要防止IP欺骗 只需轻松配置CiscoIOS PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/205/2021_2022__E8_A6_81_E9_98_B2_E6_AD_A2I_c101_205882.htm 在典型的IP地址欺骗中，攻击者通常伪造数据包的发送地址，以便自己看起来像是来自内网。这里我们会告诉你可以采取的3个办法，让攻击者的日子不那么好过，使IP地址欺骗也无法轻易得逞。 众所周知，互联网上到处都是安全风险，其中之一便是IP地址欺骗。在典型的IP地址欺骗中，攻击者通常伪造数据包的发送地址，以便自己看起来像是来自内网。下面让我们讨论3种保护企业不受此种攻击的方法。 阻止IP地址 防止IP期骗得第一招是阻止可能造成风险的IP地址。不管背后原因是什么，攻击者可以假冒任何IP地址，最常被仿冒的IP地址是私网IP地址和其它类型的共享/特殊IP地址。这里是一些我会阻止其从互联网进入我的网络的IP地址以及它们的子网掩码的列表 ◆10.0.0.0/8 ◆172.16.0.0/12 ◆192.168.0.0/16 ◆127.0.0.0/8 ◆224.0.0.0/3 ◆169.254.0.0/16 所有上面这些地址都要么是在互联网上不可路由的私网IP地址，要么是用作其它用途而根本不应该在互联网上的IP地址。如果从互联网上进入的数据标有这些IP源地址，那么毫无疑问肯定是骗人的。 此外，其它一些经常被仿冒的IP地址是你的企业所使用的任意内网IP地址。如果你全部使用私网IP地址，那么你要阻止的地址范围就已经落入上述列表之中，然而，如果你使用的是一组公网IP地址，那么你应把它们也加入到以上列表中。 采用访问控制列表（ACLS） 阻止IP欺骗的最简单方法是对所有互联网数据使用进站过滤。过滤将扔掉所有落入以上IP地址的数据

包。换言之，通过创建一张访问控制列表，可以剔除所有来自上述范围内的IP地址的入站数据。 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