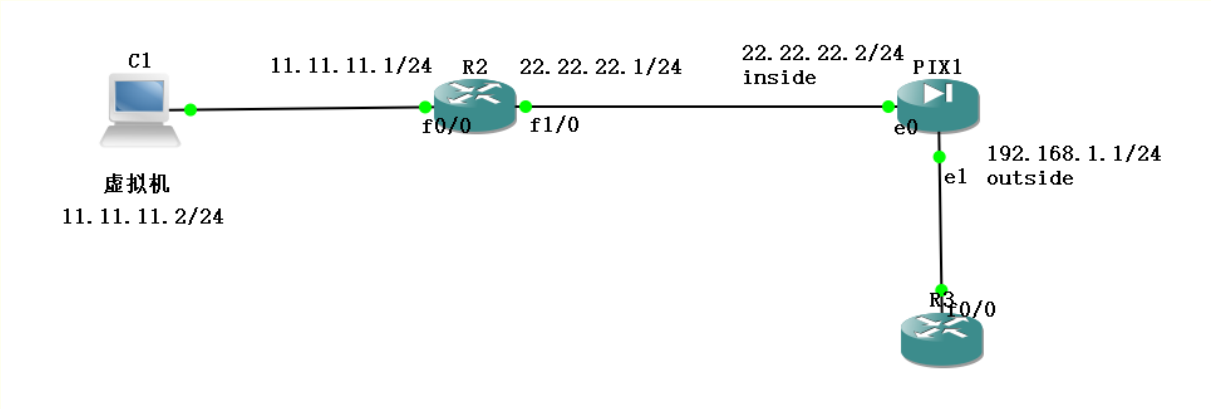
```
R3#telnet 33.33.33.3
Trying 33.33.33.3 ... Open


User Access Verification

Password:
R2>
```

