保护你的路由器远离字典攻击计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/643/2021_2022__E4_BF_9D_E6_8A_A4_E4_BD_A0_E7_c98_643999.htm 针对路由器的DoS字典攻击可以让攻击者取得Cisco路由器的访问权或者可能导致用户无法使用路由器。在本文中，你可以找到如何使用Cisco 网络操作系统的增强登陆功能来防止这种攻击。 你可能还没有认识到使用针对Telnet、SSH或者HTTP端口的字典式拒绝服务的（DoS）攻击可能成功的攻击你的Cisco路由器。事实上，我敢打赌，即便是大多数网络管理员没有全部打开这些端口，那么他至少也会打开其中一个端口用于路由器的管理。 当然，在公网中开放这些端口要比在私网中开放这些端口危险的多。但是，无论是对公网开放还是对私网开放这些端口，你都需要保护你的路由器防止它们受到字典DoS攻击，通过这种攻击，攻击者可能获得路由器的访问权或者在你的网络中创建一个简单的服务出口。 不过由于在网络操作系统 12.3(4)T以及以后的版本中都有了增强的登陆功能，因此你可以为你的路由器提供额外的保护。这些新的增强的登陆功能提供以下各个方面的优势： 在发现连续登陆尝试后，创建一个登陆延迟。 如果出现太多的登陆尝试失败的话，将不再允许登陆。 在系统日志中创建相应的登陆信息或者发送SNMP陷阱来警告和记录有关失败和不允许登陆的额外信息。 如何知道你的路由器中是否包含这些代码？最简单的查找方法是到"全局配置模式（Global Configuration Mode）并且输入"login（登陆）""，这个命令将返回一个选择列表，具体显示如下： block-for--用于设置安静模式活动时间周期。

delay--用于设置连续失败登陆的时间间隔。 on-failure--用于设置试图登陆失败后的选项。 on-sucess--用于设置试图登陆成功后的选项。 quiet-mode--用于设置安静模式的选项。 如果你的路由器中的网络操作系统中没有这个代码，它将返回一个"无法识别的命令"错误。 如果你的路由器中没有这个功能，那么使用Cisco 网络操作系统的特征导航来为你的路由器找到这个功能（参照Cisco 网络操作系统增强登陆功能）你还可以使用这个工具来查找你所需要的其他功能。记住，下载网络操作系统代码和访问特征导航工具需要Cisco的维护合同。用于配置这些功能的最基本的基表的命令是login block-for命令，这也是唯一的命令。一旦你激活了这个命令，其缺省的登陆延迟时间是一秒。在你指定的时间内，如果试图登陆的最大次数超过你所给定的次数的话，系统将拒绝所有的登陆尝试。 在全局配置模式下，执行下面的命令： login block-for （在多长时间内拒绝所有的登陆尝试） attempts （如果登陆的次数超过此数）within （在多少秒以内） 下面给出一个例子 login block-for 120 attempts 5 within 60 该命令对系统进行如下配置：如果在60秒以内有五次登陆失败的话，路由器系统将在120秒以内拒绝所有的登陆。如果此时你输入show login的话，你将接收到以下输出信息： 缺省情况下登陆延迟时间是一秒钟。 没有配置安静模式访问列表。 路由器激活了登陆攻击监控程序。 如果在60秒左右的时间内有五次登陆失败的话， 系统将禁用登陆操作120秒。 路由器目前处于正常模式。 目前的监控窗口还有54秒钟。 目前的登陆失败次数为0。 这些信息显示了你的设置，包括缺省的登陆延迟时间为一秒钟，以及其他的附加信息。它还告诉你目前路由器处于正常模

式，这意味着路由器目前还允许你登陆。 如果路由器认为有人对其进行攻击，它将进入安静模式，并且开始拒绝所有的登陆操作。你还可以配置一个ACL，在其中说明这个路由器对哪些主机和网络例外，无论是处于安静模式还是处于其他状态，都允许这些主机和网络登陆路由器。 下面是这些命令中用于配置系统的一些选项： 登陆延迟（数字）： 在失效登陆后增加延迟的秒数。你可以选择1到10之间的任何数字。 登陆失败和登陆成功：这些选项允许你选择在登陆成功或者失败时使用的日志和SNMP警告的类型。 登陆安静模式访问类（ACL数字）：增加ACL数字，使用这个选项可以增加一个隔绝列表，无论路由器处于安静模式还是处于正常模式，这个列表中的主机和网络都可以登陆路由器。 通常情况下，为了安全，我建议在所有的路由器上都激活login block-for选项。这些新功能将可以帮助你更好的保证路由器的安全。 如果你正好从事这方面的工作，并且你还没有做好准备的话，那么可以考虑只在路由器上使用SSH并且只允许从内网访问。SSH加密所有从PC到路由器的通信信息（包括用户名和密码）。 