Access Control List

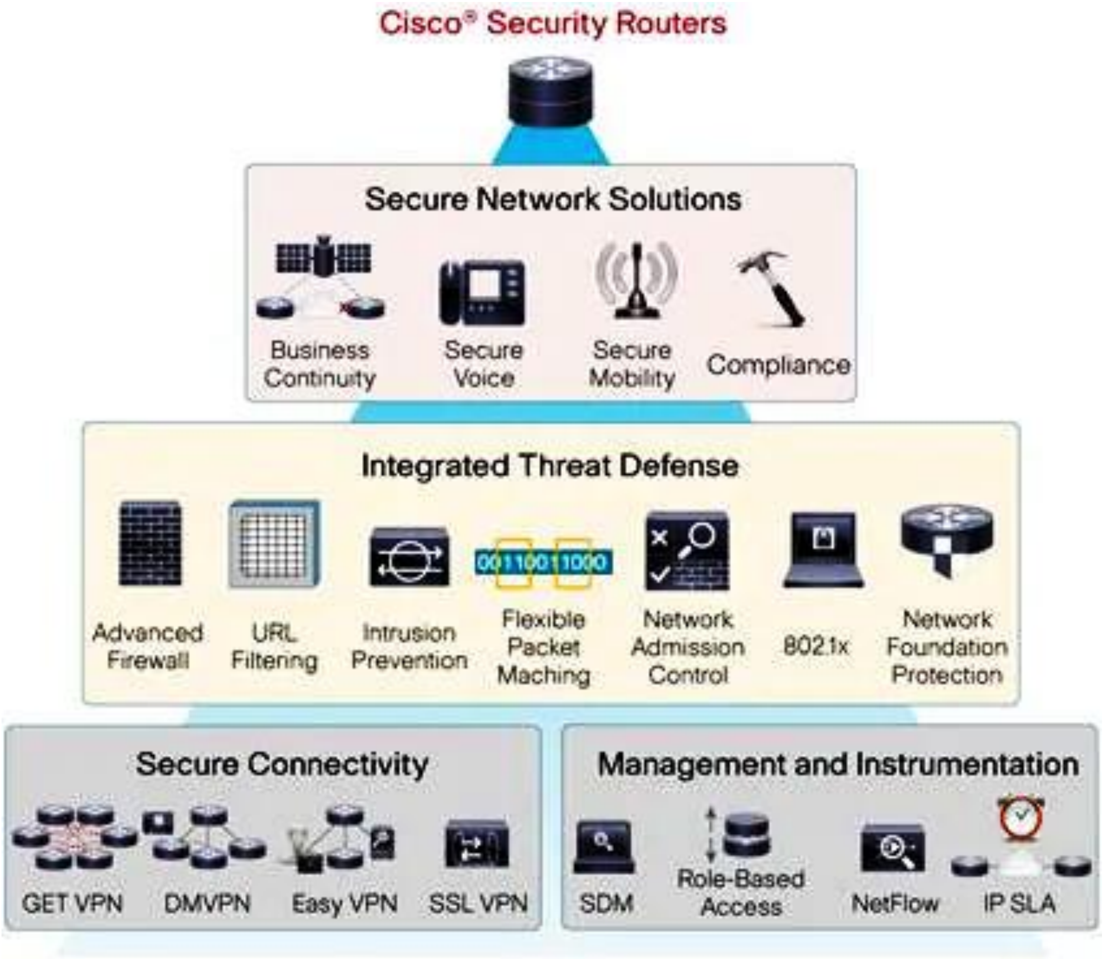
Speaker: Songyut Phoemphon

Contact: songyut@sut.ac.th

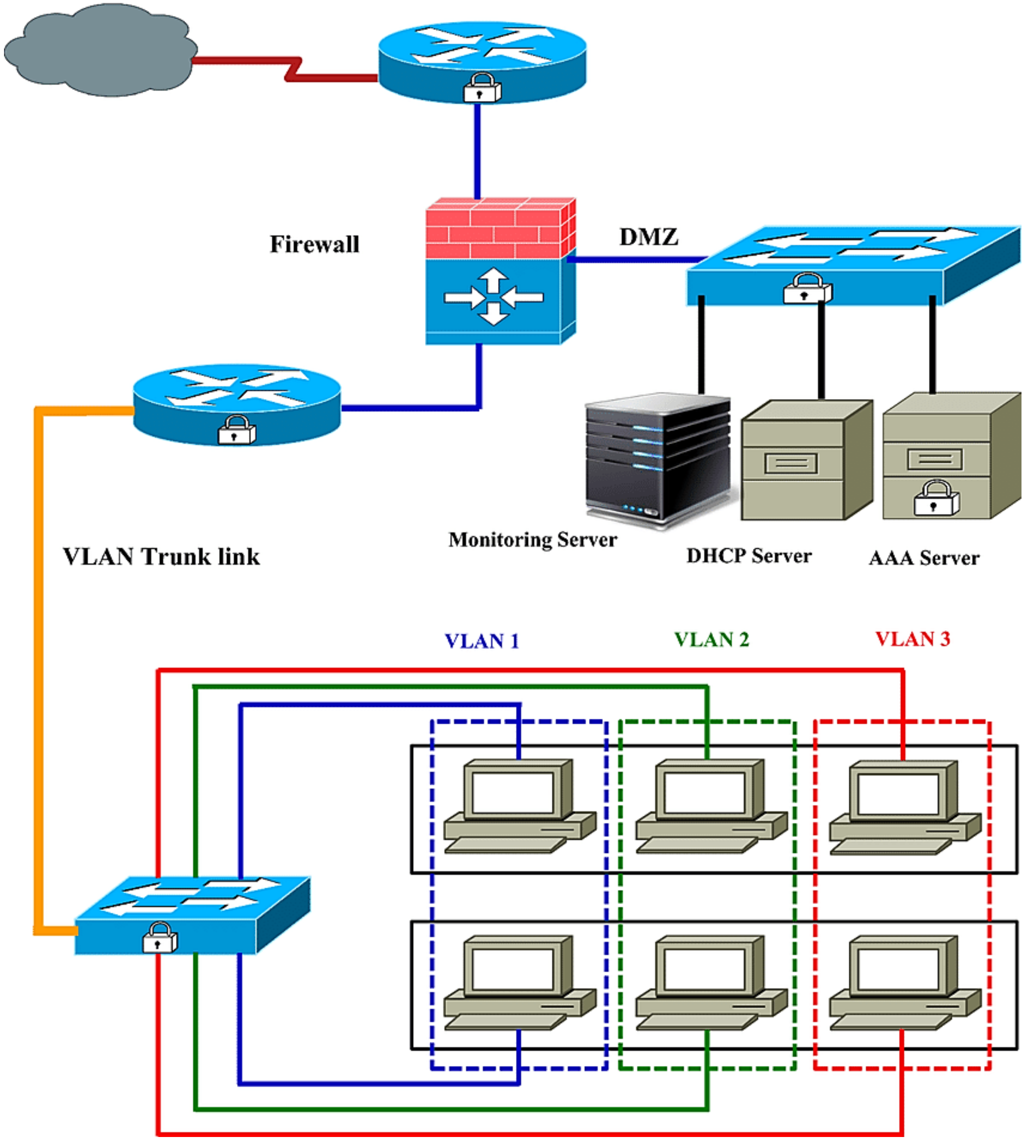
Objective

Student are able to

- understand security of a router



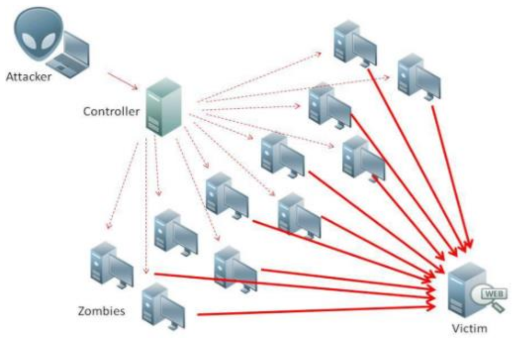
Secure network structure

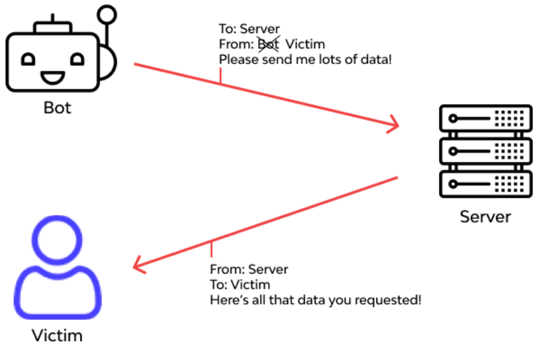


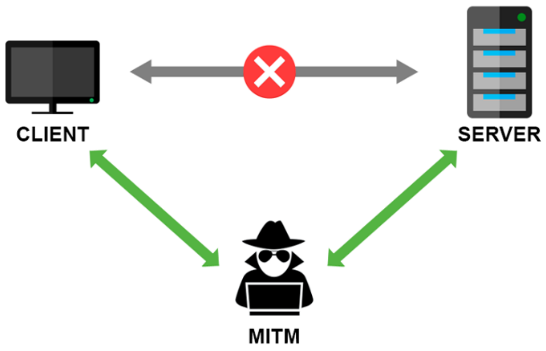
Basic Security

Attack

- Application-layer (e.g., bugs in FTP, HTTP)
- Autorooters (e.g., rootkit)
- Backdoors (e.g., Trojan horse)
- (Distributed) Denial of service (e.g., SYN flood)
- IP Spoofing (impersonate as legitimate IP)
- Man-in-the-middle attacks
- Packet Sniffers
- Brute force attacks
- …



