

一个思科PIX防火墙的实际应用配置 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/284/2021_2022__E4_B8_80_E4_B8_AA_E6_80_9D_E7_c101_284834.htm

PIX：一个合法IP完成inside、outside和dmz之间的访问 现有条件：100M宽带接入，分配一个合法的IP（222.134.135.98）（只有1个静态IP是否够用？）；Cisco防火墙PiX515e-r-DMZ-BUN1台（具有Inside、Outside、DMZ三个RJ45接口）！

请问能否实现以下功能：

1、内网中的所有用户可以访问Internet和DMZ中的WEB服务器。 2、外网的用户可以访问DMZ区的Web平台。 3、DMZ区的WEB服务器可以访问内网中的SQL数据库服务器和外网中的其它服务器。

注：DMZ区WEB服务器作为应用服务器，使用内网中的数据库服务器。

解决方案：一、概述 本方案中，根据现有的设备，只要1个合法的IP地址（电信的IP地址好贵啊，1年租期10000元RMB），分别通过PIX515所提供的NAT、PAT、端口重定向、ACL和route功能完全可以实现所提的功能要求。

二、实施步骤 初始化Pix防火墙：给每个边界接口分配一个名字，并指定安全级别

```
pix515e(config)# nameif ethernet0 outside security0
```

```
pix515e(config)# nameif ethernet1 inside security100
```

```
pix515e(config)# nameif ethernet2 dmz security50
```

给每个接口分配IP地址

```
pix515e(config)# ip address outside
```

```
222.134.135.98 255.255.255.252
```

```
pix515e(config)# ip address inside
```

```
192.168.1.1 255.255.255.0
```

```
pix515e(config)# ip address dmz 10.0.0.1
```

```
255.255.255.0
```

为Pix防火墙每个接口定义一条静态或缺省路由

```
pix515e(config)# route outside 0.0.0.0 0.0.0.0 222.134.135.97 1
```

（通过IP地址为222.134.135.97的路由器路由所有的出站数据包）

```
/ 外部接口 / ) pix515e(config)# route dmz 10.0.0.0
255.255.255.0 10.0.0.1 1pix515e(config)# route inside 192.168.1.0
255.255.255.0 192.168.1.1 1pix515e(config)# route outside
222.134.135.96 255.255.255.252 222.134.135.98 1 配置Pix防火墙作
为内部用户的DHCP服务器pix515e(config)# dhcpd address
192.168.1.2-192.168.1.100 insidepix515e(config)# dhcpd dns
202.102.152.3 202.102.134.68pix515e(config)# dhcpd enable inside
100Test 下载频道开通，各类考试题目直接下载。详细请访问
www.100test.com
```