四招教你打败僵尸网络的拒绝服务攻击思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/630/2021_2022__E5_9B_9B_E6_8B_9B_E6_95_99_E4_c101_630743.htm 也许很多人还没有注意到，据Arbor Networks的统计，2008年僵尸网络的拒绝服务攻击超过了每秒40GB的限度。这也就是说，当前的僵尸网络的攻击规模已经达到一个僵尸网络有 190万台僵尸电脑的程度，而僵尸网络的拒绝服务攻击是最难防御的攻击之一。因此，这也是拒绝服务攻击成为勒索者试图把在线商家作为人质获取赎金的常用手段的原因。这对于犯罪分子来说是一笔大买卖，而且这个生意很兴隆。 下面这种情况就很常见：犯罪分子利用一个僵尸网络大军渗透和消除对于你有价值的服务。攻击目标的范围包括仅用一个拒绝服务攻击使你的一台重要服务器达到饱和或者使你的互联网连接达到饱和，有效地中断你的全部互联网服务。在某些情况下，这些坏蛋首先发起攻击，中断网络服务，然后要求支付赎金。有时候，这些坏蛋仅仅发出赎金的要求，并且威胁说如果不在某日之前满足他们的要求，他们将中断攻击目标的网站。 当然，这些可能对我们来说已经不是什么新鲜事了。但是，如果你遭到过僵尸网络的拒绝服务攻击或者遭到过多次这种攻击，你是否想过你和你的公司应该采取什么措施吗?你如何准备应对这种类型的攻击?许多公司(包括大企业和小企业)都这样对待这个问题，他们解释说“ 我们没有黑客要的东西 ”或者“ 我们是小目标，不值得这样麻烦 ”。在某些情况下，这种事情是非常真实的，就是拒绝服务攻击的风险不值得安全投资。但是，在许多情况下，这种想法是一种危险的错误。这种风险实

际上比想象的要大。如果我从一个坏蛋的角度考虑这个问题，我在追求一二样东西，金钱或者名誉。如果你能够提供其中任何一样东西，你就有机会成为攻击目标。 因此，现在我们就来解决这个问题。你如何能够打败一个僵尸网络的拒绝服务攻击?这个答案取决于你遇到的拒绝服务攻击的类型、你的网络基础设施、你拥有的安全工具和其它变量。尽管在你的独特的环境中你如何防御拒绝服务攻击有许多变量，但是，强调一些最流行的策略是有价值的。 下面是打败拒绝服务攻击的一些技巧。其中有些方法过去在防御拒绝服务攻击中取得了成功。有些方法是全新的，但是，提供了一种非常令人心动的解决方案。 由ISP提供的拒绝服务攻击防御产品或者拒绝服务攻击服务 这种防御策略是通常是最有效的，当然也是最昂贵的。许多ISP(互联网服务提供商)为你的互联网链路提供某种方式的云计算拒绝服务攻击保护。这个想法是ISP在允许通讯进入你的互联网线路之前先清理你的通讯。由于这种防御是在云计算中完成的，你的互联网链路不会被拒绝服务攻击阻塞。不被阻塞至少是这个防御的目标。再说一次，没有一劳永逸的高明办法。这种服务也可以由第三方在云计算拒绝服务攻击防御服务中提供。在发生拒绝服务攻击时，他们把你的通讯转移到他们那里。他们清理你的通讯然后再把这些通讯发回给你。这一切都是在云计算中发生的，因此，你的互联网线路不会被阻塞。ISP提供的拒绝服务攻击服务的例子包括AT&amp.T的互联网保护服务和Verizon Business提供的拒绝服务攻击防御减轻服务。 RFC3704过滤 基本的访问控制列表(ACL)过滤器。RFC3704的主要前提是数据包应该来自于合法的、分配的地址段、与结构和空间分配一致。要达

