Easy Steps to Cisco Extended Access List

The purpose of this document is to explain in simple words how you can easily create an Extended Access List and apply it to your Cisco Router interface. This document is intended for the novice network security personnel who has a basic understanding of networking essentials.

Easy Steps to Cisco Extended Access List
Nancy Navato
GSEC Practical Assignment Version 1.2e

Introduction

The purpose of this document is to explain in simple words how you can easily create an Extended Access List and apply it to your Cisco Router interface. This document is intended for the novice network security personnel who has a basic understanding of networking essentials. For example, you were recently assigned to the network security section and tasked to protect your network by creating an Extended Access-lists to block ports and suspicious Internet Protocol addresses on your router. To begin, you would need answers to the following questions:

- What is an Extended Access List?
- What do you include in your Access List?
- Where do you place the IP Access List?
- How do you apply the Access List to the Cisco Router?

Please note that the extended access-list on your router has limitations, and is one defense layer of the many layers of your Defense in Depth practice of network security. In one of the Sans Security Essentials Chapters, I like the idea of comparing the protection of data to the king within a castle protected by high walls, a massive moat, and many armed guards. Your network security should be the same way, such that if one layer is breached, your attacker still needs to overcome all this other defense layers.

What is an Extended Access List?

An extended access-list is an ordered list of statements that can deny or permit packets based on source and destination IP address, port numbers and upper-layer protocols. Standard access list can deny or permit packets by source address only and permit or deny entire TCP/IP protocol suite. Therefore by extended, it means greater functionality and flexibility. Extended access list is a good example of “packet filtering” where the flow of data packets can be controlled in your network. It can filter based on source and destination, specific IP protocol and port number.

What do you include in your access list?

A good way to start is to gather the IP addresses for your network as well as the port numbers required by your applications. Your security policy would define what services to permit into and out of your network. Once you have a good understanding of what applications you must permit, the next factor would be what router interface you are going to apply the access list and which direction either inbound or outbound.

Note that an access list is an ordered list and therefore the sequence of your statements is crucial. Also, at the end of the list is an implicit deny of everything that is not permitted. The best security practice is to only allow packets that are explicitly permitted and deny everything else. The access list can always be modified to include needed services.

The extended access list syntax is described below.
Access-list <**number 100-199**> <**permit | deny**> <*protocol*> <**source**> < **source-mask**> <*operator source port*> < *destination*> <*destination-mask*> < *operator destination port*> <*options*> < *log*>

To understand better, I am going to break down the entries into fields:

Access-list is the command use.

access list number Extended IP Access List uses a number in the range of 100 to 199. This is a required field.

permit or **deny** Allow or block traffic. This is a required field.

protocol IP, TCP, UDP, ICMP, GRE and IGRP. TCP, UDP and ICMP use IP at the network layer.

Source This is the Source IP address. This is a required field.

source mask Wildcard mask; 0 indicate positions that must match, 1s indicate don't care positions (inverted mask). This is a required field.

.

operator source port lt, gt, eq, neq (less than, greater than, equal, not equal) and a port number.

destination Destination IP address.

destination mask Wildcard mask; 0 indicate positions that must match, 1s indicate don't care positions (inverted mask)

operator destination port lt, gt, eq, neq (less than, greater than, equal, not equal) and a port number

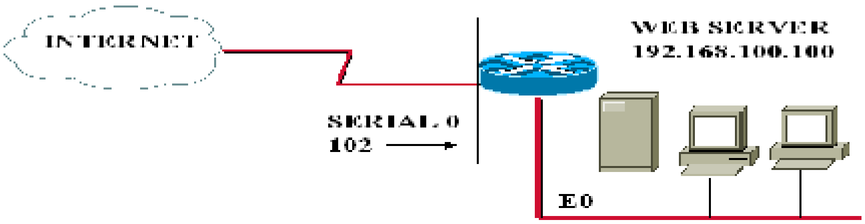
options Typical is "established" to see if ACK or RST bits is set.

Log log to the router's buffer or a syslog server

Where do you place the Extended Access-List?

