Computer Security

Labs

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

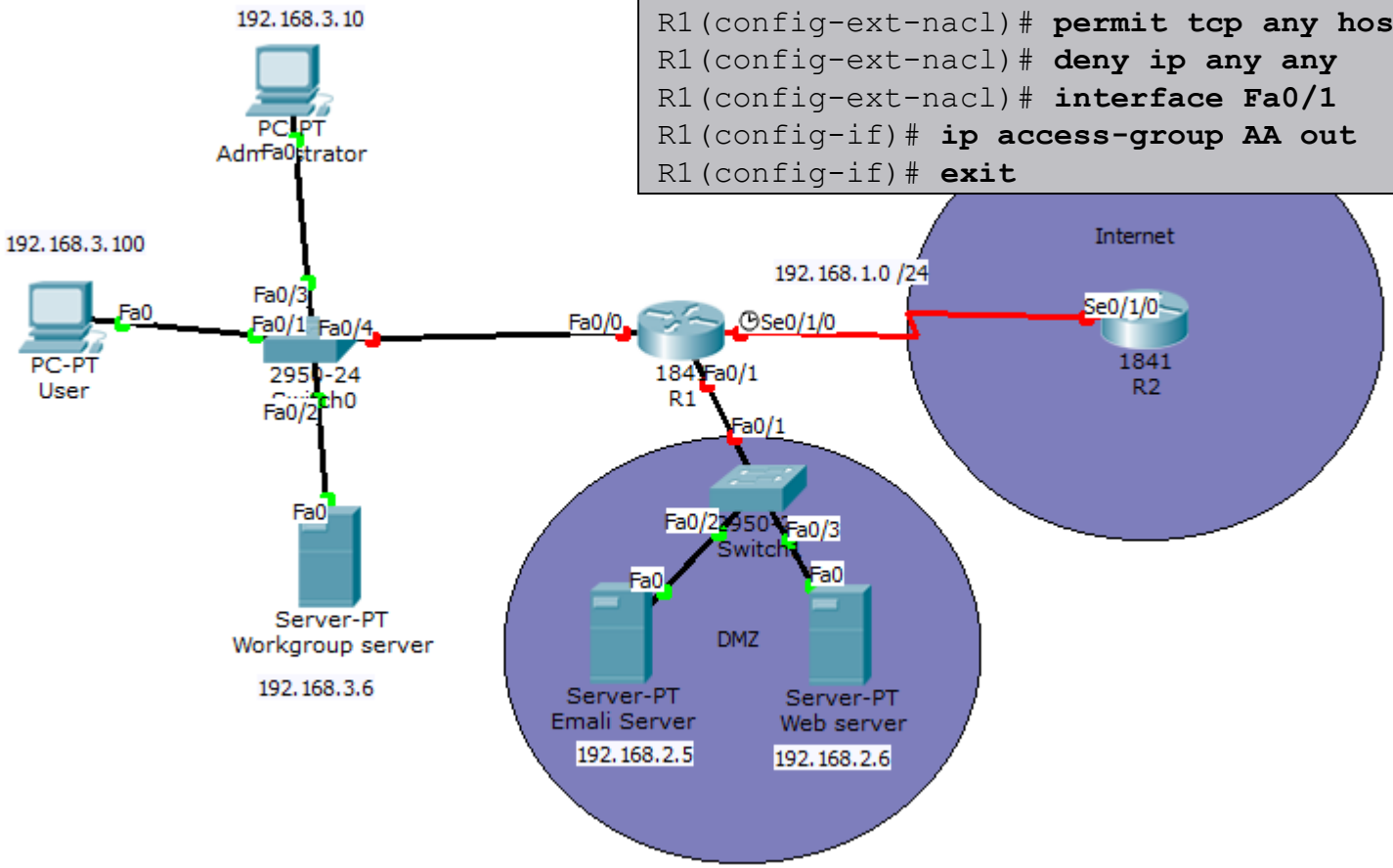
Outlines

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

Extended ACL example

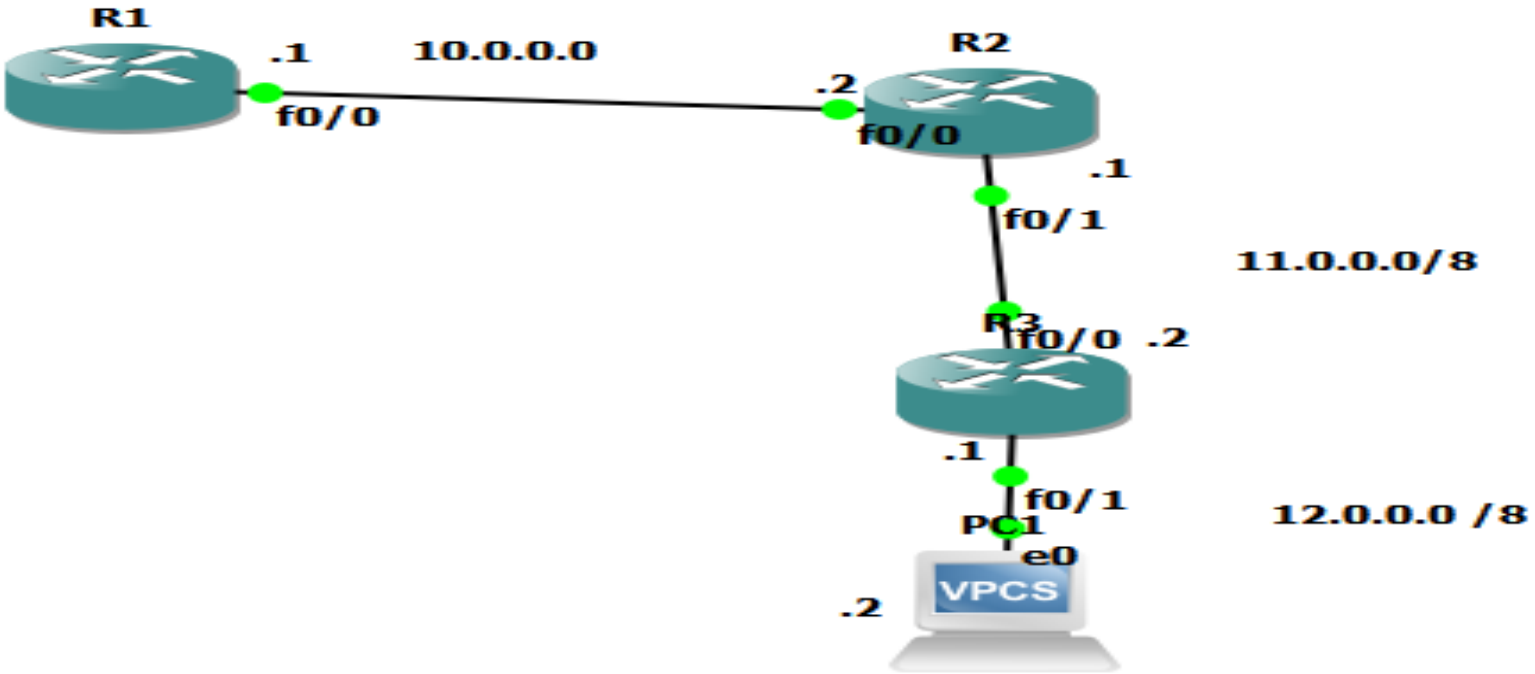
- Create an extended named ACL called **AA**, applied outgoing on the Fa0/1 DMZ interface, permitting access to the specified Web and Email servers.

```
R1(config)# ip access-list extended AA
R1(config-ext-nacl)# permit tcp any host 192.168.2.5 eq 25
R1(config-ext-nacl)# permit tcp any host 192.168.2.6 eq 80
R1(config-ext-nacl)# deny ip any any
R1(config-ext-nacl)# interface Fa0/1
R1(config-if)# ip access-group AA out
R1(config-if)# exit
```



Extended ACL example

- Create an extended access list with the following rules:
- From R1 ➔ R2 (permit telnet and deny ping)
- From R3 ➔ R2 (deny telnet and permit ping)



ACLs

Standard ACLs

Types of Cisco ACLs

Standard ACLs filter IP packets based on the [ ]

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

```
access-list {1-99} {permit | deny} source-addr [source-wildcard]
```

- **Note:**
  - Can be applied in an incoming or outgoing direction on an interface using the **`ip access-group`** command.
  - It can also be applied on a VTY port using the **`access-class`** command.

Extended ACLs

Extended ACLs filter IP packets based on several attributes, including the following:

-
-
-

```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

access-list {**100-199**} {**permit** | **deny**} *protocol source-addr* [*source-wildcard*][*operator operand*] *destination-addr* [*destination-wildcard*] [*operator operand*][**established**]

Modify an ACL using Sequence Numbers

- First use the **show** command to view the existing sequence numbers.

