

Access Control Lists: Overview and Guidelines

Cisco provides basic traffic filtering capabilities with access control lists (also referred to as *access lists*). Access lists can be configured for all routed network protocols (IP, AppleTalk, and so on.) to filter those protocols' packets as the packets pass through a router.

You can configure access lists at your router to control access to a network: access lists can prevent certain traffic from entering or exiting a network.

In This Chapter

This chapter describes access lists as part of a security solution. This chapter includes tips, cautions, considerations, recommendations, and general guidelines for how to use access lists.

This chapter has these sections:

- About Access Control Lists
- Overview of Access List Configuration
- Find Complete Configuration and Command Information for Access Lists

About Access Control Lists

This section briefly describes what access lists do; why and when you should configure access lists; and basic vs. advanced access lists.

What Access Lists Do

Access lists filter network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces. Your router examines each packet to determine whether to forward or drop the packet, based on the criteria you specified within the access lists.

Access list criteria could be the source address of the traffic, the destination address of the traffic, the upper-layer protocol, or other information. Note that sophisticated users can sometimes successfully evade or fool basic access lists because no authentication is required.

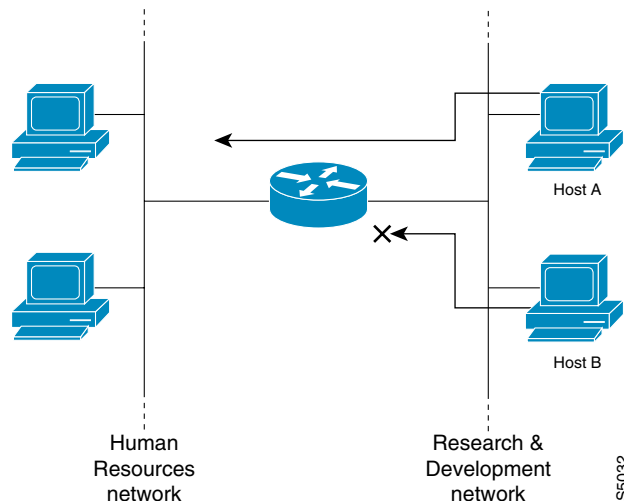
Why You Should Configure Access Lists

There are many reasons to configure access lists—for example, you can use access lists to restrict contents of routing updates, or to provide traffic flow control. But one of the most important reasons to configure access lists is to provide security for your network; this is the reason focused on in this chapter.

You should use access lists to provide a basic level of security for accessing your network. If you do not configure access lists on your router, all packets passing through the router could be allowed onto all parts of your network.

For example, access lists can allow one host to access a part of your network, and prevent another host from accessing the same area. In Figure 6, Host A is allowed to access the Human Resources network and Host B is prevented from accessing the Human Resources network.

Figure 6 Using Traffic Filters to Prevent Traffic from Being Routed to a Network



You can also use access lists to decide which types of traffic are forwarded or blocked at the router interfaces. For example, you can permit e-mail traffic to be routed, but at the same time block all Telnet traffic.

When to Configure Access Lists

Access lists should be used in “firewall” routers, which are often positioned between your internal network and an external network such as the Internet. You can also use access lists on a router positioned between two parts of your network, to control traffic entering or exiting a specific part of your internal network.

To provide the security benefits of access lists, you should at a minimum configure access lists on border routers—routers situated at the edges of your networks. This provides a basic buffer from the outside network, or from a less controlled area of your own network into a more sensitive area of your network.

On these routers, you should configure access lists for each network protocol configured on the router interfaces. You can configure access lists so that inbound traffic or outbound traffic or both are filtered on an interface.

Access lists must be defined on a per-protocol basis. In other words, you should define access lists for every protocol enabled on an interface if you want to control traffic flow for that protocol.

Note Some protocols refer to access lists as *filters*.

Basic Vs. Advanced Access Lists

This chapter describes how to use standard and static extended access lists, which are the basic types of access lists. Some type of basic access list should be used with each routed protocol that you have configured for router interfaces.

Besides the basic types of access lists described in this chapter, there are also more advanced access lists available, which provide additional security features and give you greater control over packet transmission. These advanced access lists and features are described in the other chapters within the “Traffic Filtering and Firewalls” section.

Overview of Access List Configuration

Although each protocol has its own set of specific tasks and rules required for you to provide traffic filtering, in general most protocols require at least two basic steps to be accomplished. The first step is to create an access list definition, and the second step is to apply the access list to an interface.

The two steps are described next in these sections:

- Creating Access Lists
- Applying Access Lists to Interfaces

Note that some protocols refer to access lists as *filters* and refer to the act of applying the access lists to interfaces as *filtering*.

Creating Access Lists

Create access lists for each protocol you wish to filter, per router interface. For some protocols, you create one access list to filter inbound traffic, and one access list to filter outbound traffic.

To create an access list, you specify the protocol to filter, you assign a unique name or number to the access list, and you define packet filtering criteria. A single access list can have multiple filtering criteria statements.

Cisco recommends that you create your access lists on a TFTP server, then download the access lists to your router. This can considerably simplify maintenance of your access lists. For details, see the section “Creating and Editing Access List Statements on a TFTP Server,” later in this chapter.

The protocols for which you can configure access lists are identified in Table 15 and Table 16 (following).

Assigning a Unique Name or Number to Each Access List

When configuring access lists on a router, you must identify each access list uniquely within a protocol, by assigning either a name or a number to the protocol’s access list.

