KLOUDY GRASP

WEB SECURITY CONFIGURATION NOTES

网络安全设备配置与管理

2021/6/28

www.kloudy.cn

Version 1.1

Preface

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

1. 说明

Kloudy Grasp: Web Security Configuration Notes 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 Notes

1 防火墙基础知识

1.1 网络安全介绍

5. IP 地址分类

IP地址格式

类别	首字节值范围	网络数	主机数
A	1--126	126	16777314
B	128--191	16382	65534
C	192--223	2097150	254

6. 防火墙

当访问互联网络环境中的信息时，必须创建安全区域。用来分离这些区域的设备被称为**防火墙**。

两种防火墙:

- PIX (Private Internet eXchange) 私有网络交换机
- ASA (Adaptive Security Appliance) 自适应安全设备

7. 由防火墙创建的三个区域

1. **内部区域** (inside) ——互联网络的信任区域
2. **外部区域** (outside) ——互联网络中不被信任的区域
3. **停火区** (DMZ) ——一个或多个隔离的网络，它对于外部网络通常是可以访问的。

8. 防火墙的基本职责

- 不允许外部设备访问内部网络
- 允许外部设备有限度地访问停火区
- 允许内部设备访问外部网络
- 允许内部设备有限度地访问停火区

当然，在许多网络设计中可能会对这些规则的部分或全部内容存在例外的情况

9. 防火墙的类型

防火墙可以定义为**数据包过滤器**、**代理过滤器**和**状态型数据包过滤器** 3 种类别之一。

1.2 PIX 防火墙命令行接口

10. PIX 提供了四种管理访问模式

(1) 非特权模式

当一开始访问 PIX 防火墙时，就是处于这种模式中。这种模式经常被称为用户可执行模式。显示的提示符是>。

(2) 特权模式

这种模式显示的提示符是#，在这种模式中，我们可以改变当前设置。在特权模式中，我们也可以使用任何非特权命令。

(3) 配置模式

在使用 PIX 防火墙的时候，有许多通用的维护配置命令。

(4) 监视模式

PIX 防火墙在开机或重启过程中，按住 Escape 键或发送一个“Break”字符，进入监视模式。这里可以更新操作系统映象和口令恢复。

11. 用于配置、维护和测试 PIX 防火墙的基本命令

(1) enable

如果用户知道口令，enable 命令就可以让他进入特权模式。要想退出特权模式并返回前一种模式，可以使用 disable、exit 或 quit 命令。

设置口令的命令是 enable password *password*。在 PIX 防火墙的配置文件中，口令时被加密保存的。

(2) configure terminal

如果我们想交互式地改变 PIX 防火墙的配置，应采用命令 configure terminal。任何添加的配置参数都将被归并到当前运行的配置当中。当对 PIX 防火墙进行配置修改时，修改会立刻生效，并被保存到 RAM 里正在运行的配置当中。

(3) enable password

这条配置命令的参数将设置允许我们访问特权模式的口令。在我们输入 enable 命令之后，就被要求输入这个口令。在设置 enable password 时，我们也可以选择输入口令的加密形式。具体做法是，在输入 password 后，输入可选项 encrypted。

(4) show enable

命令 show enable 显示的是口令的加密形式。

(5) passwd

命令 passwd 可以让用户为访问 PIX 防火墙的 Telnet 设置口令。缺省的口令值是“cisco”。

12. 存储配置文件

(1) write net

将当前运行的配置文件存储到 TFTP 服务器上。将所有配置文件进行离线备份存储是一个好的习惯。当指定 TFTP 服务器的 IP 地址和文件路径时，运行的配置就被存储在那个指定的位置。

(2) write erase

这条命令清除位于 Flash 存储器中的配置文件。

(3) write floppy

这条命令将运行配置存储到磁盘上。

(4) write memory

对 PIX 做出的任何改动都会立即生效。改动将被写入到位于 RAM 中的运行配置中。如果想把一个改动保存在 PIX 防火墙上，就应该用命令 write memory 将它存储在 Flash 存储器中。

(5) write standby

将位于活跃的故障切换 PIX 防火墙上 RAM 中存储的配置，写到备用 PIX 防火墙上的 RAM 中。

(6) configure memory

将运行配置与 Flash 存储器中的配置运行合并。此命令不是替代 Flash 存储器中的配置，而是将运行配置和 Flash 配置之间的不同之处添加到 Flash 存储器配置中。

13. 显示

(1) write terminal

这条命令在终端上**显示**当前运行的配置（有时被称为“当前配置（current terminal）”）。这个配置是被存储在 RAM 中的。

(2) show history

显示以前输入的命令行。可以用上下箭头逐个检查以前输入的命令。

(3) show interface

让用户可以查看关于接口的信息。在想要建立网络连接时，这是需要被首先输入的命令之一。

(4) show memory

该命令显示 PIX 防火墙的最大物理存储器和当前可用存储器的汇总信息。

(5) show version

该命令让用户可以看到当前运行在 PIX 防火墙上的操作系统版本。该命令的输出还显示了自从上次重新启动以来，PIX 防火墙已经运行了的时间。该命令的输出还显示了：硬件类型、板上的存储器、处理器类型、Flash 存储器类型、BIOS Flash 信息、接口板、许可证特性、序列号码、激活密钥。

(6) show xlate

该命令显示了翻译槽位信息。这些信息是为通过 PIX 防火墙建立的会话进行地址翻译所分配的 IP 地址。

14. 其他命令

(1) ping

用于确定 PIX 防火墙是否具有到达一个指定目标的连通性，或者在网络上的一台主机是否可用（对 PIX 防火墙是可见的）。

(2) telnet

让我们指定哪些主机可以通过 Telnet 方式访问 PIX 防火墙的控制台。

2 PIX 防火墙基本配置

2.1 基本配置

15. 安全级别

安全级别的范围是从 0 到 100

(1) 安全级别 100

对于一个接口来说，这是最高的安全级别。它被用于 PIX 防火墙的内部接口。这是 PIX 防火墙的缺省参数，不能被修改。

(2) 安全级别 0

这是最低的安全级别。这种安全级别被用于 PIX 防火墙的外部接口。这是 PIX 防火墙的缺省参数，不能被修改。

(3) 安全级别 1~99

这些安全级别可以被分配给连接 PIX 防火墙的边界接口。通常，将这些边界接口中的一个连接到作为停火区（DMZ）的一个网络。DMZ 是一台设备或网络，对于来自不被信任环境中的用户来说，DMZ 通常是可以被访问的。DMZ 是一个隔离的区域，是从内部被信任的环境中隔离出来的。

16. 配置 PIX 防火墙的 6 个基本命令

有 6 个基本配置命令被认为是 PIX 防火墙的基础。nameif、interface 和 ip address 命令对于 PIX 的运行是必要的。nat、global 和 route 命令虽然不是必需的，但是也经常会被使用。为了让数据流通过 PIX 防火墙，必须对它进行配置。nat 和 global 命令通常用于提供从一个相对可信的网络（高安全级别接口）的访问。

17. nameif 命令

命令 nameif 为 PIX 防火墙上的每个接口分配一个名字，并指定它的安全级别（PIX 防火墙的内部接口和外部接口除外，它们的名字是缺省的）。

语法：**nameif** ***hardware_id if_name security_level***

其中：

hardware_id：指定一个边界接口，以及它在 PIX 防火墙上的物理位置。PIX 防火墙可以支持三种类型的接口：以太网、FDDI 和令牌环接口。例如,以太网接口可以被标识为 ethernet1、ethernet2、ethernet3 等；

if_name：为物理边界接口指定一个名字。这个名字是由用户指定的，而且必须被用于所有未来的配置中，以提供对边界接口的引用。缺省情况下，借口 e1 的名字是 inside（内部接口），接口 e0 的名字是 outside（外部接口）。

security_level：为边界接口指定安全级别。输入取值范围为 1~99 的安全级别。

18. interface 命令

interface 命令用以确定硬件类型，设置硬件速度，并启用接口。当在 PIX 防火墙上安装一块附加的以太网接口卡时，PIX 防火墙可以自动识别这块附加的卡。

语法：**interface *hardware_id hardware_speed* [shutdown]**

例如：interface ethernet0 10baset shutdown；　　interface ethernet1 10baset

其中：
hardware_id：指定一个接口，以及它在 PIX 防火墙上的物理位置。用法与 nameif 命令中相同。
hardware_speed：确定连接速度。输入“auto”，这样 PIX 防火墙就可以自动感知设备所需的速度。对于网络接口速度，以太网可能有的值是：10baset—10Mbit/s 以太网半双工通信；10full—10Mbit/s 以太网全双工通信。
shutdown：管理性的关闭这个窗口。

19. ipaddress 命令

PIX 防火墙上的每个接口都必须用一个 IP 地址进行配置。

语法：**ip address *if_name ip_address* [*netmask*]**

其中，
ip_name：描述了这个接口。这个名字是由用户指定的，而且必须被用于所有未来的配置中，以提供对这个接口的引用。
ip_address：为接口分配的 IP 地址。
netmask：如果没有指定网络掩码，将采用“有类别（classful）”的网络掩码——A 类 255.0.0.0；B 类 255.255.0.0；C 类 255.255.255.0

20. nat 命令

网络地址翻译（NAT）让用户能够保持内部 IP 地址对于外部网络是未知的。nat 命令需要完成的工作是，在数据包被转发到外部网络之前，将内部未经注册的 IP 地址（这些地址不具有全球唯一性）翻译成经过注册的、全球接受的 IP 地址。除了 nat0 以外，nat 命令总是与 global 命令一起使用。

语法：**nat(*if_name*) *nat_id local_ip* [*netmask*]**

其中，
(if_name)：描述将使用全局地址的内部网络接口名字。数据将通过在 global 命令中指定的接口，离开 PIX。
nat_id：标识全局地址池，并使它与其相应 global 命令相匹配。
local_ip：在内部网络上，分配给设备的 IP 地址。可以使用 0.0.0.0，来允许所有的向外连接使用来自全局池中 IP 地址进行翻译。
netmask：本地 IP 地址的网络掩码。

在刚开始配置 PIX 防火墙时，可以用 **nat 1 0.0.0.0 0.0.0.0** 命令，允许所有的内部主机向外进行连接访问，并由相应的 global 命令所指定的全局地址对外进行访问。

nat 命令可以指定**一台主机**或**一段范围内的主机**，这样使访问更具有选择性。

在配置该命令的时候，可以用 0 代替 0.0.0.0。

用 0 代表 0.0.0.0 的例子如下：pixfirewall#(config) **nat(inside) 1 0 0**
在任何需要指定 0.0.0.0 的 PIX 命令中，都可以使用这种简写方式。

21. global 命令

当从一个被信任的网络向一个不被信任的网络发送数据时，通常需要翻译源 IP 地址。PIX 采用两个命令来进行这项工作。第一个命令是 nat，它定义了将要被翻译的、被信任的源地址。用来定义源地址**将要翻译成的地址**或**地址范围**的命令是 global。

语法：**global (*if_name*) *nat_id global_ip-global_ip* [netmask *global_mask*]**

其中，
if_name：描述我们将要为之使用全局地址的外部网络接口名字。
nat_id：指示全局地址池，并使它与其相应的 nat 命令相匹配。
interface：让 PIX 防火墙将由 nat 命令所指定的所有 IP 地址翻译到该指定的接口。这被称为接口 PAT。
global_ip：单个 IP 地址，或一段全局 IP 地址范围的起始 IP 地址。
-global_ip：一段全局 IP 地址范围。
netmask global_mask：全局 IP 地址的网络掩码。如果子网是有效的，就使用子网掩码（例如，255.255.255.0）。

如果我们指定的地址范围与用 netmask 命令选项指定的子网相交迭，这个命令将不使用全局地址池中的**广播或网段地址**。例如：如果我们使用网络掩码 255.255.255.128，与地址范围 192.150.50.20—192.128.50.140，那么广播地址 192.128.50.127 和网段地址 192.128.50.128 将不被包括在全局地址池中。

为了删除一个全局表项，可以使用命令 no global。
例如：no global [outside] 1 192.168.1.10-192.168.1.254 netmask 255.255.0.0

22. 翻译表

当从内部网络中的一台设备上发出的外出 IP 包到达 PIX 防火墙时，源地址被提取出来，并于内部的一张现有**翻译表**进行比较。如果该设备的地址不在这个表中，就对它进行翻译。为那台设备产生一个新的表项，并从全局 IP 地址池中为它分配一个全局 IP 地址。这被称为**翻译槽位**（translation slot）。翻译后，翻译表被更新，并转发经过翻译的 IP 包。在用户配置的时间限制后，或者缺省的三个小时后，如果在这段时间内没有那个特定 IP 地址的翻译数据包，那么，这个表项就被从表中删除，并释放全局地址，使它可以用于其他的内部设备。
如果用 nat 命令，**必须对伴随的 global 命令进行配置**，来定义翻译 IP 地址池。

23. route 命令

route 命令为接口定义一条静态路由。route 命令语句可以具有一个具有的目的地，或者可以产生一条缺省的静态路由。

语法：**route *if_name ip_address netmask gateway_ip* [*metric*]**

其中，
if_name：描述内部或外部网络接口的名字。数据将通过这个接口离开 PIX。
ip_address：描述目的地（内部或外部）网络 IP 地址。用 0.0.0.0 指定缺省路由（所有的目标网络）。

可以将 IP 地址 0.0.0.0 简写为 0。
netmask：指定应用于 ip_address 的网络掩码。用 0.0.0.0 指定一条缺省路由。可以将网络掩码 0.0.0.0 简写为 0。设置一条路由是一种比较常见的情况。
gateway_ip：指定网关路由器的 IP 地址（这条路由的下一跳地址）。
metric：制定到 gateway_ip 的跳数。如果我们不能确定，就输入 1。我们的 WAN 管理员可以提供这项信息，或者我们可以用 traceroute 命令得到跳数。如果不指定度量值（metric），缺省是 1。

24. 用六个基本命令配置 PIX 防火墙

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
nameif ethernet3 pix/intf3 security15
nameif ethernet4 pix/intf4 security20
nameif ethernet5 pix/intf5 security25

interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown

ip address outside 192.168.1.2 255.255.255.0
ip address inside 10.0.1.1 255.255.255.0
ip address dmz 172.16.1.1 255.255.255.0
ip address pix/intf3 127.0.0.1 255.255.255.255
ip address pix/intf4 127.0.0.1 255.255.255.255
ip address pix/intf5 127.0.0.1 255.255.255.255