```
R1# show access-list 150
Extended IP acess list 150
    10 permit tcp any any eq www
    20 permit tcp any any eq telnet
    30 permit tcp any any eq smtp
    40 permit tcp any any eq pop3
    50 permit tcp any any eq 21
    60 permit tcp any any eq 20
```

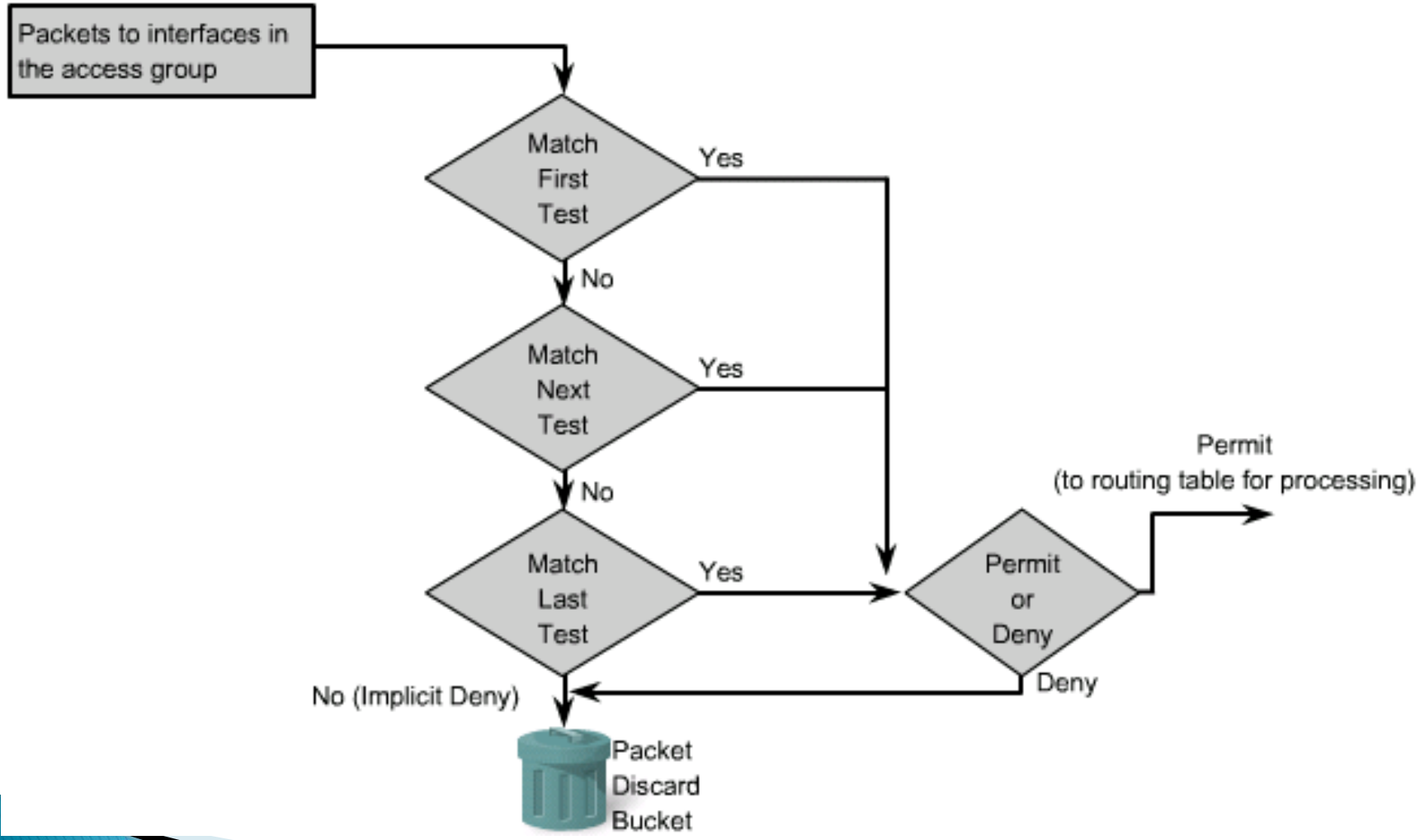
