思科认证:简单八步实现思科ASA远程访问Cisco认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/557/2021_2022__E6_80_9D_E7_A7_91_E8_AE_A4_E8_c101_557839.htm 你是否需要快速地设置用户的远程访问呢?配置远程访问可能是一件令人困惑的过程。不过，只要遵循以下的操作指南就可以事半功倍。 对于Cisco ASA的用户来说，要设置远程访问只需要简单的八步，下面开始： 步骤一：配置一个身份证书 在这里，笔者要创建一个一般的名为sslvpnkey的身份证书，并将此证书应用给“ 外部 ”接口。用户可以购买厂商的证书。下面是操作步骤： corpasa(config)#crypto key generate rsa label sslvpnkey
corpasa(config)#crypto ca trustpoint localtrust
corpasa(config-ca-trustpoint)#enrollment self
corpasa(config-ca-trustpoint)#fqdn sslvpn. mycompany.com
corpasa(config-ca-trustpoint)#subject-name CN=sslvpn.mycompany.com
corpasa(config-ca-trustpoint)#keypair sslvpnkey
corpasa(config-ca-trustpoint)#crypto ca enroll localtrust noconfirm
corpasa(config)# ssl trust-point localtrust outside 步骤二：将SSL VPN客户端映象上传到ASA 用户可以从思科的网站(cisco.com0获得客户端映象。在选择要下载哪个映象给TFTP服务器时，记住你需要为用户所使用的每种操作系统下载单独的映象。在选择并下载客户端软件后，就可以将其TFTP到ASA。 corpasa(config)#copy tftp://192.168.81.50/anyconnect-win-2.0.0343-k9.pkg flash 在将文件上传到ASA之后,配置一下这个文件,使其可用作Web VPN会

话.注意,如果你有多个客户端,就应当配置最常用的客户,使其拥有最高的优先权。在本文中，我们将仅使用一个客户端并为其设置优先权为1： corpasa(config)#webvpn
corpasa(config-webvpn)#svc image
disk0:/anyconnect-win-2.3.0254-k9.pkg 1 步骤三：启用AnyConnect VPN访问 corpasa(config)#webvpn
corpasa(config-webvpn)#enable outside
corpasa(config-webvpn)#svc enable 步骤四：创建组策略 组策略用于指定应用于所连接客户端的参数。在本文中，我们将创建一个称之为SSLClient的组策略。远程访问客户端需要在登录期间分配一个IP地址，所以我们还需要为这些客户端建立一个DHCP地址池，不过如果你有DHCP服务器，还可以使用DHCP服务器。 corpasa(config)#ip local pool SSLClientPool 192.168.100.1-192.168.100.50 mask 255.255.255.0
corpasa(config)#group-policy SSLCLient internal
corpasa(config)#group-policy SSLCLient attributes
corpasa(config-group-policy)#dns-server value 192.168.200.5
corpasa(config-group-policy)#vpn-tunnel-protocol svc
corpasa(config-group-policy)#default-domain value mysite.com
corpasa(config-group-policy)#address-pools value SSLClientPool 步骤五：配置访问列表旁路 通过使用sysopt connect命令，我们告诉ASA准许SSL/IPsec客户端绕过接口的访问列表：
corpasa(config)#sysopt connection permit-vpn 步骤六：创建连接配置文件和隧道组 在远程访问客户端连接到ASA时，也就连接到了connection profile连接配置文件，也称为隧道组。我们将用这个隧道组来定义其使用的特定连接参数。在本文中，

我们将配置这些远程访问客户端使用Cisco AnyConnect SSL客户端，不过，你还可以配置隧道组使用IPsec、L2L等。 首先，创建隧道组SSL 客户端： corpasa(config)#tunnel-group SSLClient type remote-access 下一步，分配特定的属性： corpasa(config)#tunnel-group SSLClient general-attributes corpasa(config-tunnel-general)#default-group-policy SSLCLient corpasa(config-tunnel-general)#tunnel-group SSLClient webvpn-attributes corpasa(config-tunnel-webvpn)#group-alias MY_RA enable corpasa(config-tunnel-webvpn)#webvpn corpasa(config-webvpn)#tunnel-group-list enable 注意，别名“ MY_RA ”就是你的用户们在得到提示进行登录认证时看到的组。 步骤七：配置NAT免除 现在，我们需要告诉ASA不要对远程访问客户端和要访问的内部网络之间的通信进行网络地址转换(NAT)。首先，我们要创建一个可定义通信的访问列表，然后，我们将此列表用于接口的NAT语句： corpasa(config)#access-list no_nat extended permit ip 192.168.200.0 255.255.255.0 192.168.100.0 255.255.255.0 corpasa(config)#nat (inside) 0 access-list no_nat 步骤八：配置用户账户 现在我们已经为配置用户账户做好了准备。在此，我们要创建一个用户并且将此用户指派给我们的远程访问VPN： corpasa(config)#username hyde password l3tm3in corpasa(config)#username hyde attributes corpasa(config-username)#service-type remote-access 完成任务 不要忘记将你的配置保存到存储器中： corpasa#write memory 还要建立一个远程访问会话来验证你的配置，并使用下面的show命令来查看会话的细节： corpasa #show vpn-sessiondb

svc 更多优质资料尽在百考试题论坛 百考试题在线题库 思科认证更多详细资料 但愿本文可帮助你实现远程用户的访问和运行。如果你碰到了困难，不妨运行debug webvpn命令来诊断问题。 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