Scenario 1: Your goal is to filter incoming traffic so that users outside your network can access the public web server using port 80. All other incoming traffic is denied. For this example, the Legal IP Address space for your network is 192.168.100.0 and we will use Access List number102 for inbound traffic. Apply Access List close to the source of traffic to be denied to prevent packets from traveling to other routers only to be denied.

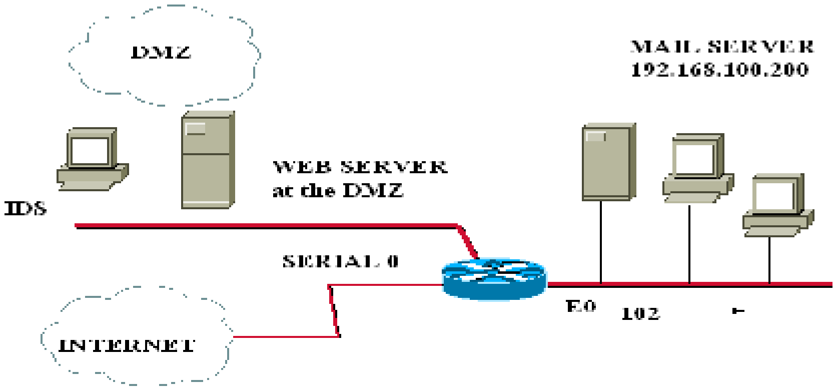
Figure 1



APPLY INBOUND ACCESS LIST TO SERIAL 0. IT IS RECOMMENDED THAT EXTENDED ACCESS LIST ARE PLACED AS CLOSE AS POSSIBLE TO THE SOURCE OF THE TRAFFIC TO BE DENIED

access-list 102 permit tcp any 192.168.100.100 0.0.0.0 eq 80
[implicit deny ip any any]

Figure 2



Scenario 2: Your goal is to filter incoming traffic so that users outside your network can access the public web server in the DMZ. No other services are allowed except access to your E-Mail server with a Legal IP Address space of 192.168.100.200. We are using Access List number102 for inbound traffic.

```
access-list 102 permit tcp any 192.168.100.200 0.0.0.0 eq 25
[implicit deny ip any any]
```

In this scenario, the inbound access-list needs to be placed on **E0** so that internet users can access the public web server at the DMZ.

How do you apply the access list to the Cisco Router?

You can create your access list and download your access list to a TFTP server using a text editor or you can create a regular text and use your computer to cut and paste the access list into the router.

You can use the console or telnet to one of the interfaces in your router.

Example 1: Applying access list 102 (Inbound) to Serial 0:

```
Router>enable                                {activates privileged mode}
Router# Config term                          {enter global configuration mode}
Router(config)# interface serial 0
Router(config-if)# ip access-group 102 in    {In for Inbound, Out for Outbound}
Router(config-if)#exit
(Config)#exit
```

Example 2: Applying access list 101 (Outbound) to Ethernet 0:

```
Router# Config term
Router(config)# interface Ethernet 0
Router(config-if)# ip access-group 101 out
Router(config-if)#exit
(Config)#exit
```

Example 3: To remove access list from Serial 0

```
Router> Config term
Router(config)# interface Serial 0
Router(config-if)#no ip access-group 101 out
Router(config-if)#exit
(Config)#exit
```

Some helpful commands to monitor and verify the access list.

```
Show running-config                {displays active configuration and presence of
                                   access group}
```

```
show access-list                          {displays all access-list}
show access-list 1xx                      {displays access list 1xx only}
show ip access-list                       {displays IP access-list}
show interface serial 0                   {displays info on serial 0 interface)
no access-list 1xx                        {remove access-list 1xx only}
copy running-config start-up config       {save the active configuration to NVRAM}
```

Access List Guidelines:

1. Access List numbers indicate which protocol is filtered. Extended IP is from 100-199
2. Only one access list per protocol, per direction, per interface is allowed.
3. Top-down processing. Most restrictive statements should be at the top.
4. At the end of the access list is an implicit deny all. Due to the implicit deny, there should be at least one permit statement on every access list.
5. New Entries are added to the bottom. Any new access list are added to the bottom of the list. If modifications are necessary, delete access list and recreate the entire access list off-line such as with text editor and upload any changes from TFTP server or Cut and Paste from a computer.
6. Create access list before applying it to the interface.
7. Access lists only filter traffic going through the router. It does not apply to traffic originated from the router.