- Resequence if necessary.
- Use the **no** *sequence-number* command to delete a statement.

```
R1(config)# ip access-list extended 150
R1(config-ext-nacl)# no 20
```

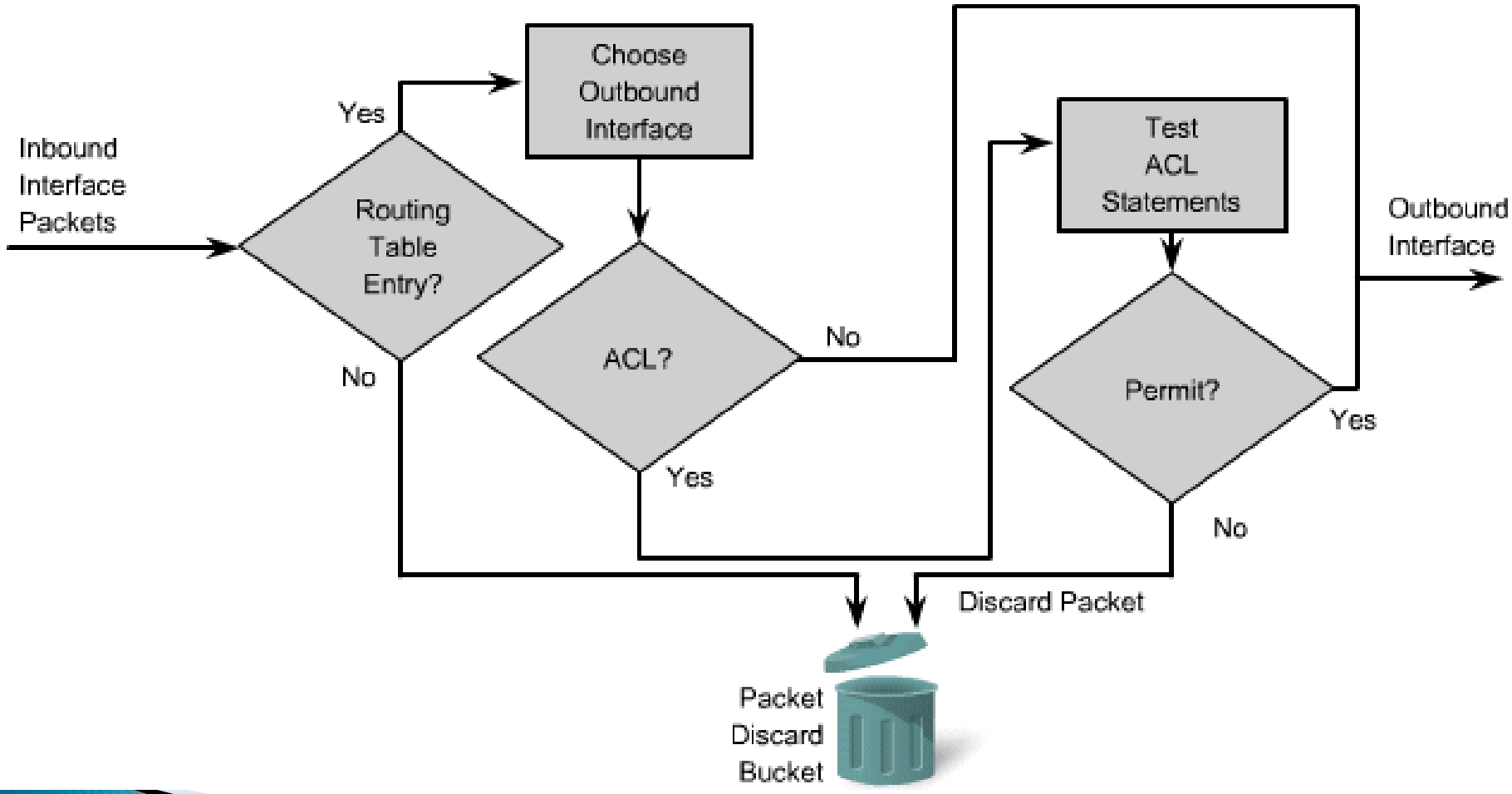
- Use the *sequence-number* **{permit | deny}** command to add a statement within the ACL.

