Computer Security

Labs

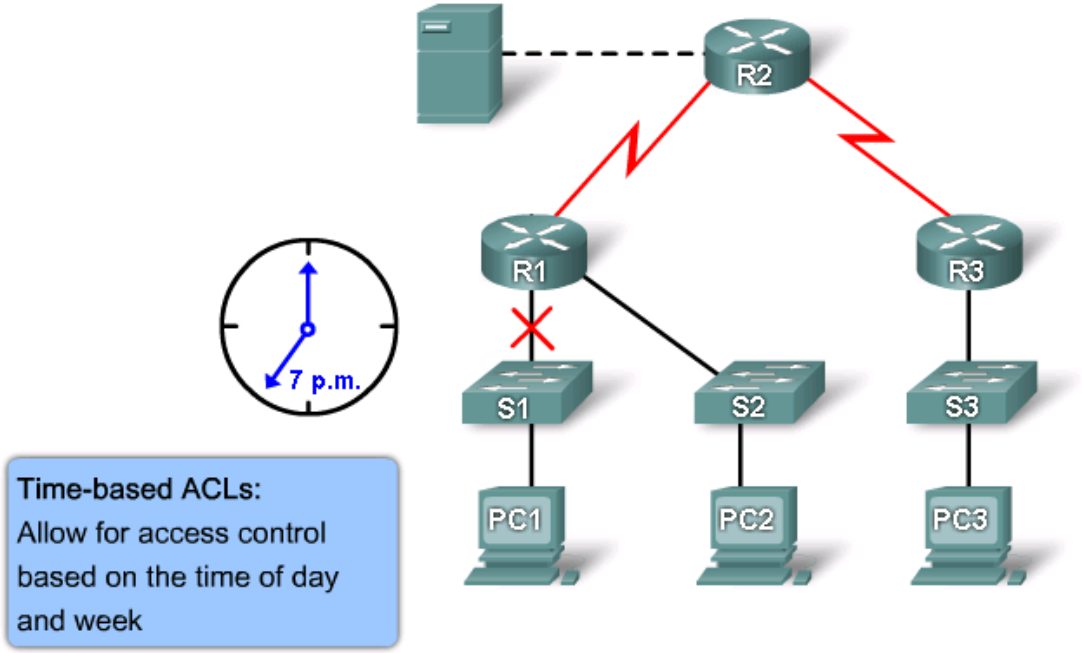
Mahmoud Abdel-Salam
Faculty of Computer and Information
Mansoura university
IT department
mahmoud20@mans.edu.eg

Outlines

- **Firewall types:**
  - Established keyword.
  - Time-based ACL.
  - Dynamic ACL.
  - Reflexive ACL and TCP intercept.
  - CBAC firewall

Time-based ACLs firewall

- Time-based ACLs allow for access control **based on time.**



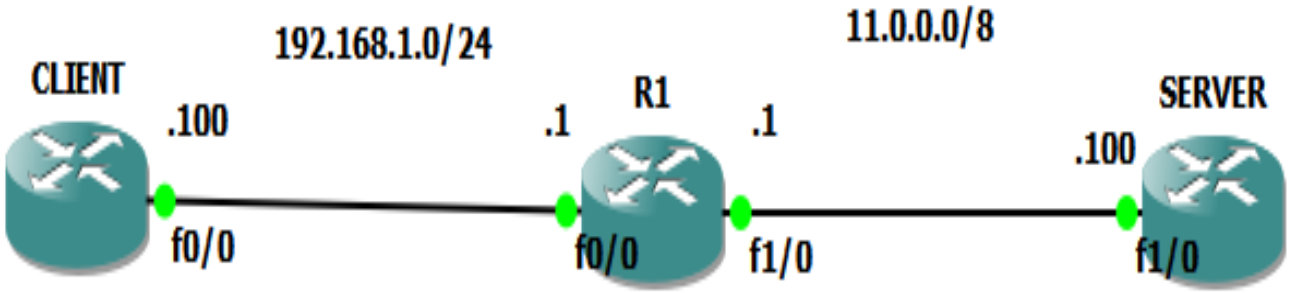
Time-based ACLs

1. Create a **time range** that defines specific times of the day and week.
2. Identify the time range with a name and then refer to it by a function.
3. The time restrictions are imposed on the function itself.