Protecting your Network with Extended Access List

1. **Anti-Spoofing and Filtering:**

1.1 **Egress Filtering.** To prevent your network from being used in spoofed Denial of Service (DOS), apply Egress Filtering at enclave (base, post, camp, station) borders. Allow only valid IP address to exit your network. The access list needs to be placed outbound on the Interface connecting to the Internet.

```
access-list 1xx permit ip <Network-Base-Address> <Hostmask> any
access-list 1xx deny ip any any log                        {log spoofing attempts}
```

1.2 **Ingress Filtering.** Accept incoming traffic only if it comes from authorized sources. Configure Remote Access Servers to allow only valid source IP addresses. Ensure that filters are in place to prevent spoofing of dial-up connections.

1.3 Filter incoming traffic from **private addresses**. Apply inbound access list at the enclave level.

```
access-list 1xx deny ip 0.0.0.0      0.255.255.255       any    {historical broadcast}
access-list 1xx deny ip 10.0.0.0     0.255.255.255       any    {private network}
access-list 1xx deny ip 127.0.0.0    0.255.255.255       any    {loopback}
access-list 1xx deny ip 169.254.0.0          0.0.255.255 any    {link local networks}
access-list 1xx deny ip 172.16.0.0           15.0.255.255 any   {private networks}
```

```
access-list 1xx deny ip 192.0.2.0          0.0.0.255      any     {link local networks}
access-list 1xx deny ip 192.168.0.0        0.0.255.255    any     {private networks}
access-list 1xx deny ip 224.0.0.0          15.255.255.255     any      {class D multicast}
access-list 1xx deny ip 240.0.0.0          7.255.255.255      any      {class E multicast}
access-list 1xx deny ip 248.0.0.0          7.255.255.255      any      {unallocated}
access-list 1xx deny ip 255.255.255.255 0.0.0.0           any     {broadcast}
```

2. **Block well-known Distributed Denial Of Service (DDOS) ports:**

2.1 Serbian badman/backdoor.subseven21 (6669/tcp, 2222/tcp, 7000/tcp)
2.2 Subseven (16959/tcp, 27374/tcp, 6711/tcp, 6712/tcp, 6776/tcp)
2.3 Stacheldrant (16660/tcp, 65000/tcp)
2.4 Trinoo communication ports (27665/tcp, 31335/udp and 27444/udp)
2.5 Trinity v 3 (33270/tcp, 39168/tcp)

Example of inbound access list:

```
access-list 1xx deny tcp any any eq 16959
access-list 1xx deny udp any any eq 27444
```

3. **Block well-knows ICMP exploits:**

3.1 Block incoming ICMP echo request (ICMP type 8). This will prevent ping attacks which can crash some systems. It will also prevent outsiders from mapping systems inside your network. Apply this filter on the external router interface to the internet.

```
access-list 1xx deny icmp any any echo-request
```

3.2 Block outgoing ICMP echo-replies (ICMP type 0). Echo Reply is used by ping. Prevent echo-reply traffic to anyone, especially in response to malicious programs that uses ICMP echo-replies. Apply this filter outbound.

```
access-list 1xx deny icmp any any echo-reply
```

3.3 Block outgoing ICMP time-exceeded (ICMP type 11). Prevent outsiders from mapping your network.

```
access-list 1xx deny icmp any any time exceeded
```

3.3 Block outgoing ICMP destination unreachable messages (ICMP type 3 except "packet too big" messages type 3, code 4). Prevent outsiders from finding out which are valid IP addresses in your network. Since "packet-too-big" is also ICMP type 3, permitting "packet-too-big" before denying host unreachable will allow the router to send information to the host that the packets are too large.

```
access-list 1xx permit icmp any any packet-too-big
access-list 1xx deny icmp any any host-unreachable
```

