

point out what to watch out for along the way.

Step 1: Configure a DNS server

Let's say we want to block access to the creatively named `www.badsite.com`. We don't know the IP address, and we don't want to know it. That's fine—the Cisco IOS can look it up for us and fill it in.

To do this, we need at least one DNS server configured on the router. To configure a DNS server, use the `ip name-server` command. Here's an example:

```
Router(config)# ip name-server 1.1.1.1 2.2.2.2
```

In this case, we configured a primary and a backup DNS server for the router to use to resolve DNS names. This doesn't affect any traffic flowing through the router; the router will use these DNS servers when we ping a Web server by name. Here's an example:

```
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#
```

In this example, the router used the domain name server we specified (i.e., 1.1.1.1) to resolve the DNS name. It successfully translated the DNS name to 216.239.113.101.

If we hadn't already specified a DNS server, then the router would have returned something like the following:

```
Translating "www.techrepublic.com"...domain server (255.255.255.255)
% Unrecognized host or address, or protocol not running.
```

Step 2: Create the ACL

To actually block the undesirable Web site, we need to create an access control list (ACL) to define exactly what we want to block. Here's an example:

```
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
```

This ACL denies all Web traffic from any source going to the specified Web site. After blocking that traffic, it will also allow all other Web traffic from any source to any destination. Finally, because of the implied deny, it will deny all other traffic.

What if you want to determine which IP addresses are trying to go to the blocked Web site? You can log this information using the *log* keyword. Here's an example:

```
Router(config)# access-list 101 deny tcp any host www.badsite.com eq  
www log
```

Step 3: Avoid this "gotcha"

Here's one issue to keep in mind. After we entered the first line of the ACL above, notice how the router used the DNS server to resolve the DNS name. It then replaced the IP address that the hostname resolved to in the ACL. Here's a closer look at the configuration:

```
Router# sh run | inc access-list 101  
access-list 101 deny tcp any host 66.116.109.62 eq www
```

This is a nice feature, but it can be problematic for a couple of reasons. First, the IP address entered is only the first IP address that the DNS server responded to. If this is a large Web site that has multiple servers (such as a search engine), the ACL only contains the first IP address that the DNS server responded with—you'll need to manually block the other IP addresses. Here's an example:

```
C:\> 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
```

In addition, if the IP address of the blocked Web server changes, your ACL will remain the same. You would need to manually update the ACL.

Step 4: Apply the ACL

Just because we've created the ACL doesn't mean the router is actually using it—we still have to apply the ACL. We created this ACL with the assumption that it's blocking traffic from our local LAN that's going out to the WAN (i.e., the Internet). That's because we formatted the ACL with source then destination.

Because of this design, we need to apply the ACL in the OUTBOUND direction on the router. Here's an example:

```
Router(config)# int serial 0/0  
Router(config-if)# ip access-group 101 out
```

Have you used the Cisco IOS to block a Web site before? What did your ACL look like? Do you have a good ACL to share? Post your comments in this article's discussion.