```
R1(config)# ip access-list extended 150
R1(config-ext-nacl)# 20 permit tcp host 192.168.1.100 any eq telnet
```

Inbound ACL Operation Flow



Outbound ACL Operation Flow



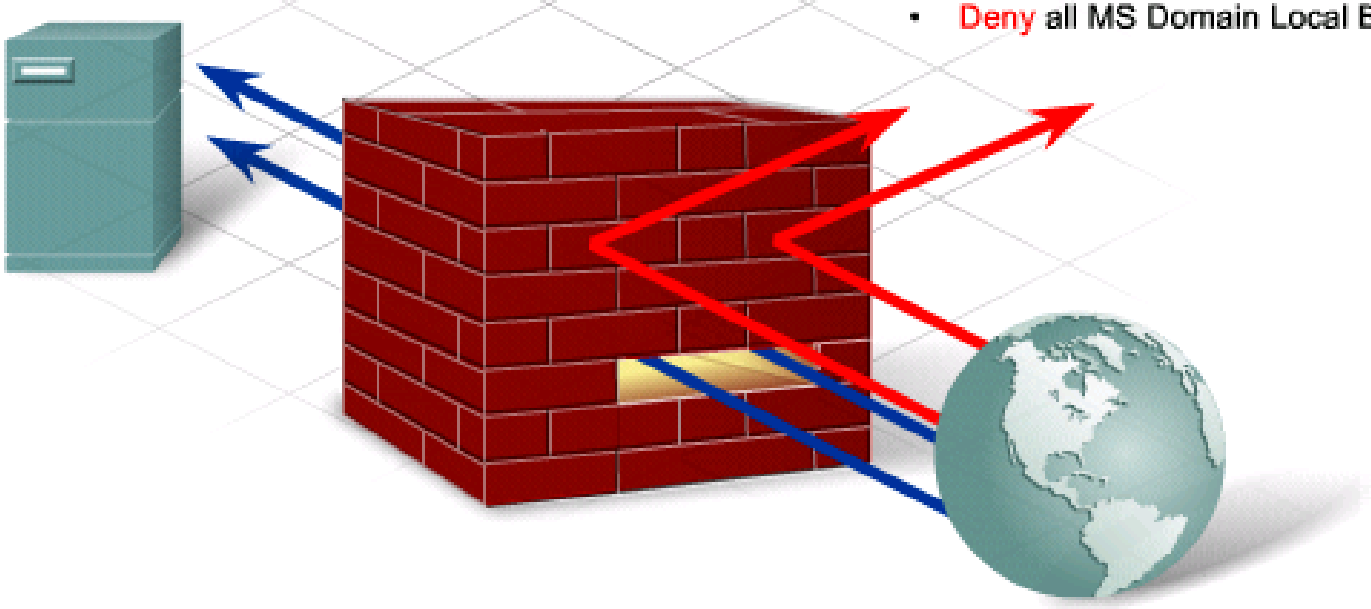

Firewall
technologies

Firewall

- A firewall prevents undesirable traffic from entering prescribed areas within a network.
- A firewall is a **system** or ***group of systems*** that enforces an access control policy between networks.
  - For example:
    - A packet filtering router
    - A switch with two VLANs
    - Multiple hosts with firewall software

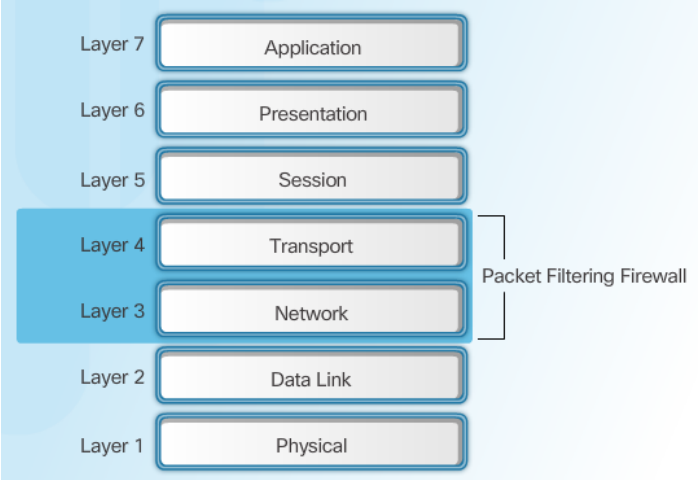
Firewall

- Allow web traffic from any external address to the web server
- Allow traffic to FTP server
- Allow traffic to SMTP server
- Allow traffic to internal IMAP server
- Deny all inbound traffic with network addresses matching internal-registered IP addresses
- Deny all inbound traffic to server from external addresses
- Deny all inbound ICMP echo request traffic
- Deny all inbound MS Active Directory
- Deny all inbound MS SQL server ports
- Deny all MS Domain Local Broadcasts

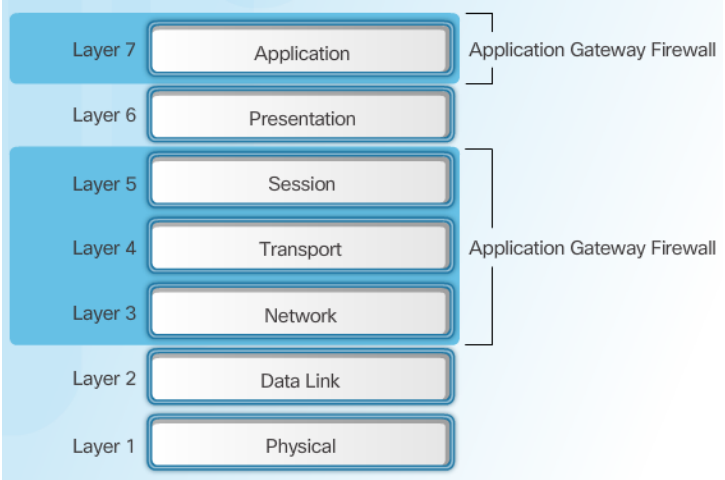


Firewall types

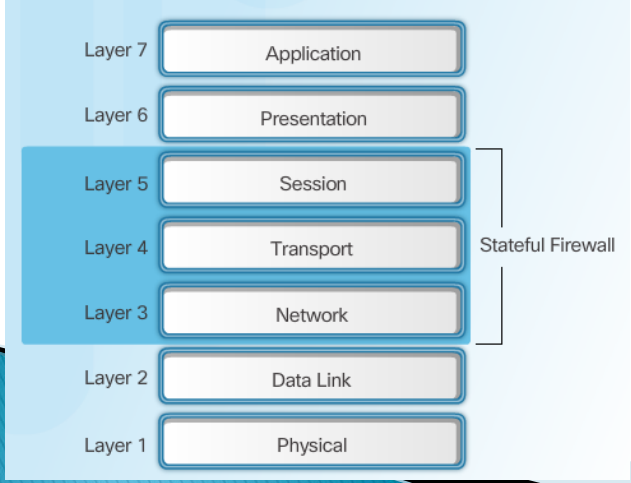
Packet Filtering Firewall



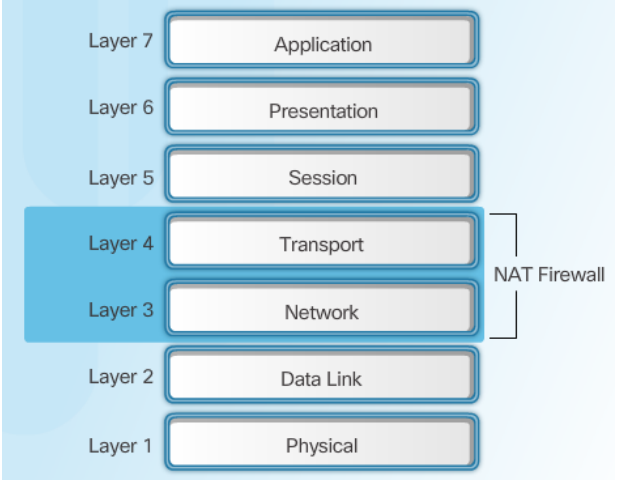
Application Gateway Firewall



Stateful Firewall

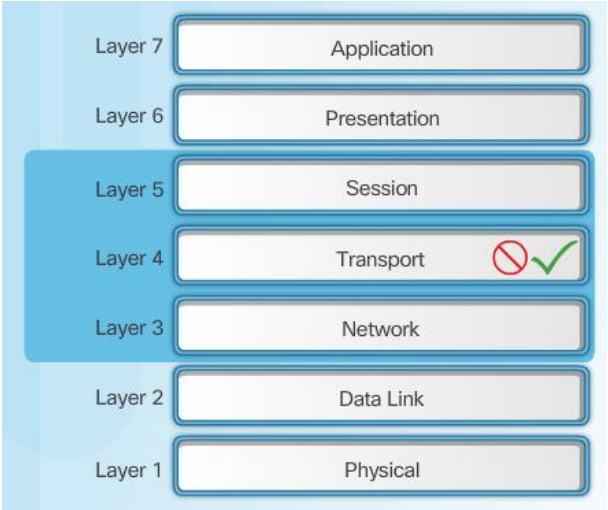


NAT Firewall