4.0 Let your **security policy** be your guide. If chat is not allowed, block some of the known chat ports at the network enclave level. Such as: IRC ports 6660 – 6669/tcp, ICQ ports 1027/tcp, 1029/tcp, 1032/tcp, AIM, 5190/tcp.

```
access-list 1xx deny tcp any any eq 6660
access-list 1xx deny tcp any any eq 1027
access-list 1xx deny tcp any any eq 5190
```

4.1 If there is no need for echo (7 tcp/udp) and chargen (19 tcp/udp) services, deny these ports on the access-list.

Limitations of Extended Access List:

1. Extended access-list examines each packet as a stand-alone entity and cannot determine if the packet is part of an existing conversation through the use of the established keyword. Established is only useful for TCP and not UDP.
2. Extended access list has limited capability of examining information in the layer 4 headers.
3. Human Errors when creating access list can lead to security holes.
   3.1 Failure to create and add access list entries in the correct sequence.
   3.2 Failure to apply the access list to an interface in the correct direction.
   3.3 Failure to apply the access list to an interface.

Summary.

In this document, we learned about how we can protect our networks using an extended access list. When creating and applying access list always consider the potential effects before implementing it. Monitor the CPU and Memory usage of the router before and after applying the access list. After applying the access list on the router, recommend reviewing the access list you just applied by doing a "show access-list". Before denying a recommended port block, monitor the port in your Intrusion Detection System at the DMZ to ensure that the port is not use by legitimate services. Permitting only allowed services and denying all others will be better practice for network security. Recommend frequently visiting security websites, such as the Carnegie Mellon Software Engineering Institute (CERT) at www.cert.org and most notably the System Administration, Networking and Security Institute (SANS) at http://www.sans.org which has a plethora of valuable and much needed information on how to secure your network.

Routers can be an effective means to filter traffic when used in a layered approach with other network security devices such as the firewall, anti-virus protection, network based and host based intrusion detection system. As always, Defense in Depth is the best approach to network security.

References:

"How To Eliminate The Ten Most Critical Internet Security Threats, The Experts' Consensus." Version 1.33. 25 June 2001. URL: http://www.sans.org/topten.htm (29 Jun 2001).

"Increased SubSeven Activity." 26 Jun 2001. URL: http://www.cert.org/current/current_activity.html#SubSeven (29 Jun 01)

"Advisory 01-014 New Scanning Activity (with W32-Leaves.worm) Exploiting SubSeven Victims." 23 Jun 2001. URL:http://www.nipc.gov/warnings/advisories/2001/01-014.htm (29 Jun 01)

"Consensus Roadmap for Defeating Distributed Denial of Service Attacks." A Project of the Partnership for Critical Infrastructure Security. Version 1.10. 23 Feb 2000. URL: http://www.sans.org/ddos_roadmap.htm (24 Jun 2001).

Winters, Scott. "Top Ten Blocking Recommendations Using Cisco ACLs. Securing the Perimeter with CISCO IOS 12 Routers." 15 AUG 2000. URL: http://www.sans.org/infosecFAQ/firewall/blocking_cisco.htm (25 Jun 2001)

Benton, Chris. "Poor Man's NT Auditing. Verifying That Your Systems Remain Secure With Cheap Tools." SANS Security Essentials Online Course. 9 Feb 2001. 5-51

Held, Gil and Hundley, Kent. Cisco Security Architecture. McGraw-Hill, 1999. 119 – 171

Interconnecting Cisco Devices, Revision 1.0a: Student Guide. CISCO Systems, 2000. 4-73, 10-3 – 10-36

Lindsay, Paul. "Cisco Reflexive Access Lists." 10 MAY 2001. URL: http://www.sans.org/infosecFAQ/firewall/reflex.htm (25 Jun 2001)

Benton, Chris. "Setting router filters to prevent spoofing examples for Cisco Routers and Check Point FW-1." SANS Flash Advisory Supplement. 1999-2000. URL: http://www.sans.org/newlook/resources/router_filters.htm (25 Jun 2001)

"Cisco Anti-Spoof Egress Filtering." Revision 1.26. 23 Mar 2000. URL: http://www.sans.org/dosstep/cisco_spoof.htm (25 Jun 2001)

Benton, Chris. "What is Egress Filtering and How can I Implement It?" Egress Filtering v 0.2. 29 Feb 2000. URL:http://www.sans.org/infosecFAQ/firewall/egress.htm (25 Jun 2001)