Step 1	R1(config)#**time-range EVERYOTHERDAY** R1(config-time-range)#**periodic Monday Wednesday Friday 8:00 to 17:00**
Step 2	R1(config)#**access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq telnet time-range EVERYOTHERDAY**
Step 3	R1(config)#**interface s0/0/0** R1(config-if)#**ip access-group 101 out**

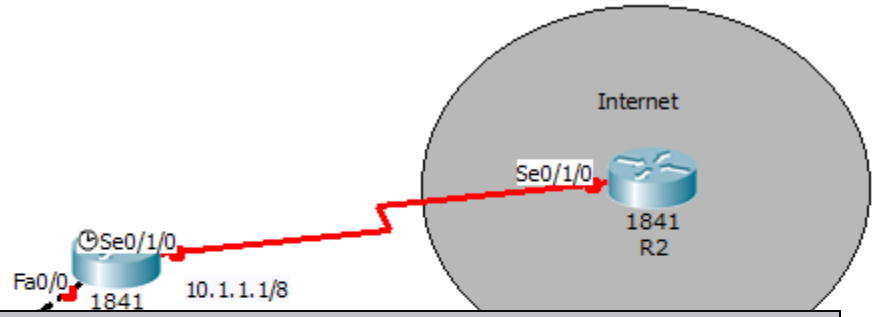
Time-based Lab

- **Objective:**
- Configure filtering list on R1 so that the CLIENT can Telnet the SERVER on work hours only; i.e. from 9 AM to 5 PM.



Time-based ACL Example

- Users are not allowed to access the Internet during business hours, except during lunch (12 p.m. to 1 p.m.) and after hours between 5 p.m. and 7 p.m.




```
R1(config)# time-range EMPLOYEE-TIME
R1(config-time-range)# periodic weekdays 12:00 to 13:00
R1(config-time-range)# periodic weekdays 17:00 to 19:00
R1(config-time-range)# exit
R1(config)# access-list 100 permit ip 192.168.1.0 0.0.0.255 any time-range EMPLOYEE-TIME
R1(config)# access-list 100 deny ip any any
R1(config)# interface FastEthernet 0/1
R1(config-if)# ip access-group 100 in
R1(config-if)# exit
```