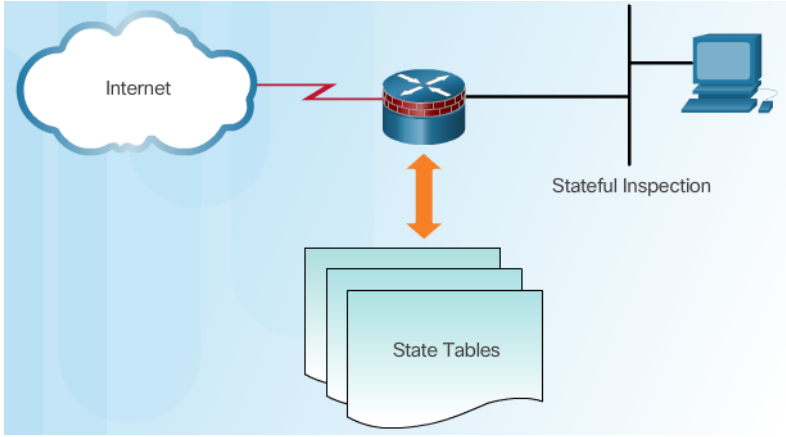


Firewall types

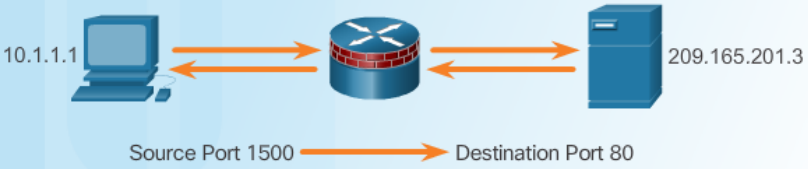
Stateful Firewalls



State Tables



Stateful Firewall Operation



Inside ACL (Outgoing Traffic)	Outside ACL (Incoming Traffic)
permit ip 10.0.0.0.0.0.0.255 any	Dynamic: permit tcp host 209.165.201.3 eq 80 host 10.1.1.1 eq 1500

Stateless versus Stateful Packet Filtering

- ***Stateless packet filtering:***
  - ACLs filter traffic based on **source and destination IP addresses, TCP and UDP port numbers, TCP flags, and ICMP types and codes.**
- ***Stateful packet filtering:***
  - Inspection ***remembers*** certain details, or the state of that request.
  - Device maintains **records of all connections passing through the** firewall, and is able to determine whether a packet is the start of a new connection, **or part of an existing connection.**
  - A stateful firewall **monitors** the state of connections, whether the connection is in an initiation, data transfer, or termination state.


Firewall design

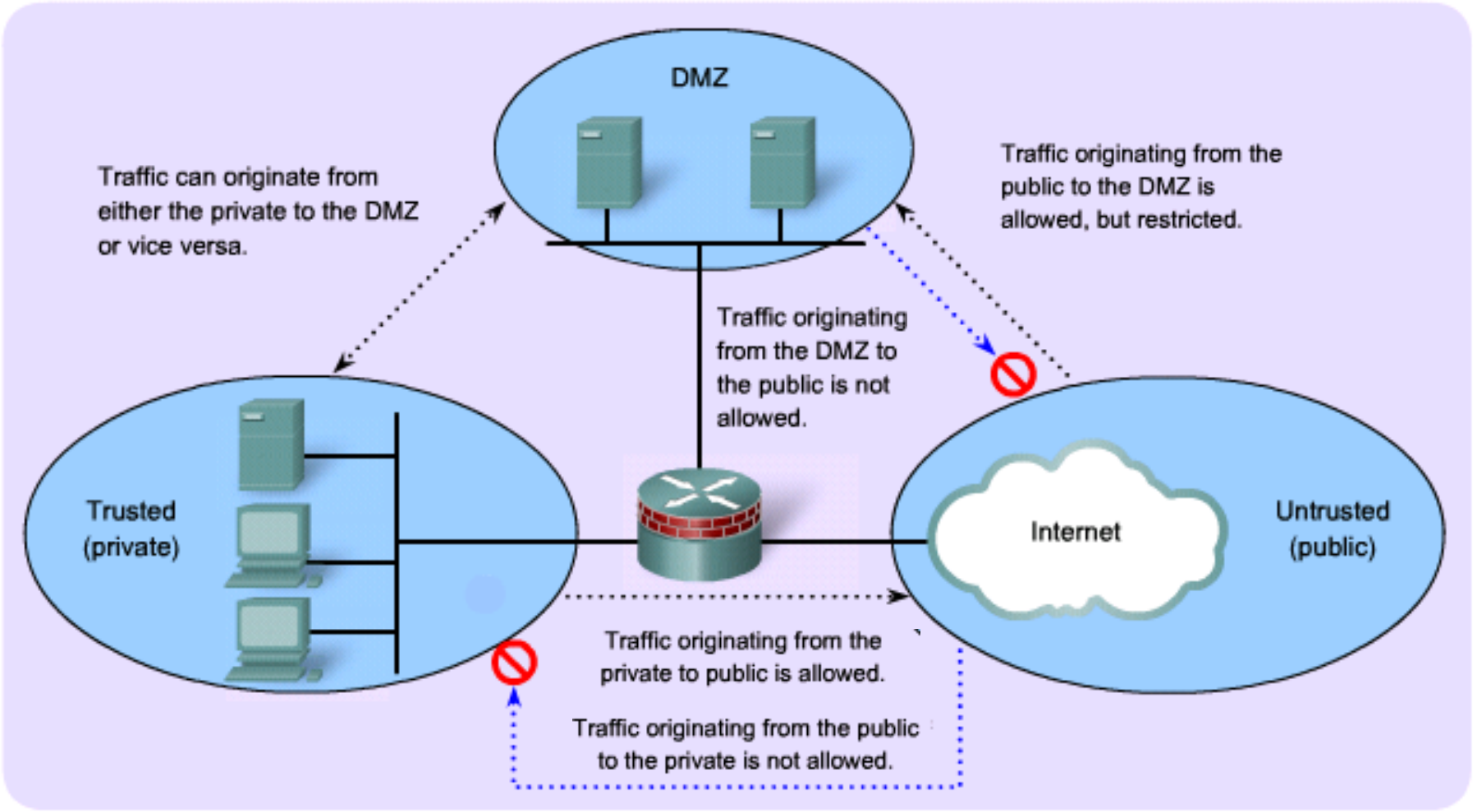
Simple Firewall Design

- Firewall designs can be as **simple as having an inside network and outside network using two interfaces.**
  - The **inside** network (or private network) is **trusted**.
    - The traffic from the **inside is usually permitted** to traverse the firewall to the outside with little or no restrictions.