2 日志服务器配置

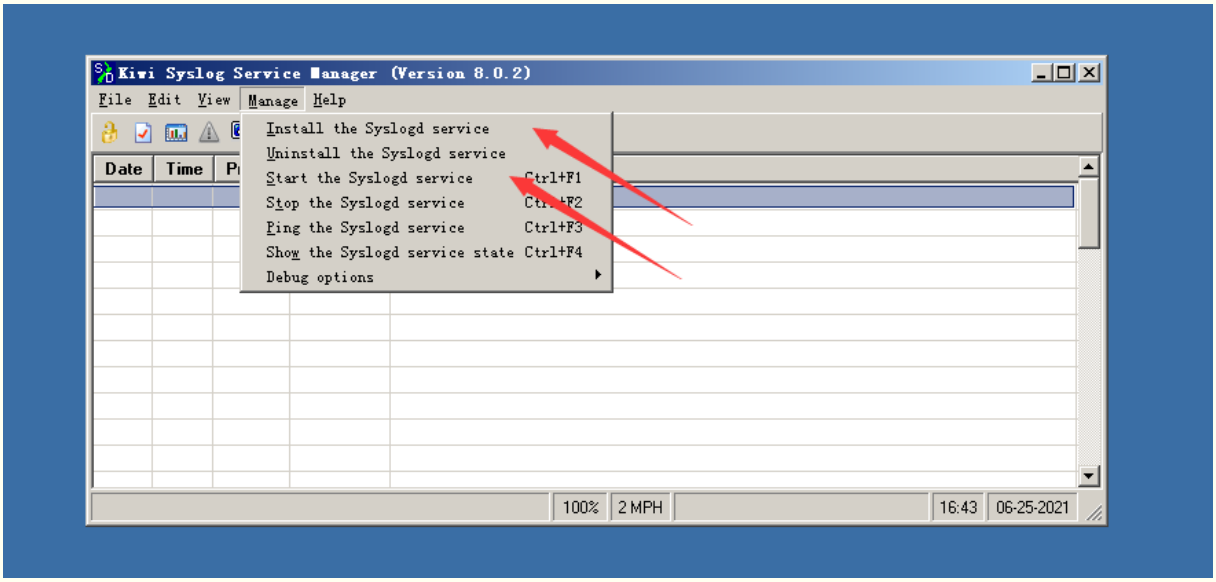
17. 实验拓扑



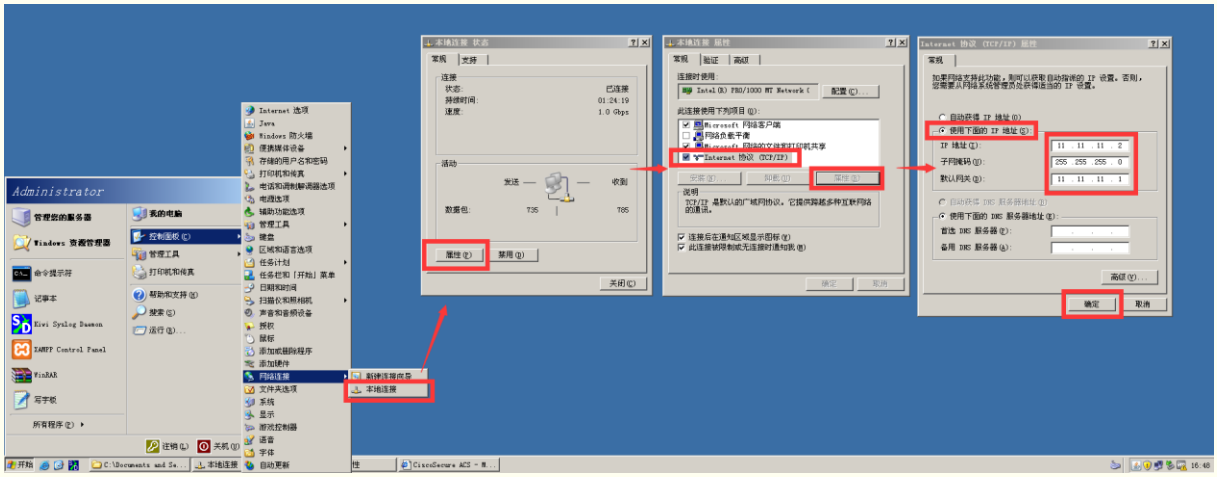
18. 在虚拟机安装日志软件

需要服务器系统，比如 Windows Server 2003

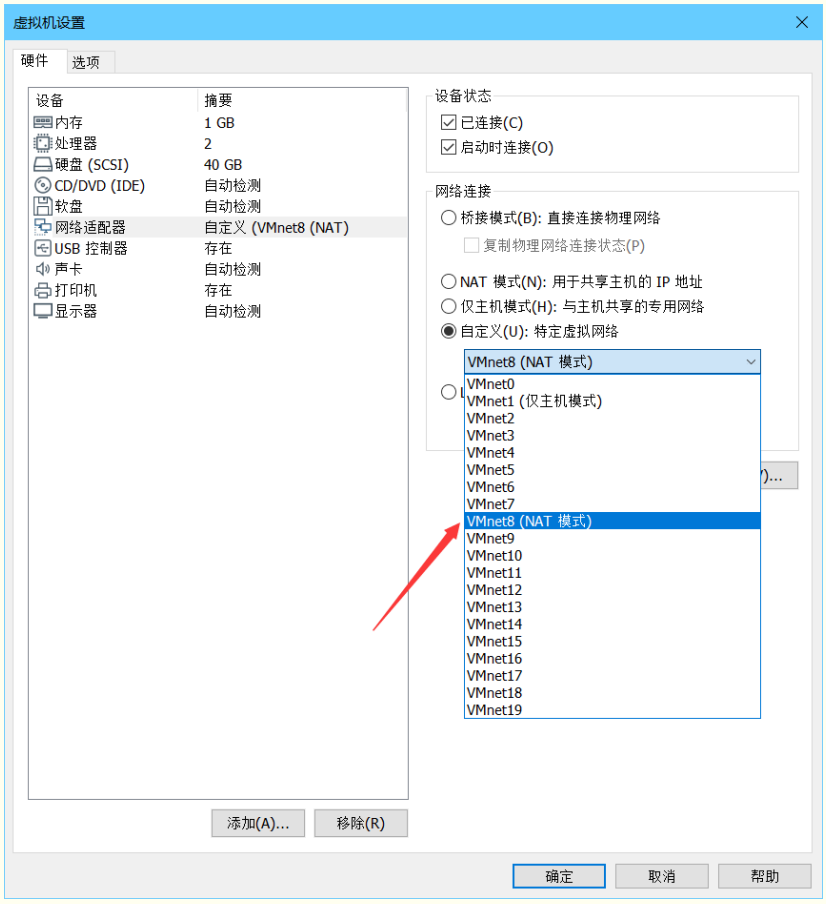
注意：安装完需要安装并启用服务

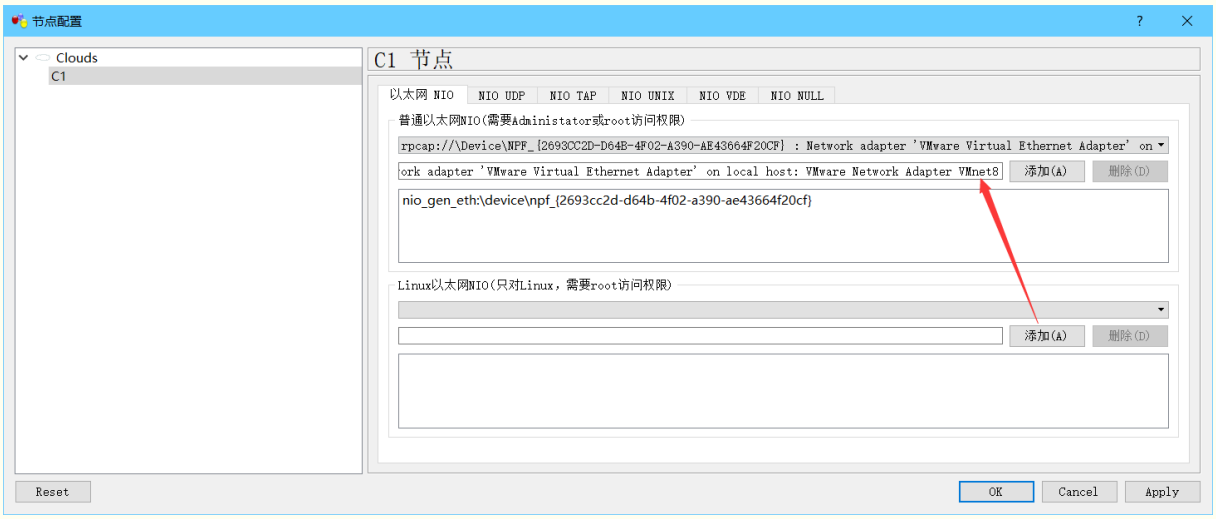


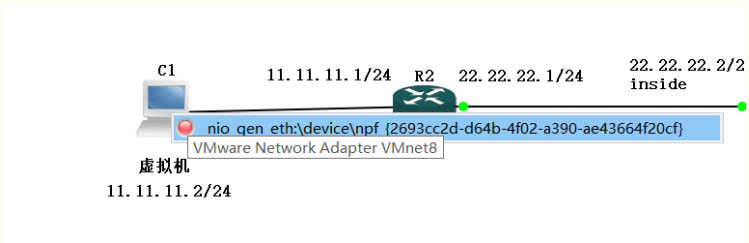
19. 配置虚拟机 IP 地址



20. 配置虚拟机网络连接







21. 配置路由器接口 IP

需要为每个路由的每个接口配置 IP 地址并打开

同上一个实验

22. 配置防火墙接口 IP 和名称

需要为防火墙的每个接口配置 IP 地址并打开
为每个接口配置 nameif 以及 security-level

同上一个实验

23. 配置防火墙路由（静态路由）

到外网的数据包下一跳为 192.168.1.2
pixfirewall(config)# route outside 0.0.0.0 0.0.0.0 192.168.1.2

到内网 11.11.11.0/24 网络的数据包下一跳为 22.22.22.1
pixfirewall(config)# route inside 11.11.11.0 255.255.255.0 22.22.22.1