global(outside) 1 192.168.1.10-192.168.1.245 netmask
255.255.255.0

nat(inside) 1 0.0.0.0 0.0.0.0

route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
```

2.2 PIX 防火墙翻译

在 PIX 防火墙上设置地址翻译时，可以有两种选择。内部地址可以被翻译成一个指定的全局地址，这被称为静态地址翻译。第二种选择是，在数据穿越 PIX 防火墙时，将内部地址翻译到一个全局地址池中的某个地址。这种翻译类型是动态地址翻译。

2.2.1 静态地址翻译

25. 静态地址翻译

如果每次通过 PIX 防火墙建立一个向外的会话时，要求同一台主机都被翻译成相同的地址，就需要采用静态地址翻译。它也可以用来让较低安全级别接口上的设备能够访问位于较高安全级别接口上的 IP 地址。对于由同一个源地址创建的每条连接，PIX 防火墙为之建立的翻译槽位都将具有相同的源 IP 地址和相同的翻译地址。

26. static 命令

语法：static [(*internal_if_name*, *external_if_name*)] *global_ip local_ip* [netmask *network_mask*] [*max_conns* [*em_limit*]] [norandomseq]

其中，
internal_if_name：内部网络接口名称。我们正在访问的较高安全级别的接口。
external_if_name：外部网络接口名称。我们正在访问的较低安全级别的接口。

global_ip：全局 IP 地址。这个地址不可以是一个 PAT（端口地址翻译）IP 地址。我们正在访问的较低安全级别的接口上的 IP 地址。
local_ip：内部网络的本地 IP 地址。我们正在访问的较高安全级别的接口上的 IP 地址。
netmask：在制定网络掩码之前所需的保留字。
network_mask：用于 global_ip 和 local_ip 的网络掩码。对于主机地址，总采用 255.255.255.255。对于网络地址，使用适当类别的掩码或子网掩码。
max_conns：每个 IP 地址的最大连接数量，允许同时通过该静态地址翻译的连接数量。
em_limit：未完成连接限制数。设置这个限制，以防止未完成连接风暴攻击。缺省是 0，这意味着不限制连接数。
norandomseq：不对 TCP/IP 数据包的序列号进行随机化处理。如果另一台在线防火墙也在对序列号进行随机化，结果就会扰乱数据，只有这时才使用这个选项。

27. 内部主机的外部 IP 地址

当允许通过 PIX 防火墙访问一台特定的内部主机时，必须为外部的用户定义该主机的外部 IP 地址。外部主机必须用内部主机的静态全局地址（翻译地址），作为目的 IP 地址。

28. conduit 命令

conduit 命令允许通过 PIX 防火墙的访问，命令如下：
conduit {permit | deny} ***protocol*** *global_ip foreign_ip*

static (inside,outside) 192.168.1.101 10.0.1.10
conduit permit tcp host 192.168.1.101 eq telnet host 172.16.1.1

在这个 Telnet 会话中，具有**外部 IP 地址 172.16.1.1** 的主机正在建立一个会话，其目的地是**具有全局 IP 地址 192.168.1.101 的一台内部主机**。PIX 防火墙将全局 IP 地址 192.168.1.101 翻译成本地 IP 地址 10.0.1.10。

29. 翻译一段地址范围（网络静态翻译）

我们还可以用 static 命令翻译一段地址范围。

如果要将 A 类网络的一个子网 10.1.1.0 255.255.255.0 翻译成 C 类网络 192.168.1.0 255.255.255.0，相应的命令语法是：
static (inside, outside) 192.168.1.0 10.1.1.0
这被称为网络静态 net static 翻译。

在这个例子中，子网 10.1.1.0/24 中的每个具体 IP 地址每次被翻译成相同的全局 IP 地址。例如，IP 地址为 10.1.1.100 的主机，对于通过 PIX 建立的每个会话，都被翻译成 192.168.1.100。

30. 翻译成自身

我们还可以用 static 命令将地址翻译成自身。在这种情况下，本地 IP 地址和全局地址是一样的：
static (inside,outside) 192.168.1.10 192.168.1.10

2.2.2 动态地址翻译

31. 动态地址翻译

动态地址翻译用来将一段本地地址范围翻译成一段全局地址范围，或者一个全局地址。将一段本地地址范围翻译成一段全局地址范围，这被称为网络地址翻译（NAT）。将一段本地地址范围翻译成一个全局地址，这被称为端口地址翻译（PAT）。

32. 网络地址翻译 NAT

对于采用 NAT 的动态地址翻译，必须用 nat 命令来定义本地主机。然后必须用 global 命令定义全局地址池。根据用 nat 命令选择的 nat_id，在输出接口上选择用于地址翻译的全局地址池。用户指定的 IP 全局地址池的数量可以多达 256 个。

具体语法如下：

nat(inside) 1 0.0.0.0 0.0.0.0
global (outside) 1 192.168.1.10-192.168.1.254 netmask 255.255.255.0

如果主机 10.0.1.10 是通过 PIX 向 Internet 发起第一条连接的主机，它就会被翻译成全局地址 192.168.1.10

33. 端口地址翻译 PAT

当采用端口地址翻译时，所有的本地地址都被翻译到同一个全局地址。PAT 的配置与 NAT 的配置很相似。其中一个区别是，“global”命令语句中只包含一个 IP 地址，而不是在一段 IP 地址范围，

语法：

nat(inside) 1 0.0.0.0 0.0.0.0
global (outside) 1 193.168.1.10 netmask 255.255.255.255

当连接到 Internet 时，所有的内部 IP 地址都将被翻译到同一个地址 192.168.1.10

34. 下面是关于 PAT 的一些重要的考虑

- PAT 让多个向外的会话看起来像是源自同一个 IP 地址。启用 PAT 后，防火墙为每个向外的 xlate（翻译槽位），从 PAT 的 IP 地址中，选择一个唯一的**端口号**。当 ISP 不能为我们的向外连接分配足够多的唯一 IP 地址时，这个功能特性就非常有价值。
- 我们为 PAT 指定的那个 IP 地址不能被用于另一个全局地址池。
- 当 PAT 被用于扩充全局地址池时，首先使用的是全局池中的地址，当全局地址池中的地址被用尽后，下一条连接将选取 PAT 地址。如果全局地址池中有一个地址变成可用的，下一条连接就采用那个地址。**全局地址池中的地址总是先于 PAT 地址被使用。**可以通过在产生全局地址池和 PAT 的 global 命令语句中使用相同的“nat_id”，用 PAT 来扩充全局地址池。
  例如：
  global (outside) 1 172.16.201.1-172.16.201.10 netmask 255.255.255.224
  global (outside) 1 172.16.201.22 netmask 255.255.255.224

35. xlate 命令

翻译和连接翻译时在 TCP/IP 协议栈的 IP 层，连接是在传输层。连接是翻译的子集。在一个翻译之

下，我们可以有许多连接。

xlate 命令让我们可以**显示或清除翻译槽位的内容**。

当建立一个通过 PIX 防火墙的会话时，将产生一个翻译槽位。在修改了配置之后，翻译槽位仍然会保留。在我们的配置中增加、改变或删除 alias、conduit、blobal、nat、route 或 static 命令之后，最好使用 clear xlate 命令。对 PIX 防火墙应用 reload 命令，或者重新开关电源，也可以达到清除翻译槽位的目的。

clear xlate 和 show xlate 命令如下：

show xlate **[global | local ip1 [-ip2] [netmask mask]]** **[port | gportport [-port]]** **[interface if1 [,if2] [,ifn]]** [state static [,dump] [,portmap] [,norandomseq] [,identity]]

clear xlate **[global | lacalip1 [-ip2] [netmask mask]]** **[port | gportport [-port]]** **[interface if1 [,if2] [,ifn]]** [state static [,dump] [,portmap] [,norandomseq] [,identity]]

其中：
[global | local ip1 [-ip2]] [netmask mask]：根据全局 IP 地址或本地 IP 地址，显示活动的翻译，用网络掩码限定 IP 地址的范围；
[port|gportport [-port]：根据指定的本地和全局端口，显示活动的翻译；
[interface if1 [,if2][,ifn]]：根据接口，显示活动的翻译；
[state]：根据状态，显示活动的翻译：

- static 翻译（static），
- dump（cleanup），
- PAT global（portmap），
- 具有 norandomseq 设置（norandomseq）的 nat 或 static 翻译，
- 或 nat 0 标识特性的使用（identity）。

2.3 访问控制列表 ACL 配置

36. 访问控制列表（Access Control List）

是一个有序的语句集，它通过对比报文中字段值与访问控制列表参数，来允许或拒绝报文通过某个接口。

37. ACL 基本规则

- ACL 规则按名称或编号进行分组
- 列表中每条 ACL 语句有一组条件和一个操作，如果需要多个条件或多个操作，则必须使用多个 ACL 语句来完成
- 如果当前语句的条件没有匹配，则处理列表中的下一条语句
- 如果条件匹配，则执行语句后面的操作，且不再与其他 ACL 语句进行匹配
- 如果列表中的所有语句都不匹配，那么丢弃该数据包

38. ACL 注意事项

- 由于 ACL 语句**默认是拒绝不匹配的数据包**，所以在列表中至少要有一个允许的操作。否则，所有数据包都会被拒绝掉
- 注意语句的顺序。条件严的语句应该放在列表的顶部，条件宽的语句应该放在列表的底部。从而，避免条件严的语句永远也得不到执行
- 只能在设备的每个接口、每个协议、每个方向上应用一个 ACL
- ACL 只能应用在接口上
- 先处理入站 ACL，再进行数据路由
- 先进行数据路由，再处理出站接口上的出站 ACL
- ACL 会影响通过接口的流量和速度，但不会过滤路由器本身产生的流量

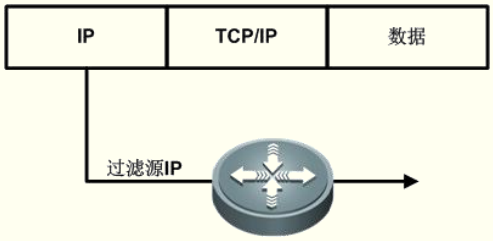
39. ACL 放置位置

- 只过滤数据包**源地址**的 ACL 应该放置在**离目的地尽量近的地方**
- 过滤数据包的源地址和目的地址以及其他信息的 ACL，则应该尽量放在离源地址近的地方

40. 两种 ACL

(1) 标准 ACL

标准 ACL 只能过滤 IP 数据包头中的源 IP 地址

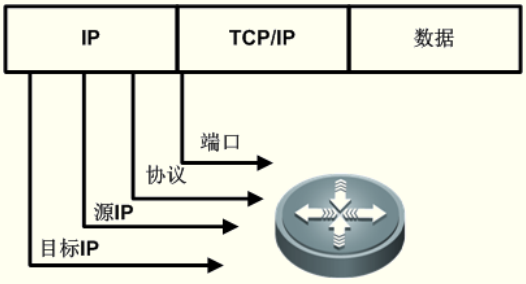


标准 ACL 通常配置在路由器上实现以下功能：

- 限制通过 VTY 线路对路由器的访问（telnet、SSH）
- 限制通过 HTTP 或 HTTPS 对路由器的访问
- 过滤路由更新

(2) 扩展 ACL

扩展的 IP 访问表用于扩展报文过滤的能力。



扩展访问列表允许过滤内容：

源和目的地址、协议、源和目的端口以及在特定报文字段中允许进行特殊位比较的各种选项。

41. 创建标准 ACL P196

(1) 使用编号创建

创建 ACL

(config)#access-list *listnumber* {permit | deny} *address* [*wildcard–mask*]

listnumber：ACL 编号（1-99 之间）

address：源地址

wildcard–mask：源地址通配符掩码[1]

(2) 使用命名创建

定义 ACL 名称

(config)#ip access-list standard *name*

name：ACL 名称

定义规则

(config-std-nacl)#{deny | permit} [*source wildcard* | any]

source：源地址

wildcard：源地址通配符掩码

42. 创建扩展 ACL P199

(1) 使用编号创建

创建 ACL

(config)#access-list *listnumber* {permit | deny} *protocol* ***source source-wildcard–mask*** [*operator port*] ***destination destination-wildcard–mask*** [*operator port*]

listnumber：ACL 编号（100-199 之间）

protocol：协议名称或编号（tcp, udp, icmp, ip）

source：源地址

source-wildcard–mask：源地址通配符掩码

destination：目的地址

destination-wildcard–mask：目的地址通配符掩码

operator：等于 eq，不等于 neq，大于 gt，小于 it，范围 range

port：TCP 或 UDP 十进制端口号或名称（http, ftp, www 等）

(2) 使用命名创建

定义 ACL 名称

(config)#ip access-list extended name

定义规则

(config-ext-nacl)#{deny | permit} *protocol* {*source source-wildcard* | host *source* | any} [*operator port*] {*destination destination-wildcard* | host *destination* | any} [*operator port*]

43. 在接口上应用

(config-if)#ip access-group *{id | name}* {in | out}

in：当数据流入路由器接口时

out：当数据流出路由器接口时

---

[1] 通配符掩码与子网掩码相反。例如子网掩码 255.255.255.0 的通配符掩码为 0.0.0.255。

2.4 虚拟防火墙配置

44. 打开防火墙虚拟防火墙功能

pixfirewall(config)# mode multiple

注：打开前需要激活防火墙，配置完需要重启防火墙

pixfirewall# show mode

若激活成功则会显示 Security context mode: multiple

45. 配置防火墙子接口，为其分配 VLAN

pixfirewall(config)# int e1.2

pixfirewall(config-subif)# vlan 2

46. 配置安全上下文，为其分配接口，指定其配置文件存放位置

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

47. 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

修改 MAC 地址命令

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

48. 回到系统

通过下面命令可以回到系统

pixfirewall/admin(config)# changeto system

在主接口打开接口

pixfirewall(config)# int e1

pixfirewall(config-if)# no sh

注：只有主接口才能 no sh

3 PIX 防火墙系统日志配置

49. ★启用日志功能

在缺省情况下，PIX 防火墙上的全部日志功能都是被禁用的。为了启用日志功能，应使用 **logging on** 命令。

50. 日志级别

在我们配置 PIX 防火墙上的日志功能之前，一个需要掌握的重要概念是，应用于各种日志命令中的“**日志级别**（logging level）”。日志级别决定了我们想要在日志中反映出什么级别的细节。由于在繁忙的网络中，系统日志可能会产生大量的数据，所以这是一个需要重点考虑的问题。

日志级别	日志级别描述		系统状况
0	紧急	Emergencies	系统不可用消息
1	告警	Alerts	应立即采取行动
2	严重的	Critical	严重的情况
3	错误	Errors	错误消息
4	警告	Warnings	警告信息
5	通知	Notifications	正常但是重要的情况
6	信息	Informational	信息消息
7	调试	Debugging	调试消息并记录 FTP 命令和 WWW 的 URL

当设置了一个日志级别号时，任何**更高级别的日志消息都将被抑制**。这就是说，如果我们将日志级别设置为 4，我们就不会看到任何来自级别 5、6 或 7 的系统日志消息。在设置日志级别时，我们可以在命令中使用数字或名称，但是 PIX 防火墙在配置中会将数字翻译成名称。

51. logging 命令

logging 命令用来在 PIX 防火墙上管理和配置系统日志的所有方面。下面是 logging 命令的不同组合的语法：

(1) ★on

开始向所有的输出位置发送系统日志消息。用 no logging on 命令停止所有的日志记录。

(2) buffered

向内部缓冲区发送系统日志消息，可以用 show logging 命令查看缓冲区中的信息。用 clear logging 命令清除消息缓冲区。新消息将被添加到缓冲区的末尾。

(3) level

将系统日志消息级别指定为一个数字或字符串。我们指定的级别意味着，我们需要这个级别和低于这个级别的消息。例如，如果级别是 3，那么系统日志将显示 0、1、2 和 3 级别的消息。

(4) console

当每条系统日志消息发生时，制定让系统日志消息出现在 PIX 防火墙的控制台上。我们可以用级别来限制出现在控制台上的消息类型。Cisco 推荐我们不要再实际的生产运行模式中使用这条命令，因为它的使用将降低 PIX 防火墙的性能。

(5) facility

指定系统日志设备。缺省是 20。

(6) history

为发送系统日志陷捕消息而设置 SNMP 消息级别。

(7) ★host

指定系统日志服务器，让它接收从 PIX 防火墙发送的消息。

我们可以使用多个 logging host 命令，来指定附加的服务器，让它们都接收系统日志消息。但是，一台服务器只可以被指定为接收 UDP 或 TCP，而不能两者都接收。PIX 防火墙只将 TCP 系统日志消息发送到 PIX 防火墙系统日志服务器。

(8) in_if_name

系统日志服务器所位于的接口。

(9) ip_address

系统日志服务器的 IP 地址。

(10) protocol

发送系统日志消息所采用的协议：tcp 或 udp。

PIX 防火墙只把 TCP 系统日志消息发送到 PIX 防火墙系统日志服务器。我们只能用 write terminal 命令来查看我们先前输入的端口和协议值——TCP 协议被列为 6，UDP 协议被列为 17，这还需要我们在该命令的输出重查找“logging”命令语句。

(11) port

PIX 防火墙发送 UDP 或 TCP 系统日志消息所采用的端口。

这个端口必须是系统日志服务器侦听的同一端口。对于 UDP 端口，缺省时 514，改变这个值所允许的范围是 1025 到 65535。对于 TCP 端口，缺省时 1470，允许的范围是 1025 到 65535。TCP 端口只能与 PIX 防火墙系统日志服务器一起工作。

(12) message

指定将被允许的消息。

使用 no logging message 命令来抑制系统日志消息。使用 clear logging disabled 命令来将不被允许的消息复位成最初状态。使用 show message disabled 命令来列出被抑制的消息。除了明确指出不被允许的以外，所有的系统日志消息都被允许。“PIX Startup begin”消息不能被拦阻，每个具有一条以上消息的命令语句也不能被拦阻。

(13) syslog_id

指定一个允许或不被允许的消息号。

(14) disabled

清除或显示被抑制的消息。我们可以使用 no logging message 命令来抑制消息。

(15) monitor

指定系统日志消息出现在到 PIX 防火墙控制台的 Telnet 会话中。

(16) queue queue_size

指定用于存储系统日志的队列长度。在处理系统日志消息之前，使用这个参数。队列参数缺省为 512 条消息，0(zero)表示不受限制，最小为一条消息。可以使用 show logging queue 命令，来确定队列中的消息数量。

(17) standby

让故障切换的备用单元也发送系统日志消息。缺省情况下，这个选项是关闭的。我们可以启用它，以确保在发生故障切换的情况下，备用单元的系统日志消息能保持同步。但是，这个选项将在系统日志服务器上，造成两倍的数量流量。用“no logging standby”命令禁止这个选项。

(18) ★timestamp

指定发送到系统日志服务器的系统日志消息应该在每条消息中**具有一个时间标记**。

(19) ★trap

只为系统日志消息**设置日志级别**。

(20) clear
清除由“logging buffered”命令使用的缓冲区。
(21) show
列出启用了哪位日志选项。如果使用了 logging bufered 命令，show logging 命令还会列出当前的消息缓冲区。

52. ★logging host 命令
语法：logging host [if_name] ip_address[protocol/port]
这条日志命令指定系统日志服务器的 IP 地址，还可以选择指定协议和端口。当不指定协议端口时，PIX 防火墙缺省的 UDP 端口是 514。

53. ★logging trap 命令
logging trap 命令用来决定什么级别的系统日志消息将被发送到系统日志服务器。
这条命令语法是：logging trap level

54. logging buffered 命令
使用 logging buffered 命令，向 PIX 防火墙上的内部存储器缓冲区发送系统日志消息可以用 show logging 命令查看缓冲区中的信息。

logging buffered 命令语法如下：logging buffered level

使用 clear logging 命令，可以清除消息缓冲区。新的消息被添加到缓冲区的末尾。

55. logging console 命令
使用此命令，来强制 PIX 防火墙将系统日志消息显示到控制台。使用 no logging console 命令，可以关闭控制台日志记录。
这条命令的两种形式如下：
logging console level
no logging console
发送到控制台的系统日志消息的数量和类型，将取决于在 logging console 命令中设置的级别。

56. logging facility 命令
logging facility 命令语法如下：logging facility facility
这条命令设置被发送给系统日志服务器的系统日志消息的设备号。存在 8 个设备，LOCAL0(16)到 LOCAL7(23)；缺省是 LOCAL(20)。较旧的系统日志主机只能根据消息中的设备号，对输入进行存档。大多数较新的系统日志实现方式能够根据设备或硬件设备的源 IP 地址灵活地对消息存档。

57. logging monitor 命令
使用此命令，可以让 PIX 防火墙将系统日志消息发送给到 PIX 防火墙的 Telnet 会话。
no logging monitor 命令让 PIX 防火墙停止向 Telnet 会话发送系统日志消息。

这条命令的两种形式如下：
logging monitor level
no logging monitor

58. logging standby 命令

此命令能够让用于故障切换的备用单元也发送系统日志消息。在缺省情况下，standby 选项是被关闭的。我们可以启用它，以确保在在发生故障切换的情况下，备用单元的系统日志消息能保持同步。但是，这个选项将在系统日志服务器上，造成两倍的数据流量。

59. ★logging timestamps 命令

此命令强制 PIX 防火墙用自己的内部时钟，为每条系统日志消息打上时间标记。我们应用 show clock 命令，来确认 PIX 防火墙上的时间被正确地进行了设置。
一个很好的习惯是，将 PIX 防火墙的时钟设置为 UTC（格林尼治标准时间），以维持跨越多个时区的日志时间一致性。如果我们还需要将系统日志记录用作法律活动中的证据，则需要所有的时间标记都被设置为 UTC。

60. no logging message 命令

此命令的语法如下：
logging message syslog_id
no logging message syslog_id

使用 no logging message 命令，来指定将要被抑制的系统日志消息。缺省情况下，除了明确指出不被允许的消息之外，所有的系统日志消息都被允许。“PIX Startup begin”消息不能被拦阻，每个具有一条以上消息的命令语句也不能被拦阻。

指定一个消息号，使它不被允许或被允许。如果在系统日志中，一条消息被列为%PIX-1-101001，就可以使用 no logging message 101001 命令，来抑制这个 syslog_id。把被抑制的系统日志消息添加到 PIX 防火墙的配置文件中。

为了查看在运行配置中被抑制的系统日志消息，可以使用 write terminal 命令。为了查看在启动配置中被抑制的系统日志消息，可以使用 show config 命令。

61. show logging 命令

此命令可以列出启用了哪些日志选项。如果已使用了 logging buffered 命令，show logging 命令还将列出当前的消息缓冲区。
下面例子显示了此命令的一个输出：

```
pixfirewall(config)# show logging
Sysloglogging:enabled
Timestamp logging:disabled
Standby logging:disabled
Console logging:disabled
Monitor logging:disabled
Buffer logging:disabled
Trap logging:level debugging,facility20,46498 message logged
Logging to inside 192.168.111.3
History logging:level debugging,facility20,46498 message logged
```

62. clear logging 命令

此命令可以清楚被 logging buffered 命令使用的缓冲区。

因为 PIX 防火墙只向日志缓冲区记录 100 条消息，所以通常不需要清除缓冲区。在缓冲区被充满之后，缓冲区中最旧的消息将被最新的消息所覆盖。在一个实际生产运行环境中，每分钟可能会有几百条消息，或者更多条消息。这条命令可以用来初始化本地日志缓冲区。

63. 实例

现在，我们熟悉了各种日志选项，下例显示了一台 PIX 防火墙的配置条目，它将 PIX 防火墙配置成向内部接口上的系统日志服务器发送一条打上时间标记的系统日志消息。系统日志消息 111001”Begin configuration:consolewriting to memory”将被抑制。

例：使用 TCP 方式将日志记录发送给 Cisco PIX 防火墙系统日志服务器的 PIX 防火墙系统日志配置实例。