    - Traffic returning **from the outside that is associated with traffic originating from the inside is permitted** to traverse from the untrusted interface to the trusted interface.
  - The **outside** network (or public network) is **untrusted**.
    - Traffic originating from the **outside** is **generally blocked** entirely or **very** selectively permitted.

Modern Firewall Design

- Designs involve three or more interfaces on a firewall:
  - *One inside network*
    - Traffic **to the outside** is freely **permitted**.
    - Traffic **to the DMZ** is freely **permitted**.
  - *One outside network*
    - Traffic **from the outside is generally blocked entirely unless it is associated with traffic originating** from the inside or the DMZ.
  - *One DMZ network*
    - Traffic **from the outside should be very specific such as email, DNS, HTTP, or HTTPS traffic.**
    - Traffic to the outside is freely permitted.

Firewall design



TCP Established ACLs firewall

- The TCP **established** keyword blocks all traffic coming from the Internet except for the TCP reply traffic associated with established TCP traffic initiated from the inside of the network.

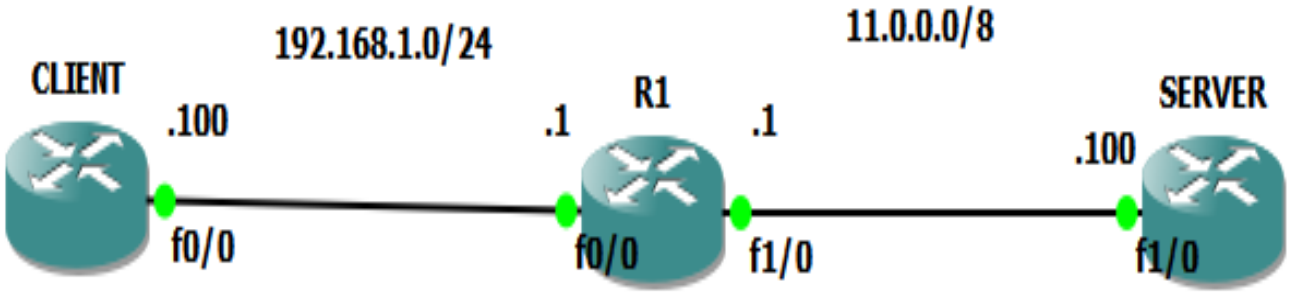
- The **`established`** keyword forces the router to check whether the TCP **ACK** or RST control flag is set.
  - If the ACK flag is set, the TCP traffic is allowed in.
  - If not, it is assumed that the traffic is associated with a new connection initiated from the outside.