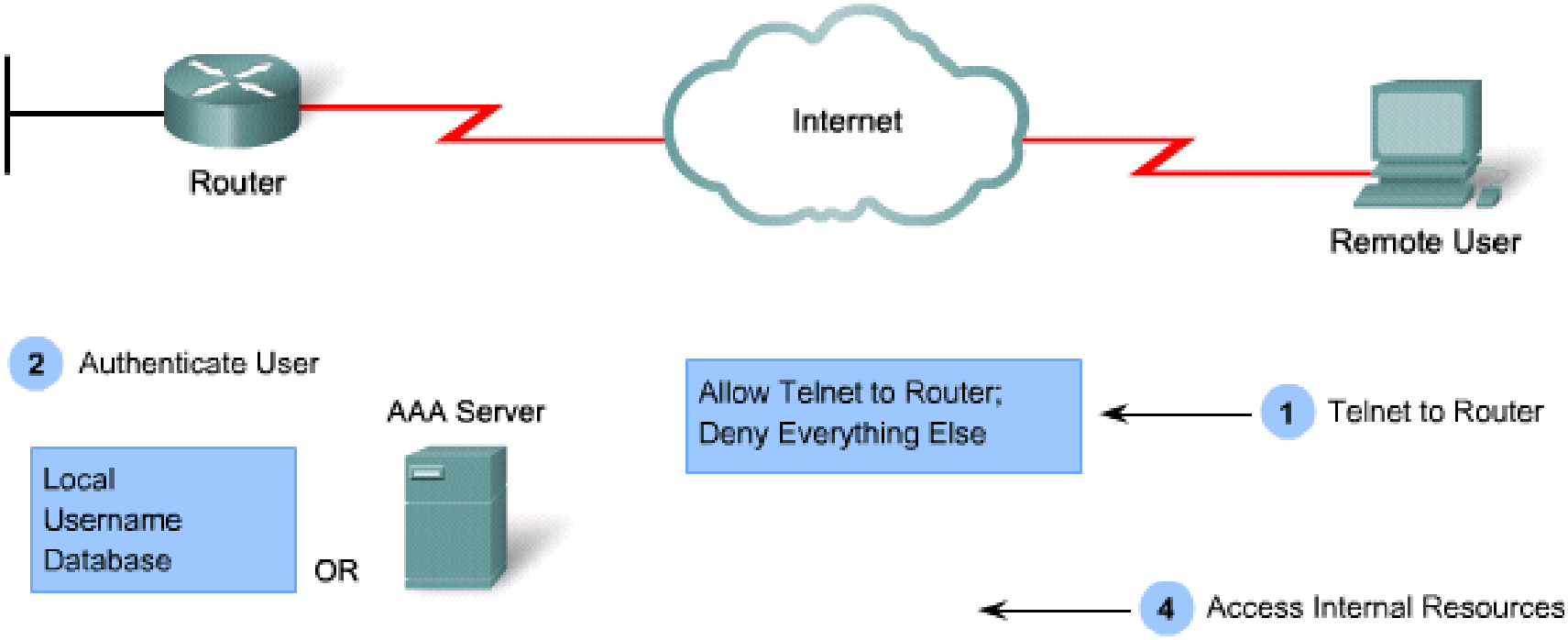
Dynamic ACLs firewall

- Dynamic ACLs are also called **lock-and-key** ACLs.
- Dynamic ACLs **authenticate the user and then permits** limited access through your firewall router for a host or **subnet for a finite period**.
- Dynamic ACLs are dependent on:
  - **Telnet** connectivity
  - **Authentication** (local or remote)
  - **Extended** ACLs

Implementing Dynamic ACLs firewall

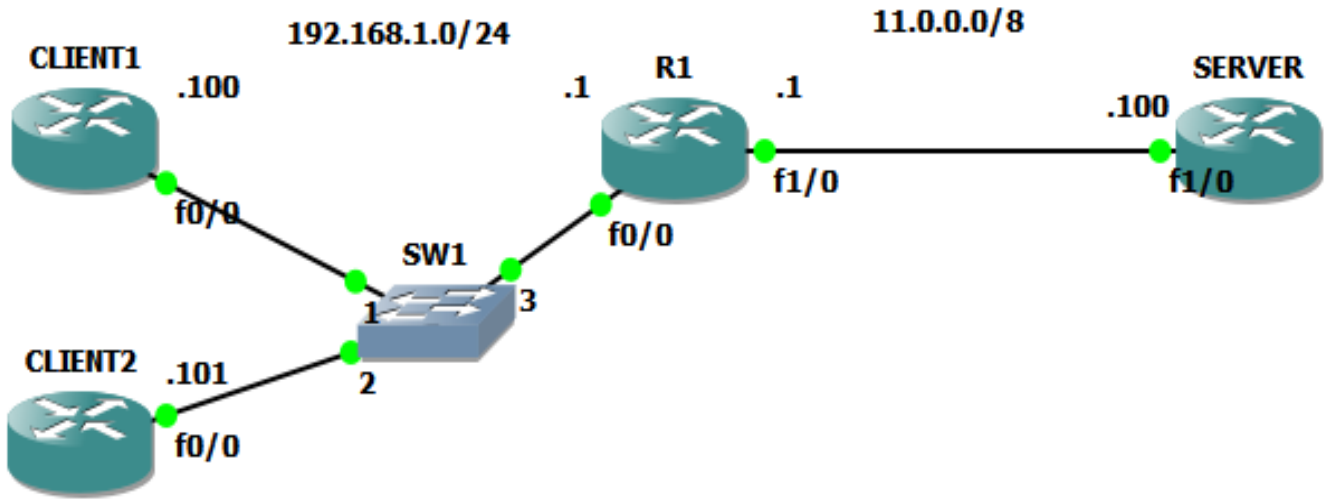
- An extended ACL is applied to block all traffic through the router except Telnet.
  - Users who want to traverse the router are blocked by the ACL **until they use Telnet to connect to the router** and are ***authenticated***.
- Users authenticate **using Telnet, and then dropped.**
  - A **single-entry dynamic ACL is added to the extended** ACL that exists.
  - This **permits traffic for a particular period**;
  - **idle and absolute timeouts** are possible.

