如何依靠思科ASA设备构建安全V 网络 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/461/2021_2022__E5_A6_82_E4_BD_95_E4_BE_9D_E9_c101_461779.htm 问：我所工作的企业近来购买了一台思科Cisco ASA 5510和三台ASA 5505，用以替换几台我们在几个工作组家庭用户中所拥有的SonicWalls。这些设备是为了组建一个站点到站点的VPN通道，这样我们的工作组家庭用户就可以访问我们的VoIP电话以及远程的,以进入我们的终端服务器。我还设法从家里测试ASA设备，并且试验了多个方面，不过全都失败了。您有何指教? 答：既然是从一个不同品牌的防火墙转移，你可能需要几步才能完成这项工作。在你工作时作好记录是很重要的，随着你对防火墙的操作越来越熟悉，这对你有很大帮助。 笔者所建议你做的第一件事情是看一下关于你各个防火墙的许可证。虽然思科引用了不同的许可级别，我还是发现了与你所期望的有点儿不同的术语：假设5510有十个用户许可，而5505有5个用户许可，如果你从5505端到5510端遇到了一个VPN链接，访问一个复杂的Web站点，你就会耗尽5510上的所有许可，而且由于在思科ASA设备上处理许可的方法，VPN连接看似失效。 因此请检查你所拥有的ASA设备之间的许可：如果你拥有三个ASA 550设备，每个设备上安装了一个10用户的许可，你会想到为5510设备的总共许可增加许可的用户数目，直到其数目达到总公司的用户数。假设在总公司你有20个用户，你会想到在5510设备上安装一个许可，至少支持50个用户。你可能会发现，在5510上需要一个较高的许可数量。你需要进行一些测试以确保这一点。不幸的是，你不会真正地看到这

种现象。 一旦你解决了许可问题，就可以在ASA 5510和一个5505之间的两个WAN端口连接起来。你可能需要使用一根交叉电缆在两个防火墙之间建立连接。你还可以试着在两个ASA设备之间安装一台交换机-一台三层交换机是比较理想的，或者可以试用一台拥有两个以太网接口的路由器。这会允许你从不同的子网分配IP地址分别给那些你正在测试的ASA设备。应当设置一个站点到站点的VPN连接。要确保你能够在两台ASA设备之间正确地路由选择，并在连接的每一个端能够看到所有的系统。这会为你建立一个VPN连接提供帮助。 下一步你所做的依赖于你如何在站点间建立连接。如果你只是在自己的总公司的位置需要提供给服务器的通信，以通过VPN通道，并允许其余的互联网通信直接通过本地连接发送出去,你可能会希望建立一个分离隧道配置。这种配置可能意味着你需要更多的维护工作，因为你会需要维护多套防火墙规则。在允许通信转发到互联网上之前，强制所有的通信流回到总公司可能意味着远程的位置将要两次占用你的带宽，其中一次用于从远程站点进入的连接，另外一次用于它们试图访问的互联网资源。 因为你正从一个品牌的VPN/防火墙设备转向另外一种设备，你还要做另外一个决定：是一下子改变所有的设备，还是分步骤地迁移到新的系统。第一种方案意味着在你建立起每个站点之前，所有的人都要“宕机”。采用后一种方案需要你的ISP为你分配额外的IP地址，以使设备协调运行直到迁移完成。 在总公司，你可能还需要添加一些静态的路由，用于为一个特定的站点指引通信，以到达正确的VPN设备，直到你将全部都转化到新的系统上。虽然这最后一个选项可能需要更多的工作，不过笔者认为

你会发现这能使事情变得容易一些，因为它有助于减少转化过程的压力。 虽然上面叙述的并非绝对完整的回答，不过却有助于你开始工作。可以访问思科的Web站点，你会发现几个有用的参考文档，这会有助于你理解笔者在此所讨论的配置问题。在你使其运行后，应当保存副本，并使其与ASA设备相分离。然后删除配置，并重新创建它。这有助于你确信：在你重新创建配置而它第二次或第三次都不能运行，这样你就有一个基本的配置来进行比较，以帮助你修正问题，并且可以帮助你诊断故障。 一旦你使自己的配置正常运行后，可能需要将机器的IP改为ISP所分配的真实IP地址，由此你便可以一展身手了。 