24. 5 步配置防火墙日志服务器

(1) 分配内网日志服务器主机 11.11.11.2

pixfirewall(config)# logging host inside 11.11.11.2

(2) 设置日志级别 informational

pixfirewall(config)# logging trap informational

(3) 设置时间戳

pixfirewall(config)# logging timestamp

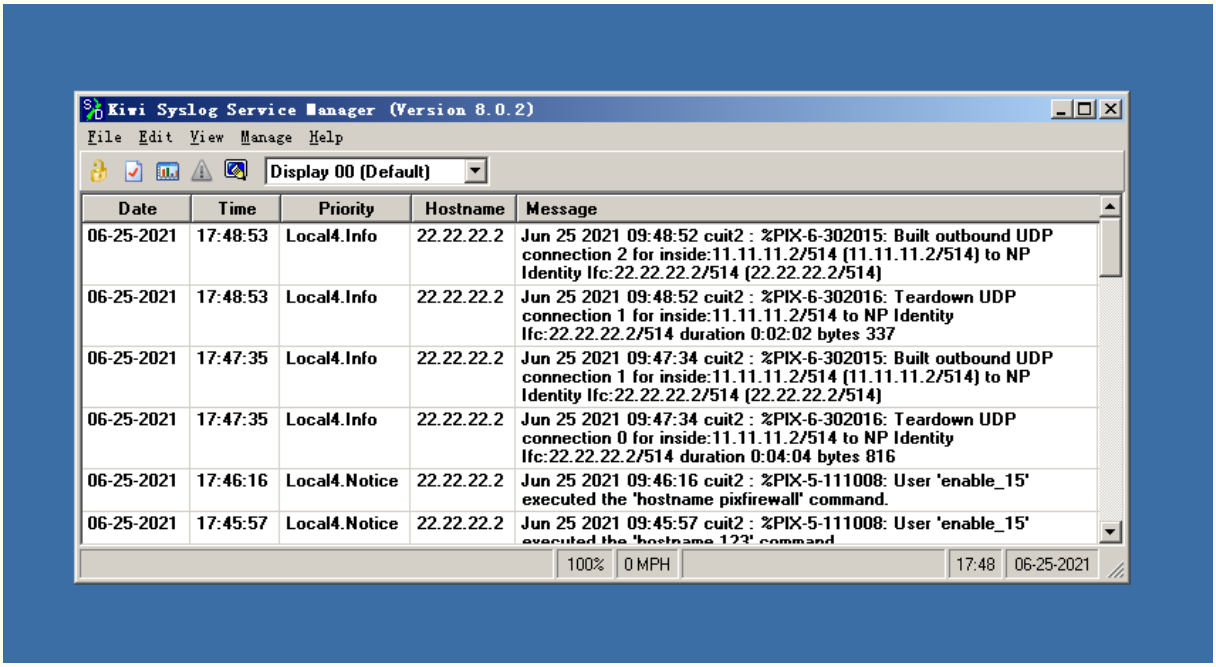
(4) 设置设备 ID 为字符串 cuit2

pixfirewall(config)# logging device-id string cuit2

(5) 启用日志服务器

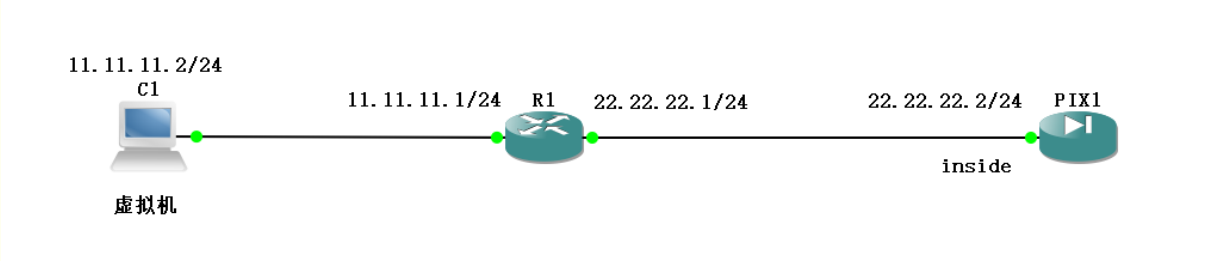
pixfirewall(config)# logging on

25. 验证配置：在虚拟机软件可以看到日志



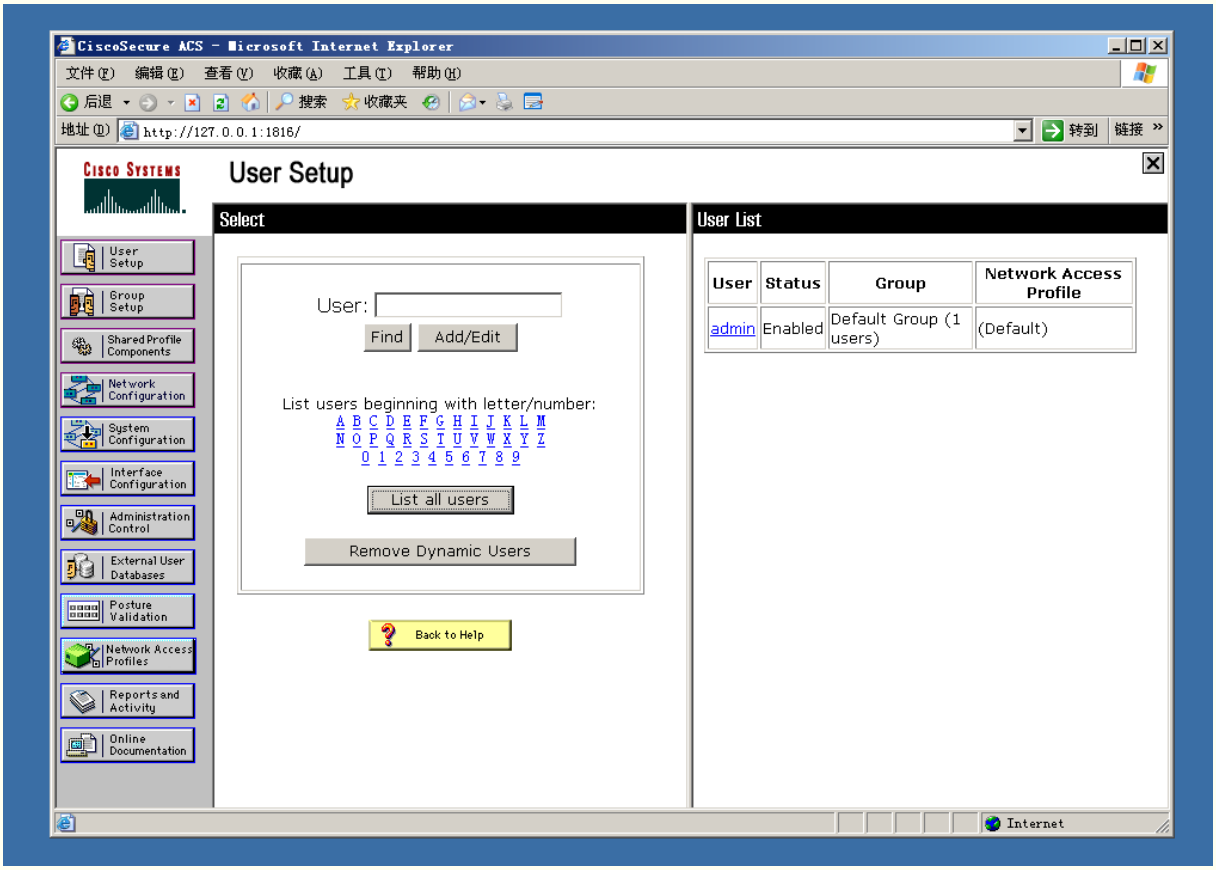
3 AAA 认证配置

26. 实验拓扑



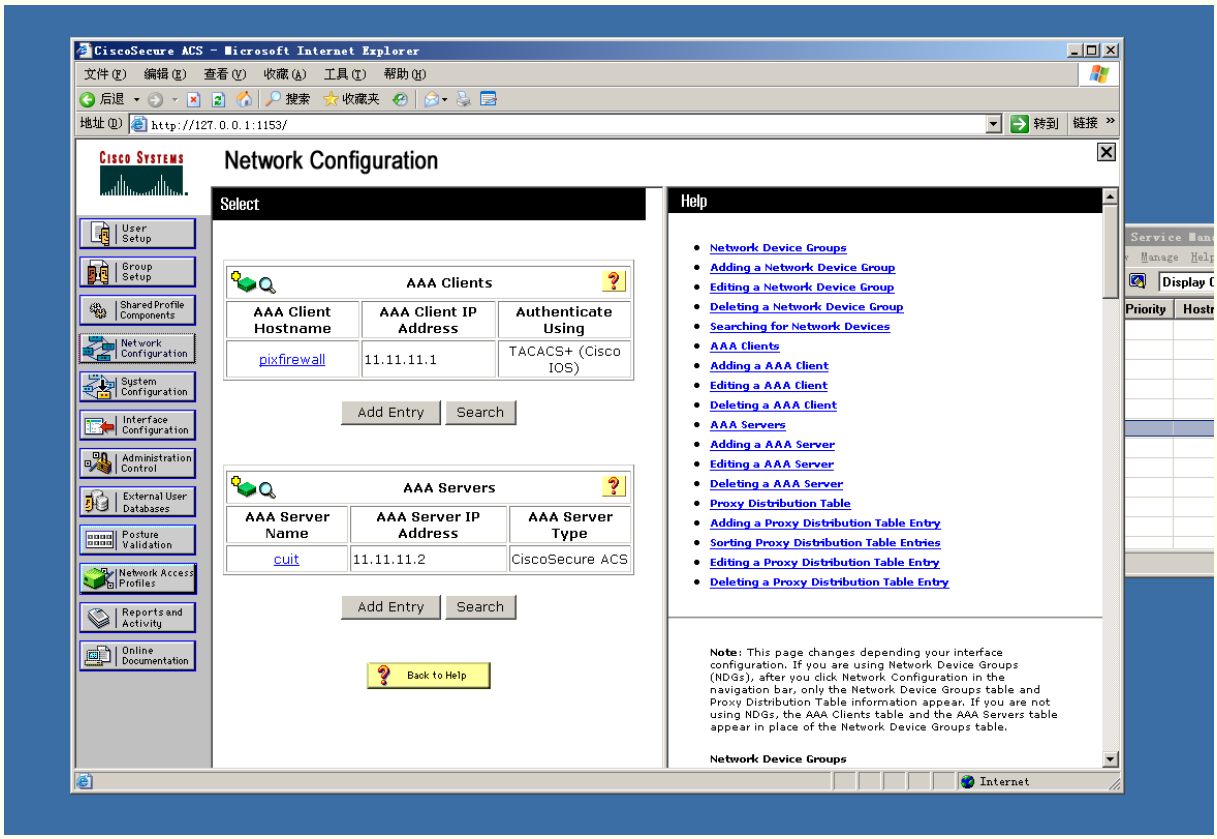
27. 在虚拟机安装 AAA 软件

需要服务器系统，比如 Windows Server 2003

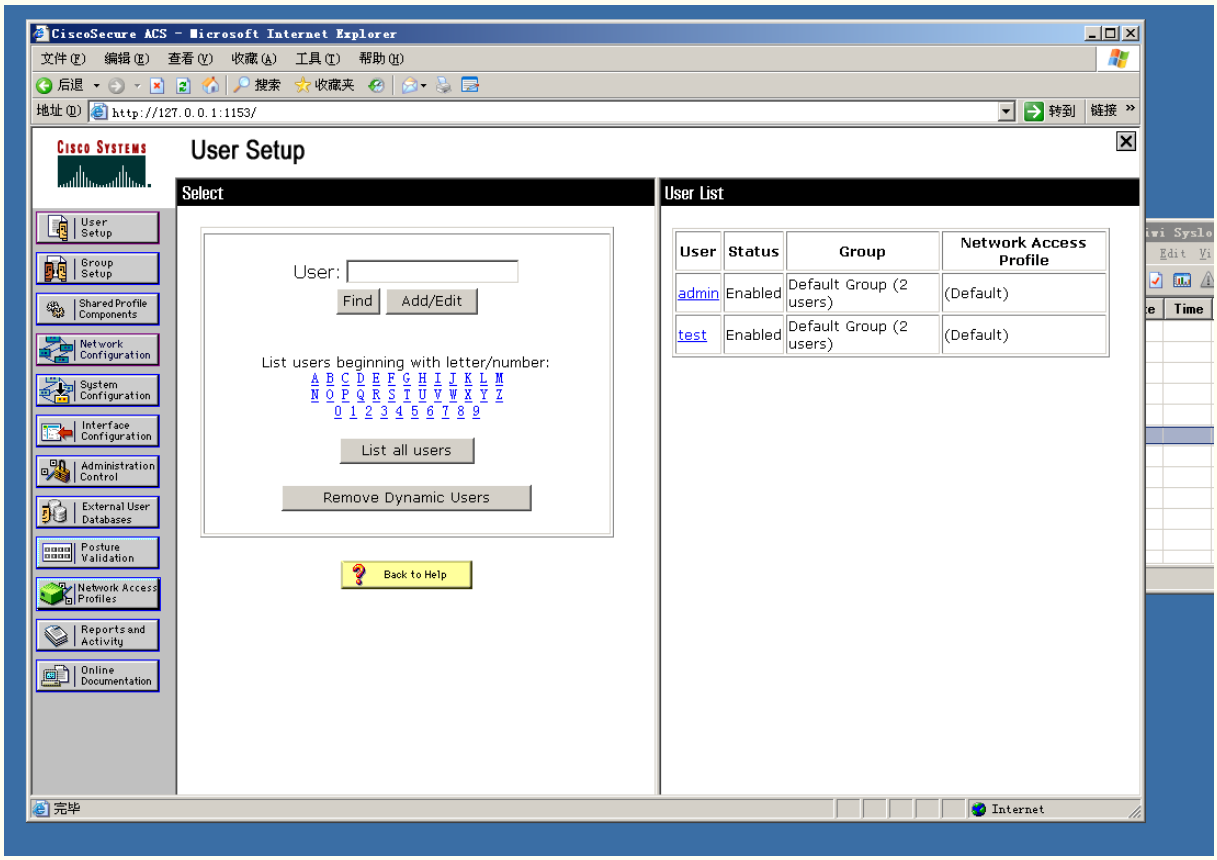


注意：需要安装 JDK 才能正常使用软件

28. 在 AAA 软件中添加 AAA 客户（防火墙）