```
logging on
logging host inside 10.10.1.10 tcp/1470
logging trap informational
logging timestamp
no logging message 111001
```

4 PIX 防火墙 AAA 配置

4.1 AAA（认证 授权 审计）

64. 定义 AAA

认证(authentication)可以确定用户的身份，并对信息进行验证。传统的认证方法使用一个用户(或者某个唯一的标识符)和一个固定的口令。利用一个用户 ID 来访问一台设备或网络，可以识别用户是谁。一旦用户被认证，认证服务器就可以被配置成根据该用户 ID 和口令，允许指定的授权行为。

授权(authorization)定义了用户可以作什么。当一个用户已经登录进来，并正在访问一种服务、主机或网络时，这个用户正在做什么的记录可以被保存下来。

审计(accounting)是跟踪记录用户在做什么的一种行为。如果拥有一条审计记录，它记录了网络中的哪些资源正在被访问，这将非常有帮助。如果网络中发生了故障，拥有历史记录将有助于确定并最终排除这些故障。审计记录也可以用来计费、提供法律依据和进行规划。

65. AAA 处理

当 AAA 用于 PIX 时，通常按照下列方式对 AAA 进行处理：
1、客户端请求访问某项服务。PIX 防火墙作为客户端和服务所驻留的设备之间的网关，要求客户端发送一个用户 ID 和口令。
2、PIX 防火墙收到这些信息后，将它转发给 AAA 服务器，在那里确定对该请求是允许还是拒绝。服务器被定义为一个逻辑实体，它可以提供三个 AAA 功能中的任意一个。AAA 服务器可以拥有用户 ID/口令数据库，用来确认客户端是否可以访问所请求的服务。

66. 认证、授权和审计(AAA)

PIX 防火墙使用认证、授权和审计(AAA)，来确定**用户是谁**，**用户可以做什么**，以及**用户曾经做过什么**。PIX 自身的基本访问控制是基于 IP 地址和端口的。这些访问控制不能提供一种机制来标识每个用户，并根据那个用户进行数据流量控制。在没有授权的情况下，认证也是有效的。但在没有认证的情况下，授权永远不会是有效的。

67. 口令和用户名字符限制

PIX 防火墙支持的认证(AAA)用户名可以最多具有 127 个字符，口令可以最多具有 63 个字符。因为当使用 AAA 时，对通过 FTP 或 HTTP 登录要进行的特殊处理，所以口令或用户名不可以包含"@"字符，不可以将该字符作为口令或用户名字符串的一部分。

4.2 配置认证 authentication

68. 配置认证

一旦配置了 CSACS，必须将一个用于 AAA 服务器的相应配置条目输入到 PIX 服务器的配置中。对于 AAA，PIX 防火墙管理员可以为之配置许多不同的选项。

- 首先，必须创建一个 AAA 组，并指定一个认证协议。

- 其次，创建一个 AAA 服务器，并将它分配到 AAA 组中。

可以将多个 AAA 服务器定义成为同一个 AAA 组的成员。这样就允许服务器访问失败时的接续处理。如果第一个 AAA 服务器不可达，PIX 防火墙将把请求发送给下一个定义的 AAA 服务器。
使用 aaa-server 命令，可以指定 AAA 服务器组。对于 PIX 防火墙，管理员可以定义单独的 TACACS+或 RADIUS 服务器组，用来指定不同类型的数据流，比如一个 TACACS+服务器用于输入的流量，一个不同的 TACACS+服务器用于输出的流量。AAA 命令通过参考组标记，将认证、授权或审计流量引导到适当的 AAA 服务器。

管理员可以拥有最多 16 个标记组，每个组可以拥有最多 16 台 AAA 服务器，总共最多 256 台 TACACS+或 RADIUT 服务器。通过指定多台 AAA 服务器，管理员可以提供热备份。当用户登录时，一次只访问一台服务器，从标记组中指定的第一台服务器开始，直到一台服务器做出相应为止。

缺省配置提供了两种 AAA 服务器协议。
下面两个配置参数在缺省情况下，将出现在配置文件中：
aaa-server tacacs+ protocol tacacs+
aaa-server radius protocol radius

PIX OS 较老的版本不需要创建 AAA 组。将这两个参数作为缺省参数的好处是，或具有一个缺省的组。这意味着，当把一个较老的版本升级为一个较新的版本时，其他的 AAA 命令将不会被丢失。

69. ★aaa-server 命令

aaa-server 命令的语法如下：
aaa-server *group_tag* **(***if_name***) host** *server_ip key* **timeout** *second*
aaa-server *group_tag* **protocol** *auth_protocol*

其中，
group_tag：一个字母数字型的字符串，它是服务器组的名称。
if_name：与服务器所在网络连接的接口名称。
host server_ip：TACACS+或 RADIUT 服务器的 IP 地址
key：一个区分大小写的字母数字型密码，他最多包含 127 个字符，与 TACACS+服务器上的密钥是同一个值。输入长度超过 127 的任何字符将被忽略。在密钥中，不允许有空格。
timeout seconds：一个重新发送定时器，它指定了重发之前等待的时间，PIX 防火墙在选择下一台 AAA 服务器之前，对 AAA 服务器会进行 4 次访问尝试。缺省是 5s。最长可以使 30s。
protocol auth_protocol：AAA 服务器的类型，可以是 tacacs+或 radius

例子：指定 AAA 服务器组。
aaa-server MYTACACS protocol tacacs+
aaa-server MYTACACS (inside) host 10.0.0.2 secretkey timeout 10

例子中的第一条语句是创建组，并指定认证协议。组的名称是 MYTACACS，认证协议是 TACACS+。例子第二条语句将服务器分配到组 MYTACACS 中，指定 AAA 服务器将与 PIX 进行通信的接口(insede)，定义 AAA 服务器的 IP 地址(10.0.0.2)，分配一个密钥，定义超时时间。

70. aaa authentication 命令

配置完 aaa-server 命令之后，现在需要管理员来配置认证。aaa authentication 命令用以启用或禁止用户认证服务，其语法如下：

aaa authentication include | exclude *authen_service* inbound | outbound | if_name *local_ip local_mask foreign_ip foreign_mask* group_tag

参数描述：
authentication：启用或禁止用户认证，提示用户输入用户名和口令，并用认证服务器验证这些信息。

include：创建一条新规则来包括指定服务。
exclude：通过将到指定主机的指定服务排除在认证之外，为一条以前设置过的规则创建一个例外事例。

authen_service：一种应用，用户使用它来访问网络。可以使用的值有 any、ftp、http 或 telnet。any 值将为所有的 TCP 服务启用认证。

inbound：认证向内的连接。
outbound：认证向外的连接。
if_name：用户被要求认证时所来自的接口名称。

local_ip：将被认证的主机或网络的 IP 地址。
local_mask：local_ip 的网络掩码。

foreign_ip：将要被允许访问 local_ip 地址的主机 IP 地址。用 0 来指代所有的主机。
foreign_mask：foreign_ip 的网络掩码。

group_tag：用“aaa-server”设置的组标记。

71. 配置 aaa authentication 实例

下面例子显示了如何配置 aaa authentication 命令，并通过足名称 MYTACACS，将该命令语句与 aaaserver 命令绑定。将任何 IP 地址或网络设置为 0，相应的掩码也设置为 0，这就等效于 any 或 all hosts。

例，配置 AAA 认证，并将它绑定到 AAA 服务器。
aaa-server MYTACACS protocol tacacs+
aaa-server MYTACACS (inside) host 10.0.0.2 secretkey timeout 10
aaa authentication include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 MYTACACS
aaa authentication include telnet outbound 0.0.0.0 0.0.0.0. 0.0.0.0 0.0.0.0 MYTACACS
aaa authentication include ftp dmz 0.0.0.0. 0.0.0.0 0.0.0.0 0.0.0.0 MYTACACS
aaa authentication exclude any outbound 10.0.0.33 255.255.255.255 0.0.0.0 0.0.0.0 MYTACACS

72. ★控制台访问的认证

可以使用 aaa authentication console 命令，来要求对 PIX 防火墙的串行、enable 或 Telnet 控制台访

问进行认证检查。串行控制台选项还向系统日志服务器记录任何通过串行控制台做出的改动。

语法：**aaa authentication [serial | enable | telnet] console** group_tag

其中，
serial：在串行控制台连接上出现第一命令行提示符之前，要求用户名和口令。
enable：对于串行或 Telnet 连接，在访问特权模式之前，要求用户名和口令。
telnet：在 Telnet 控制台连接的第一个命令行提示符之前，强制用户指定用户名和口令。
console：指定对 PIX 防火墙控制台的访问需要认证，而且可以选择将配置改动记录到系统日志服务器上。
group_tag：用“aaa-server”命令设置的组标记。

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

73. 改变认证超时时间

使用 timeout uauth 命令，指定在用户连接变成空闲之后，缓存中的信息应该被保存多长时间。通常情况下，timeout 命令的值必须至少是 2min。使用 clear uauth 命令，为所有用户删除所有的授权缓存信息，这样会让所有用户在下次建立连接时，需要进行重新认证。可以将 timeout uauth 命令设置成 0，这样禁止使用缓存。

语法：timeout uauth [hh:mm:ss] [absolute | inactivity]

其中，
uauth [hh:mm:ss]：在认证和授权缓存超时之前的持续时间，用户对下一条连接必须进行重新认证。这段持续时间必须小于 xlate 的值。将它设置成 0 来禁止使用缓存。如果在连接中使用被动 FTP，就不能将它设置成 0。
absolute：连续运行 uauth 定时器，但是定时器超时之后，等待对用户进行 chognxin 提示，直到用户开始一条新的连接为止，比如在 web 浏览器中点击一个链接。缺省的 uauth 定时器设置是 absolute。要想禁止 absolute，将 uauth 定时器设置成 0。
inactivity：在连接变成空闲之后，启动 uauth 定时器。

74. 改变认证提示

我们可以使用 auth-prompt 命令，为 HTTP、FTP 和 Telnet 访问创建 AAA 挑战文本。这条文本显示的是，在登录时所显示的上述用户名和口令提示。认证拒绝和接受的文本也可以被改变。

语法：auth-prompt [accept | reject | prompt] string

其中，
accept：表示如果接受一个用户通过 Telnet 的认证，显示提示字符串。
reject：如果拒绝一个用户通过 Telnet 的认证，显示提示字符串。
prompt：这个关键词后面的是 AAA 挑战提示字符串。为了保持后向兼容性，这个关键词是可选的。
string：这个字符串最多具有 255 个字母数字型字符。不能使用特殊字符；但是，允许使用空格和标点符号。输入一个问号，或按回车键可以结束这个字符串。(问号将会出现在字符串中)

4.3 配置授权 authorization

PIX 防火墙与访问控制服务器使用 TACACS+授权服务来决定一个被认证的用户可以访问什么服务。在对 FTP、Telnet 和 HTTP 进行授权时，可以在 aaaauthorization 命令中使用应用名称。
需要重点记住，没有被指名的服务是被隐含授权的。如果想为以前设置的规则产生一个例外事例，可以使用 exclude 参数。

75. aaa authorization 命令

语法：
aaa authorization include | exclude ***author_service*** inbound | outbound | if_name local_ip local_mask foreign_ip foreign_mask

参数：
authorization：为服务启用或禁止 TACACS+用户授权。由认证服务器决定用户被授权访问什么服务。
include：创建一条新规则来包括制定的服务。
exclude：通过将到指定主机的指定服务排除在认证、授权或审计之外，为一条以前设置的规则创建一个例外事例。exclude 参数通过允许用户指定排除到一台或多台特定主机的一个端口，改进了以前的 except 选项。
author_service：需要授权的服务。可以使用 any、ftp、http、telnet 或 protocol/port。没有被指明的服务是被隐含授权的。

76. 实例

aaa authorization include udp/53-1024 inside 0 0 0 0

这个例子为所有的客户端启用了到内部接口进行 DNS 查找的授权，并授权访问位于端口范围 53 到 1024 的任何其他服务。
指定端口范围可能在授权服务器上产生非预期的后果。PIX 防火墙将端口范围作为字符串发送给服务器，期望服务器将对它进行分析，找出指定的端口。并不是所有的服务器都这样做。而且当我们的意图是对指定的服务进行用户授权认证时，如果范围不被接受，这将不能实现。

77. 实例

aaa authorization include ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 MYTACACS
aaa authorization exclude ftp outbound 10.0.0.33 255.255.255.255 0.0.0.0 0.0.0.0 MYTACACS

4.4 配置审计 accounting

在配置完认证和授权之后，通常还需要配置审计。审计信息可以用来跟踪记录谁正在访问指定的主机或应用。审计记录可以显示用户登录进入系统的时间长度。他们还可以显示发送和接收的信息量。这些信息可以被用来计费。

78. aaa accounting 命令

语法：
aaa accounting include | exclude ***acctg_service*** inbound | outbound | if_name local_ip local_mask

foreign_ip foreign_mask group_tag

参数:
acctg_service: 审计服务。可以为所有服务提供审计，管理员也可以只为一种或多种服务提供审计。可以使用的值有 any、ftp、http、telnet 或 protocol/port。

79. 实例

aaa accounting include any outbound 0.0.0.0 0.0.0.00.0.0.00.0.0.0 MYTACACS
aaa accounting exclude any outbound 10.0.0.33 255.255.255.255 0.0.0.0 0.0.0.0 MYTACACS

5 PIX 防火墙 IPSec VPN 配置

5.1 IPSec VPN 基础知识

80. Cisco 安全 PIX 防火墙支持安全的 VPN

虚拟专用网络(VPN)服务可以通过一个共享的公用网络基础设施(比如 Internet)，提供安全、可靠的连接。由于网络设施是共享的，所以连接所需的费用通常比现有的采用专线的专用网低很多。

PIX 防火墙可以很好地支持 VPN 服务。PIX 防火墙的高性能符合开放标准，以及容易配置，可以使它成为一个通用的 VPN 网关。VPN 加速卡(VPN Accelerator Card，VAC)选件可以用于 PIX 515、520、525 和 535。VAC 提供了 100 一 Mbit / s 3DES 处理性能，而不需要增加软件，也不需要改动 PIX 防火墙配置。

81. IPSec

IPSec 是一套安全协议和算法，用来在网络层保护数据的安全。

IPSec 提供了一种机制，可以保证通过 IP 网络传输的数据安全，确保通过不受保护的网络(比如 Internet)实现数据通信的保密性、完整性和真实性。

IPSec 启用了下列 PIX 防火墙 VPN 特性：

- 数据保密性——IPSec 发送者在向网络发送数据包之前，可以加密数据包。
- 数据完整性——IPSec 接收者可以认证 IPSec 对等体，并对 IPSec 发送者发送的数据包进行鉴别，确保数据在传输过程中没有被修改。
- 数据起源认证——IPSec 接收者可以对发送 IPSec 数据包的源进行认证。这项服务依赖于数据完整性服务。
- 防重放(Anti replay)——IPSec 接收者可以检测并拒绝重放数据包，这有助于防止欺骗和中途干扰者(man-in-the-middle)攻击。

82. IKE

IKE 是一个混合协议，它由 ISAKMP 和 Oakley 标准组成，向 IPSec 提供实用的服务：认证 IPSec 对等体、协商和 IPSec 安全关联，为 IPSec 使用的加密算法建立密钥。IKE 通过指定的 UDP 端口 500 运行。

83. SA

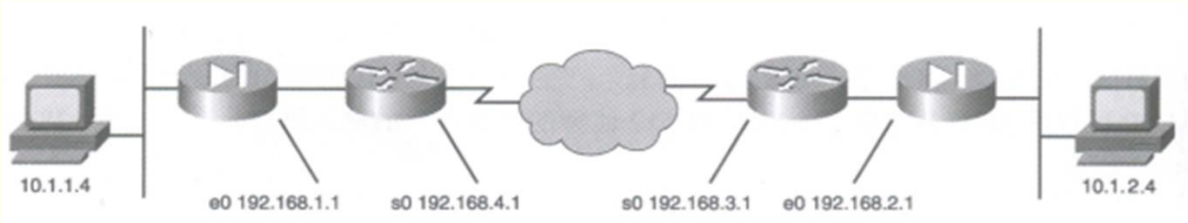
安全关联(SA)的概念是 IPSec 的基础。一个 SA 是 IPSec 对等体之间的一条连接，它决定了对等体之间可用的：IPSec 服务，类似于一个'FCP 或 UDP 端口。每个 IPSec 对等体都在内存中维护一个 SA 数据库，其中包含了 SA 参数。SA 可以通过 IPSec 对等体地址、安全协议和安全参数索引(SPI)，来被唯一性地标识。我们需要配置 SA 参数，并在 PIX 防火墙上监视 SA。

84. CA

PIX 防火墙支持**证书授权中心**(CA)，这通过为每台设备提供一种数字身份卡，允许被 IPSec 保护的网络可以较容易地进行扩展。这些数字 ID 卡被称为数字证书。当两个 IPSec 对等体想要进行通信时，它们就交换数字证书，以此证明彼此的身份(因此，不再需要为每个对等体手工交换公钥，或者在每个对等体上手工指定一个共享密钥)。数字证书是从 CA 中心那里获取的。PIX 防火墙上的 CA 支持将使用 RSA 签名来对 CA 交换进行认证。

5.2 配置 PIX 防火墙的 IPSec 支持

85. 配置 IPSec 的任务



在 PIX 防火墙上，用预共享密钥配置 IPSec 加密的过程中，涉及的 4 个关键任务是：

- 任务 1：为 IPSec 做准备——为 IPSec 做准备将涉及确定加密策略的细节，包括标明我们想要保护的主机和网络、选择一种认证方法、确定关于 IPSec 对等体的细节、标明我们需要的 IPSec 特性，并确保现有的访问控制列表允许 IPSec 数据流。如果在我们的 PIX 防火墙前面有一台执行过滤功能的边界路由器，它必须允许 IP 协议 50 和 5 1，以及 UDP 端口 500。

- 任务 2：为预共享密钥配置 Internet 密钥交换(IKE)——配置 IKE 将涉及启用 IKE、创建 IKE 策略、设置身份模式、并且使配置生效。

- 任务 3：配置 IPSec——IPSec 配置包括创建加密用访问控制列表，定义变换集 (transform set)，创建加密图条目，并将加密图集应用于接口。

- 任务 4：测试并检验 IPSec 的总体配置——这项任务涉及使用 show、debug 及相关命令测试并检验 IPSec 加密的工作情况，并解决相关问题。

5.2.1 任务 1 为 IPSec 做准备

要想实现一个成功的 IPSec 网络，就需要在开始配置每台 PIX 防火墙和其他 IPSec 对等体之前，仔细地进行规划。配置 IPSec 加密可能会比较复杂。我们开始先应该根据公司的总体安全策略，定义详细的 IPSec 安全策略。下面是为 IPSec 进行准备的一些规划步骤：

86. 为 IPSec 进行准备

步骤 1：根据对等体的个数和位置，定义 IPSec 对等体之间的 IKE(IKE 阶段 1，或主模式)策略。

步骤 2：定义 IPSec(IKE 阶段 2，或快捷模式(quick mode))策略，包括 IPSec 对等体细节，比如 IP 地址和 IPSec 变换集和模式。

步骤 3：通过使用 write terminal、show isakmp、show isakmp policy、show crypomap 和其他 show 命令，检查当前的配置。

步骤 4：确保网络在没有使用加密的情况下可以正常工作，在测试加密之前，通过使用 ping 命令，并发送测试数据流，以此来排除基本的路由问题。

步骤 5：确保在边界路由器和 PIX 防火墙中现有的访问控制列表允许 IPSec 数据流，或者所需的数据流将被过滤出来。

5.2.2 任务 2 为预共享密钥配置 IKE

87. ★步骤 1：用 isakmp enable 命令启用或禁止 IKE。

配置 IKE 的第一步是在用来终结 IPSec 隧道的接口上启用或禁止 IKE。我们可以使用 isakmp enable 命令，在每个接口上启用和禁止 IKE。在缺省情况下，IKE 是被启用的，我们可以使用这条命令的 no 形式来禁止 IKE。

命令语法如下所示：**isakmp enable *interface-name***

例如：pixfirewall#(config)isakmp enable outside

interface-name 参数指定了接口名称，在这个接口上启用 IKE 协商。

88. ★步骤 2：用 isakmp policy 命令创建 IKE 策略。

配置 PIX 防火墙 IKE 支持的下一个主要步骤是，定义一套 IKE 策略。定义一套 IKE 策略的目标是在两个 IPSec 端点之间建立对等关系。使用在规划任务的过程中收集到的 IKE 策略细节。

