思科:面对思科ASA与DNS冲突我们如何应对Cisco认证考试
 在本文中，思科专家洛里海德将向你介绍，在思科自适应安全产品（ASA）默认配置丢弃数据包的情况下，如何对域名系统信息进行替换使得用户可以访问内部网络资源。 设定的环境：你拥有一家小型公司或者一个没有自己专用内部域名系统服务器提供域名系统(DNS)解决方案的远程站点。它们采用的是由互联网服务提供商提供的外部域名系统服务器。公司站点是利用静态网络地址转换对私人网络IP地址进行转换，以实现可以公开访问互联网的目标，并且，该私人网络IP地址受到思科ASA防火墙的保护。 需求：位于内部服务器上的公司用户应该可以访问位于互联网上的该公司网站。 ASA默认配置导致的结果：由于数据包被丢弃导致内部用户无法实现对公司网站的访问。 这个问题的关键在于ASA是怎样对域名系统解决方案的工作进行限制的。 在这个例子中，我们要实现的目标是让内部用户可以访问公司网站。在这个过程中，包含公司网站网络IP地址信息的域名系统数据包被创建。这个请求返回的数据包就会经过思科ASA，接着其中包括了它本身的网络IP地址以及由外部互联网服务提供商提供的域名系统服务器提供的相关请求的数据包就会被进行源地址重写处理。 域名系统服务器将会对经过ASA处理包含了公共网络IP地址由公司网站发送的查询包进行响应。ASA收到回复后，会利用用户系统的网络IP地址对目的地地址进行重写，并将数据包转发到用户系统中。 然后，用户系统就会试图通过建立一条采用

超文件传输协议的通道打开公司网站。 由于网站的网络IP地址已经转换为公共IP地址，用户的请求数据包将会通过ASA的内部接口，在已经与外部建立连接的情况下，就到达了外部接口。接着，该数据包将会被ASA丢弃，因为它不会被容许返回到内部接口中。具体过程如图A所示。 图A 这项功能被称做发夹。在默认设置下，ASA没有启用发夹功能。实际上，不至一种方法可以解决这个问题。通常情况下，最简单的解决方案就是域名系统替换。 只要改变静态网络地址转换模式的一个选项，就可以让ASA实现利用内部万维网服务器提供的网络IP地址而不是公共IP地址来进行内部域名系统的查寻。 静态网络地址转换模式的原始设置： static (inside,outside) 172.16.20.200 10.10.10.10 netmask 255.255.255.255 静态网络地址转换模式更新后的设置，并且启用了域名系统替换选项： static (inside,outside) 172.16.20.200 10.10.10.10 netmask 255.255.255.255 dns 更新后的域名系统查询过程 由公司网站所在的网络IP地址发出域名系统查询请求。这个请求的数据包会经过思科ASA，接着就会对数据包进行源地址重写，其中包括了它本身的网络IP地址以及由外部互联网服务提供商提供的域名系统服务器提供的相关请求。 域名系统服务器将会对经过ASA处理包含了公共网络IP地址由公司网站发送的查询包进行响应。ASA收到回复后，会利用用户系统的网络IP地址对目的地地址进行重写，并将域名系统查询结果利用内部万维网服务器提供的网络IP地址进行重写，接着将数据包转发到用户系统中。整个过程如图B所示。 图B 通过思科ASA自适应安全设备管理器接口进行这样的设置是非常方便的。 进入配置|防火墙|网络地址转换规则选项。然后，

选择静态网络地址转换模式，并进行编辑。在连接设置项，选择对域名系统答复信息匹配翻译规则即可。设置如图C所示。 图C 务必确认修改后的设置已经保存! 总的来说，这是一个快速简洁的解决方案。但在多数情况下，还是可能存在多种解决方案的。我们还可以选择在另一种情况下，启用全发夹模式。 在使用思科ASA的时间，你遇到过什么样的问题?