29. 在 AAA 软件中添加用户



30. 配置路由器接口 IP

需要为每个路由的每个接口配置 IP 地址并打开

同之前实验

31. 配置防火墙接口 IP 和名称

需要为防火墙的每个接口配置 IP 地址并打开
为每个接口配置 nameif 以及 security-level

同之前实验

32. 配置防火墙路由（静态路由）

到内网 11.11.11.0/24 网络的数据包下一跳为 22.22.22.1
pixfirewall(config)# route inside 11.11.11.0 255.255.255.0 22.22.22.1

33. 3 步配置 AAA 认证

(1) 步骤 1：指定服务器类型 aaa-server *

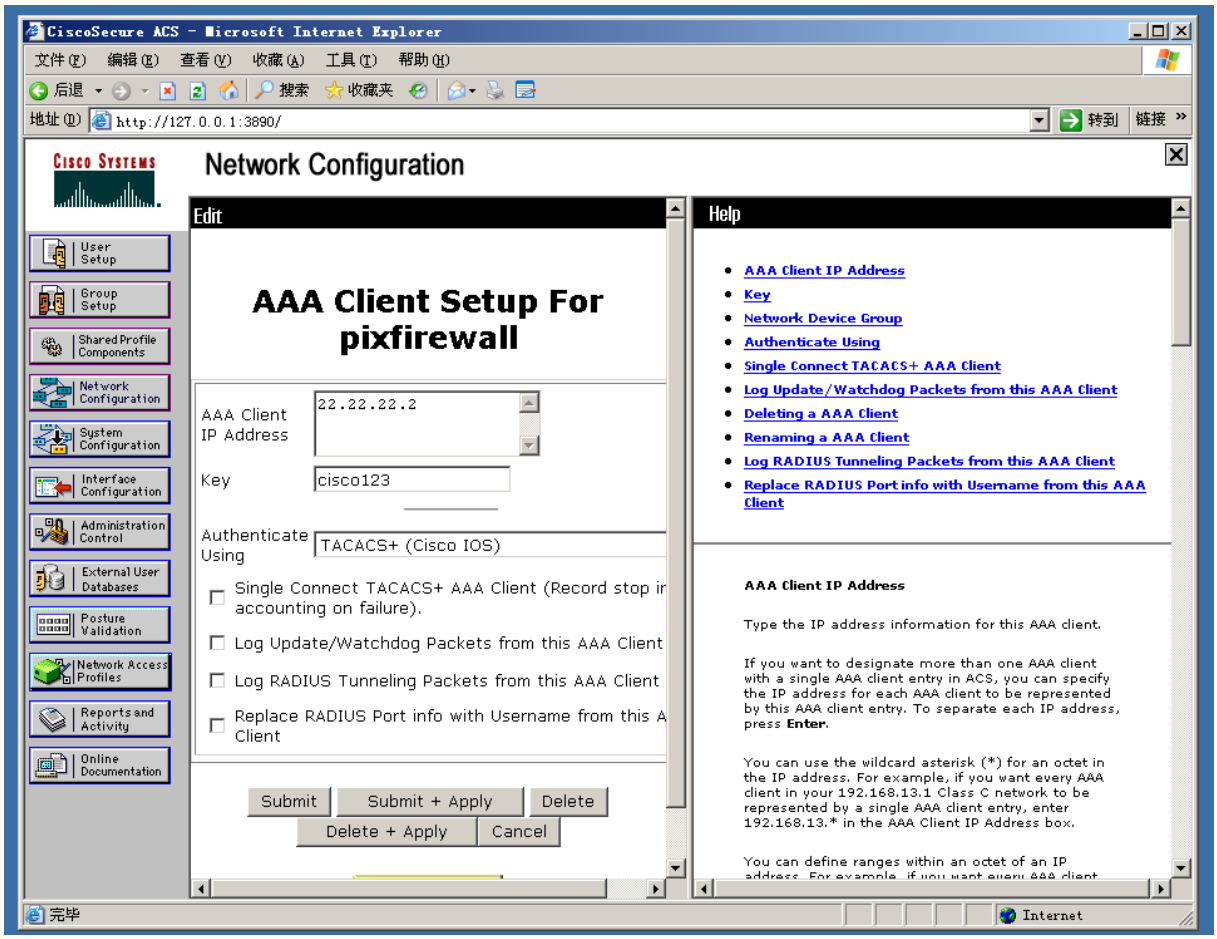
指定服务器 cuit 的类型为 tacacs+
pixfirewall(config)# aaa-server cuit protocol tacacs+

(2) 步骤 2：指定认证服务器 aaa-server * host

指定服务器 cuit 的主机地址为 11.11.11.2
pixfirewall(config-aaa-server-group)# aaa-server cuit host 11.11.11.2

设置密码和超时时间
pixfirewall(config-aaa-server-host)# key cisco123
pixfirewall(config-aaa-server-host)# timeout 10

