使用Cisco命令阻止访问特定网站思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/641/2021_2022__E4_BD_BF_E7_94_A8Cisc_c101_641704.htm 步骤1：配置一个DNS服务器 假设我们打算屏蔽一个名为www.badsite.com的网站。我们并不知道该网站的具体IP地址，而且我们也不想知道。没问题Cisco IOS会自己 把地址找出来并填上它。 要做到这一点，我们需要至少在路由器上配置一台DNS服务器。若想配置一台DNS服务器，应使用ip name-server命令。下面是个例子： Router(config)# ip name-server 1.1.1.1 2.2.2.2 本例中，我们配置了一个主DNS服务器1.1.1.1，以及一个备用DNS服务器2.2.2.2，以便路由器对域名进行解析。这不会影响路由器的任何流量 。当我们需要对某个域名进行Ping服务时，路由器将使用这些DNS服务器。以下是具体示例： Router# ping www.techrepublic.com Translating "www.techrepublic.com"...domain server (1.1.1.1) [OK] Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 216.239.113.101, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms Router# 在上述例子中，路由器使用了我们指定的域名服务器地址（1.1.1.1）来尝试解析域名。它成功的将域名www.techrepublic.com解析为对应的IP 216.239.113.101。 如果我们不曾指定DNS服务器，那么路由器很可能会返回下述这些反馈： Translating "www.techrepublic.com"...domain server (255.255.255.255) % Unrecognized host or address, or protocol not running. （不认识的主机或地址，或可能协议未运行） 步骤2：建立ACL 想真

正阻止访问某个网站，我们必须建立一个存取控制列表（access control list，简称ACL）来具体定义我们想阻止什么。下面是个例子： Router(config)# access-list 101 deny tcp any host www.badsite.com eq www Translating "www.badsite.com"...domain server (1.1.1.1) [OK] Router(config)# access-list 101 permit tcp any any eq www ! to allow all other web traffic 这个ACL拒绝了所有对特定网站www.badsite.com的访问。在阻止访问该网站的同时，它允许所有人访问其他任意网站。 最后，由于ACL的隐含禁止，除WWW外所有的其他通信将全部被禁止。 如果您想知道到底是哪些IP地址在试图访问被阻止的网站，可以通过使用LOG关键字，记录相关信息。下面是个例子。 Router(config)# access-list 101 deny tcp any host www.badsite.com eq www log 步骤3：避免“ 遗漏 ”有一点需要注意。在我们输入了上述ACL的第一行之后，cisco认证网，加入收藏留意路由器是如何使用DNS服务器来解析域名的。然后它会用解析域名所得的IP地址替 换掉ACL中的主机名。我们来仔细看看配置： Router# sh run | inc access-list 101 access-list 101 deny tcp any host 66.116.109.62 eq www 这是个很好的功能，但是可能由于几个原因导致出现问题。首先，该IP仅仅是DNS服务器响应的第一个IP。如果这是个大型网站，有多台服务器（比如一个搜索引擎），而ACL却仅仅包含了DNS首先响应的第一个IP您将不得不手工屏蔽其余的IP地址。下面是个示例： C:\&gt. nslookup www.google.com Server: DNSSERVER Address: 1.1.1.1 Non-authoritative answer: Name: www.l.google.com Addresses: 64.233.167.104, 64.233.167.147, 64.233.167.99 Aliases: www.google.com 其次，如果被禁止的网页服务器更改了IP地

址，ACL中的地址并不会跟随变化。您必须对ACL进行人为更新。 步骤4：实施ACL 仅仅创建了ACL并不意味着路由器就用上了它我们还必须对ACL进行实施。下面，假设我们要建立一个ACL，以阻止内部局域网访问外部的广 域网（比如Internet）。因此我们应当用ACL的源地址过滤，而不是目标地址的过滤。 同样，基于设计的目的，我们需要在路由器的Out方向实施这个ACL。下面是示例。 Router(config)# int serial 0/0 Router(config-if)# ip access-group 101 out 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