



Computer Security

Labs

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

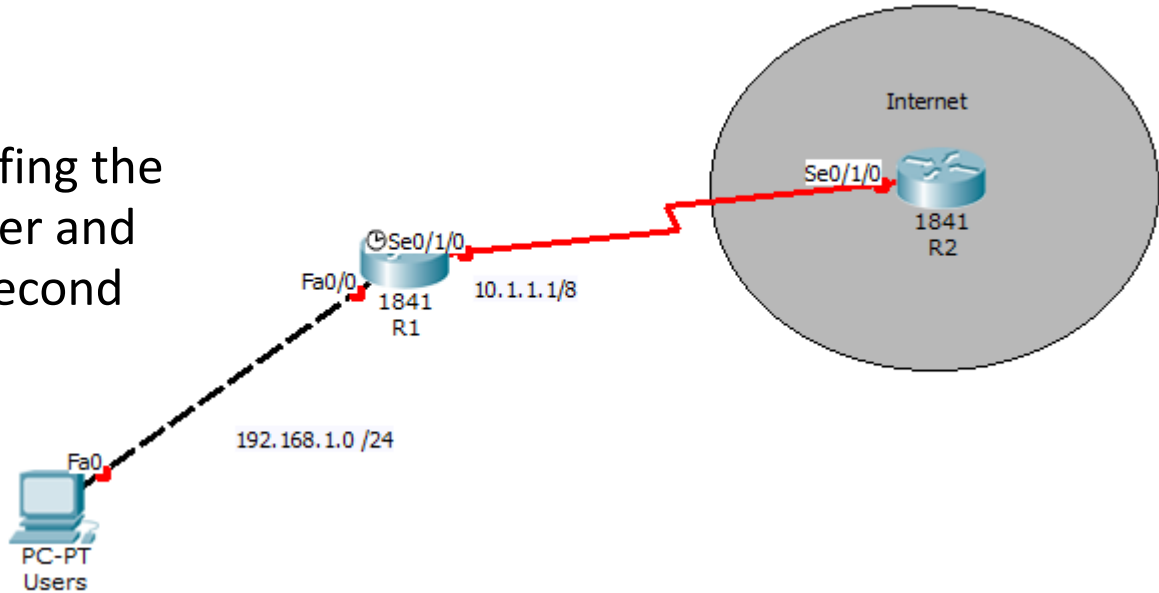
Outlines

► Firewall types:

- Established keyword.
- Time-based ACL.
- Dynamic ACL.
- Reflexive ACL and TCP intercept.
- CBAC firewall

Reflexive ACL Example

- ▶ Create a reflexive ACL that matches internal users surfing the Internet with a web browser and relying on DNS with a 10 second timeout period.



```
R1(config)# ip access-list extended INTERNAL_ACL
R1(config-ext-nacl)# permit tcp any any eq 80 reflect WEB-ONLY-REFLEXIVE-ACL
R1(config-ext-nacl)# permit udp any any eq 53 reflect DNS-ONLY-REFLEXIVE-ACL timeout 10
R1(config-ext-nacl)# exit
R1(config)# ip access-list extended EXTERNAL_ACL
R1(config-ext-nacl)# evaluate WEB-ONLY-REFLEXIVE-ACL
R1(config-ext-nacl)# evaluate DNS-ONLY-REFLEXIVE-ACL
R1(config-ext-nacl)# deny ip any any
R1(config-ext-nacl)# exit
R1(config)# interface s0/1/0
R1(config-if)# ip access-group INTERNAL_ACL out
R1(config-if)# ip access-group EXTERNAL_ACL in
```

