九大妙招:增强边界路由安全防护能力 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/0/2021_2022__E4_B9_9D_E5_A4_A7_E5_A6_99_E6_c99_485.htm 导读:在下列指南中，我们将研究一下你可以用来保护网络安全的9个方便的步骤。1.修改默认的口令、2.关闭IP直接广播（IP Directed Broadcast）、3.如果可能，关闭路由器的HTTP设置、4.封锁ICMP ping请求、5.关闭IP源路由、6.确定你的数据包过滤的需求、7.建立准许进入和外出的地址过滤政策、8.保持路由器的物理安全、9.花时间审阅安全记录。 这些步骤能够保证你拥有一道保护你的网络的砖墙，而不是一个敞开的大门。 1.修改默认的口令 据卡内基梅隆大学的CERT/CC（计算机应急反应小组/控制中心）称，80%的安全突破事件是由薄弱的口令引起的。网络上有大多数路由器的广泛的默认口令列表。你可以肯定在某些地方的某个人会知道你的生日。 SecurityStats.com网站维护一个详尽的可用/不可用口令列表，以及一个口令的可靠性测试。 2.关闭IP直接广播（IP Directed Broadcast） 你的服务器是很听话的。让它做什么它就做什么，而且不管是谁发出的指令。Smurf 攻击是一种拒绝服务攻击。在这种攻击中，攻击者使用假冒的源地址向你的网络广播地址发送一个“ ICMP echo ”请求。这要求所有的主机对这个广播请求做出回应。这种情况至少会降低你的网络性能。 参考你的路由器信息文件，了解如何关闭IP直接广播。例如，“ Central（config）#no ip source-route ”这个指令将关闭思科路由器的IP直接广播地址。 3.如果可能，关闭路由器的HTTP设置 正如思科的技术说明中简要说明的那样，HTTP使用的身份识别

协议相当于向整个网络发送一个未加密的口令。然而，遗憾的是，HTTP协议中没有一个用于验证口令或者一次性口令的有效规定。 虽然这种未加密的口令对于你从远程位置（例如家里）设置你的路由器也许是非常方便的，但是，你能够做到的事情其他人也照样可以做到。特别是如果你仍在使用默认的口令！如果你必须远程管理路由器，你一定要确保使用SNMPv3以上版本的协议，因为它支持更严格的口令。 4.封锁ICMP ping请求 ping的主要目的是识别目前正在使用的主机。因此，ping通常用于更大规模的协同性攻击之前的侦察活动。通过取消远程用户接收ping请求的应答能力，你就更容易避开那些无人注意的扫描活动或者防御那些寻找容易攻击的目标的“ 脚本小子 ”（script kiddies）。 请注意，这样做实际上并不能保护你的网络不受攻击，但是，这将使你不太可能成为一个攻击目标。 5.关闭IP源路由 IP协议允许一台主机指定数据包通过你的网络的路由，而不是允许网络组件确定最佳的路径。这个功能的合法的应用是用于诊断连接故障。但是，这种用途很少应用。这项功能最常用的用途是为了侦察目的对你的网络进行镜像，或者用于攻击者在你的专用网络中寻找一个后门。除非指定这项功能只能用于诊断故障，否则应该关闭这个功能。 6.确定你的数据包过滤的需求 封锁端口有两项理由。其中之一根据你对安全水平的要求对于你的网络是合适的。 对于高度安全的网络来说，特别是在存储或者保持秘密数据的时候，通常要求经过允许才可以过滤。在这种规定中，除了网路功能需要的之外，所有的端口和IP地址都必要要封锁。例如，用于web通信的端口80和用于SMTP的110/25端口允许来自指定地址的访问，而所有其它

端口和地址都可以关闭。 大多数网络将通过使用“ 按拒绝请求实施过滤 ”的方案享受可以接受的安全水平。当使用这种过滤政策时，可以封锁你的网络没有使用的端口和特洛伊木马或者侦查活动常用的端口来增强你的网络的安全性。例如，封锁139端口和445（TCP和 UDP）端口将使黑客更难对你的网络实施穷举攻击。封锁31337 （TCP和UDP）端口将使Back Orifice木马程序更难攻击你的网络。 这项工作应该在网络规划阶段确定，这时候安全水平的要求应该符合网络用户的需求。查看这些端口的列表，了解这些端口正常的用途。 7.建立准许进入和外出的地址过滤政策 在你的边界路由器上建立政策以便根据IP地址过滤进出网络的违反安全规定的行为。除了特殊的不同寻常的案例之外，所有试图从你的网络内部访问互联网的IP 地址都应该有一个分配给你的局域网的地址。例如，192.168.0.1这个地址也许通过这个路由器访问互联网是合法的。但是， 216.239.55.99这个地址很可能是欺骗性的，并且是一场攻击的一部分。 相反，来自互联网外部的通信的源地址应该不是你的内部网络的一部分。因此，应该封锁入网的192.168.X.X、172.16.X.X和10.X.X.X等地址。 最后，拥有源地址的通信或者保留的和无法路由的目标地址的所有的通信都应该允许通过这台路由器。这包括回送地址127.0.0.1或者E类（class E）地址段240.0.0.0-254.255.255.255. 8.保持路由器的物理安全 从网络嗅探的角度看，路由器比集线器更安全。这是因为路由器根据IP地址智能化地路由数据包，而集线器相所有的节点播出数据。如果连接到那台集线器的一个系统将其网络适配器置于混乱的模式，它们就能够接收和看到所有的广播，包括口令、POP3通信和Web通信。

然后，重要的是确保物理访问你的网络设备是安全的，以防止未经允许的笔记本电脑等嗅探设备放在你的本地子网中。
9.花时间审阅安全记录 审阅你的路由器记录（通过其内置的防火墙功能）是查出安全事件的最有效的方法，无论是查出正在实施的攻击还是未来攻击的征候都非常有效。利用出网的记录，你还能够查出试图建立外部连接的特洛伊木马程序和间谍软件程序。用心的安全管理员在病毒传播者作出反应之前能够查出“ 红色代码 ”和“ Nimda ”病毒的攻击。 此外，一般来说，路由器位于你的网络的边缘，并且允许你看到进出你的网络全部通信的状况。 编辑特别推荐: #0000ff>烽火网络交换机防雷解决方案 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