inside、outside和dmz之间的访问 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_inside_E3_80_81o_c101_240553.htm 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防问Internet和DMZ中的WEB服务器。 2、外网的用户可以防问DMZ区的Web平台。 3、DMZ区的WEB服务器可以防问内网中的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 security0pix515e(config)# nameif ethernet1 inside security100pix515e(config)# nameif ethernet2 dmz security50给每个接口分配IP地址pix515e(config)# ip address outside 222.134.135.98 255.255.255.252pix515e(config)# ip address inside 192.168.1.1 255.255.255.0pix515e(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DPCH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 1 、配置Pix防火墙来允许处于内部接口上的用户防问Internet和堡垒主机 同时允许DMZ接口上的主机可以防问Internet 通过设置NAT和PAT来实现高安全级别接口上的主机对低安全级别接口上的主机的防问。 （1）命令如下：pix515e(config)# nat (inside) 10 192.168.1.0 255.255.255.0pix515e(config)# nat (dmz) 10 10.0.0.0 255.255.255.0pix515e(config)# global (outside) 10 interfacepix515e(config)# global (dmz) 10 10.0.0.10-10.0.0.254 netmask 255.255.255.0（2）第一个nat命令允许在安全级别为100的内部接口上的主机，去连接那些安全级别比它低的接口上的主机。在第一个命令中，低安全级别接口上的主机包括外部接口上的主机和非军事区／DMZ／上的主机。第二个nat命令允许在安全级别为50的DMZ上的主机，去连接那些安全级别比它低的接口上的主机。而在第二个命令中，低安全级别的接口只包含外部接口。 （3）因为全局地址池和nat（inside）命令都使用nat_id为10，所以在192.168.1.0网络上的主机地址将被转换成任意地址池中的地址。因此，当内部接口上用户访问DMZ上的主机时，它的源地址被转换成global（dmz）命令定义的10.0.0.10-10.0.0.254范围中的某一个地址。当内部接口上的主机防问Internet时，它的源地址将被转换成global （outside）命令定义的222.134.135.98和一个源端口大

于1024的结合。（4）当DMZ上用户访问外部主机时，它的源地址被转换成global（outside）命令定义的222.134.135.98和一个源端口大于1024的结合。Global（dmz）命令只在内部用户访问DMZ接口上的Web服务器时起作用。（5）内部主机访问DMZ区的主机时，利用动态内部NAT把在较安全接口上的主机地址转换成不太安全接口上的一段IP地址或一个地址池（10.0.0.10-10.0.0.254）。内部主机和DMZ区的主机防问Internet 时，利用PAT1个IP地址和一个源端口号的结合，它将创建一个惟一的对话，即PAT全局地址（222.134.135.98）的源端口号对应着内部或DMZ区中的唯一的IP地址来标识唯一的对话。PAT全局地址（222.134.135.98）的源端口号要大于1024.理论上，在使用PAT时，最多可以允许64000台内部主机使用一个外部IP地址，从实际环境中讲大约4000台内部的主机可以共同使用一个外部IP地址。） 2、 配置PIX防火墙允许外网的用户可以防问DMZ区的Web服务器 通过配置静态内部转换、ACL和端口重定向来实现外网对DMZ区的Web防问。（1）命令如下static (dmz,outside) tcp interface www 10.0.0.2 www dns netmask 255.255.255.255 0 0access-list outside_access_in line 1 permit tcp any interface outsideaccess-group 101 in interface outside （2）PIX防火墙静态PAT所使用的共享全局地址可以是一个惟一的地址，也可以是一个共享的出站PAT地址，还可以与外部接口共享一个地址。（3）Static静态转换中“ DNS ”表示进行“ DNS记录转换 ”DNS记录转换应用在当内部的主机通过域名连接处于内部的服务器，并且用来进行域名解析的服务器处于PIX防火墙外部的情况下。 一个处于内网中的客户端通过域名向地址为10.0.0.2的Web服务器发送

一个HTTP请示。首先要通过PIX防火墙外部接口上的DNS服务器进行域名解析，因此客户端将DNS解析请求包发送到PIX防火墙上。当PIX防火墙收到客户端的DNS解析请求包时，将IP头中不可路由的源地址进行转换，并且将这个DNS解析请求转发到处于PIX防火墙外部接口上的DNS服务器。DNS服务器通过A-记录进行地址解析，并将结果返回到客户端。当PIX防火墙收到 DNS解析回复后，它不仅要将目的地址进行转换，而且还要将DNS解析回复中的地址替换成Web服务器的实际地址。然后PIX防火墙将DNS解析发回客户端。这样所产生的结果是，当客户端收到这个DNS解析回复，它会认为它与Web服务器处于内部网络中，可以通过DMZ接口直接到达。 3、DMZ区的WEB服务器可以防问内网中的SQL数据库服务器和外网中的其它服务器 通过静态内部转换可以实现DMZ区的主机对内网中的主机的防问。 （1）命令如下：static (inside,dmz) 10.0.0.9 192.168.1.200 netmask 255.255.255.255 0 0access-list dmz_access_in line 1 permit tcp any anyaccess-group dmz_access_in in interface dmz （2）静态内部地址转换可以让一台内部主机固定地使用PIX防火墙全局网络中的一个地址。使用Static命令可以配置静态转换。Static命令创建一个在本地IP地址和一个全局IP地址之间的永久映射（被称为静态转换槽或xlate），可以用来创建入站和出站之间的转换。 除了Static命令之外，还必须配置一个适当的访问控制列表（ACL），用来允许外部网络对内部服务器的入站访问。 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