使用 isakmp policy 命令来定义 IKE 策略。IKE 策略定义了一套参数，这些参数将在 IKE 协商期间使用。可以使用这条命令的 no 形式来删除 IKE 策略。

isakmp policy 命令参数

命令参数	描　述
policy *priority*	唯一地指定了 IKE 策略，并为它分配了一个优先级。使用一个从 1 到 65534 的整数，其中 1 是最高优先级，65534 是最低优先级
authentication pre-share	指定预共享密钥作为认证手段
authentication rsa-sig	指定 RSA 签名作为认证手段
encryption des	指定 56 位 DES-CBC 作为将被用于 IKE 策略的加密算法。这是缺省的值
encryption 3des	指定三重 DES 加密算法将被用于 IKE 策略
group 1	指定 768 比特 Diffie-Hellman 组将被用于 IKE 策略。这是缺省的值
group 2	指定 1024 比特 Diffie-Hellman 组将被用于 IKE 策略
hash md5	指定 MD5（HMAC 变种）作为将被用于 IKE 策略的散列算法
hash sha	指定 SHA-1（HMAC 变种）作为将被用于 IKE 策略的散列算法。这是缺省的散列算法
lifetime *seconds*	指定每个安全关联在到期之前应该存在多少秒。使用一个从 60 到 86400 秒（一天）的整数值。我们通常可以将这个值保留为缺省值 86400

命令语法如下所示：

isakmp policy priority authentication pre-share

pixfirewall # (config) isakmp policy 10 authentication pre-share

isakmp policy priority encryption (des | 3des)
pixfirewall # (config) isakmp policy 10 encryption 3des

isakmp policy priority (group1 | group2)
pixfirewall#(config)isakmp policy 10 group2

isakmp policy priority hash (md5 | sha)
pixfirewall#(config)isakmp policy 10 hash sha

isakmp policy priority lifetime *seconds*
pixfirewall#(config)isakmp policy 10 lifetime 86400

如果我们不为策略指定这些命令，那么将使用参数的缺省值。我们可以通过使用这条命令的 no 形式，将一个值复位成它的缺省值。例如，如果以前将加密方法设置为 3DES，要想将它复位成 DES，可以使用 no isakmp policy 100 encryption 命令。

89. ★步骤 3：配置 Tunnel Group
命名 tunnel group，并指定 VPN 连接类型
tunnel-group *name* type *type*
fw1(config)# tunnel-group 192.168.6.2 type ipsec-l2l

配置预共享密钥
tunnel-group *name* [general-attributes | ipsec-attributes]
pre-shared-key *key*
fw1(config)# tunnel-group 192.168.6.2 ipsec-attributes
fw1(config-ipsec)# pre-shared-key cisco123

90. 步骤 4：用 show run crypto isakmp 命令，检验 IKE 配置。
我们可以用 show run crypto isakmp 命令显示已配置的和缺省的策略。

5.2.3 任务 3 配置 IPSec

配置 PIX 防火墙 IPSec 的下一项主要任务是配置以前收集的 IPSec 参数。

91. ★步骤 1：用 access-list 命令配置加密用访问控制列表。
(1) ACL
加密用访问控制列表定义了 IPSec 将保护哪些 IP 数据流，不保护哪些 IP 数据流。加密用访问控制列表为 IPSec 执行下列功能：

- 选择 IPSec 将保护的向外的数据流。
- 为了过滤出并丢弃本来应该被(但却没有被) IPSec 所保护的数据流，对向内的数据流进行处理。
- 在处理 IKE 协商时，决定是否接受请求数据流的 IPSec 安全关联请求。

加密用访问控制列表用于识别要被保护的数据流。虽然加密用访问控制列表的语法与常用访问控制

列表的语法一样，但是对于加密用访问控制列表，含义稍微有些不同：permit 是指必须对匹配的数据包进行加密，deny 是指匹配的数据包将不被加密。加密用访问控制列表的操作类似于在 PIX 防火墙接口上应用到向外数据流的访问控制列表。

要想配置加密用访问控制列表，可以使用 access-list 配置命令。要想删除访问控制列表中的一行配置，可以使用这条命令的 no 形式。要想删除整个访问控制列表和它的相关 access group 命令，可以使用 clear access-list 命令。

命令语法如下所示：

access-list *acl_name* [deny I permit] *protocol src_addr src_mask* [operator port [port]] *dest_addr dest_mask* [operator port [port]]

下表描述了这条命令的参数和选项。

命令参数	描　述
acl_name	指定访问控制列表的名字或号码
deny	不为 IPSec 保护选择数据包。在那个特定加密图条目的环境中，防止数据流被 IPSec 保护
permit	为 IPSec 保护选择数据包。使得所有匹配指定条件的 IP 数据包被 IPSec 保护，使用相应的加密图条目所描述的策略
protocol	指定 IP 协议的名称或号码。它可以是下列一个关键字：**icmp**、**ip**、**tcp** 或 **udp**，或者是一个代表 IP 协议号码的整数，范围是 1 到 254。要想匹配任何 Internet 协议，就使用关键字 **ip**
src_addr dest_addr	指定网络或主机的地址，将从那里发送数据包或接收数据包。有 3 种方式可以指定源或目的地址： 使用一个分为 4 部分的 32 比特点分十进制格式。 使用关键字 **any**，将它作为 0.0.0.0 0.0.0.0 的源地址和源地址掩码，或目的地址和目的地址掩码的简写形式。对于 IPSec，通常不推荐使用这个关键字。 使用 host source 或 host destination，将它作为 255.255.255.255 的源地址和源地址掩码，或 255.255.255.255 目的地址和目的地址掩码的简写形式
src_mask dest_mask	指定应用于源或目的地址的网络掩码比特位。有 3 种方式指定源或目的地址网络掩码： 使用一个分为 4 部分的 32 比特点分十进制格式。在我们想要忽略的比特位置处，设置为零。 使用关键字 **any**，将它作为 0.0.0.0 0.0.0.0 的源地址和源地址掩码，或目的地址和目的地址掩码的简写形式。通常不推荐使用这个关键字。 使用 host source 或 host destination，将它作为 255.255.255.255 的源地址和源地址掩码，或 255.255.255.255 目的地址和目的地址掩码的简写形式
operator	（可选）指定一个端口或端口范围，与源或目的端口进行比较。可以使用的运算符有 **lt**（小于）、**gt**（大于）、**eq**（等于）、**neq**（不等于）和 **range**（包括的范围）。**range** 运算符需要两个端口号，其他的运算符只需要一个端口号
port	根据 TCP 或 UDP 协议，我们允许的 IP 服务。可以通过一个文字名称或一个 0 到 65535 范围中的数字，指定端口。如果不指定端口值，我们就指定了所有的端口

警告：CISCO 不推荐我们使用 any 关键字来指定源或目的地址。尤其不鼓励使用 permit any 语句，

因为它使得到所有目的地的所有向外的数据流都被加密(以及所有发往在相应的加密图条目中指定的对等体的数据流)，并要求所有向内的数据流被加密。然后，所有缺少 IPSec 保护的向内数据流都将被悄悄地丢弃。而且，这样可能会使 CPU 的利用率升高，以及随之而来的网络吞吐量下降。

我们有必要配置 IPSec 使用的镜像加密用访问控制列表。在每个对等体上的加密用访问控制列表应该是对称的。注意：如果在两个加密对等体上创建对称访问控制列表失败，将会导致不能形成一个 SA。

例如

fw1(config)# access-list 101 permit ip 10.0.1.0 255.255.255.0 10.0.6.0 255.255.255.0
fw6(config)# access-list 101 permit ip 10.0.6.0 255.255.255.0 10.0.1.0 255.255.255.0

(2) NAT 0

设置不翻译该访问控制列表

fw1(config)# nat (inside) 0 access-list 101

92. ★步骤 2：用 crypto ipsec transform-set 命令配置变换集。

配置 PIX 防火墙 IPSec 的下一个关键步骤是使用 IPSec 安全策略，来定义一个变换集。变换集是多个单独的 IPSec 变换的组合，IPSec 变换为数据流制定安全策略。变换集组合了下列 IPSec 因素：

- 数据包认证机制——AH 变换。
- 净载加密和可选的认证机制——ESP 变换。
- IPSec 模式，即传送模式或隧道模式。

我们可以用 crypto ipsec transform-set 命令定义一个变换集。要想删除一个变换集，可以使用这条命令的 no 形式。

命令语法如下所示：

crypto ipsec transform-set *transform-set-name transform1[transform2[transform3]]*

crypto ipsec transform-set 命令的参数：

命令参数	描　述
transform-set-name	指定要创建（或修改）的变换集的名字
transform1 *transform2* *transform3*	指定最多三种变换。变换定义了 IPSec 安全协议和算法。每种变换代表了一个 IPSec 安全协议（ESP、AH、AH 加 ESP、AH 加 ESP 和 ESP-HMAC）加上我们想要使用的算法

下表显示了 PIX 防火墙支持的 IPSec 变换：

变换	描　述
ah-md5-hmac	用于认证的 AH-md5-hmac
ah-sha-hmac	用于认证的 AH-sha-hma。
esp-des	使用 DES 加密（56 位）的 ESP 变换
esp-3des	使用 3DES 加密（168 位）的 ESP 变换
esp-md5-hmac	具有 HMAC-MD5 认证的 ESP 变换，与 **esp-des** 或 **esp-3des** 变换一起使用，来向 ESP 数据包提供附加的完整性
esp-sha-hmac	具有 HMAC-SHA 认证的 ESP 变换，与 **esp-des** 或 **esp-3des** 变换一起使用，来向 ESP 数据包提供附加的完整性

93. 步骤 3：(可选)用 crypto ipsec security-association lifetime 命令配置全局 IPSec 安全关联生存期。

IPSec 安全关联生存期决定在 IPSec SA 需要被重新协商之前，可以保持多长时间有效。

94. ★步骤 4：用 crypto map 命令配置加密图。

我们使用 crypto map 配置命令来产生或修改一个加密图条目。我们在设置加密图条目时，将引用动态加密图作为一个加密图集中的最低优先级条目(也就是说，具有最大的序列号)。使用这条命令的 no 形式，可以删除一个加密图条目或者加密图集。

命令的语法如下所示：

crypto map *map-name seq-num* (ipsec-isakmp ipsec-manual) [dynamic *dynamic-map-name*]
crypto map *map-name seq-num* **match address** *acl_name*
crypto map *map-name seq-num* **set peer (***hostname* **|** *ip_address***)**
crypto map *map-name seq-num* set pfs [group1 | group2]
crypto map *map-name seq-num* **set security_attciation lifetime (seconds** *seconds* **| kilobytes** *kilobytes***)**
crypto map *map-name seq-num* **set transform-set** *transform-set-name1* **[***transform-set-name6***]**
crypto map *map-name* client authentication aaa-server-name
crypto map *map-name* client configuration address (initiate l respond)

命令参数	描　述
map-name	指定分配给该加密图集的名字
seq-num	指定分配给该加密图条目的序号
ipsec-manual	指示不使用 IKE 来建立 IPSec 安全关联以保护由该加密图条目指定的数据流
ipsec-isakmp	指示用 IKE 来建立 IPSec 安全关联以保护由该加密图条目指定的数据流
acl_name	标识已定义过的加密用访问控制列表。这个名字应该匹配已定义过的加密用访问控制列表中的 name 参数
match address	为加密图条目指定一个访问控制列表
set peer	在一个加密图条目中指定一个 IPSec 对等体。通过重复这条命令，可以指定多个对等体。该对等体是 IPSec 对等体的终结接口
hostname	通过主机名称指定一个对等体。这是对等体的主机名称加上它的域名称，比如 myhost.example.com
ip-address	通过 IP 地址指定一个对等体
set pfs	指定 IPSec 应该请求完美转发秘密（Perfect Forward Secrecy）。采用 PFS，每次协商一个新的安全关联时，都进行一次新的 Diffie-Hellman 交换。PFS 为密钥的产生提供了额外的安全，它的代价是需要进行额外的处理
group 1	指示 IPSec 应该在执行新的 Diffie-Hellman 交换时使用 768 比特的 Diffie-Hellman 主模块组。与 **esp-des** 或 **esp-3des** 变换一起使用
group 2	指示 IPSec 应该在执行新的 Diffie-Hellman 交换时使用 1024 比特的 Diffie-Hellman 主模块组。与 **esp-des** 或 **esp-3des** 变换一起使用
set transform-set	指示哪个变换集可以被用于加密图条目。按照优先级的顺序列出多个变换集，其中具有最高优先级（最安全）的变换集在前面
transform-set-name	指定变换集的名字。对于一个 ipsec-manual 加密图条目，我们可以只指定一个变换集。对于一个 ipsec-isakmp 或 dynamic 加密图条目，我们可以指定多达六个变换集

命令参数	描　述
kilobytes *kilobytes*	指定在一个安全关联过期之前，在 IPSec 对等体之间能够通过用该安全关联传送的数据流量（以千字节为单位）。缺省是 4608000KB。在一个加密图条目中的安全关联生存期可以覆盖全局安全关联生存期的值
seconds *seconds*	指定安全关联在过期之前可以生存的秒数。缺省是 3600s（一个小时）
dynamic	（可选）指示该加密图条目引用一个已存在的静态加密图。如果我们使用这个关键字，任何加密图配置命令都将不可用
dynamic-map-name	（可选）指定应该被用作策略模板的动态加密图集的名字
aaa-server-name	指定在 IKE 认证期间，对用户进行认证的 AAA 服务器的名字。可用的两种 AAA 服务器是 TACACS+ 和 RADIUS
initiate	指示 PIX 防火墙试图为每个对等体设置 IP 地址
respond	指示 PIX 防火墙接受来自任何请求对等体的 IP 地址请求

实例：

fw1(config)# crypto map FW1MAP 10 match address 101
fw1(config)# crypto map FW1MAP 10 set peer 192.168.6.2
fw1(config)# crypto map FW1MAP 10 set transform-set pix6
fw1(config)# crypto map FW1MAP 10 set security-association lifetime seconds 28800

95. ★步骤 5：用 crypto map map-name interface 命令，将加密图应用到终结 / 起源接口。

在实际的 IPSec 配置过程中，最后一步是将加密图集应用到一个接口上。我们可以在配置模式中，使用 crypto map 命令，将加密图应用到 PIX 防火墙连接 Internet 的接口上。使用这条命令的 no 形式，可以从接口上删除一个加密图集。

命令语法如下所示：
crypto map *map-name* interface *interface-name*

map-name 用来指定加密图集的名字，
interface-name 参数用来指定 PIX 防火墙使用的标识接口，PIX 将使用该接口向对等体标识它自己。如果启用了 IKE，而且我们正使用 CA 来获得证书，那么这个接口具有的地址就应该在 CA 证书中指定。

例如：
fw1(config)# crypto map FW1MAP interface outside

96. 步骤 6：用各种可用的 show 命令检验 IPSec 配置。

在 PIX 防火墙上配置 IPSec 的最后一步是使用各种可用的 show 命令，检验 IPSec 配置。

(1) show access-list
我们可以用 show access list 命令查看所有经过配置的访问控制列表。

(2) show crypto ipsec transform-set
我们可以用 show crypto ipsec transform-set 命令，查看当前定义的变换集。这条命令的，语法如下所示：show crypto ipsec transform-set [tag *transform-set-name*]
这里的可选参数 tag transfom-set-name 将只显示具有指定变换集名字(transform-set-name)的变换集。如果不使用任何关键字，将显示 PIX 防火墙上配置的所有变换集。

(3) show crypto ipsec security-association lifetime
我们可以使用 show crypto ipsec security-association lifetime 命令，查看当前的全局 IPSec SA 生存期。

(4) show crypto map
我们可以使用 show crypto map 命令，查看加密图的配置。如果不使用任何关键字，将显示在 PIX 防火墙上配置的所有加密图。这条命令的语法如下所示：
show crypto map [interface *interface* | tag *map-name*]
这里的 interface interface 参数只显示应用到这个指定接口的加密图集。

5.2.4 任务 4：测试并检验 IPSec 的总体配置

为预共享密钥配置 IPSec 中的最后一项任务是验证所有的 IKE 和 IPSec 值都被正确配置了，并测试它的工作情况是否正常。PIX 防火墙含有很多可用于测试并检验 IKE 和 IPSec 的 show、clear 和 debug 命令，本节将对这些命令进行总结。

97. 测试并检验 IKE 配置

可以使用下表中总结的命令，来检查 IKE 配置和操作。

命　令	描　述
show isakmp	显示经过配置的 IKE 策略，它的显示格式与 **write terminal** 命令相似
show isakmp policy	显示缺省的和任何经过配置的 IKE 策略

98. 测试并检验 IPSec 配置

我们可以使用下表中列出的命令，测试并检验 PIX 防火墙上的 IPSec 配置。

命　令	描　述
show access-list	*列出配置中的* **access-list** *命令语句。用来检验加密用访问控制列表选择了感兴趣的数据流。显示匹配访问控制列表的数据包个数*
show crypto map	显示指派给一个加密图的加密用访问控制列表。显示经过配置的加密图参数
show crypto ipsec transform-set	显示经过配置的 IPSec 变换集
show crypto ipsec security-association lifetime	显示正确的全局 IPSec SA 生存期的值

99. 监视并管理 IKE 和 IPSec 通信

我们可以用下中列出的命令，检查 IKE 和 IPSec 的建立，监视并管理 PIX 防火墙和 IPSec 对等体之间的 IKE 和 IPSec 通信。

注意：我们必须在配置模式中执行 debug 命令。

命　令	描　述
show isakmp sa	显示 IKE 安全关联的当前状态。
show crypto ipsec sa	显示 IPSec 安全关联的当前状态。用来确保数据流被进行了加密处理。还显示通过那个 SA 加密和解密数据包的数量。
clear crypto isakmp sa	清除 IKE 安全关联。
clear crypto ipsec sa	清除 IPSec 安全关联。
debug crypto isakmp	显示 PIX 防火墙和 IPSec 对等体之间的 IKE 通信。
debug crypto ipsec	显示 PIX 防火墙和 IPSec 对等体之间的 IPSec 通信。

clear isakmp 命令可以清除活跃的 IKE 连接，如例 11-18 所示。

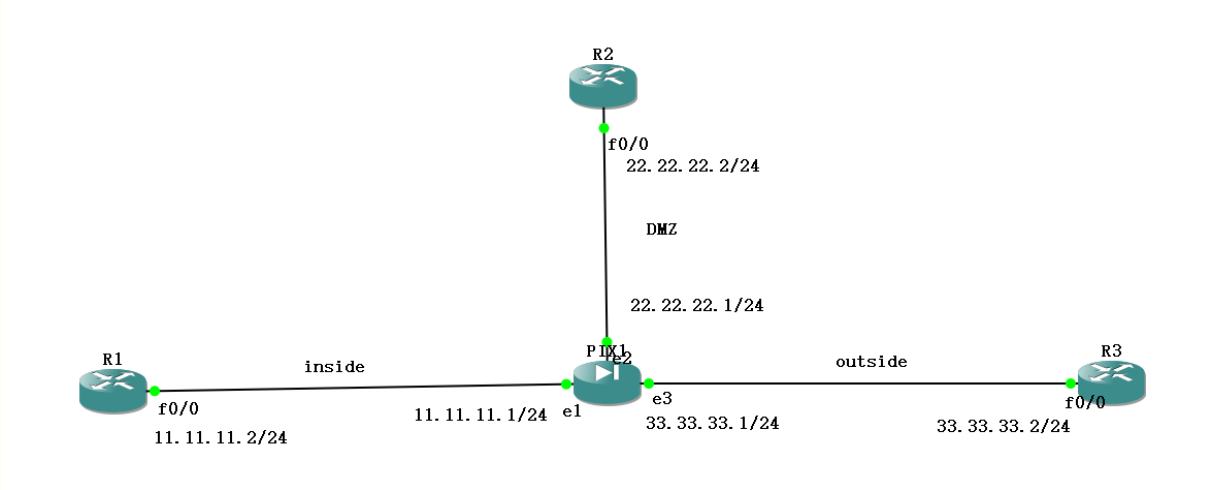
例 11-18　**clear isakmp** 命令用来清除活跃的 IKE 连接