Context-Based Access Control

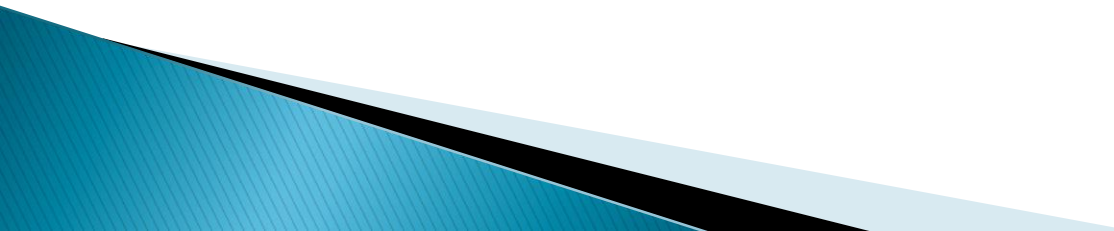
CBAC firewall

- ▶ CBAC intelligently **filters TCP and UDP packets** based on Application Layer protocol session information.
 - Provides **stateful Application Layer filtering for protocols that are specific to unique applications**, as well as applications and protocols that require multiple ports, such as FTP and H.323.
- ▶ CBAC provides four main functions:
 - Traffic filtering
 - Traffic inspection
 - Intrusion detection
 - Generation of audits and alerts

CBAC Traffic Filtering

- ▶ Permit specified TCP and UDP return traffic through a firewall.
 - It creates **temporary openings in an ACL that would otherwise deny the traffic.**
- ▶ Inspect traffic that originate from either side of the firewall.
 - Can be used for intranet, extranet, and Internet perimeters.
- ▶ Examines **Layer 3, Layer 4 and Layer 7 protocols.**

CBAC Traffic Inspection

- ▶ Inspect layer 7 packets and maintains TCP and UDP session information, it can detect and prevent certain types of network attacks such as SYN-flooding.
 - ▶ Inspect packet sequence numbers in TCP connections to see if they are within expected ranges and **drops any suspicious packets.**
 - ▶ Drop half-open connections, which **require firewall processing and** memory resources to maintain.
- 

CBAC Intrusion Detection

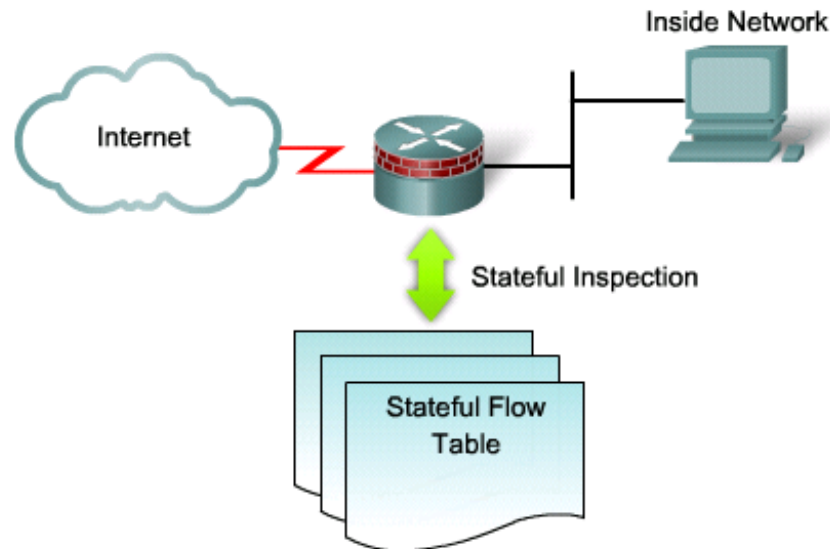
- ▶ Reset the **offending** connections and sends **syslog** information.
 - CBACs can identify certain types of **network attacks** because **they** have specific characteristic or signatures.

