

# Cisco IOS Reflexive Access Lists

Greg Ferro

There are so many really cool features in IOS these days that you often don't even know they are there. You don't hear much about them and you don't see them used very often. That doesn't mean they aren't useful. In fact, some of them should be used every day.

In CCIE Corner, we'll look at some of the lesser-known capabilities of IOS and give practical case studies showing how to use them every day. We'll address configuring and debugging, so that you can really get down to business in your network.

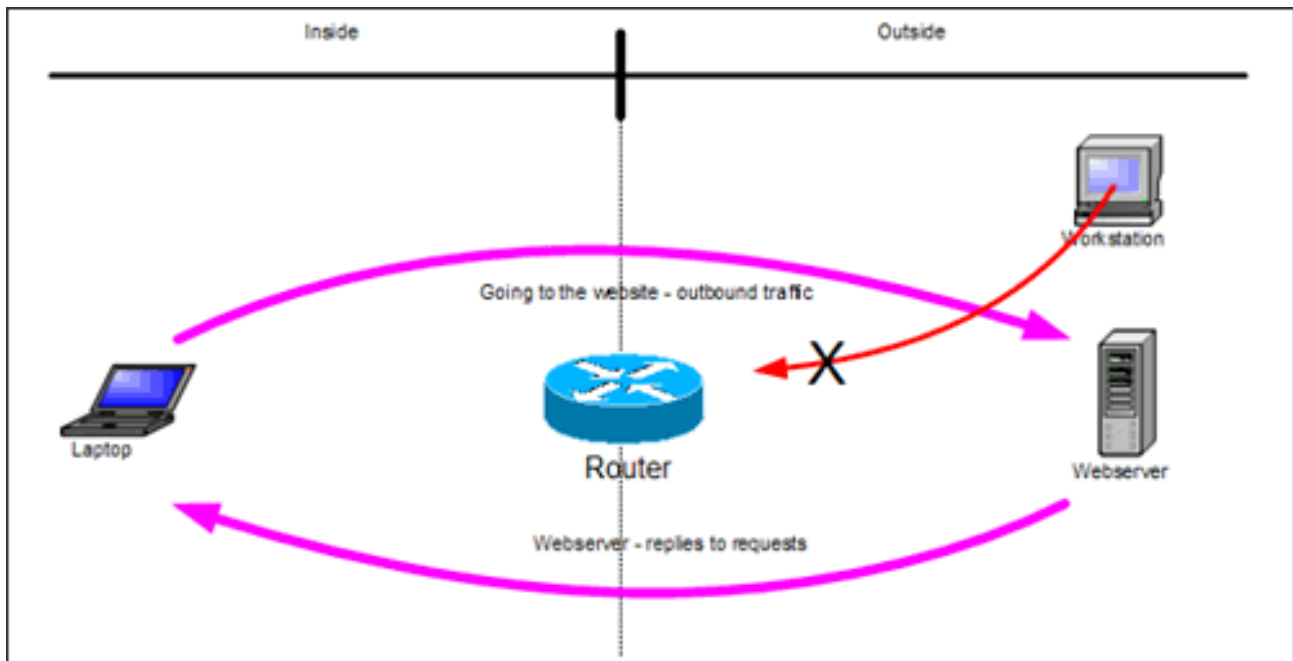
## What Are Reflexive Access Lists?

How many times have you said to yourself, "I want to allow everything out and nothing in"? You get out your trusty access lists and proceed to try and configure something that will do just that. It's not easy, and it's even harder to debug. And after your done, it's still not very secure.

This might be the time to consider using reflexive access lists, or session filtering. This is a special type of access list that allows traffic from the inside out to be allowed to return in a stateful and secure way. When Cisco first brought these lists out, they were called "reflexive access lists," but they have since been renamed "session filters." I like the term "reflexive" so that's what I'll use here.

You know all about normal access lists. (Hey, this is an advanced article! Check out the Router Expert articles by Michael Martin if you need to bring yourself up to date on access lists.) There are times, however, when regular access lists don't cut the mustard. Let's look at a practical example.