```
Pix1# show crypto isakmp sa
dst             src          state        conn-id      slot
192.168.1.2     192.168.2.2  QM_IDLE      93           0
Pix1# clear crypto isakmp 93
2w4d:ISADB:reaper checking SA,
Pix1# show crypto isakmp sa
dst             src          state        conn-id      slot
```

Web Security Configuration Experience

1 基本配置

100.实验拓扑



101.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
```

102.配置路由器 telnet

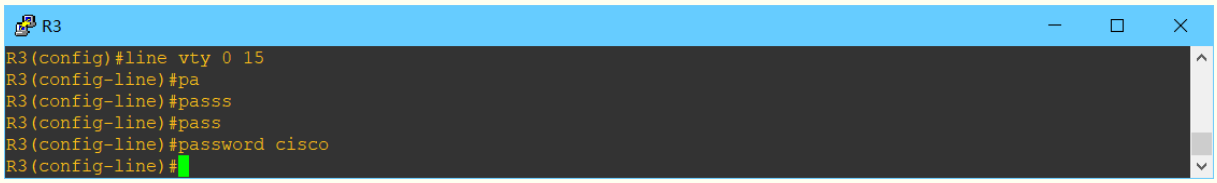
连接线路为 0 到 15

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



103.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

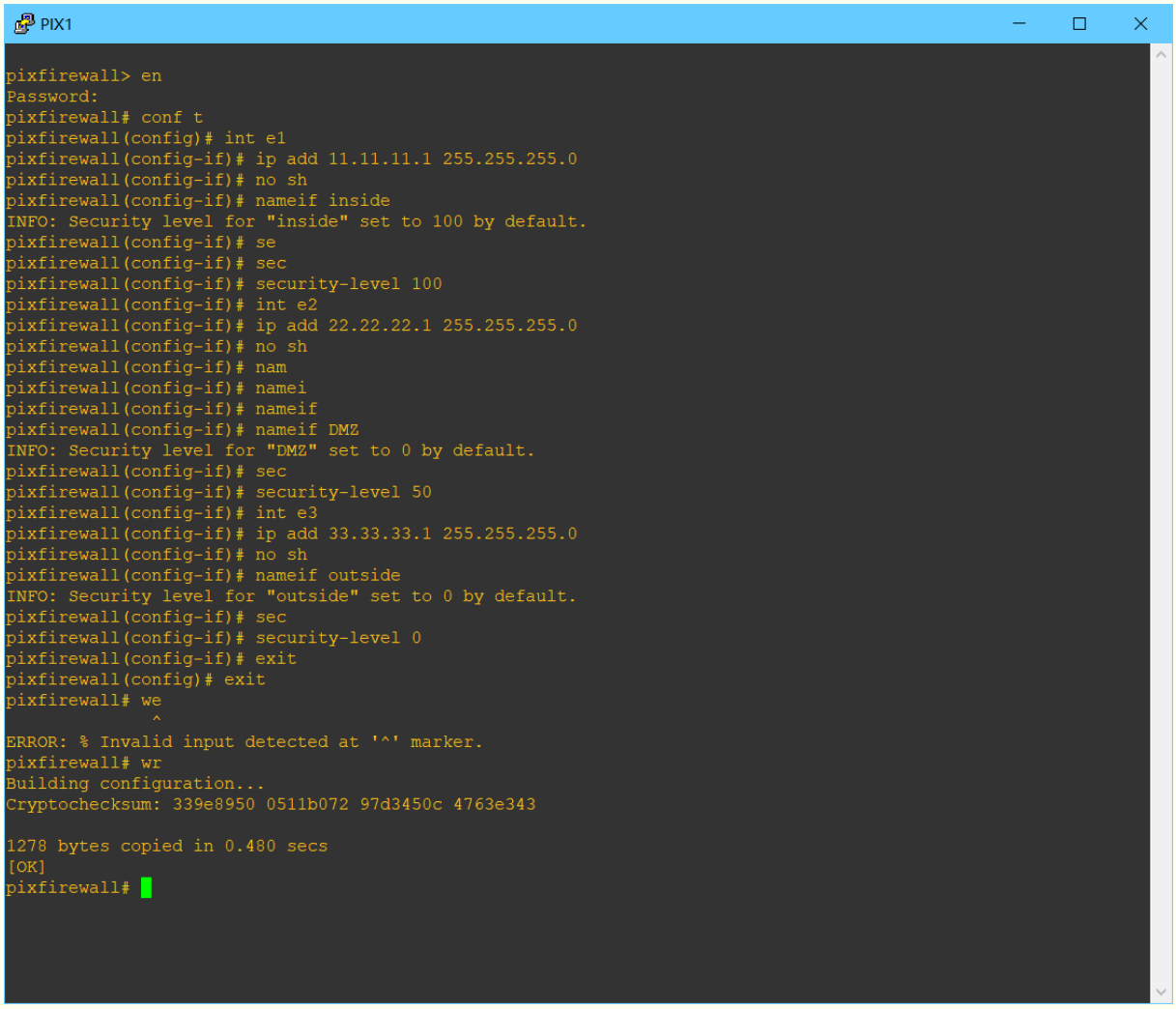
pixfirewall(config-if)# no sh

命名接口

pixfirewall(config-if)# nameif inside

为接口设置安全级别

pixfirewall(config-if)# security-level 100



104.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)#
```

105.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
```