Last Updated: December 16th, 2018

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Sonoma 2019	**Santa Rosa, CAUS**	**Jan 14, 2019 - Jan 19, 2019**	**Live Event**
SANS Threat Hunting London 2019	**London, GB**	**Jan 14, 2019 - Jan 19, 2019**	**Live Event**
SANS Amsterdam January 2019	**Amsterdam, NL**	**Jan 14, 2019 - Jan 19, 2019**	**Live Event**
SANS Miami 2019	**Miami, FLUS**	**Jan 21, 2019 - Jan 26, 2019**	**Live Event**
Cyber Threat Intelligence Summit & Training 2019	**Arlington, VAUS**	**Jan 21, 2019 - Jan 28, 2019**	**Live Event**
SANS Dubai January 2019	**Dubai, AE**	**Jan 26, 2019 - Jan 31, 2019**	**Live Event**
SANS Las Vegas 2019	**Las Vegas, NVUS**	**Jan 28, 2019 - Feb 02, 2019**	**Live Event**
SANS Security East 2019	**New Orleans, LAUS**	**Feb 02, 2019 - Feb 09, 2019**	**Live Event**
SANS SEC504 Stuttgart 2019 (In English)	**Stuttgart, DE**	**Feb 04, 2019 - Feb 09, 2019**	**Live Event**
SANS Anaheim 2019	**Anaheim, CAUS**	**Feb 11, 2019 - Feb 16, 2019**	**Live Event**
SANS Northern VA Spring- Tysons 2019	**Vienna, VAUS**	**Feb 11, 2019 - Feb 16, 2019**	**Live Event**
SANS London February 2019	**London, GB**	**Feb 11, 2019 - Feb 16, 2019**	**Live Event**
SANS Zurich February 2019	**Zurich, CH**	**Feb 18, 2019 - Feb 23, 2019**	**Live Event**
SANS Secure Japan 2019	**Tokyo, JP**	**Feb 18, 2019 - Mar 02, 2019**	**Live Event**
SANS Scottsdale 2019	**Scottsdale, AZUS**	**Feb 18, 2019 - Feb 23, 2019**	**Live Event**
SANS New York Metro Winter 2019	**Jersey City, NJUS**	**Feb 18, 2019 - Feb 23, 2019**	**Live Event**
SANS Dallas 2019	**Dallas, TXUS**	**Feb 18, 2019 - Feb 23, 2019**	**Live Event**
SANS Riyadh February 2019	**Riyadh, SA**	**Feb 23, 2019 - Feb 28, 2019**	**Live Event**
SANS Brussels February 2019	**Brussels, BE**	**Feb 25, 2019 - Mar 02, 2019**	**Live Event**
SANS Reno Tahoe 2019	**Reno, NVUS**	**Feb 25, 2019 - Mar 02, 2019**	**Live Event**
Open-Source Intelligence Summit & Training 2019	**Alexandria, VAUS**	**Feb 25, 2019 - Mar 03, 2019**	**Live Event**
SANS Baltimore Spring 2019	**Baltimore, MDUS**	**Mar 02, 2019 - Mar 09, 2019**	**Live Event**
SANS Training at RSA Conference 2019	**San Francisco, CAUS**	**Mar 03, 2019 - Mar 04, 2019**	**Live Event**
SANS Secure India 2019	**Bangalore, IN**	**Mar 04, 2019 - Mar 09, 2019**	**Live Event**
SANS St. Louis 2019	**St. Louis, MOUS**	**Mar 11, 2019 - Mar 16, 2019**	**Live Event**
SANS London March 2019	**London, GB**	**Mar 11, 2019 - Mar 16, 2019**	**Live Event**
SANS Secure Singapore 2019	**Singapore, SG**	**Mar 11, 2019 - Mar 23, 2019**	**Live Event**
SANS San Francisco Spring 2019	**San Francisco, CAUS**	**Mar 11, 2019 - Mar 16, 2019**	**Live Event**
SANS Bangalore January 2019	**OnlineIN**	**Jan 07, 2019 - Jan 19, 2019**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**