Note Access lists of some protocols must be identified by a name, and access lists of other protocols must be identified by a number. Some protocols can be identified by either a name or a number. When a number is used to identify an access list, the number must be within the specific range of numbers that is valid for the protocol.

You can specify access lists by names for the protocols listed in Table 15.

Table 15 Protocols with Access Lists Specified by Names

Protocol
Apollo Domain
IP
IPX
ISO CLNS
NetBIOS IPX
Source-route bridging NetBIOS

You can specify access lists by numbers for the protocols listed in Table 16. Table 16 also lists the range of access list numbers that is valid for each protocol.

Table 16 Protocols with Access Lists Specified by Numbers

Protocol	Range
IP	1 to 99 and 1300 to 1999
Extended IP	100 to 199 and 2000 to 2699
Ethernet type code	200 to 299
Ethernet address	700 to 799
Transparent bridging (protocol type)	200 to 299
Transparent bridging (vendor code)	700 to 799
Extended transparent bridging	1100 to 1199
DECnet and extended DECnet	300 to 399
XNS	400 to 499
Extended XNS	500 to 599
AppleTalk	600 to 699
Source-route bridging (protocol type)	200 to 299
Source-route bridging (vendor code)	700 to 799
IPX	800 to 899
Extended IPX	900 to 999
IPX SAP	1000 to 1099
Standard VINES	1 to 100
Extended VINES	101 to 200
Simple VINES	201 to 300

Defining Criteria for Forwarding or Blocking Packets

When creating an access list, you define criteria which are applied to each packet that is processed by the router; the router decides whether to forward or block each packet based on whether or not the packet matches the criteria.

Typical criteria you define in access lists are packet source addresses, packet destination addresses, or upper-layer protocol of the packet. However, each protocol has its own specific set of criteria that can be defined.

For a single access list, you can define multiple criteria in multiple, separate access list statements. Each of these statements should reference the same identifying name or number, to tie the statements to the same access list. You can have as many criteria statements as you want, limited only by the available memory. Of course, the more statements you have, the more difficult it will be to comprehend and manage your access lists.

The Implied “Deny All Traffic” Criteria Statement

At the end of every access list is an implied “deny all traffic” criteria statement. Therefore, if a packet does not match any of your criteria statements, the packet will be blocked.

Note For most protocols, if you define an inbound access list for traffic filtering, you should include explicit access list criteria statements to permit routing updates. If you do not, you might effectively lose communication from the interface when routing updates are blocked by the implicit “deny all traffic” statement at the end of the access list.

The Order In Which You Enter Criteria Statements

Note that each additional criteria statement that you enter is appended to the *end* of the access list statements. Also note that you cannot delete individual statements after they have been created. You can only delete an entire access list.

The order of access list statements is important! When the router is deciding whether to forward or block a packet, the Cisco IOS software tests the packet against each criteria statement in the order the statements were created. After a match is found, no more criteria statements are checked.

If you create a criteria statement that explicitly permits all traffic, no statements added later will ever be checked. If you need additional statements, you must delete the access list and retype it with the new entries.

Creating and Editing Access List Statements on a TFTP Server

Because the order of access list criteria statements is important, and because you cannot reorder or delete criteria statements on your router, Cisco recommends that you create all access list statements on a TFTP server, and then download the entire access list to your router.

To use a TFTP server, create the access list statements using any text editor, and save the access list in ASCII format to a TFTP server that is accessible by your router. Then, from your router, use the **copy tftp:file_id system:running-config** command to copy the access list to your router. Finally, perform the **copy system:running-config nvram:startup-config** command to save the access list to your router’s NVRAM.

Then, if you ever want to make changes to an access list, you can make them to the text file on the TFTP server, and copy the edited file to your router as before.

Note The first command of an edited access list file should delete the previous access list (for example, type a **no access-list** command at the beginning of the file). If you do not first delete the previous version of the access list, when you copy the edited file to your router you will merely be appending additional criteria statements to the end of the existing access list.

Applying Access Lists to Interfaces

For some protocols, you can apply up to two access lists to an interface: one inbound access list and one outbound access list. With other protocols, you apply only one access list which checks both inbound and outbound packets.

If the access list is inbound, when the router receives a packet, the Cisco IOS software checks the access list's criteria statements for a match. If the packet is permitted, the software continues to process the packet. If the packet is denied, the software discards the packet.

If the access list is outbound, after receiving and routing a packet to the outbound interface, the software checks the access list's criteria statements for a match. If the packet is permitted, the software transmits the packet. If the packet is denied, the software discards the packet.

Note Access lists that are applied to interfaces do not filter traffic that originates from that router.

Find Complete Configuration and Command Information for Access Lists

The guidelines discussed in this chapter apply in general to all protocols. The specific instructions for creating access lists and applying them to interfaces vary from protocol to protocol, and this specific information is not included in this chapter.

To find complete configuration and command information to configure access lists for a specific protocol, see the appropriate protocol's chapters in the Cisco IOS configuration guides and command references. For example, to configure access lists for the IP protocol, refer to the "Configuring IP Services" chapter in the *Network Protocols Configuration Guide, Part 1*.

For more information on dynamic access lists, see the chapter "Configuring Lock-and-Key Security (Dynamic Access Lists)" in this guide.

For more information on reflexive access lists, see the chapter "Configuring IP Session Filtering (Reflexive Access Lists)" in this guide.