106.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)#
```

107.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>
```

108.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#
```

109.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)#
```

110.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)#
```

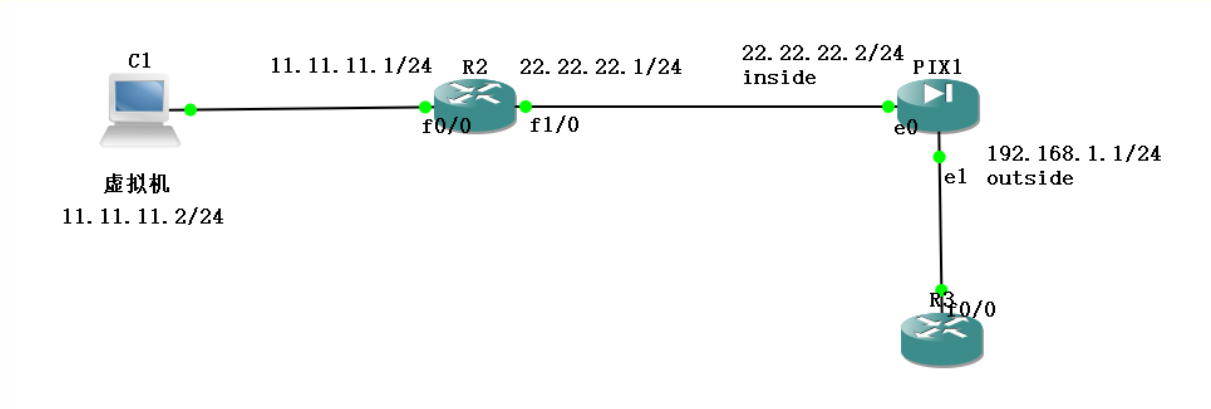
111.验证配置：从 R3（外网）可以 telnet 到 R2（DMZ）（使用翻译过的外网 IP 地址）

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

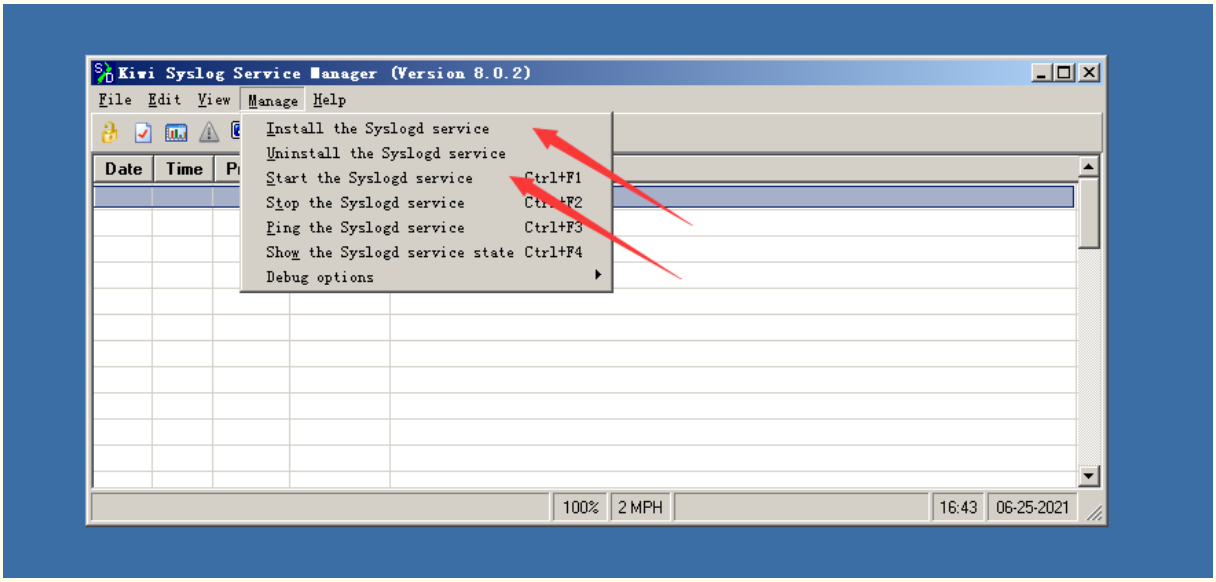
112.实验拓扑



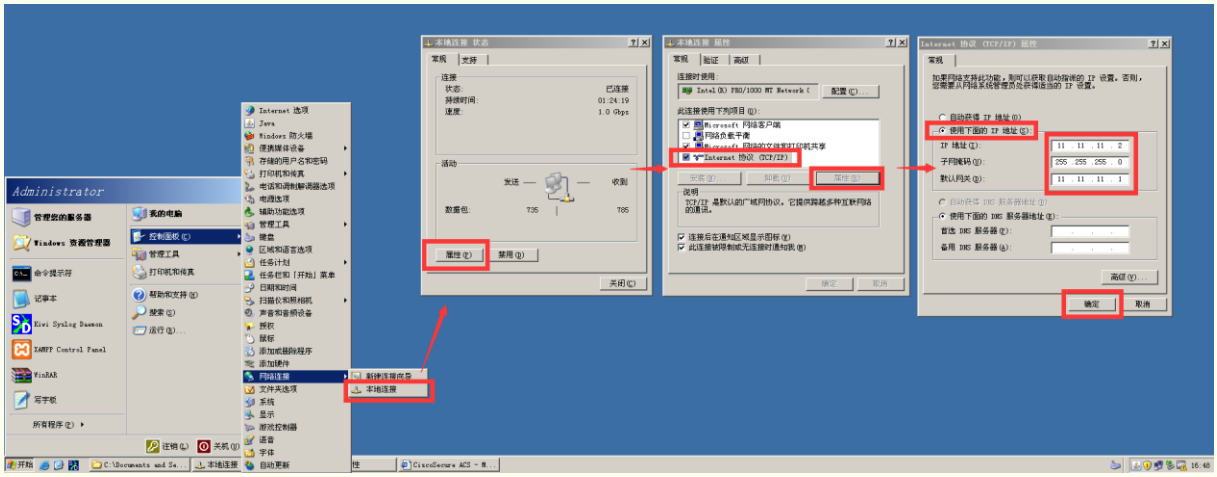
113.在虚拟机安装日志软件

需要服务器系统，比如 Windows Server 2003

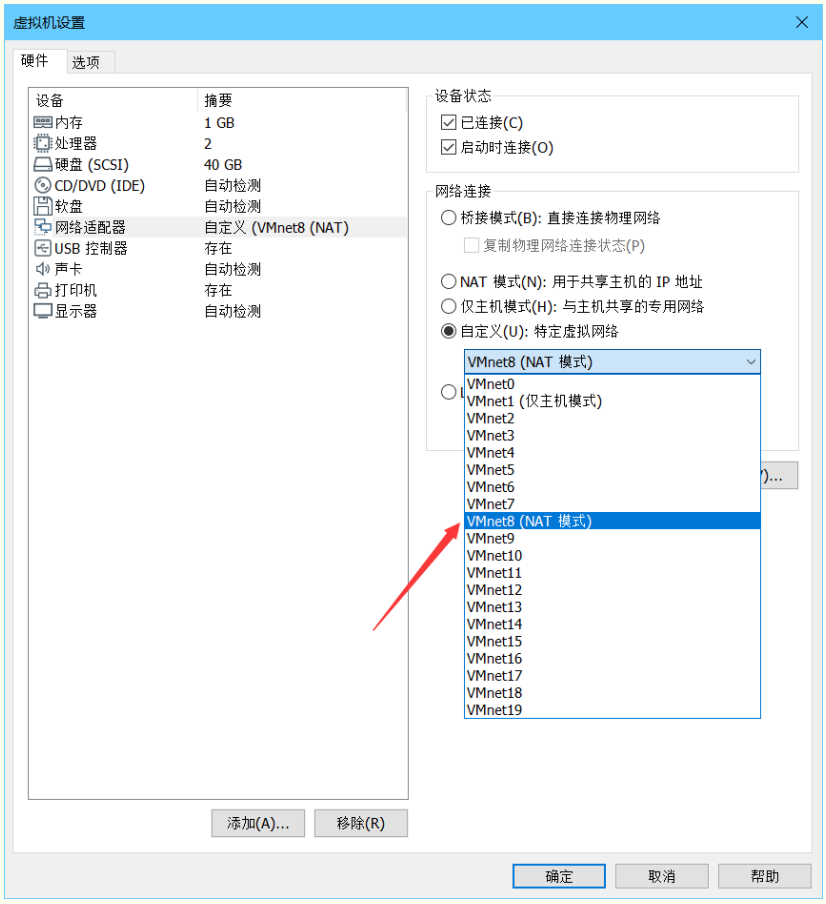
注意：安装完需要安装并启用服务

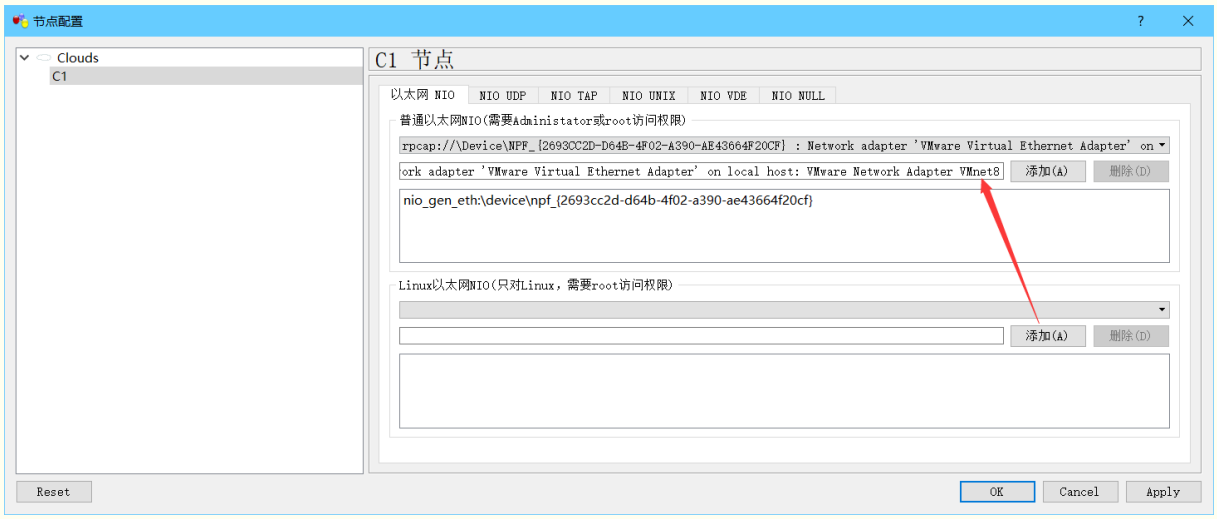


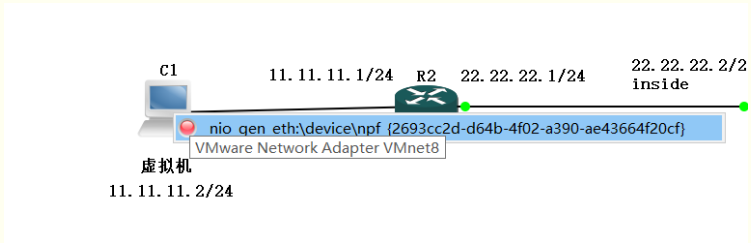
114.配置虚拟机 IP 地址



115.配置虚拟机网络连接



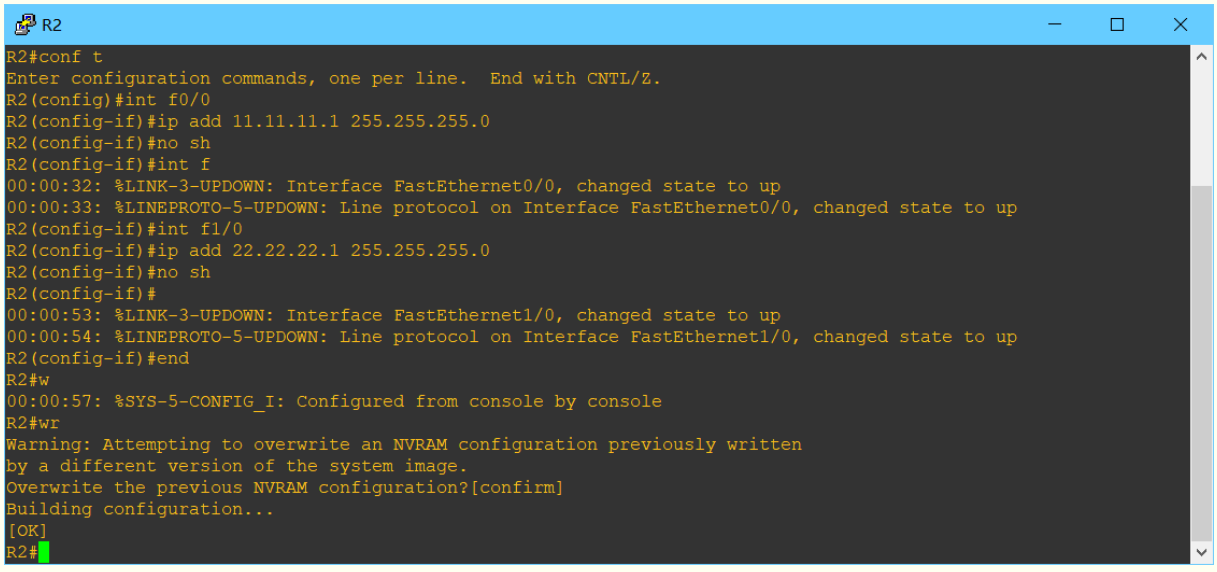




116.配置路由器接口 IP

需要为每个路由的每个接口配置 IP 地址并打开

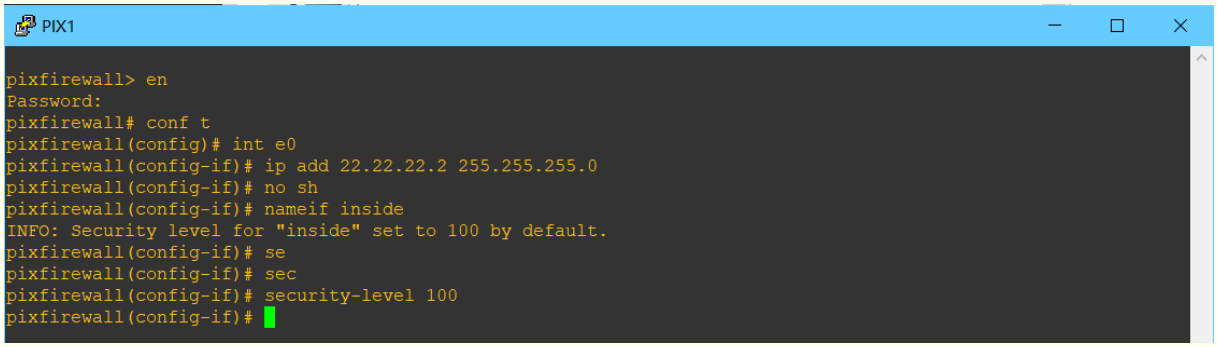
同上一个实验



117.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



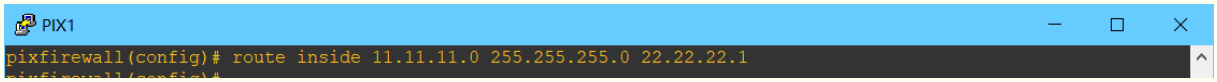
118.配置防火墙路由（静态路由）

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



119.5 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

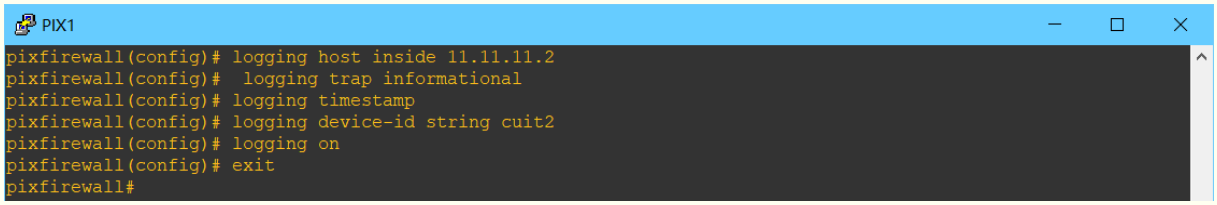
pixfirewall(config)# logging **timestamp**

(4) 设置设备 ID 为字符串 cuit2

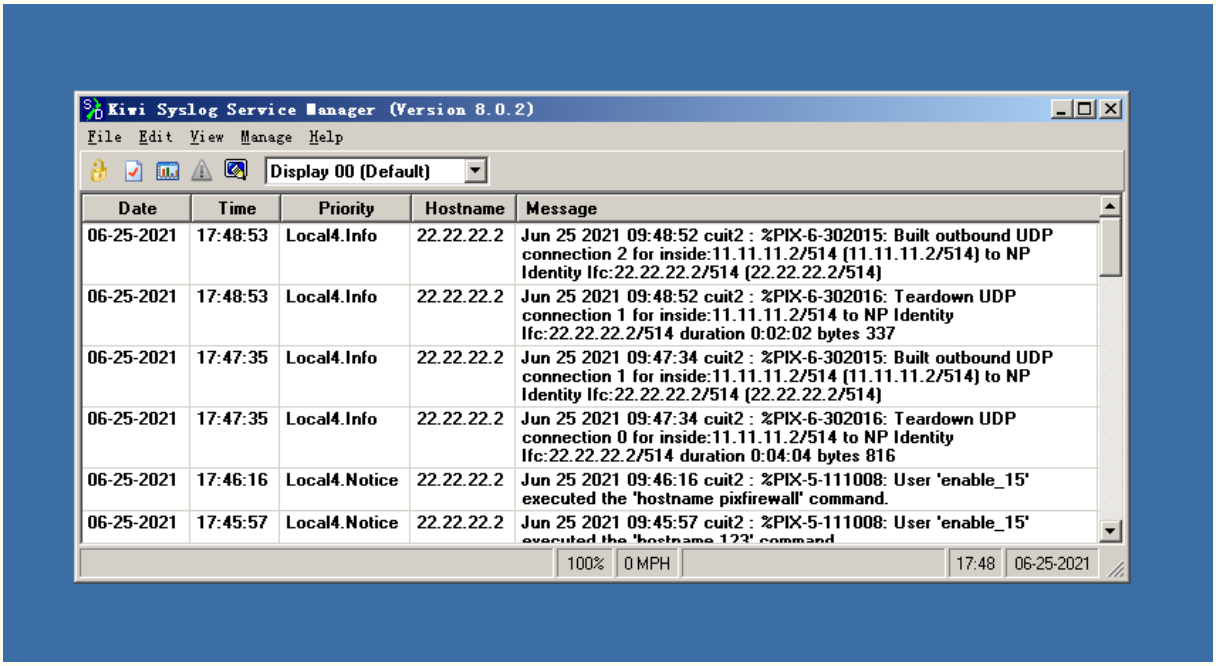
pixfirewall(config)# logging **device-id** string cuit2

(5) 启用日志服务器

pixfirewall(config)# logging **on**



120.验证配置：在虚拟机软件可以看到日志

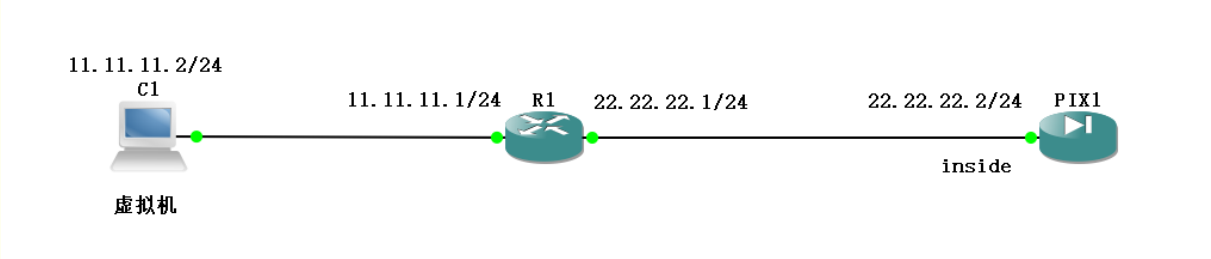


3 AAA 认证配置

121.实验拓扑

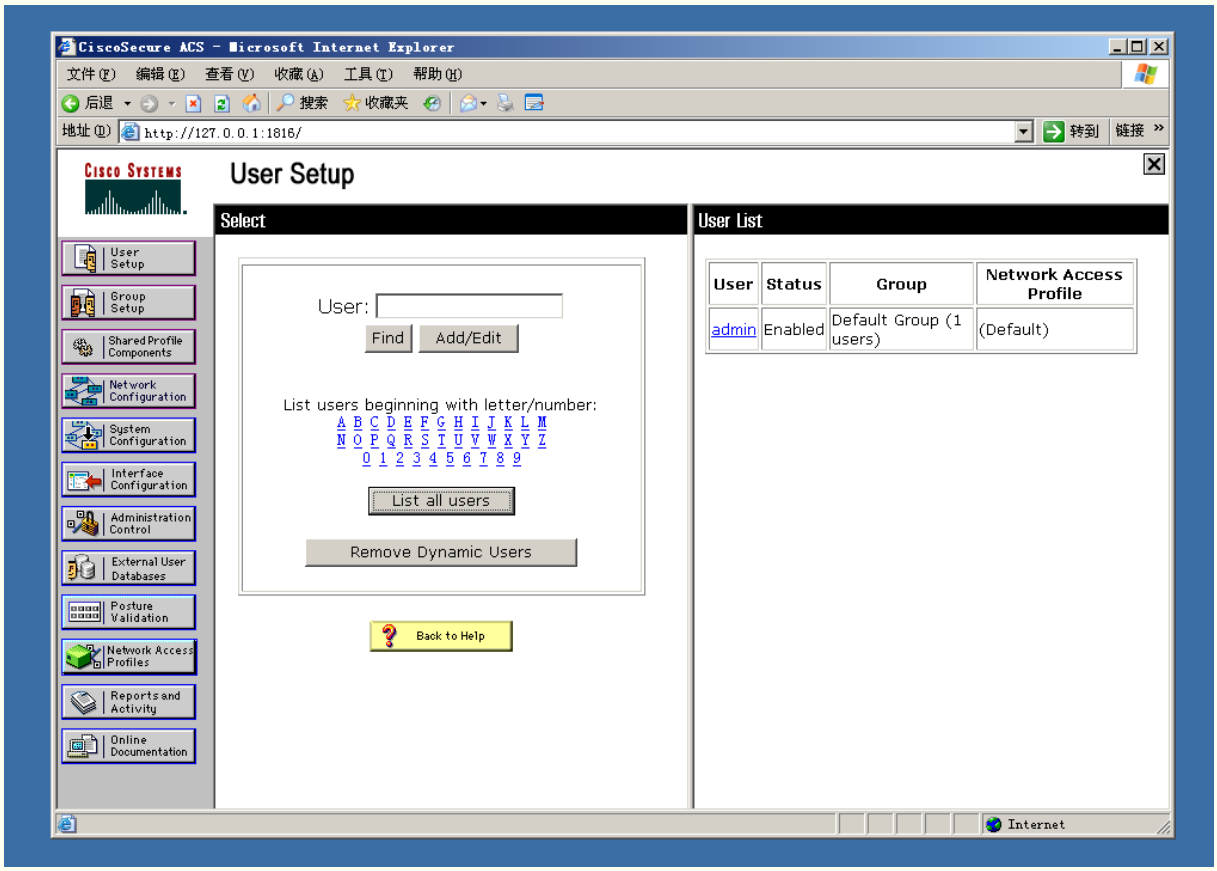
与上个实验相同

可以在上个实验的基础上进行



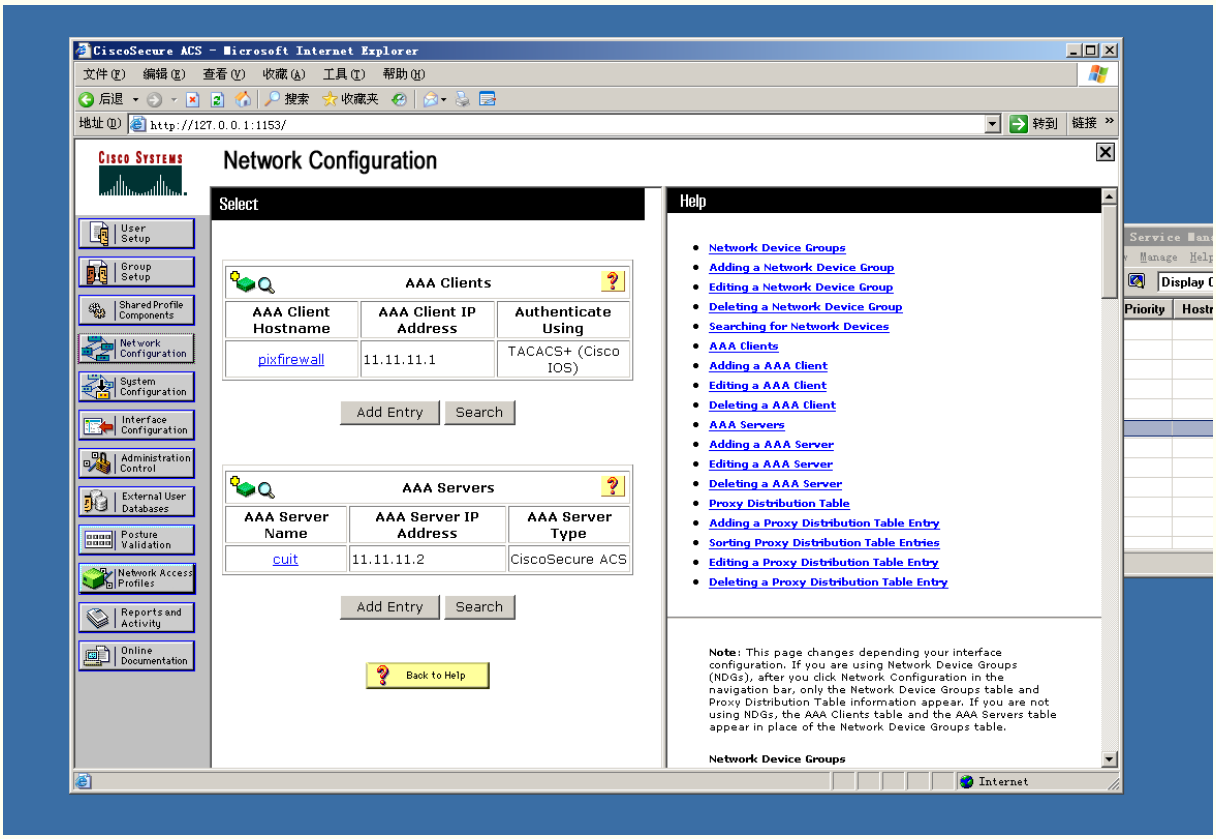
122.在虚拟机安装 AAA 软件

需要服务器系统，比如 Windows Server 2003

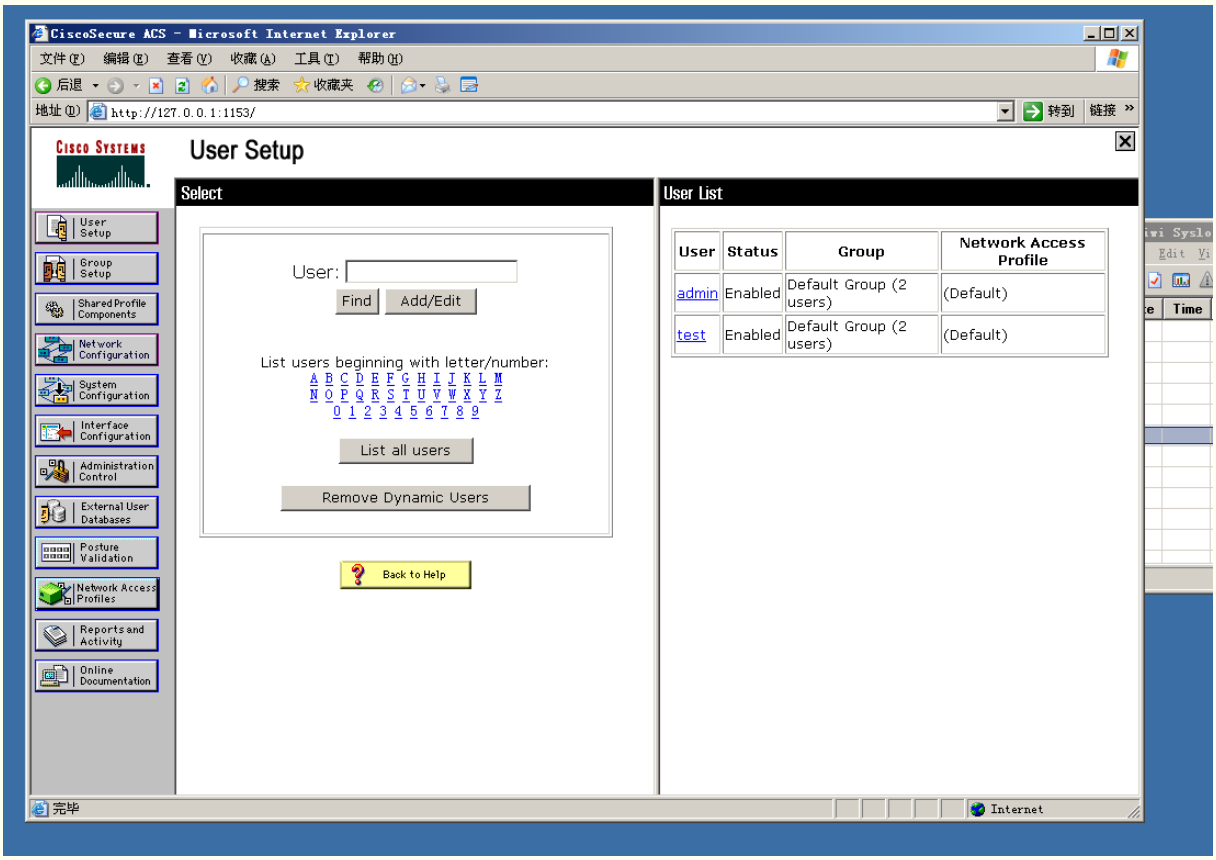


注意：需要安装 JDK 才能正常使用软件

123.在 AAA 软件中添加 AAA 客户（防火墙）



124.在 AAA 软件中添加用户



125.基本配置

下面三步配置与上个实验完全相同，如果是在上个实验的基础上进行实验的，那么可以跳过这些配置。

(1) 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

(2) 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

(3) 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

126.3 步配置 AAA 认证

(1) 步骤 1：指定服务器类型 aaa-server * protocol _

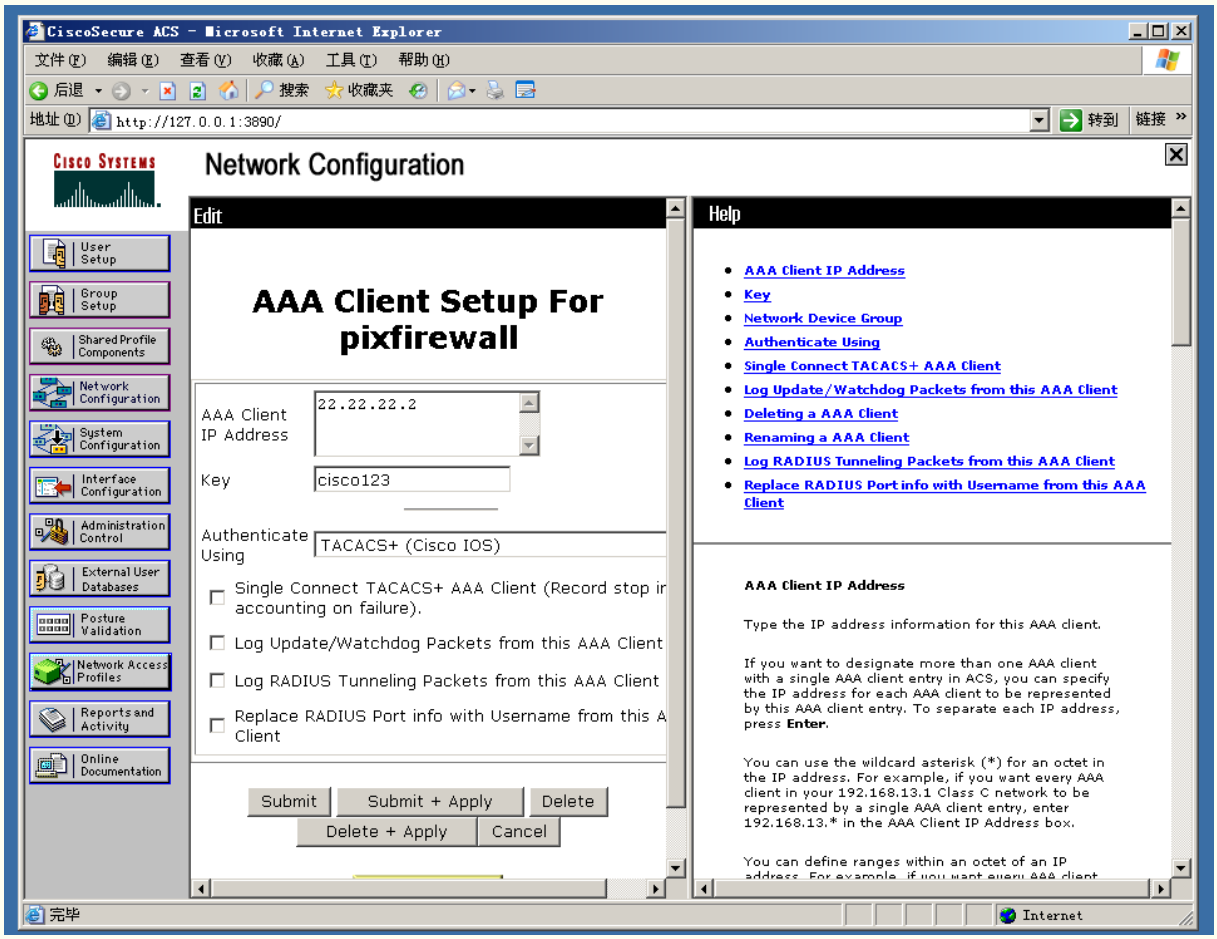
指定服务器 cuit 的类型为 tacacs+
pixfirewall(config)# aaa-server cuit protocol tacacs+

(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

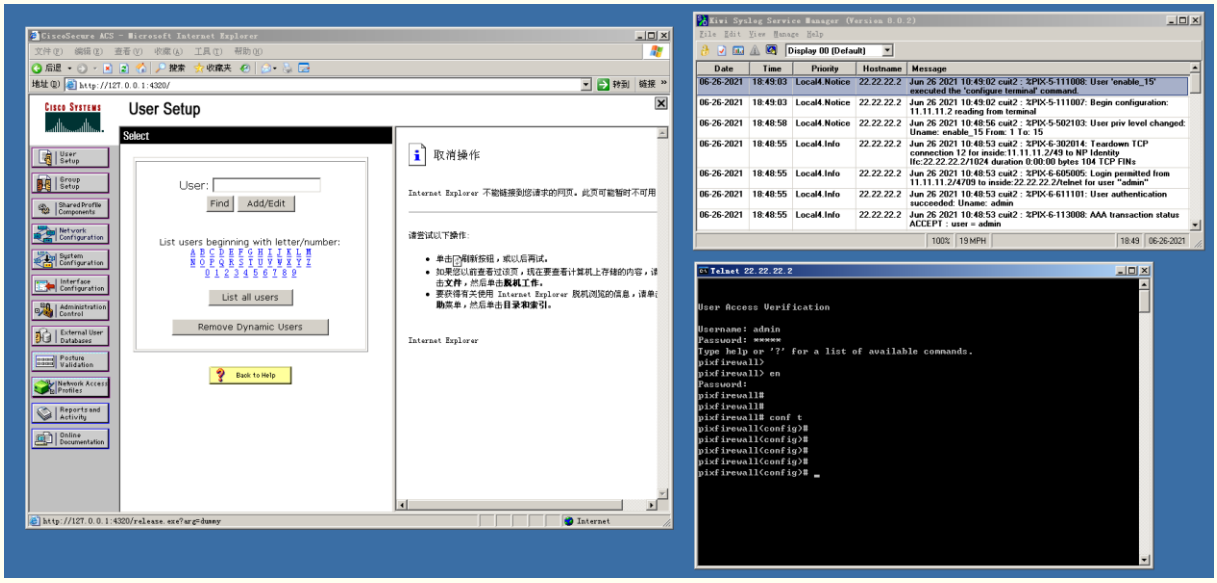
```
PIX1
pixfirewall# conf t
pixfirewall(config)# aaa-server cuit protocol tacacs+
pixfirewall(config-aaa-server-group)# aaa-server cuit host 11.11.11.2
pixfirewall(config-aaa-server-host)# key cisco123
pixfirewall(config-aaa-server-host)# timeout 10
pixfirewall(config-aaa-server-host)# aaa authentication telnet console cuit
pixfirewall(config)#
```

127.允许 telnet 登录

pixfirewall(config)# telnet 11.11.11.2 255.255.255.255 inside

