

思科防火墙PIXASA精华配置总结思科认证 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/644/2021_2022__E6_80_9D_E7_A7_91_E9_98_B2_E7_c101_644072.htm 思科防火墙 PIX ASA

配置总结一（基础）：思科防火墙已经从PIX发展到ASA了

，IOS也已经从早期的6.0发展到7.2。但总体的配置思路并没有多少变化。只是更加人性化，更加容易配置和管理了。下面是我工作以来的配置总结，有些东西是6.3版本的，但不影响在7.*版本的配置。

一：6个基本命令：nameif、interface、ip address、nat、global、route。二：基本配置步骤：

step1: 命名接口名字 nameif ethernet0 outside security0 nameif

ethernet1 inside security100 nameif ethernet2 dmz security50 * * 7

版本的配置是先进入接口再命名。 step2：配置接口速率

interface ethernet0 10full auto interface ethernet1 10full auto

interface ethernet2 10full step3：配置接口地址 ip address outside

218.106.185.82 ip address inside 192.168.100.1 255.255.255.0 ip

address dmz 192.168.200.1 255.255.255.0 step4：地址转换（必须

）* 安全高的区域访问安全低的区域（即内部到外部）

需NAT和global. nat(inside) 1 192.168.1.1 255.255.255.0

global(outside) 1 222.240.254.193 255.255.255.248 * * * nat

(inside) 0 192.168.1.1 255.255.255.255 表示192.168.1.1这个地址不

需要转换。直接转发出去。 * 如果内部有服务器需要映射到

公网地址(外网访问内网)则需要static和conduit或者acl. static

(inside, outside) 222.240.254.194 192.168.1.240 static (inside,

outside) 222.240.254.194 192.168.1.240 10000 10 后面的10000为限制

连接数，10为限制的半开连接数。 conduit permit tcp host

222.240.254.194 eq www any conduit permit icmp any any (这个命令在做测试期间可以配置，测试完之后要关掉，防止不必要的漏洞) ACL实现的功能和conduit一样都可实现策略访问，只是ACL稍微麻烦点。conduit现在在7版本已经不能用了。

```
Access-list 101 permit tcp any host 222.240.254.194 eq www
```

Access-group 101 in interface outside (绑定到接口) * * * 允许任何地址到主机地址为222.240.254.194的www的tcp访问。

Step5：路由定义：Route outside 0 0 222.240.254.193 1 Route

inside 192.168.10.0 255.255.255.0 192.168.1.1 1 * * 如果内部网段不是直接接在防火墙内口，则需要配置到内部的路由。 Step6

：基础配置完成，保存配置。 Write memory write erase 清空配置 reload 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