注意：密码要与软件里一致

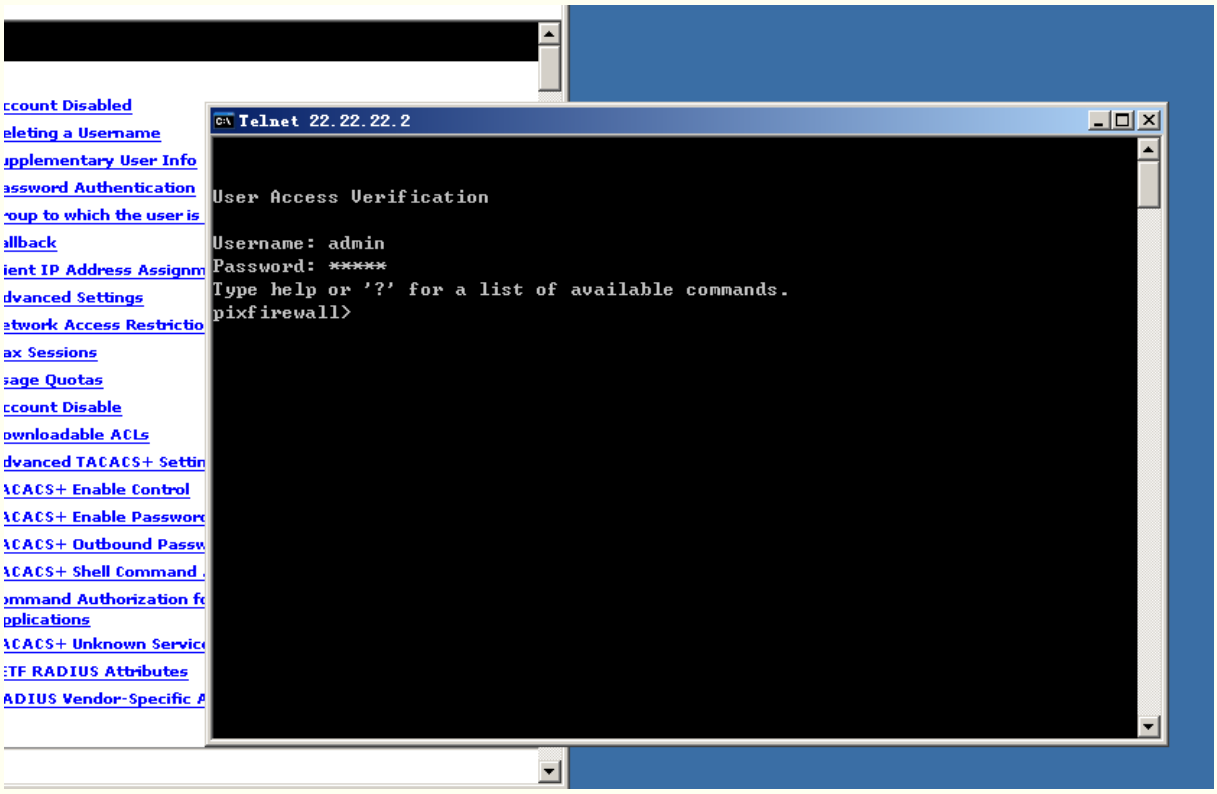


(3) 步骤 3：设置认证方式 aaa authentication

设置为 telnet

pixfirewall(config-aaa-server-host)# aaa authentication telnet console cuit

34. 验证配置：从虚拟机 telnet 到防火墙，需要输入用户名和密码

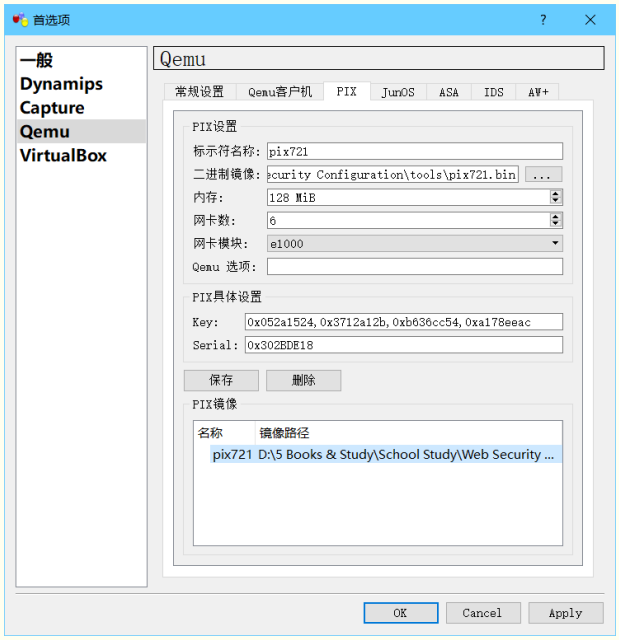


4 VPN 配置

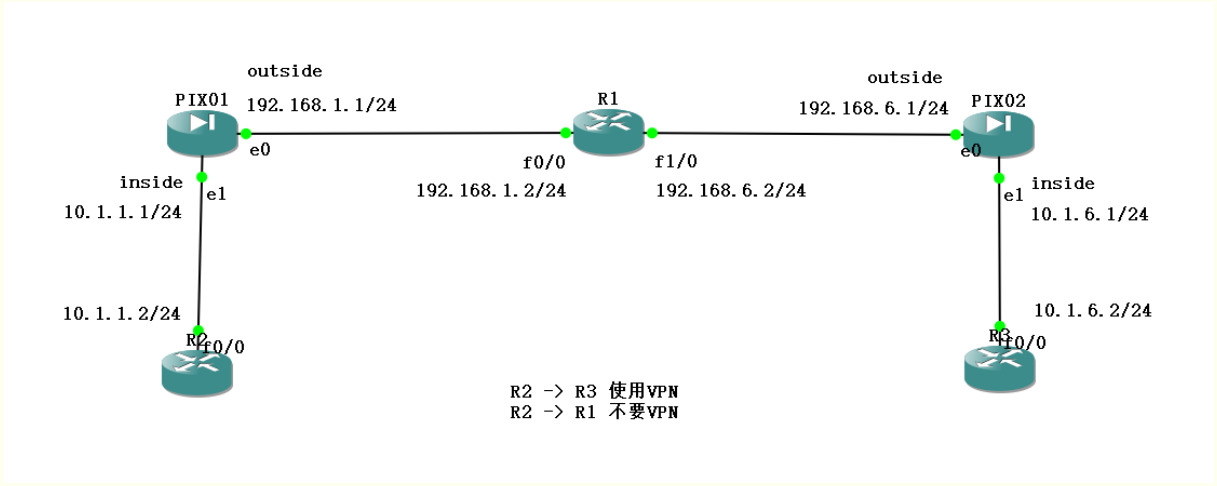
35. 配置 PIX Key 和 Serial

注：此步骤需要在放置防火墙之前完成

Running Activation Key: 0x052a1524,0x3712a12b,0xb636cc54,0xa178eeac
Serial Number: 0x302BDE18



36. 实验拓扑



37. 配置路由器接口 IP

需要为每个路由的每个接口配置 IP 地址并打开

同之前实验

38. 配置路由器默认路由

R2(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.1

R3(config)# ip route 0.0.0.0 0.0.0.0 10.1.6.1

R1(config)# ip route 10.1.1.0 255.255.255.0 192.168.1.1
R1(config)# ip route 10.1.6.0 255.255.255.0 192.168.6.1

39. 配置防火墙接口 IP 和名称

需要为防火墙的每个接口配置 IP 地址并打开
为每个接口配置 nameif 以及 security-level

同之前实验

40. 配置防火墙路由（静态路由）

PIX01 到外网的下一跳地址为 192.168.1.2
pixfirewall(config)# route outside 0.0.0.0 0.0.0.0 192.168.1.2

PIX02 到外网的下一跳地址为 192.168.6.2
pixfirewall(config)# route outside 0.0.0.0 0.0.0.0 192.168.6.2

