

CiscoPIX防火墙PPTPVPN相关配置 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/240/2021_2022_CiscoPIX_E9_98_c101_240548.htm 一、基础知识：PPTP：点对点隧道协议
点对点隧道协议（PPTP：Point to Point Tunneling Protocol）是一种支持多协议虚拟专用网络的网络技术。通过该协议，远程用户能够通过 Microsoft Windows NT 工作站、Windows 95 和 Windows 98 操作系统以及其它装有点对点协议的系统安全访问公司网络，并能拨号连入本地 ISP，通过 Internet 安全链接到公司网络。PPTP 可以用于在 IP 网络上建立 PPP 会话隧道。在这种配置下，PPTP 隧道和 PPP 会话运行在两个相同的机器上，呼叫方充当 PNS.PPTP 使用客户机 - 服务器结构来分离当前网络访问服务器具备的一些功能并支持虚拟专用网络。PPTP 作为一个呼叫控制和管理协议，它允许服务器控制来自 PSTN 或 ISDN 的拨入电路交换呼叫访问并初始化外部电路交换连接。PPTP 只能通过 PAC 和 PNS 来实施，其它系统没有必要知道 PPTP.拨号网络可与 PAC 相连接而无需知道 PPTP.标准的 PPP 客户机软件可继续在隧道 PPP 链接上操作。PPTP 使用 GRE 的扩展版本来传输用户 PPP 包。这些增强允许为在 PAC 和 PNS 之间传输用户数据的隧道提供低层拥塞控制和流控制。这种机制允许高效使用隧道可用带宽并且避免了不必要的重发和缓冲区溢出。PPTP 没有规定特定的算法用于低层控制，但它确实定义了一些通信参数来支持这样的算法工作。二、配置 1、命令行方式直接在PIX上配置PPTP的VPN，即PIX作为PPTP方式VPDN的服务器ip local pool pptp 10.0.0.1-10.0.0.50//定义一个pptp方式的vpdn拨入后获得的IP地

址池，名字叫做pptp。此处地址段的定义范围不要和拨入后内网其他计算机的IP冲突，并且要根据拨入用户的数量来定义地址池的大小

```
vpdn group PPTP-VPDN-GROUP accept dialin
pptpvpdn group PPTP-VPDN-GROUP ppp authentication
papvpdn group PPTP-VPDN-GROUP ppp authentication
chapvpdn group PPTP-VPDN-GROUP ppp authentication
mschapvpdn group PPTP-VPDN-GROUP ppp encryption mppe
auto//以上为配置pptp的vpdn组的相关属性
```

vpdn group PPTP-VPDN-GROUP client configuration address local pptp//上面定义pptp的vpdn组使用本地地址池组pptp，为一开始定义的vpdn group PPTP-VPDN-GROUP pptp echo 60

```
vpdn group PPTP-VPDN-GROUP client authentication local//此处配置pptp的vpdn拨入用户口令认证为本地认证，当然也可以选择AAA服务器认证，本地认证属于比较方便的一种实现
```

```
vpdn username test1 password *****
vpdn username test2 password *****//上面为定义本地用户认证的用户帐号和密码，可以定义多个
```

vpdn enable outside//在pix防火墙的outside口起用vpdn功能，也可以在其他接口上应用

2、使用pix防火墙内部的某个pptp的VPDN服务器作为专门的VPN服务器，只是在pix上开放相应的服务端口

pptp使用1723端口，而通常pix里面的服务器对外都是做的静态NAT转换，但是光双向开放1723端口仍旧无法建立pptp的vpn连接，那么对于pix 6.3以上版本的pptp穿透可以用一条命令

```
fixup protocol pptp 1723
```

来解决这个问题。

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