到这个目的，有一个全部没有使用的或者保留的IP地址的列表。这些地址是你从互联网中永远看不到的。如果你确实看到了这些地址，那么，它肯定是一个欺骗的源IP地址，应该丢弃。这个列表的名称是Bogon列表，你应该咨询一下你的ISP，看他们是否能在这个欺骗的通讯进入你的互联网链路之前在云计算中为你管理这种过滤。Bogon列表大约每个月修改一次。因此，如果ISP没有为你做这个事情，那么，你必须自己管理你的Bogon访问控制列表规则(或者找另一家 ISP)。黑洞过滤 这是一个非常有效的常见的技术。一般来说，这需要与你的ISP一起做。RTBH(远程触发黑洞)过滤是一种能够提供在不理想的通讯进入一个保护的网络之前放弃这种通讯的能力的技术。这种技术使用 BGP(边界网关协议)主机路由把发往受害者服务器的通讯转接到下一跳的一个null0接口。RTBH有许多变体，但是，其中一个变态值得特别关注。与你的ISP一起试试RTBH过滤，让他们为你在云计算中放弃那种通讯，从而防止拒绝服务攻击进入你的通讯线路。 思科IPS 7.0源IP声誉过滤 思科最近发布了IPS 7.0代码更新。这个升级包括一个名为全球关联的功能。简言之，全球关联功能检查它看到的每一个源IP地址的声誉得分。如果这个来源的声誉不好，入侵防御系统(IPS)的传感器就可以放弃这个通讯或者提高一个点击的风险级别值。下面是思科对全球关联功能的解释： IPS 7.0包含一个名为“ 思科全球关联 ”的新的安全功能。这个功能利用了我们在过去的许多年里收集的大量的安全情报。思科IPS将定期从思科 SensorBase网络接收威胁更新信息。这个更新的信息包括互联网上已知的威胁的详细信息，包括连续攻击者、僵尸网络收获者、恶意爆发和黑网 (dark

nets)等。IPS使用这个信息在恶意攻击者有机会攻击重要资产之前过滤掉这些攻击者。IPS然后把全球威胁数据结合到自己的系统中以便更早地检测和防御恶意活动。 当然，你可以设置全球关联，这样的话，你的传感器就能够知道有恶意活动声誉的网络设备，并且能够对这种设备采取行动。 思科调整SensorBase的方法之一是接收来自思科7.0 IPS传感器的信息。企业可以选择使用这个程序，也可以选择不适用这个程序。思科IPS使用的SensorBase有不同的威胁种类。其中两种是僵尸网络收获者和以前的拒绝服务攻击实施者。因此，当你遭到僵尸网络拒绝服务攻击的时候，这个传感器将放弃所有的来至声誉不良的来源的通讯。这个过程在使用这种特征之前就开始了，对于传感器资源(处理器、背板等)来说是非常便宜的。这使它成为在拒绝服务攻击期间使用的一个理想的方法。这也是思科IPS在处理IPS 特征之前检查SensorBase的原因。 许多僵尸网络拒绝服务攻击使用通向你的网络服务器的SSL(安全套接字层)。这有助于攻击者隐藏其负载，防止你可能拥有的检测引擎的检查。然而，考虑到全球关联仅使用源IP地址的声誉得分做出决定，防御SSL分布式拒绝服务攻击是没有问题的。没有任何其它厂商为自己的IPS解决方案增加基于声誉的检查功能，因此，它们不能防御任何形式的SSL分布式拒绝服务攻击。一些IPS厂商确实能够能通过解密传输中的数据打开和查看SSL数据包内部。然而，这个过程在IPS资源(处理器、背板、内存等)方面太昂贵，不能用于分布式拒绝服务攻击。它会迅速消除传感器本身的通讯瓶颈。 当然，如果这个分布式拒绝服务攻击阻塞了你的链路，这个策略可能就不起作用。但是，如果分布式拒绝服务攻击仅仅阻塞了

部分服务器，而没有阻塞整个网络，那就表明这个防御措施的作用很好。全球关联不是一个妙方，而是你的工具箱中的另一个工具。 IP源防护 这个问题不是五大主要问题的一部分，不过，这个问题仍然值得一提。这个技巧是打开你的交换机中的IP源防护功能。这个功能可以阻止主机在变成僵尸电脑的时候发出欺骗性的数据包。这不是一个防御工具，而是一个守法公民工具，尽管它能够阻止内部的欺骗性的分布式拒绝服务攻击。如果每一家公司都打开IP源防护功能，它就能够帮助减少我们遇到的欺骗性分布式拒绝服务攻击的数量。启用IP源防护功能的一项增加的好处是能够帮助你找到你的网络中已经成为僵尸网络一部分的主机。当这个恶意软件发动欺骗性攻击的时候，这个交换机端口能够自动锁死，并且向你的安全监视站点报告这个事件。或者你报告这个事件并且保持打开这个端口，但是，除了真正的IP地址源通讯之外，放弃所有的通讯。 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 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