41. 验证配置：ping

可以从 PIX1 ping 通 R2、R1 和 PIX2 的外部接口。
可以从 PIX2 ping 通 R3、R1 和 PIX1 的外部接口。

42. 激活防火墙

两个防火墙都需要激活

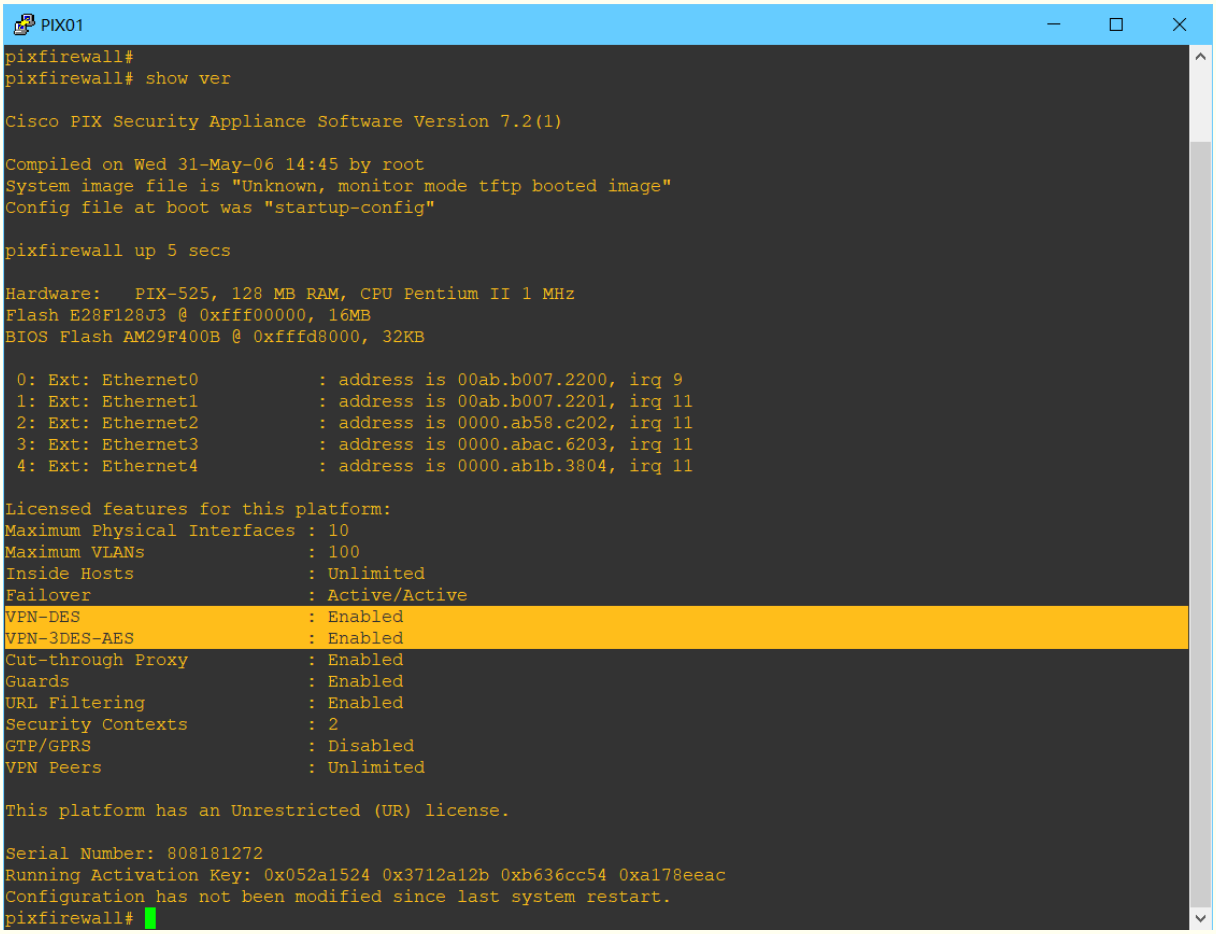
pixfirewall(config)# activation-key 0x052a1524 0x3712a12b 0xb636cc54 0xa178eeac

注：激活后需要重启防火墙

43. 验证配置：show version

pixfirewall# show version

若下面项为 Enable，则说明防火墙已经激活



44. 配置 IKE

(1) 打开防火墙功能

pixfirewall(config)# isakmp enable outside

(2) 配置策略

建立策略 10

pixfirewall(config)# isakmp policy 10

配置策略 10

pixfirewall(config-isakmp-policy)# encryption des
pixfirewall(config-isakmp-policy)# hash sha
pixfirewall(config-isakmp-policy)# authentication pre-share
pixfirewall(config-isakmp-policy)# group 1
pixfirewall(config-isakmp-policy)# lifetime 86400

(3) 配置隧道

创建隧道，并选择隧道模式（选择对方接口 IP 地址作为隧道名字，便于区分）

pixfirewall(config)# tunnel-group 192.168.6.1 type ipsec-l2l

（另一个防火墙为 pixfirewall(config)# tunnel-group 192.168.1.1 type ipsec-l2l）

进入隧道 192.168.6.1，设置预存地址密钥 cisco123
pixfirewall(config)# tunnel-group 192.168.6.1 ipsec-attributes
pixfirewall(config-tunnel-ipsec)# pre-shared-key cisco123

45. 显示 IKE 配置

pixfirewall# show run crypto isakmp

46. 配置 IPSec

(1) 设置感兴趣流量

感兴趣流量为 10.1.1.0 到 10.1.6.0 的流量（另一个防火墙相反）

创建访问控制列表 101
pixfirewall(config)# access-list 101 permit ip 10.1.1.0 255.255.255.0 10.1.6.0 255.255.255.0
（另一个防火墙为 pixfirewall(config)# access-list 101 permit ip 10.1.6.0 255.255.255.0 10.1.1.0 255.255.255.0）

设置不对该流量做地址翻译
pixfirewall(config)# nat (inside) 0 access-list 101

(2) 设置传输模式

设置名为 test（随便取），采用 esp-des 传输模式，采用 esp-md5-hmac 加密算法
pixfirewall(config)# crypto ipsec transform-set test esp-des esp-md5-hmac

要求两个防火墙传输模式一致。

(3) 设置映射集

- 映射集名称 CUIT
- 策略 10
- 访问控制列表 101（感兴趣流量）
- 对等地址（另一端的外部接口地址）：PIX1 是 192.168.6.1；PIX2 是 192.168.1.1
- 传输模式集 test

- 生存时间 28800

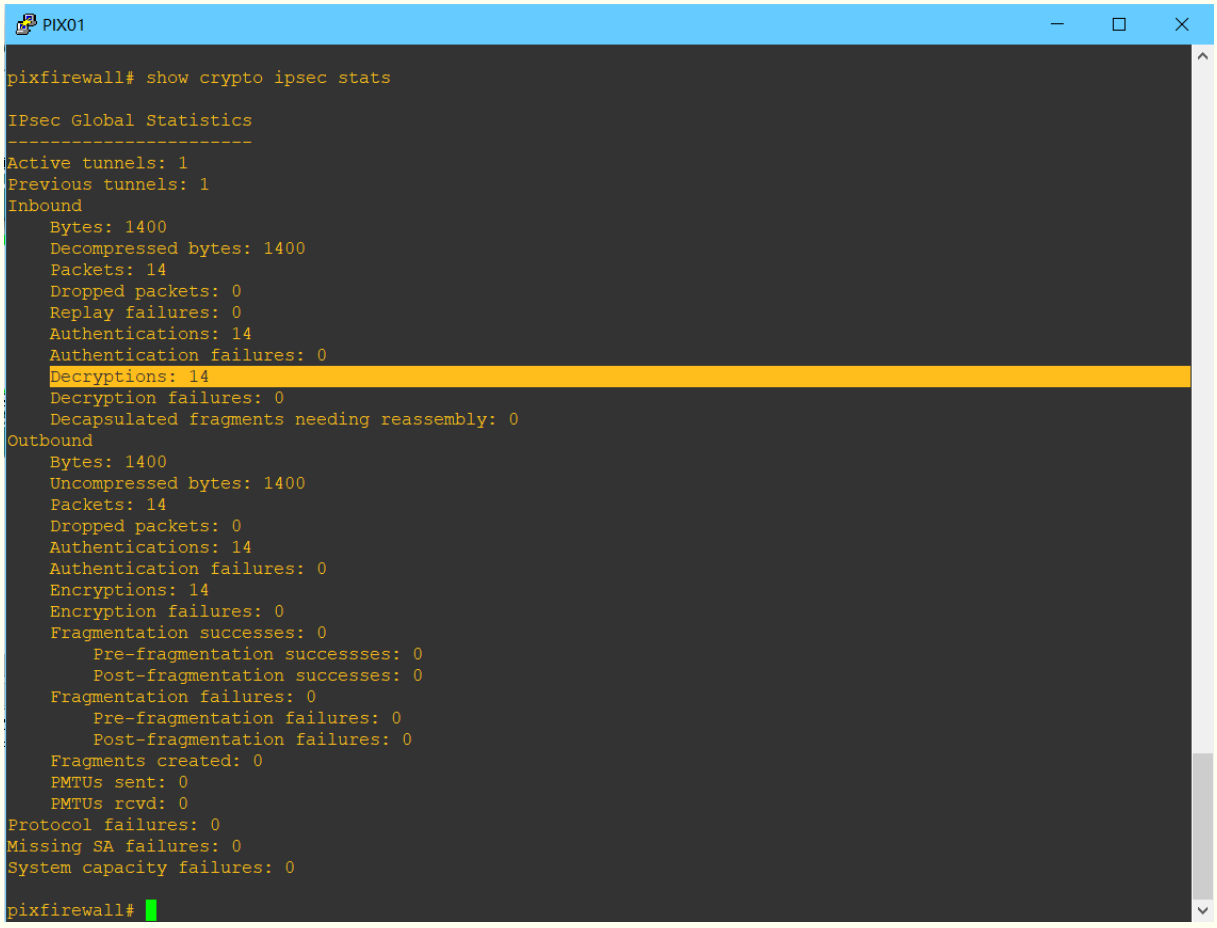
pixfirewall(config)#crypto map CUIT 10 match address 101
pixfirewall(config)# crypto map CUIT 10 set peer 192.168.6.1
pixfirewall(config)# crypto map CUIT 10 set transform-set test
pixfirewall(config)# crypto map CUIT 10 set security-association lifetime seconds 28800