TCP Established ACLs

- Using the **`established`** keyword does not implement a stateful firewall on a router.
- The **`established`** parameter allows any TCP segments with the appropriate control flag.
- **No stateful information** is maintained **to keep track of traffic initiated from the inside of the network since the router does not keep track of** conversations to determine whether the traffic is return traffic associated with a connection initiated from inside the network.

Established keyword Lab

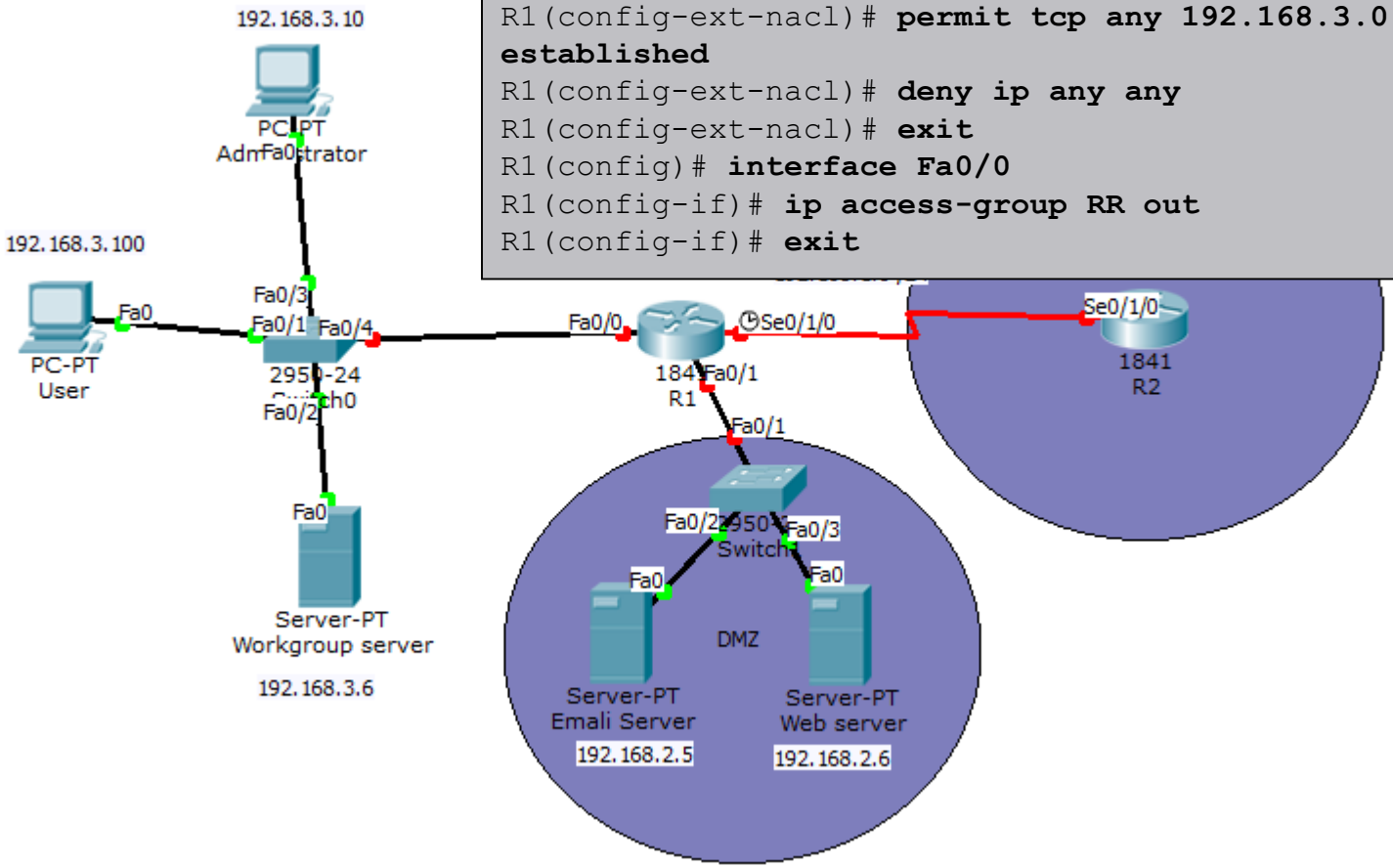
- **Objective:**
- Configure established filtering list on R1 so that only WWW, SSL and Telnet traffic is permitted if only sourced from the CLIENT to the SERVER.



Established keyword Lab 2

- Create an extended named ACL called **RR**, applied incoming on the Fa0/0 interface, that denies the workgroup server outside access but permits the remainder of the LAN users outside access tcp sessions using the **`established`** ACL.

```
R1(config)# ip access-list extended RR
R1(config-ext-nacl)# deny ip host 192.168.3.6 any
R1(config-ext-nacl)# permit tcp any 192.168.3.0 0.0.0.255
established
R1(config-ext-nacl)# deny ip any any
R1(config-ext-nacl)# exit
R1(config)# interface Fa0/0
R1(config-if)# ip access-group RR out
R1(config-if)# exit
```



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