 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。 这里是一个配置的示例：Router# conf t Enter configuration commands, one per line. End with CNTL/Z. Router(config)# ip access-list ext ingress-antispoof Router(config-ext-nacl)# deny ip 10.0.0.0 0.255.255.255 any Router(config-ext-nacl)# deny ip 172.16.0.0 0.15.255.255 any Router(config-ext-nacl)# deny ip 192.168.0.0 0.0.255.255 any Router(config-ext-nacl)# deny ip 127.0.0.0 0.255.255.255 any Router(config-ext-nacl)# deny ip 224.0.0.0 31.255.255.255 any Router(config-ext-nacl)# deny ip 169.254.0.0 0.0.255.255 any Router(config-ext-nacl)# permit ip any any Router(config-ext-nacl)# exit Router(config)#int s0/0 Router(config-if)#ip access-group ingress-antispoof in 根据RFC 2267规定，互联网服务提供商（ISP）必须在网络上使用类似这一类的过滤。注意末尾处ACL包含permit ip any any的方式。在“真实世界”中，你的路由器中可能拥有一个状态式防火墙（stateful fireful），它可以保护你的内部局域网。 当然你可以在这方面更进一步，即过滤所有来自内网中其他子网的进站信息，以便保证没有人在一个子网内向其它子网进行IP地址欺骗。你还可以实施出站ACL来防止你的网络中的用户仿冒其他网络的IP地址。不过记住这只是整个网络安全策略中的一个方面。 使用反向路径转发（reverse path forwarding，即IP验证） cisco认证网，加入收藏另一个避免IP地址欺骗的方法是使用反向路径转发（RPF），或者叫IP验证。在Cisco IOS中，反向路径转发的命令以ip verify开头。 RPF的工作原理和反垃圾邮件解决方案非常类似。反垃圾邮件解决方案收到

了邮件消息后，先提出源邮件地址，然后执行向发送服务器查询的操作，确定发送者是否真的在发出消息的服务器上存在。如果发送者不存在，服务器则丢弃该邮件消息，因为根本就没法回复这种消息，而且大体上属于垃圾邮件。 RPF对数据包所作的操作与此类似。它从互联网收到数据包，取出源IP地址，然后查看该路由器的路由表中是否有该数据包的路由信息。如果路由表中没有其用于数据返回的路由信息，那么极有可能是某人伪造了该数据包，于是路由便把它丢弃。 下面是在路由器配置RPF的方法： Router（config）# ip cef Router（config）# int serial0/0 Router（config-if）# ip verify unicast reverse-path 注意这对多重网络（multi-homed network）没有效果。 保护私网不受来自互联网的攻击很重要。这三个方法对于防御IP地址欺骗已能起巨大效果。 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