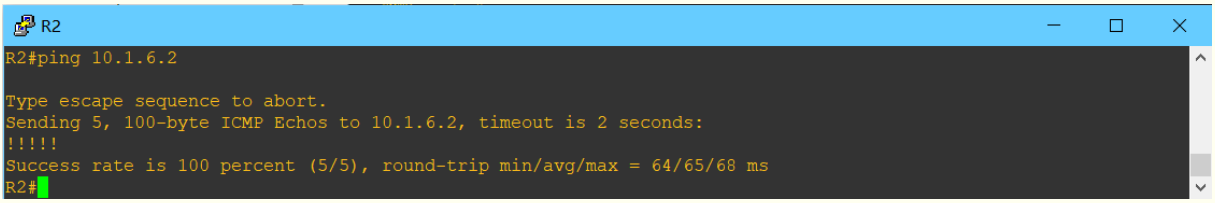
(4) 应用映射集到防火墙外部接口
pixfirewall(config)# crypto map CUIT interface outside

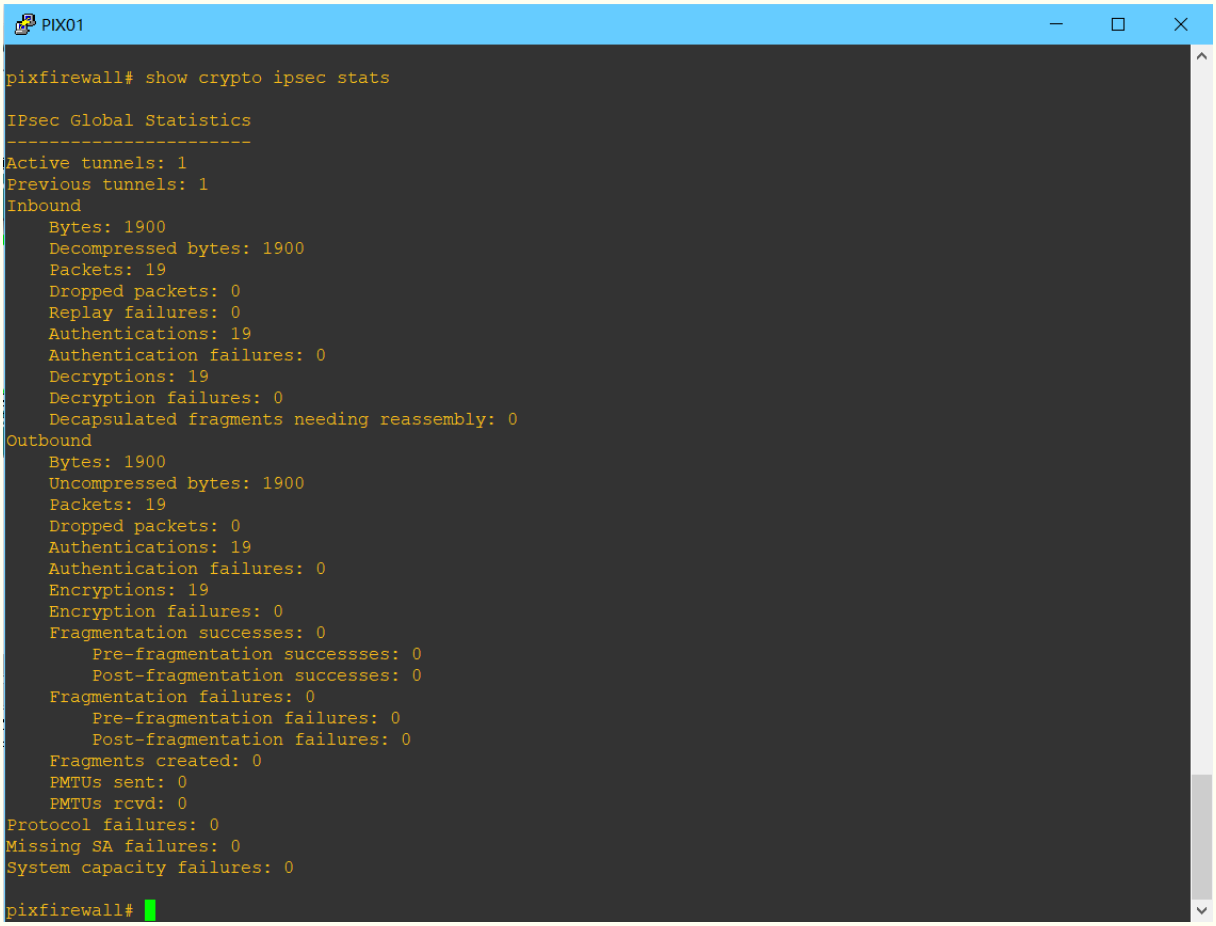
47. 查看防火墙加密包
pixfirewall# show crypto ipsec stats