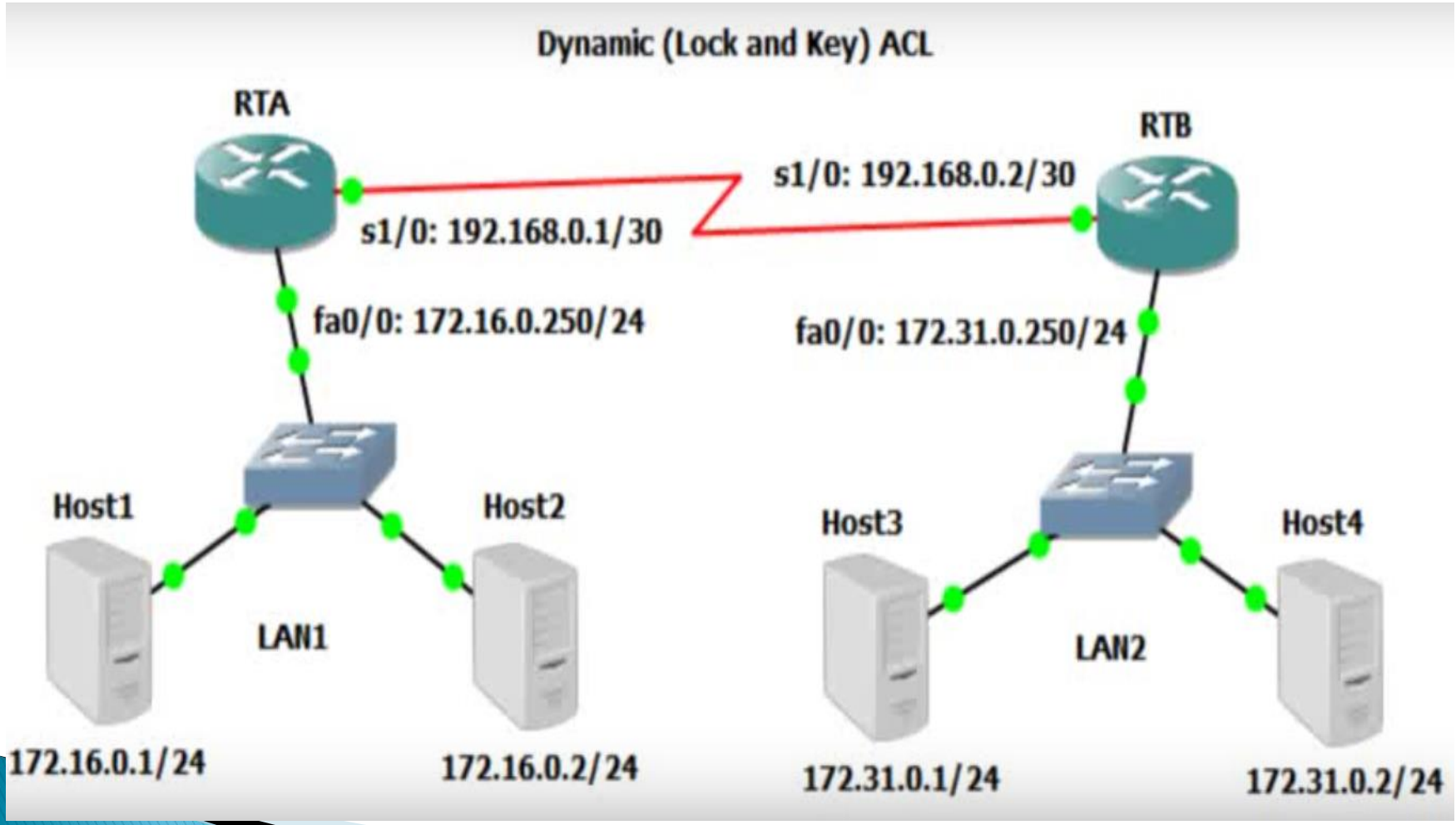
Configuring Dynamic ACLs firewall



Dynamic ACL Lab

- **Objective:**
- Configure dynamic ACL on R1 so that CLIENT1 or CLIENT2 can open TCP sessions on SERVER.




Dynamic (Lock and Key) ACL
RTA
RTB
s1/0: 192.168.0.2/30
s1/0: 192.168.0.1/30
fa0/0: 172.16.0.250/24
fa0/0: 172.31.0.250/24
Host1
Host2
Host3
Host4
LAN1
LAN2
172.16.0.1/24
172.16.0.2/24
172.31.0.1/24
172.31.0.2/24

Reflexive ACLs firewall

- **Unlike** the TCP Established feature which **just used ACK and RST** bits, reflexive ACLS filter traffic based on **source, destination addresses, and port numbers.**
- **S**ession filtering uses **temporary filters** that are **removed** when a session is **over adding a time limit** on a hacker's attack opportunity.

Reflexive ACLs firewall

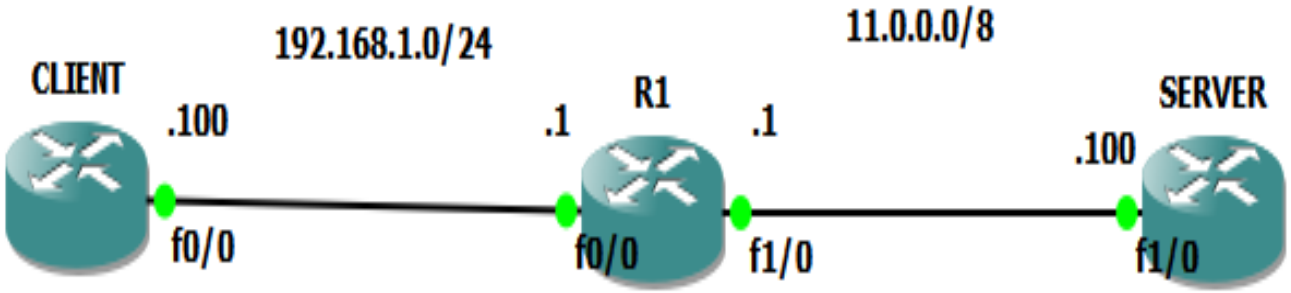
- Network administrators use reflexive ACLs to **allow** IP traffic for sessions originating **from their network while denying IP traffic for sessions originating outside the network.**
- The router examines the outbound traffic and when it sees a new connection**, it adds an entry to a *temporary ACL to allow replies back in.***
  - These entries are **automatically created when a new IP session begins.**

Configuring a Reflexive ACL firewall

- **Step 1.**
  - Create ***an internal ACL that looks for new outbound*** sessions and creates temporary reflexive ACEs.
- **Step 2.**
  - Create an ***external ACL that uses the reflexive ACLs*** to **examine** return traffic.
- **Step 3.**
  - Activate the **Named ACLs on the appropriate interfaces**.

Reflexive ACL Lab

- **Objective:**
- Configure reflexive ACL on R1 so that it allows all traffic sourced from the CLIENT to the SERVER, not vice versa.



References

- https://www.ciscopress.com/articles/article.asp?p=1697887
- https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html