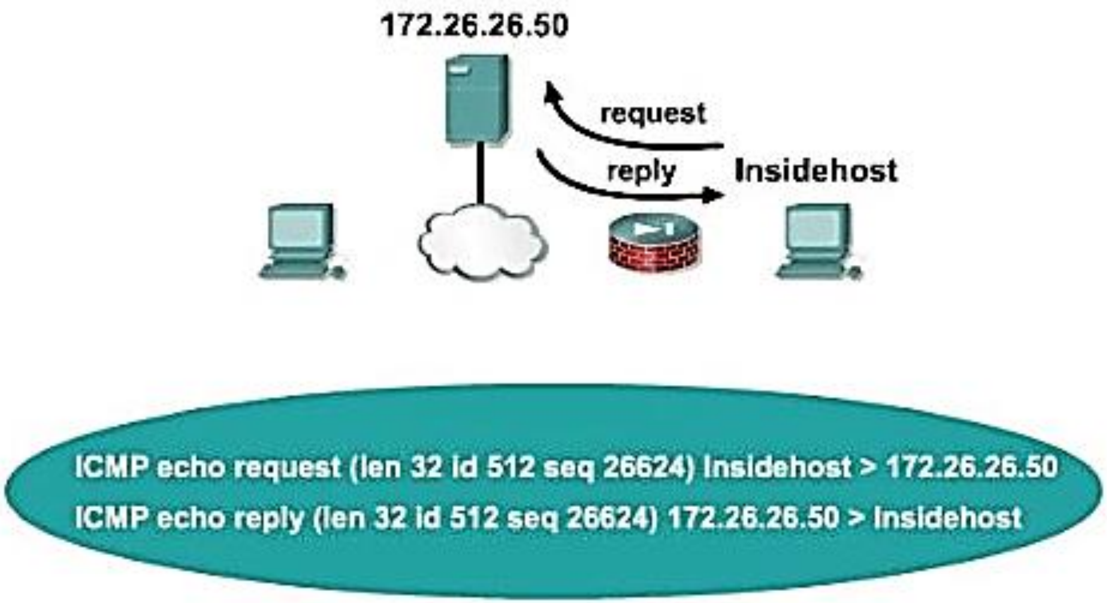




Basic Security System

Attack Prevention

- IDS, IPS
- Firewall
- ICMP inspection
- Authentication proxy



ICMP echo request (len 32 id 512 seq 26624) Insidehost > 172.26.26.50

ICMP echo reply (len 32 id 512 seq 26624) 172.26.26.50 > Insidehost

Access Lists

Function Matching

- Allow / deny packet go through router
- Allow / deny telnet in to/out of router

Matching

- Packet will match in order
- Stop when match
- If nothing match, deny!

Category of Access Lists

Standard Access Lists

- Filter by source IP

Extended Access Lists

- Filter by source IP, destination IP, Protocol, Port

Named Access Lists

- Name the list (both standard and extended)

Direction: Inbound vs. Outbound Access Lists

Building an Access

- One value per interface / protocol / direction
- Specific tests before General tests
- New values always append at the end
- By default, end with “deny all”
- ACL can’t filter traffic from the router itself
- Standard ACL is configured close to the destination
- Extended ACL is configured close to the source