Consider accessing a Web server across your router, just like when you access the Internet, as shown in this diagram:



You can create an access list to allow traffic out to Web server, but you don't want the workstation out there to be able to come in. So you deny all traffic from the outside. An access list filter looks at each packet by comparing information in the IP header against the rules in your access list. So when a packet goes through your access list, it is allowed or denied. When you use simple access lists to block the workstation but allow the Web server, that creates a problem. You either allow no access

# Cisco IOS Reflexive Access Lists

Greg Ferro

from the Web server traffic to return (and thus break your Web access), or you allow too much access for the Web server. That creates a security problem because you allow all ports above 1024.

What you really want is to permit inbound traffic from the Web server in reaction to your outbound traffic flow. And guess what? That's what reflexive access lists do.

## Why Use Reflexive Access Lists?

To summarize, reflexive access lists are useful if:

- You need to block all access coming in to your network
- You want to allow access out of your network (and thus you must allow that traffic to return)
- You might want to allow any traffic out...
- Or only specific IP addresses or port numbers
- You want to allow certain types of traffic inbound
- You don't want a firewall solution, just access control.

## When To Use Reflexive Access Lists

I often use reflexive access lists when two companies wish to connect their networks, especially when the security profile is not high or there is some level of trust. They work well when you need to consider:

Cost savings -- reflexive access lists became available in the IOS 11.2 release and mainlined on 11.3, so most routers have the feature. You can probably use your existing router and save money.

Setup time -- you need to something fast (your firewall has just blown up and you need to do something to get the connection back up)

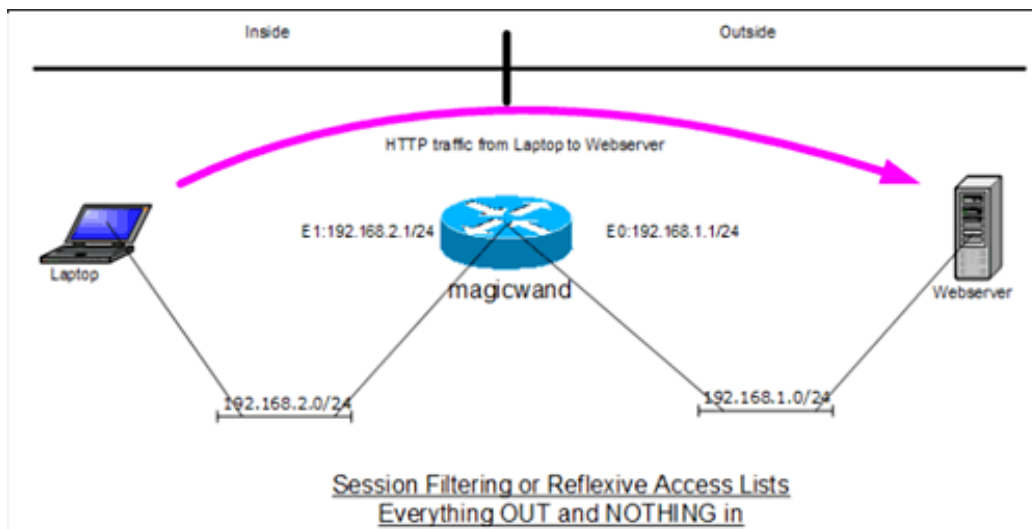
Interim -- you need something for a short time

Ease of implementation -- reflexive access lists are easy to create and easy to look after.

## Using Reflexive Access Lists To Allow Traffic Out But Not In

This is the simplest configuration. You want to allow everything that you initiate from the inside interface to be allowed to the Internet. But you don't want any traffic to be allowed in from the Internet.

The diagram below will help you orient yourself.



# Cisco IOS Reflexive Access Lists

Greg Ferro

The first thing to do is define our access lists:

```
magicwand#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

Create the access list for the inside interface for traffic flowing to the outside:

```
magicwand(config-ext-nacl)#ip access-list extended from-inside-to-outside
```

Allow all traffic out and create reflexive access list entry for traffic returning:

```
magicwand(config-ext-nacl)# permit ip any any reflect do-reflex
```

Create the access list for the outside interface for traffic destined for the inside:

```
magicwand(config)#ip access-list extended from-outside-to-inside
```

Check traffic against the reflexive access lists created by the "reflect" statement:

```
magicwand(config-ext-nacl)# evaluate do-reflex
```

Deny all traffic that doesn't match the reflexive access list:

```
magicwand(config-ext-nacl)# deny ip any any
```

```
magicwand(config-ext-nacl)# exit
```

And now, apply the access lists to their interfaces:

```
magicwand(config)# interface ethernet0
magicwand(config)# ip address 192.168.2.1 255.255.255.0
magicwand(config)# ip access-group from-outside-to-inside in
magicwand(config)# interface ethernet1
magicwand(config)# ip address 192.168.2.1 255.255.255.0
magicwand(config)# ip access-group from-inside-to-outside in
magicwand(config)# exit
magicwand#
```

You can also change some of the names to make it a little bit clearer:

```
magicwand(config-ext-nacl)#ip access-list extended from-workstation-to-
outside
magicwand(config-ext-nacl)# permit ip any any reflect create-reflex-lists
```

The first line defines an extended access list named "from-workstation-to-outside." The second line permits any IP traffic from any IP address to any IP address. The extra switch "reflect do-reflex" enables the inspection of outbound packets.

```
magicwand(config)#ip access-list extended coming-back-to-you
magicwand(config-ext-nacl)# evaluate create-reflex-lists
magicwand(config-ext-nacl)# deny ip any any
```

# Cisco IOS Reflexive Access Lists

Greg Ferro

Now we have defined the inbound access list and flicked the switch that turns on the reverse path for your IP traffic that went out with the "evaluate coming-back-to-you." Then we denied any traffic coming in from anywhere else.

## Show Commands Prior To Traffic Flow

Now let's go to the console of my "magicwand" and check out the new access lists:

```
magicwand#sh access-lists
Reflexive IP access list do-reflex
Extended IP access list from-inside-to-outside
    permit ip any any reflect do-reflex
Extended IP access list from-outside-to-inside
    evaluate do-reflex
    deny ip any any
magicwand#
```

## Show Commands After Traffic Flow

Now I check out a Web page on my Web server:

```
magicwand#sh access-lists
Reflexive IP access list do-reflex
Reflexive IP access list do-reflex
    permit tcp host 192.168.1.42 eq www host 192.168.2.2 eq 3767 (10
matches) (time left 809794)
    permit tcp host 192.168.1.42 eq www host 192.168.2.2 eq 3766 (10
matches) (time left 809794)
    permit tcp host 192.168.1.42 eq www host 192.168.2.2 eq 3765 (10
matches) (time left 809794)
Extended IP access list from-inside-to-outside
    permit ip any any reflect do-reflex
Extended IP access list from-outside-to-inside
    evaluate do-reflex
    deny ip any any
magicwand#
```

Now you can see that the reflexive access list has dynamically created an access list for traffic to come back through the outside interface. Let's look very carefully at this line:

```
permit tcp host 192.168.1.42 eq www host 192.168.2.2 eq 3669 (time left
812079)
```

This line will permit my Web server (192.168.1.42) return traffic from port 80 to my workstation (192.168.2.2) on port 3669. That is exactly what I want. It has been dynamically created and will expire at some time in the future (after the time left interval expires).

If we check the "show access lists" command a little bit later:

```
magicwand#sh access-list
Reflexive IP access list do-reflex
Extended IP access list from-inside-to-outside
    permit ip any any reflect do-reflex
    permit icmp any any
```

# Cisco IOS Reflexive Access Lists

Greg Ferro

```
Extended IP access list from-outside-to-inside
  evaluate do-reflex
  deny ip any any (78 matches)
magicwand#
```

You can see that the reflexive lists have been removed because they timed out. Now you are completely secured against traffic from the outside. Note that we have no DNS traffic here because I used `http://192.168.1.42` in my web browser. If you use a DNS name, you will also see a DNS server like the following:

```
Reflexive IP access list do-reflex
  permit tcp host 192.168.1.42 eq www host 192.168.2.2 eq 3767 (10
matches) (time left 809794)
  permit tcp host 192.168.1.42 eq www host 192.168.2.2 eq 3766 (10
matches) (time left 809794)
  permit tcp host 192.168.1.42 eq www host 192.168.2.2 eq 3765 (10
matches) (time left 809794)
  permit udp host 192.168.1.181 eq domain host 192.168.2.2 eq 1650 (2
matches) (time left 809794)
Extended IP access list from-inside-to-outside
  permit ip any any reflect do-reflex
  permit icmp any any
Extended IP access list from-outside-to-inside
  evaluate do-reflex
  deny ip any any
```