An extended access control list (ACL) can determine what traffic is allowed or denied access, acting as a gatekeeper for your network. It can give the system administrator setting up the network a higher degree of flexibility and control. It is highly customizable, allowing you to set rules regarding traffic on more than just the IP address. This can help to prevent network attacks while allowing the traffic you want to have access through. An extended ACL can be set up to block particular sources from having access via certain ports on targeted computers. In this way, you can manage traffic going out and coming in to a very specific degree.

What is an extended access list (ACL)?

An access control list is a set of rules allowing or blocking traffic within a network, providing basic security. An extended access list is more flexible and customizable than a standard access control list. An ACL can tell a computer operating system what users have access rights to specific system objects, such as individual files or directories. An extended ACL can serve as an extension of a standard ACL with more specific parameters. This can increase network security while prioritizing the flow of traffic within a network. Network security needs to constantly evolve as the world changes and threats evolve. It is even more important to restrict access to potential bad actors while still allowing necessary traffic through uninhibited for a smooth customer and employee interface and digital interaction.

Features of an extended ACL

A standard ACL allows or denies traffic access based on the source IP address, while an extended access control list can filter packets with a higher degree of specification. It can determine the types of traffic it allows or blocks beyond just the IP address to include TCP, ICMP, and UDP, for example. An extended ACL can filter traffic based on the following:

Source address

Destination address

Port number

Protocol

Time range

Types of Access Control Lists

Access control lists can be approached in relation to two main categories:

Standard ACL

An access-list that is developed for only using the source IP address.

These access control lists allow or block the entire protocol suite.

They don’t differentiate between IP traffics

Extended ACL

An access-list that is widely used as it can differentiate IP traffic.

It uses both source and destination IP addresses and port numbers to make more sense of IP traffic.

You can also specify which IP traffic should be allowed or denied.

They use the numbers to do so

Standard ACl

Step 1: Arranging devices and creating connections and assign IP address as shown below

creating access-list in router2 CLI as shown below

exit

hostname R0

ip route 192.168.2.0 255.255.255.0 192.168.3.2

access-list 1 deny 192.168.2.101 0.0.0.0

access-list 1 permit any

int fa0/1

ip access-group 1 out

then ping 192.168.2.100 from the PC 0

ExtendedACL

Create the layout

Configuring rip protocol

Setting the access list in Router0 > CLI

Enable

Conf t

access-list 100 deny icmp host 192.168.1.2 host 192.168.19.1

access-list 100 permit ip any any

int se0/1/0

ip access-group 100 out

open browser <http://192.168.19.2> from PC0

from PC1

ftp 192.168.19.2

ping 192.168.19.2

from pc2

ping 192.168.19.2