Access Control Lists

22nd May 2017

IT Center, University of Peradeniya

Dilum Samarasinhe
(LEARN)

Overview

- Introduction
- Benefits of ACLs
- How ACLs work
- Standard ACL and Extended ACL
- Wildcard mask
- Example

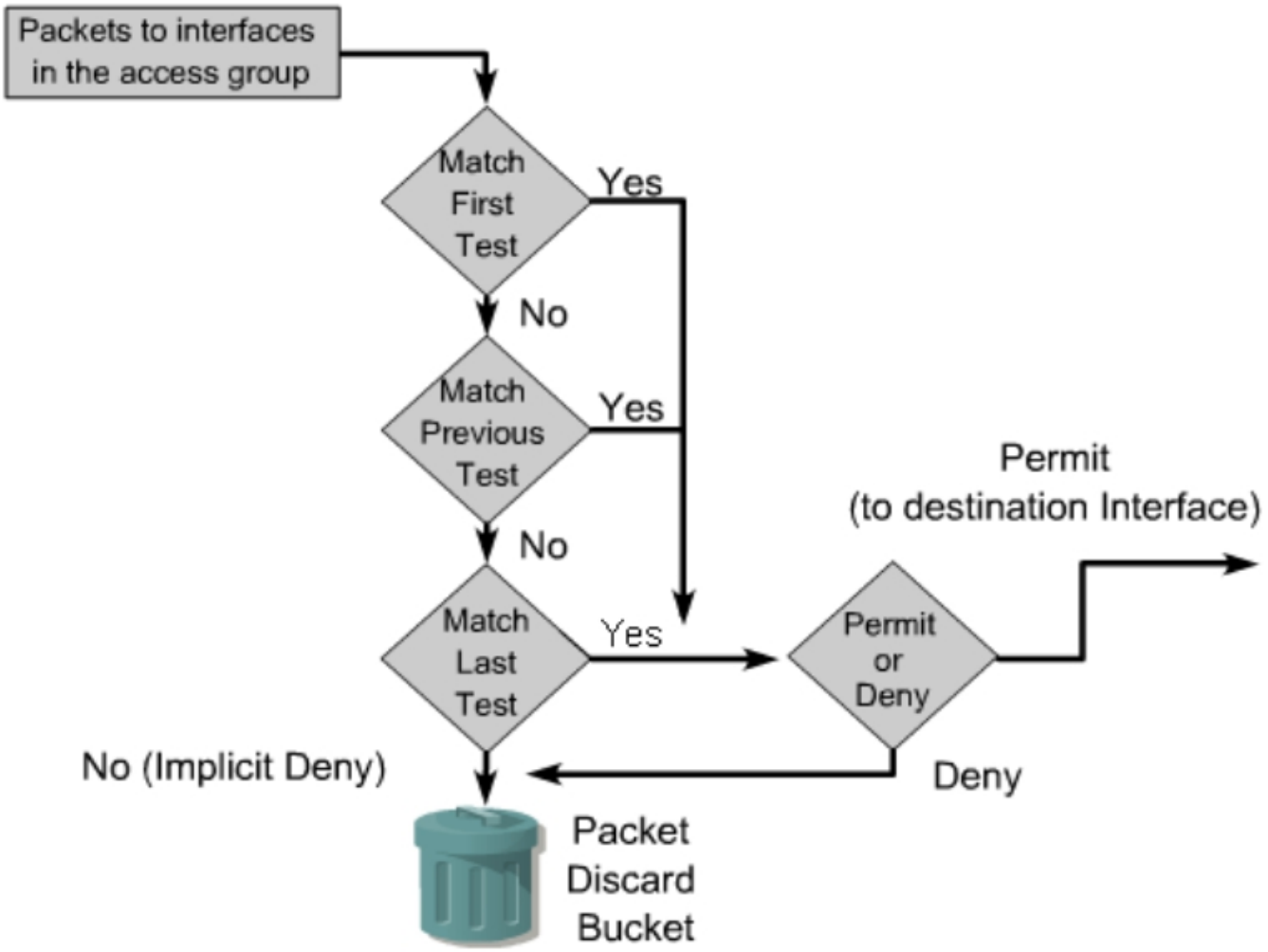
Introduction

- Access control list (ACL) consist of a table that tells a computer Operation System (OS) which access rights each user has to a particular system object, such as a file directory or individual file.
- Each object has a security attribute that identifies its access control list

Benefits of ACLs

- Limit network traffic and increase network performance.
- Provide traffic flow control.
- Provide a basic level of security for network access.
- Traffic decision (forwarded or blocked at the router interfaces).
- Area accessing
- Permit or deny Screen hosts to access a network segment

How ACLs Works



Standard ACLs & Extended ACLs

- Standard ACLs
  - Use only the packet's source address for comparison
  - Identification number range is 1-99
  - Use only source address and requires fewer CPU cycles
  - Place as close to destination as possible
- Extended ACLs
  - Provide more precise (finer tuned) packet selection based on Source and destination addresses, Protocols or Port numbers
  - Identification number range is 100-199
  - More flexible and requires more CPU cycles
  - Place as close to source as possible

Wildcard Mask

- Wildcard masking for access lists operates differently from an IP subnet mask.
- A zero in a bit position of the access list mask indicates that the corresponding bit in the address must be checked;
- A one in a bit position of the access list mask indicates the corresponding bit in the address is not “interesting” and can be ignored
- In the example below, only the 1st 2 octets will be examined:

172.16.0.0 0.0.255.255

Examples for Standard ACL

- To permit all packets for the network number 172.16.0.0

  Access-list 20 permit 172.16.0.0 0.0.255.255

- To permit traffic from the host 172.16.1.1 only

  Access-list 20 permit 172.16.1.1 0.0.0.0

- To permit traffic from any source address

  Access-list 20 permit any

- To permit traffic from the subnet 12.16.0.0 through 12.31.0.0

  Access-list 20 permit 12.16.0.0 0.15.255.255

Examples for Extended ACL

- To permit UDP traffic from 10.1.1.2 host machine to 172.16.1.1 host machine

  Access-list 101 permit udp host 10.1.1.2 host 172.16.1.1

- To deny icmp traffic from any to any network

  Access-list 101 deny ip any any

- To permit Telnet traffic from machine 10.1.1.2 to network 172.16.1.0/24

  access-list 101 permit tcp host 10.1.1.2 172.16.1.0 0.0.0.255 eq telnet

Thank You

Dilum Samarasinghe/LEARN

Email: dilum@learn.ac.lk