48. 验证配置：ping
R2 可以 ping 通 R3，ping 一次，5 个包，每通一个包都会导致下面的记录加一，以此验证防火墙 VPN 配置成功。

例如，下面情况，原来加密包数目是 14，ping 一次，5 个包全通，加密包记录数+5。







49. 验证配置：telnet

在 R3 上设置 Telnet 密码，密码是 cisco：

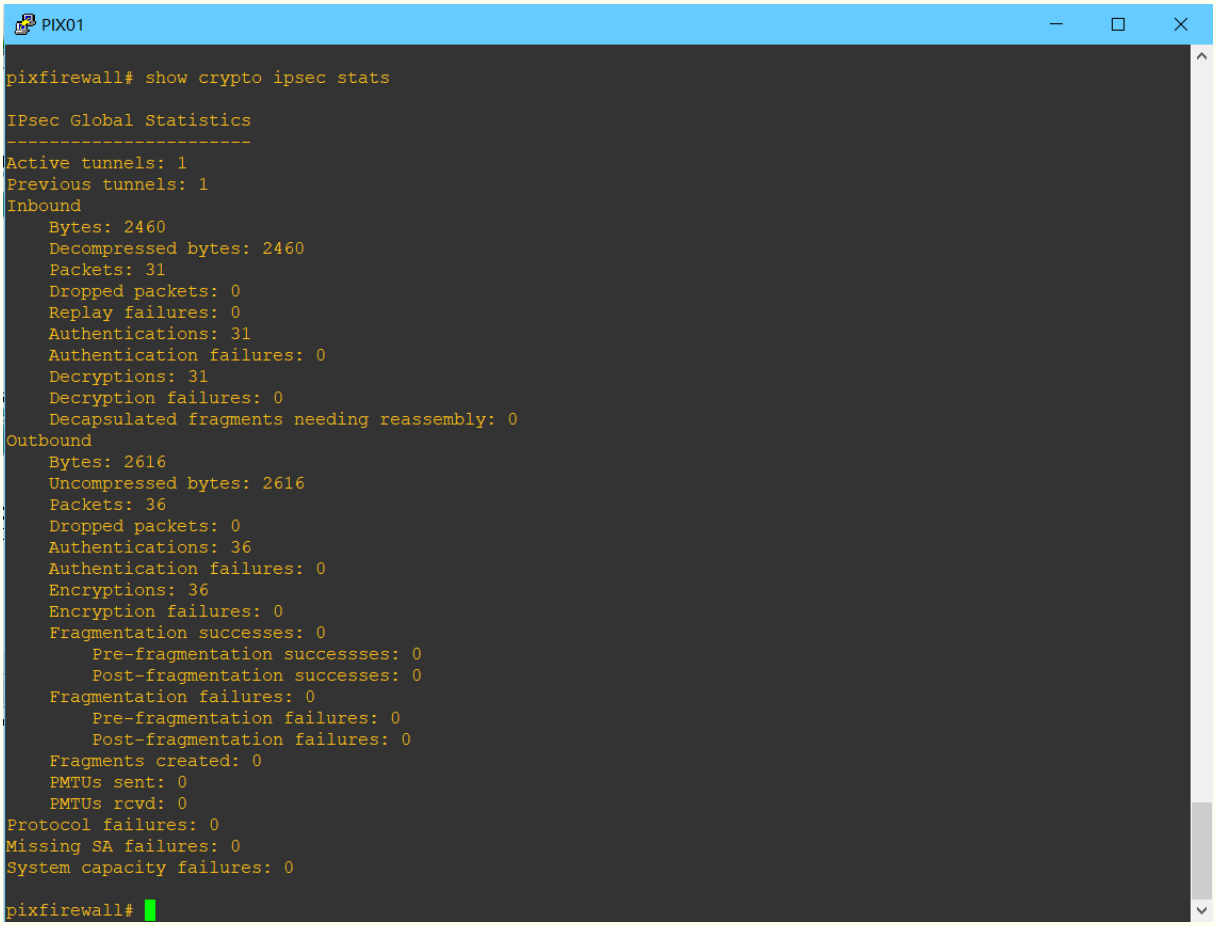
R3(config)#line vty 0 15

R3(config-line)#password cisco

从 R2 Telnet 到 R3，输入密码 cisco：

R2#telnet 10.1.6.2

会导致防火墙记录数增加



50. 验证配置：不走 VPN 的情况

在 PIX1 中配置地址翻译

pixfirewall(config)# nat (inside) 1 0 0

pixfirewall(config)# global (outside) 1 192.168.1.3 netmask 255.255.255.0

在 R1 上设置 Telnet 密码，密码是 cisco：

R1(config)#line vty 0 15

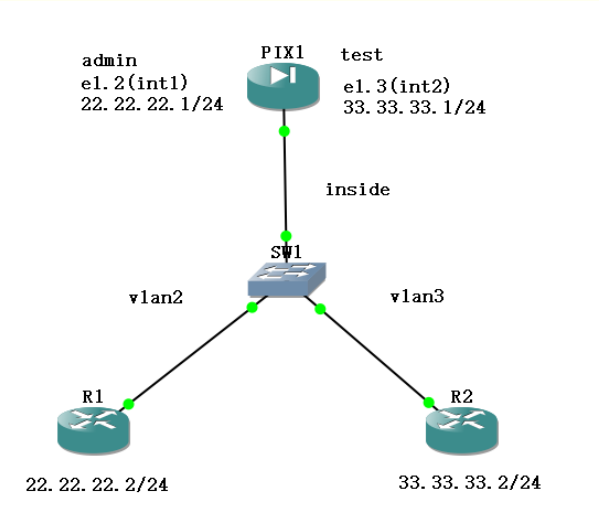
R1(config-line)#password cisco

从 R2 Telnet 到 R1，输入密码 cisco。

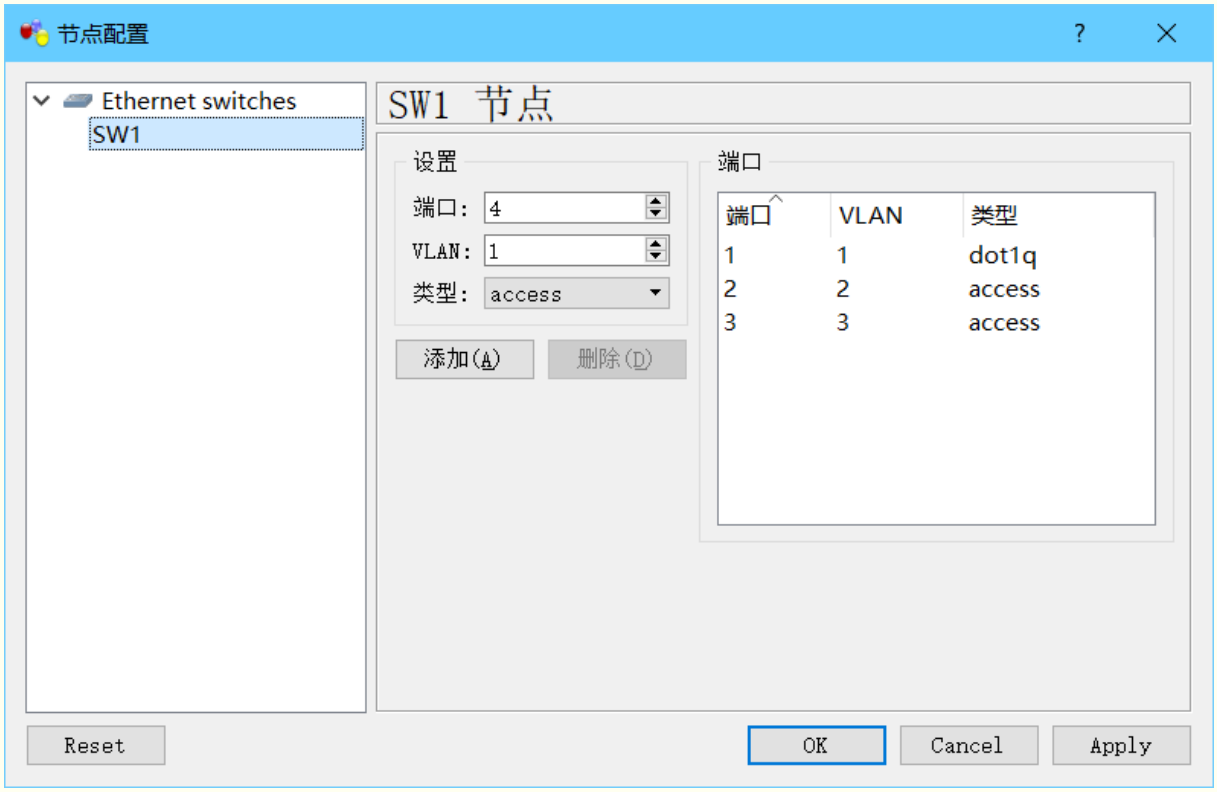
防火墙记录数不会增加，说明没有走 VPN。

5 虚拟防火墙配置

51. 实验拓扑



52. 配置交换机



53. 配置路由器接口 IP

需要为每个路由的每个接口配置 IP 地址并打开

同之前实验

54. 打开防火墙虚拟防火墙功能

pixfirewall(config)# mode multiple

注：配置完需要重启防火墙

55. 验证配置：show mode

pixfirewall# show mode
Security context mode: multiple

56. 配置防火墙子接口，为其分配 VLAN

pixfirewall(config)# int e1.2
pixfirewall(config-subif)# vlan 2
pixfirewall(config-subif)# int e1.3
pixfirewall(config-subif)# vlan 3

57. 配置安全上下文，为其分配接口

pixfirewall(config)# context admin
pixfirewall(config-ctx)# allocate-interface e1.2 int1
pixfirewall(config-ctx)# allocate-interface e0
pixfirewall(config-ctx)# config-url admin.cfg

pixfirewall(config)# context test
pixfirewall(config-ctx)# allocate-interface e1.3 int2
pixfirewall(config-ctx)# allocate-interface e0
pixfirewall(config-ctx)# config-url test.cfg

58. 转到安全上下文 changeto context

转到安全上下文 admin
pixfirewall(config)# changeto context admin
pixfirewall/admin(config)#

将这个作为一个新的防火墙使用，可以像之前一样进行配置

59. 在安全上下文中配置防火墙接口 IP 和名称

需要为防火墙的每个接口配置 IP 地址
为每个接口配置 nameif 以及 security-level

同之前实验

60. 在安全上下文中配置防火墙接口 MAC 地址

pixfirewall/admin(config-if)# mac-address 0000.0000.0002

```
pixfirewall/admin(config)# int int1
pixfirewall/admin(config-if)# ip add 22.22.22.1 255.255.255.0
pixfirewall/admin(config-if)# no sh
pixfirewall/admin(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
pixfirewall/admin(config-if)#
pixfirewall/admin(config-if)# mac
pixfirewall/admin(config-if)# mac-a
pixfirewall/admin(config-if)# mac-address 0000.0000.0002
pixfirewall/admin(config-if)#
```

61. 在主接口打开接口

通过下面命令可以回到系统

pixfirewall/admin(config)# changeto system

pixfirewall(config)# int e1

pixfirewall(config-if)# no sh

注：主接口才能 no sh

62. 验证配置：ping

R1

```
Connected to Dynamips VM "R1" (ID 20, type c3600) - Console port
Press ENTER to get the prompt.

R1#ping 22.22.22.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 22.22.22.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/16/20 ms
R1#
```

About

Kloudy Grasp: Web Security Configuration Experience
网络安全设备配置与管理实验

Reference

无参考文献

Presented by

Kloudy Grasp™
2021/6/25
Website: www.kloudy.cn

Written by

EndersKim
Email: enderskim@qq.com