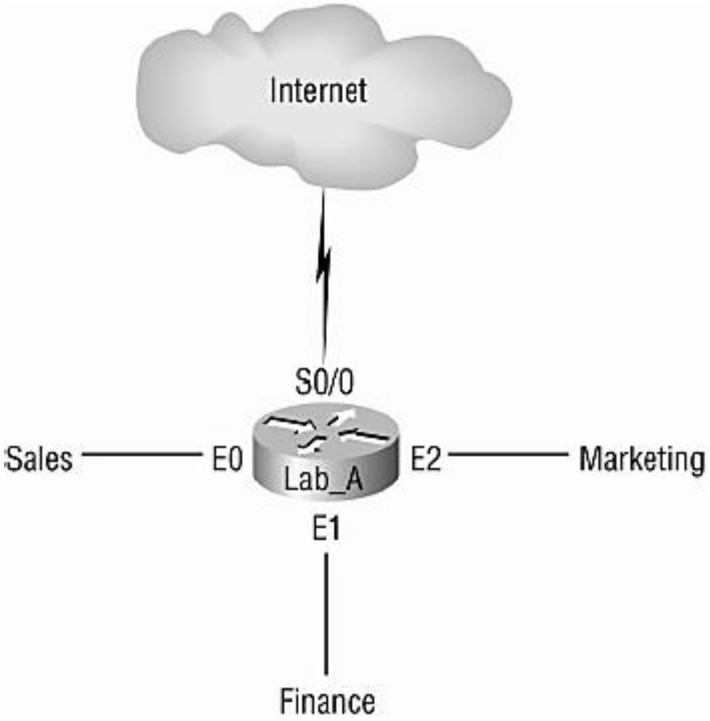
Standard IP access lists

```
Router#conf t
        Enter configuration commands, one per line. End with CNTL/Z.
        Router(config)#access-list ?
        <1-99> IP standard access list
        <100-199> IP extended access list
Router(config)#access-list 10 ?
        deny Specify packets to reject
        permit Specify packets to forward
        remark Access list entry comment
Router(config)#access-list 10 deny ?
        A.B.C.D Address to match
        any Any source host
        host A single host address
Router(config)#access-list 10 deny host 172.16.30.2
```

Question

How to prevent “Sales” to access “Finance”

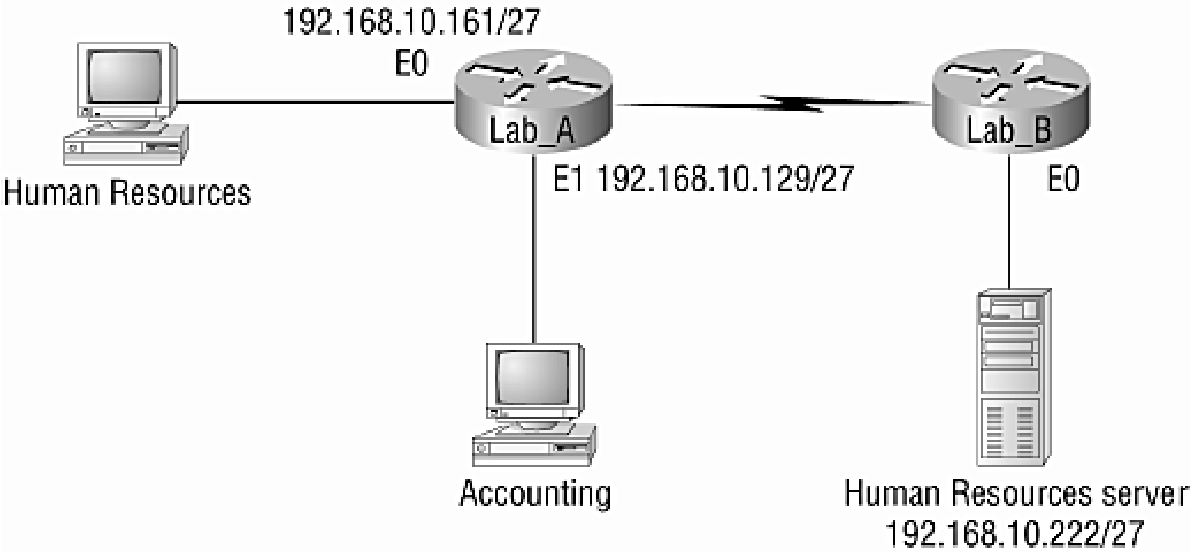
What interface should standard ACL be applied?



Example

Prevent "Accounting" to access "HR Server"