```
PIX1
pixfirewall(config)# telnet 11.11.11.2 255.255.255.255 inside
pixfirewall(config)#
```

128.验证配置：从虚拟机 telnet 到防火墙，需要输入用户名和密码

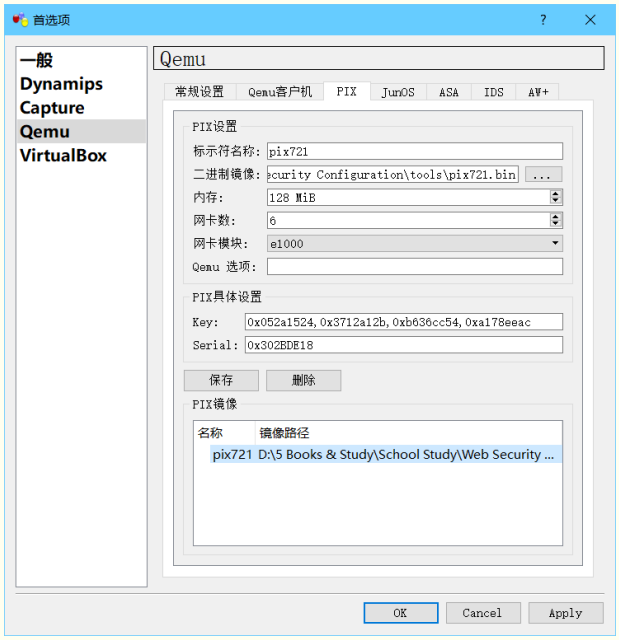


4 VPN 配置

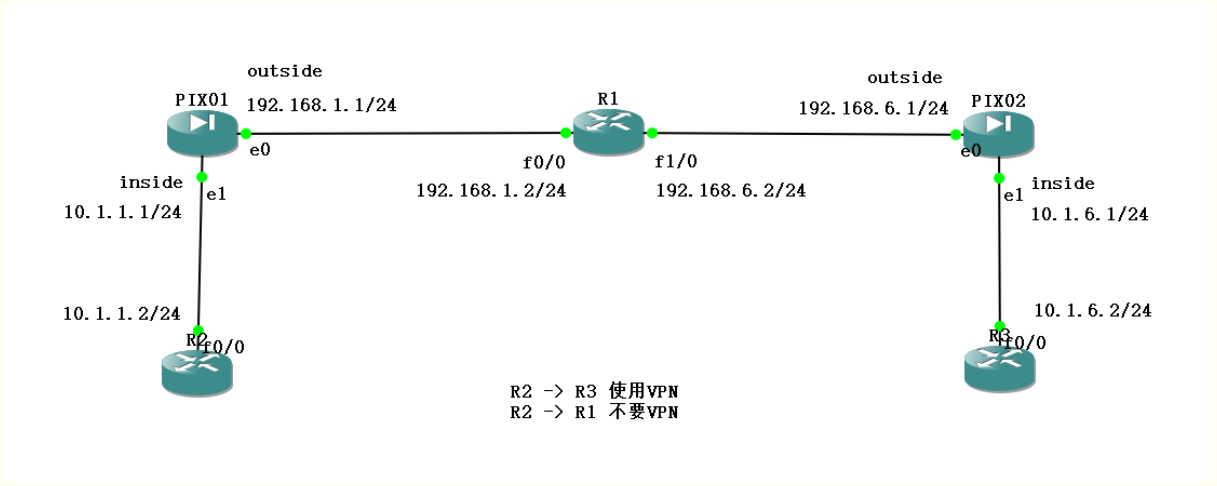
129.配置 PIX Key 和 Serial

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



130.实验拓扑

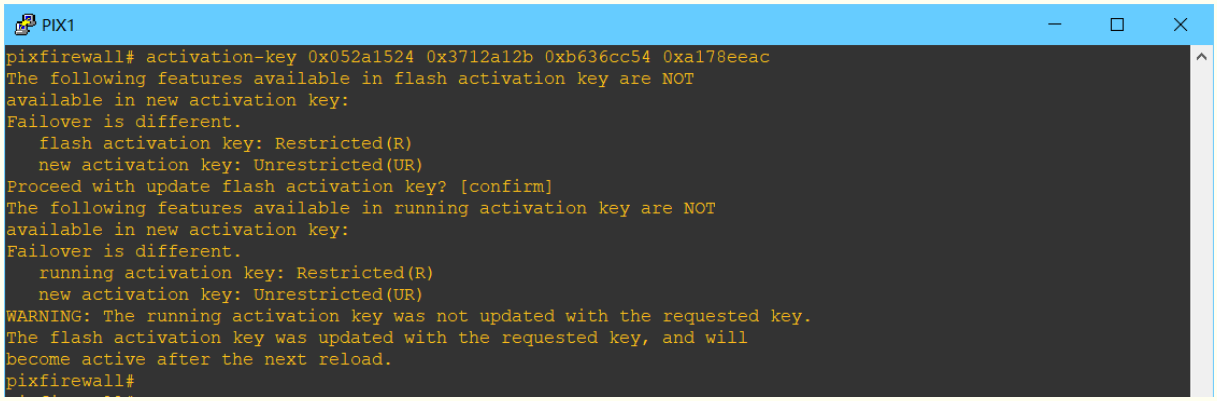


131.激活防火墙

两个防火墙都需要激活

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

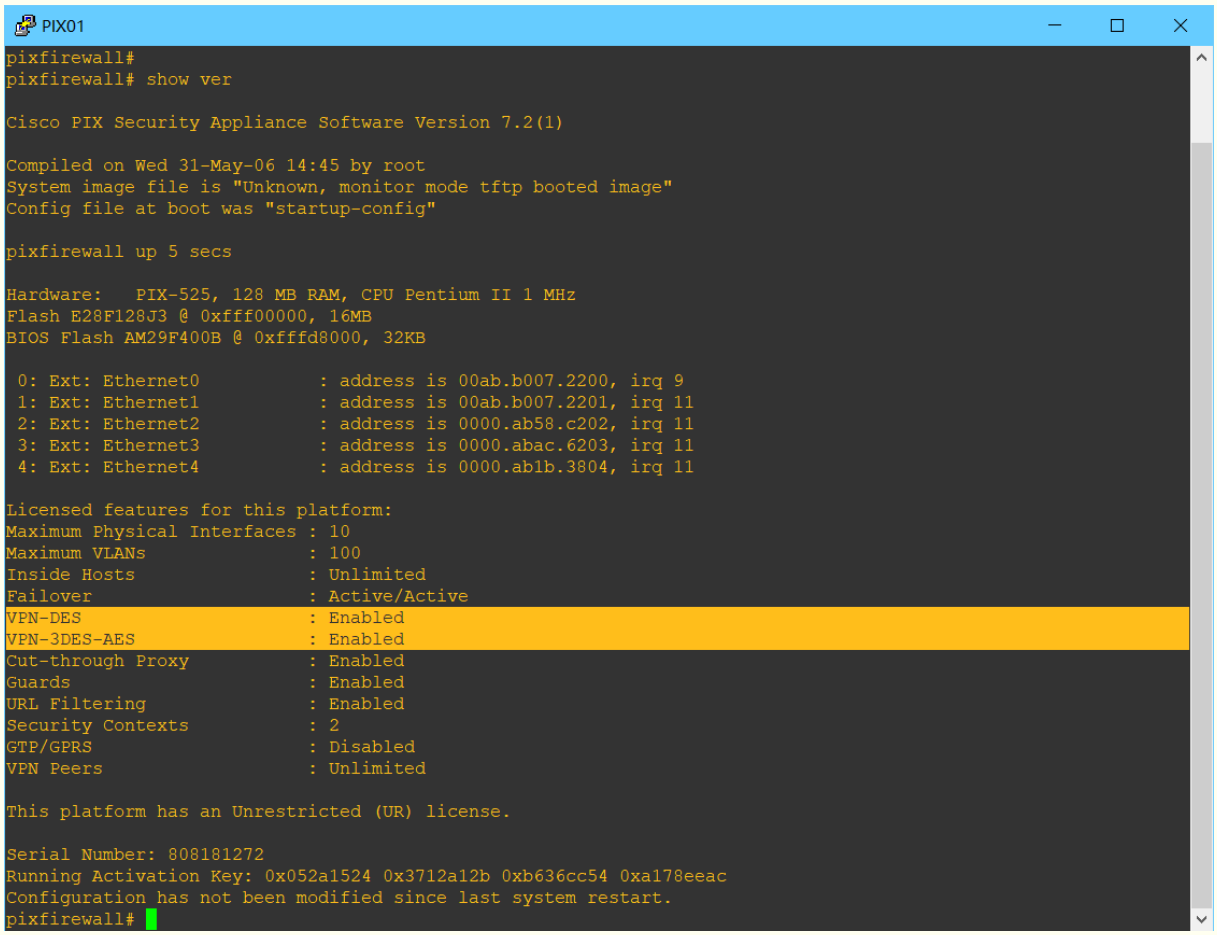
注：激活后需要重启防火墙



132.验证配置：show version

pixfirewall# show version

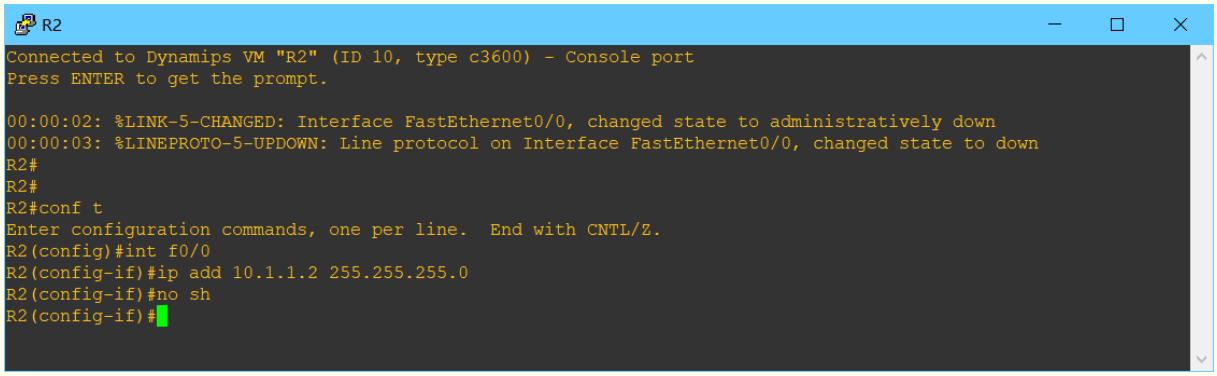
若下面项为 Enable，则说明防火墙已经激活

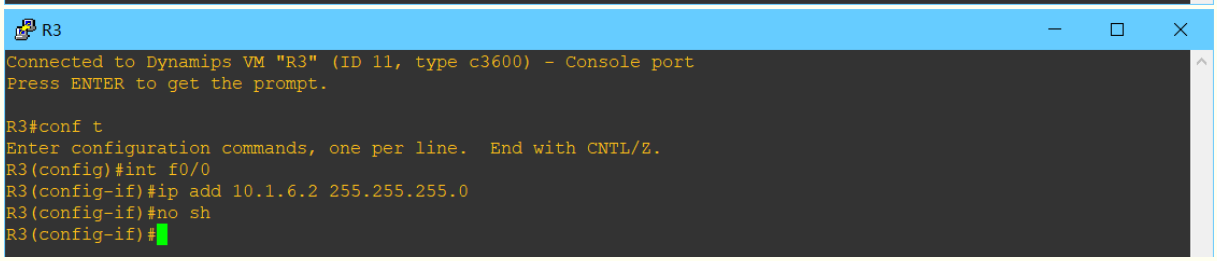


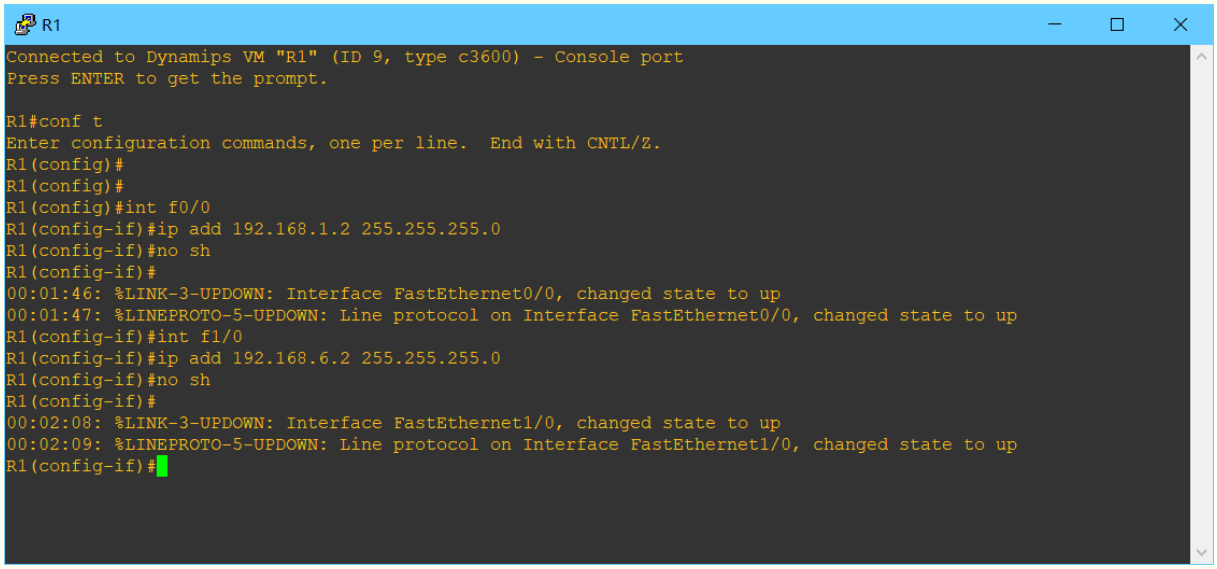
133.配置路由器接口 IP

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







134.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

```
R1
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
R1(config)#
```

135.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

```
PIX1
pixfirewall# conf t
pixfirewall(config)# int e0
pixfirewall(config-if)# ip add 192.168.1.1 255.255.255.0
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)# int e1
pixfirewall(config-if)# ip add 10.1.1.1 255.255.255.0
pixfirewall(config-if)# no sh
pixfirewall(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
pixfirewall(config-if)# sec
pixfirewall(config-if)# security-level 100
pixfirewall(config-if)#
```

```
PIX2
pixfirewall# conf t
pixfirewall(config)# int e0
pixfirewall(config-if)# ip add 192.168.6.1 255.255.255.0
pixfirewall(config-if)# no sh
pixfirewall(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
pixfirewall(config-if)# int e1
pixfirewall(config-if)# ip add 10.1.6.1 255.255.255.0
pixfirewall(config-if)# no sh
pixfirewall(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
pixfirewall(config-if)#
```

136.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

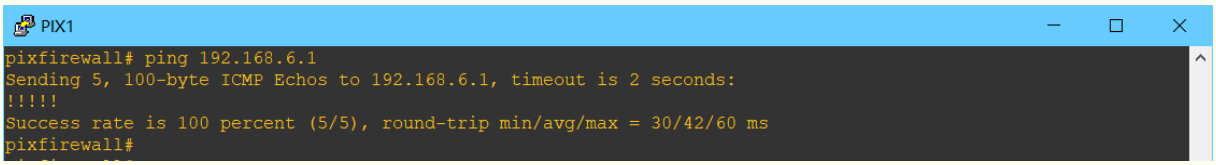
```
PIX1
pixfirewall(config)# route outside 0.0.0.0 0.0.0.0 192.168.1.2
pixfirewall(config)#
```

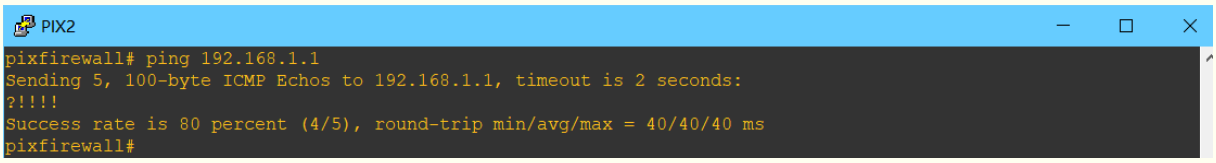
PIX02 到外网的下一跳地址为 192.168.6.2
pixfirewall(config)# route outside 0.0.0.0 0.0.0.0 192.168.6.2

```
PIX2
pixfirewall(config)# route outside 0.0.0.0 0.0.0.0 192.168.6.2
pixfirewall(config)#
```

137.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。





138.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

139.显示 IKE 配置

pixfirewall# show run crypto isakmp

140.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

PIX1

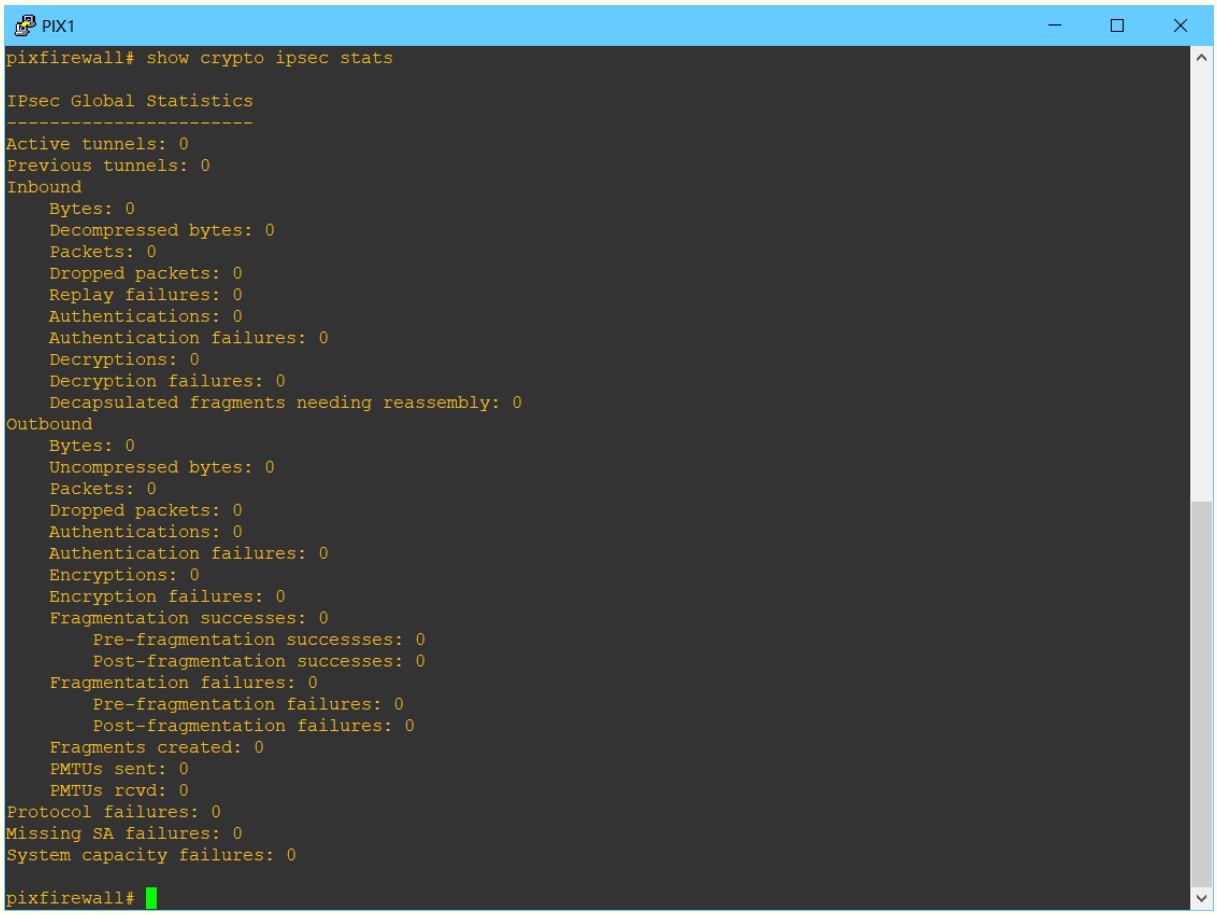
```
1306 bytes copied in 0.610 secs
[OK]
pixfirewall#
pixfirewall# conf t
pixfirewall(config)# isakmp enable outside
pixfirewall(config)# isakmp policy 10
pixfirewall(config-isakmp-policy)# encryption des
pixfirewall(config-isakmp-policy)# hash sha
pixfirewall(config-isakmp-policy)# authentication pre-share
pixfirewall(config-isakmp-policy)# group 1
pixfirewall(config-isakmp-policy)# lifetime 86400
pixfirewall(config-isakmp-policy)# tunnel-group 192.168.6.1 type ipsec-l2l
pixfirewall(config)# tunnel-group 192.168.6.1 ipsec-attributes
pixfirewall(config-tunnel-ipsec)# pre-shared-key cisco123
pixfirewall(config-tunnel-ipsec)# exit
pixfirewall(config)# access-list 101 permit ip 10.1.1.0 255.255.255.0 10.1.6.0$
pixfirewall(config)# nat (inside) 0 access-list 101
pixfirewall(config)# crypto ipsec transform-set test esp-des esp-md5-hmac
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 seco$
pixfirewall(config)# crypto map CUIT interface outside
pixfirewall(config)#
```

PIX2

```
pixfirewall# conf t
pixfirewall(config)# isakmp enable outside
pixfirewall(config)# isakmp policy 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
pixfirewall(config-isakmp-policy)# exit
pixfirewall(config)#
pixfirewall(config)# tunnel-group 192.168.1.1 type ipsec-l2l
pixfirewall(config)# tunnel-group 192.168.1.1 ipsec-attributes
pixfirewall(config-tunnel-ipsec)# pre-shared-key cisco123
pixfirewall(config-tunnel-ipsec)# exit
pixfirewall(config)#
pixfirewall(config)# access-list 101 permit ip 10.1.6.0 255.255.255.0 10.1.1.0$
pixfirewall(config)# nat (inside) 0 access-list 101
pixfirewall(config)# crypto ipsec transform-set test esp-des esp-md5-hmac
pixfirewall(config)#
pixfirewall(config)# crypto map CUIT 10 match address 101
pixfirewall(config)# crypto map CUIT 10 set peer 192.168.1.1
pixfirewall(config)# crypto map CUIT 10 set transform-set test
pixfirewall(config)# crypto map CUIT 10 set security-association lifetime seco$
pixfirewall(config)# crypto map CUIT interface outside
pixfirewall(config)# exit
pixfirewall# wr
Building configuration...
Cryptochecksum: 7fe61105 099591cc a8a860c8 3c58e3b8
```

141.查看防火墙加密包

pixfirewall# show crypto ipsec stats



142.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。

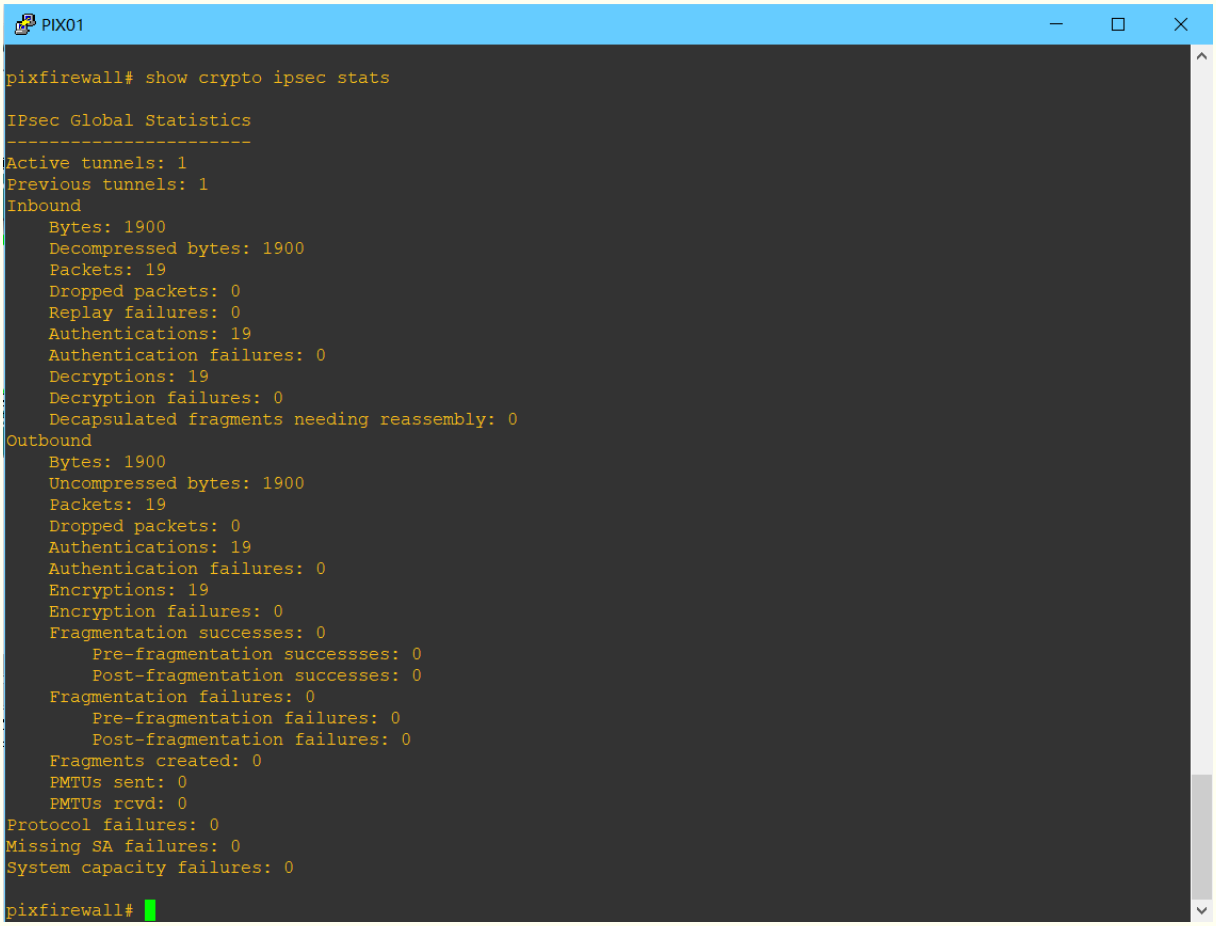
例如，下面情况，原来加密包数目是 14，ping 一次，5 个包全通，加密包记录数+5。

PIX01

```
pixfirewall# show crypto ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 1
Previous tunnels: 1
Inbound
    Bytes: 1400
    Decompressed bytes: 1400
    Packets: 14
    Dropped packets: 0
    Replay failures: 0
    Authentications: 14
    Authentication failures: 0
    Decryptions: 14
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 1400
    Uncompressed bytes: 1400
    Packets: 14
    Dropped packets: 0
    Authentications: 14
    Authentication failures: 0
    Encryptions: 14
    Encryption failures: 0
    Fragmentation successes: 0
        Pre-fragmentation successses: 0
        Post-fragmentation successes: 0
    Fragmentation failures: 0
        Pre-fragmentation failures: 0
        Post-fragmentation failures: 0
    Fragments created: 0
    PMTUs sent: 0
    PMTUs rcvd: 0
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0

pixfirewall#
```

R2

```
R2#ping 10.1.6.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.6.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/65/68 ms
R2#
```



143.验证配置：telnet

在 R3 上设置 Telnet 密码，密码是 cisco：

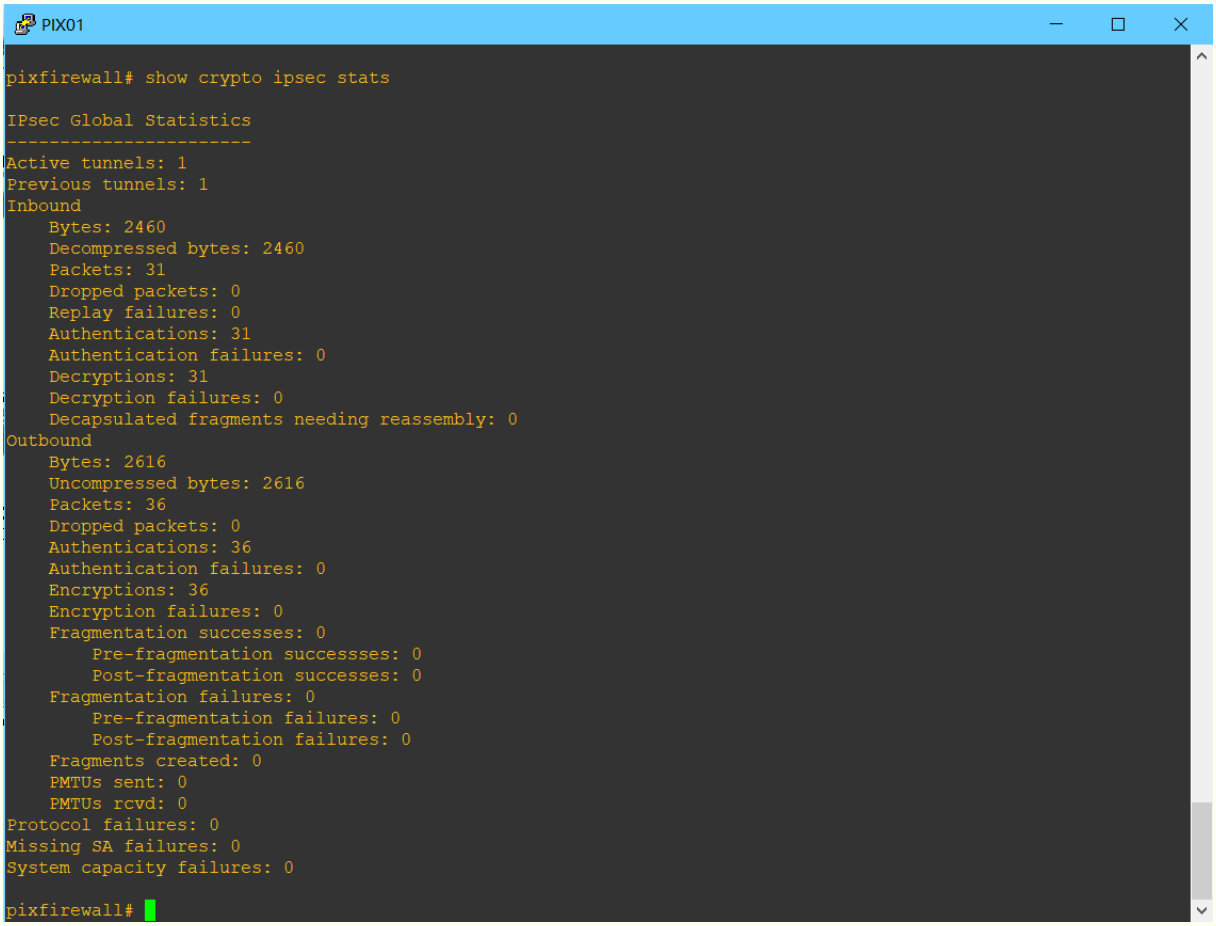
R3(config)#line vty 0 15

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



144.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

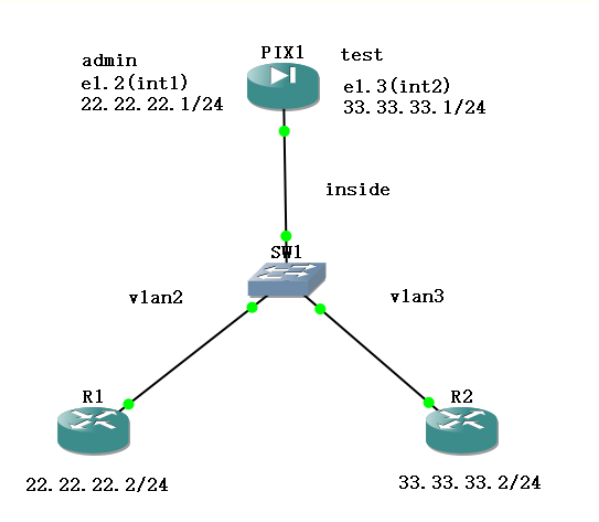
R1(config-line)#password cisco

从 R2 Telnet 到 R1，输入密码 cisco。

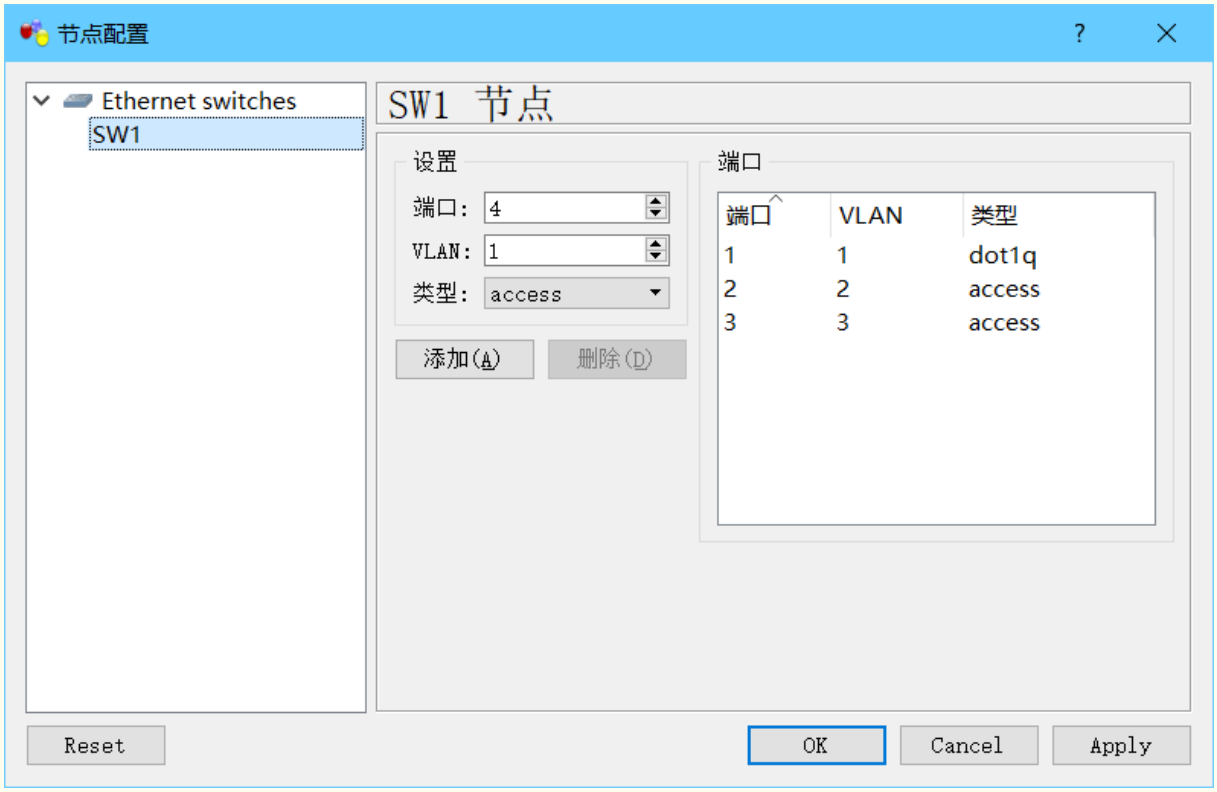
防火墙记录数不会增加，说明没有走 VPN。

5 虚拟防火墙配置

145.实验拓扑



146.配置交换机



147.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

```
R1
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int f0/0
R1(config-if)#ip add 22.22.22.2 255.255.255.0
R1(config-if)#no sh
R1(config-if)#
00:01:13: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
00:01:14: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config-if)#
```

```
R2
Connected to Dynamips VM "R2" (ID 1, type c3600) - Console port
Press ENTER to get the prompt.

R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int f0/0
R2(config-if)#ip add 33.33.33.2 255.255.255.0
R2(config-if)#no sh
R2(config-if)#
R2(config-if)#
```

148.激活防火墙

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

和之前实验一样

注：激活完需要重启防火墙

149.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

150.验证配置：show mode

pixfirewall# show mode

若成功则会显示 Security context mode: multiple

```
PIX2
pixfirewall# show mode
Security context mode: multiple
```

151.配置防火墙子接口，为其分配 VLAN

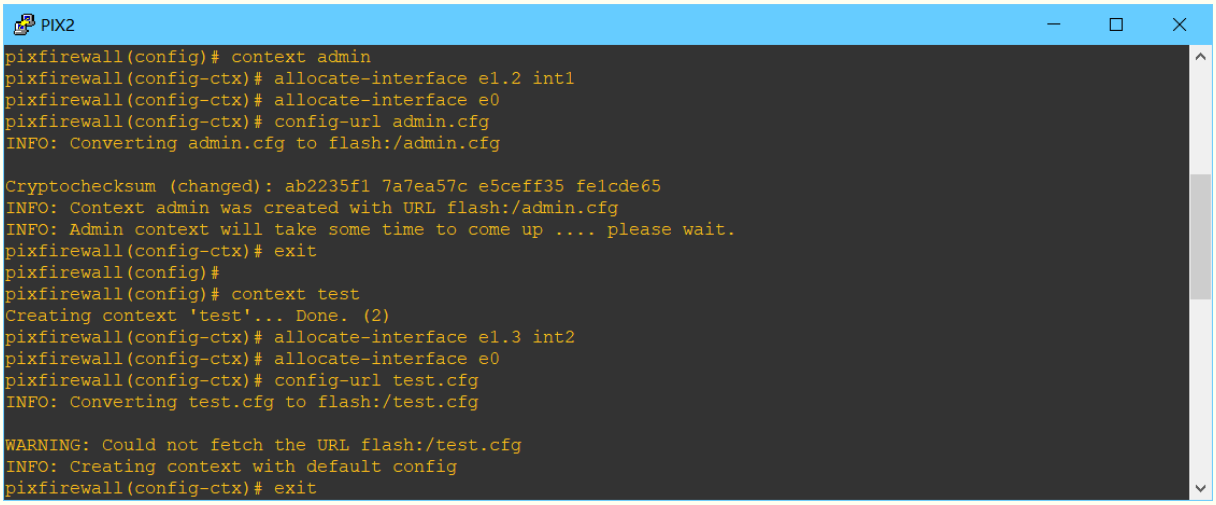
pixfirewall(config)# int e1.2
pixfirewall(config-subif)# vlan 2
pixfirewall(config-subif)# int e1.3
pixfirewall(config-subif)# vlan 3

```
PIX2
pixfirewall# conf t
pixfirewall(config)# int e1.2
pixfirewall(config-subif)# vlan 2
pixfirewall(config-subif)# int e1.3
pixfirewall(config-subif)# vlan 3
pixfirewall(config-subif)# exit
```

152.配置安全上下文，为其分配接口，指定其配置文件存放位置

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



153.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

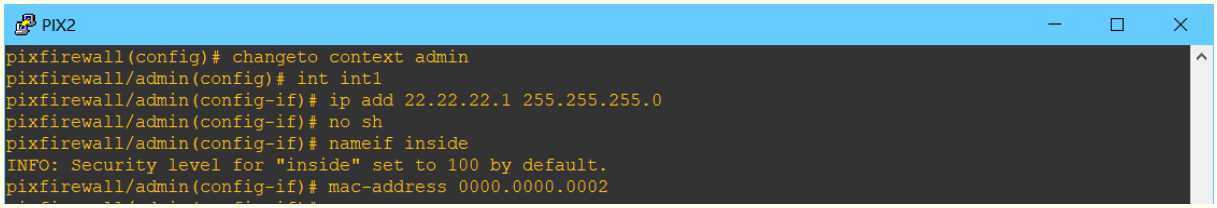
154.在安全上下文中配置防火墙接口 IP 和名称

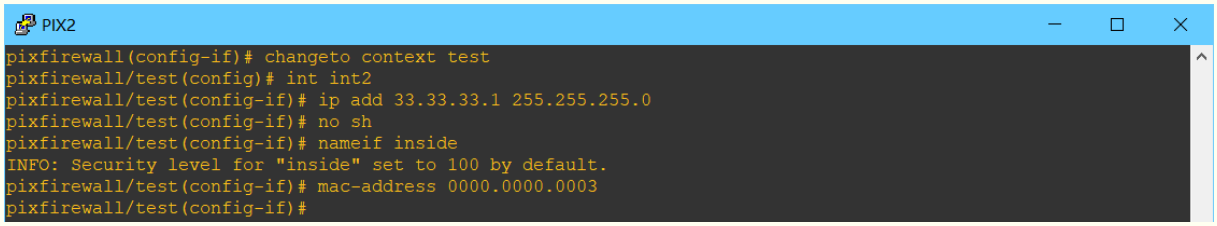
需要为防火墙的每个接口配置 IP 地址
为每个接口配置 nameif 以及 security-level

同之前实验

155.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





156.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

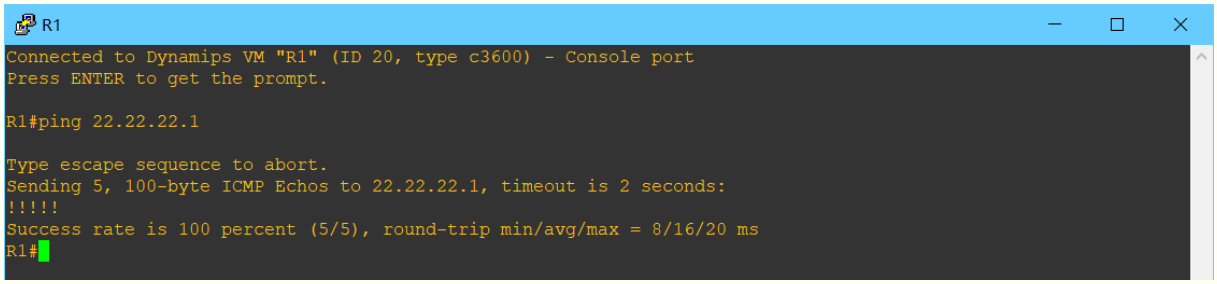
在主接口打开接口

pixfirewall(config)# int e1

pixfirewall(config-if)# no sh

注：只有主接口才能 no sh

157.验证配置：ping



About

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

Reference

无参考文献

Presented by

Kloudy Grasp™
2021/6/28
Website: www.kloudy.cn

Written by

EndersKim
Email: enderskim@qq.com