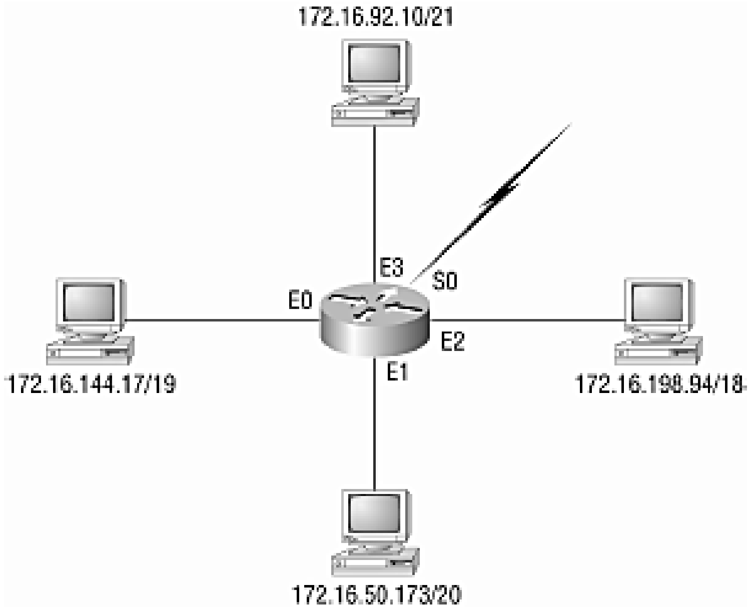
- Router(config)# access-list 10 deny 192.168.10.128 0.0.0.31
- Router(config)# access-list 10 permit any
- Router(config)# interface e0
- Router(config-if)# ip access-group 10 out



Example

Prevent all machine to access the internet (S0)

- Router(config)#access-list 1 deny 172.16.128.0 0.0.31.255
- Router(config)#access-list 1 deny 172.16.48.0 0.0.15.255
- Router(config)#access-list 1 deny 172.16.192.0 0.0.63.255
- Router(config)#access-list 1 deny 172.16.88.0 0.0.7.255
- Router(config)#access-list 1 permit any
- Router(config)#interface serial 0
- Router(config-if)#ip access-group 1 out



Wildcard mask

172.16.8.0 - 172.16.15.0

- 10101100 10101000 00001XXX XXXXXXXX
- Wildcard: 0 = exact (match), 1 = any (don’t care)
  - 172.168.8.0
    - 10101100 10101000 00001000 00000000
  - 0.0.7.255 (= CIDR [/21] = SM[255.255.248.0])
    - 00000000 00000000 00000111 11111111

Telnet Control

Access-class

- Router(config)# access-list 50 permit 172.16.10.3
- Router(config)# line vty 0 4
- Router(config-line)# access-class 50 in
  - ** imply “deny” all (except 172.16.10.3) at the end **
  - Notice: access-group is applied with an interface
    - ➢ but access-class is applied with vty (telnet)

Extended IP ACLs

```
Router(config)#access-list ?
          <1-99> IP standard access list
          <100-199> IP extended access list
Router(config)#access-list 110 ?
          deny Specify packets to reject
          permit Specify packets to forward
          remark Access list entry comment
Router(config)#access-list 110 deny ?
          ahp Authentication Header Protocol
          eigrp Cisco's EIGRP routing protocol
          esp Encapsulation Security Payload
          gre Cisco's GRE tunneling
          icmp Internet Control Message Protocol
          ip Any Internet Protocol
          ospf OSPF routing protocol
          tcp Transmission Control Protocol
          udp User Datagram Protocol
Router(config)#access-list 110 deny tcp ?
          A.B.C.D Source address
          any Any source host
          host A single source host
```

Procedures of Extended ACLs

#1: Select the access list:

```
RouterA(config)#access-list 110
```

#2: Decide on deny or permit:

```
RouterA(config)#access-list 110 deny
```

#3: Choose the protocol type:

```
RouterA(config)#access-list 110 deny tcp
```

#4: Choose source IP address of the host or network: RouterA(config)#access-list 110 deny tcp any

#5: Choose destination IP address

```
RouterA(config)#access-list 110 deny tcp any host 172.16.30.2
```

#6: Choose the type of service, port, & logging

```
RouterA(config)#access-list 110 deny tcp any host 172.16.30.2 eq 23 log
```

Example

- /* Prevent telnet (port 23) to 172.16.30.2 */
- RouterA(config)#access-list 110 deny tcp any host 172.16.30.2 eq 23 log
- /* permit all */
- RouterA(config)#access-list 110 permit ip any 0.0.0.0 255.255.255.255
  - any = 0.0.0.0 255.255.255.255
- RouterA(config-if)#ip access-group 110 (in or out)

Named Access List

Name the access list

- Lab_A(config)#ip access-list standard BlockSales
- Lab_A(config-std-nacl)#deny 172.16.40.0 0.0.0.255
- Lab_A(config-std-nacl)#permit any

Checking the ACLs

Show access-list + parameters (with out interface)

- show access-list

Show some access list

- show access-list 110

Show only ip access list

- show ip access-list

Show interfaces of access list

- show ip interface

Show name and interface

- show running-config

Conclusion

Students may work as System/Network Administrator

- with knowledge in CCNA level.

Thank you.

Speaker: Songyut Phoemphon

Contact: songyut@sut.ac.th