CBAC Alert and Audit Generation

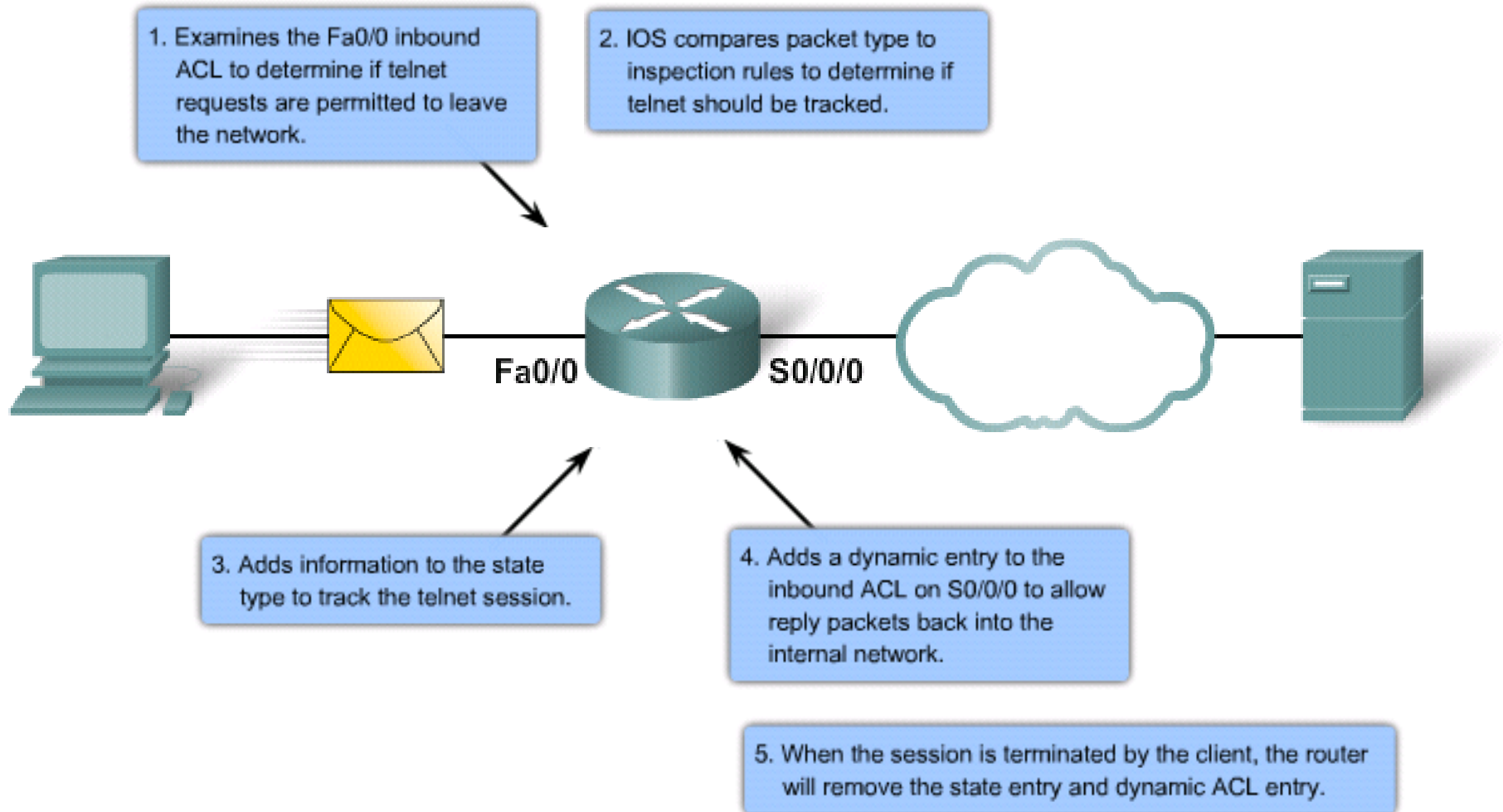
- ▶ *Provide real-time alerts:*
 - Send **syslog error messages to central management** consoles upon detecting suspicious activity.
- ▶ Provide **enhanced audit trail features:**
 - Uses **syslog to track all network transactions and record timestamps to record:**
 - **source and destination hosts**
 - **ports used**
 - **total number of transmitted bytes for advanced session-based reporting.**

How CBACs Work

- ▶ CBAC relies on a **stateful packet filter** that is **application-aware**.
 - The **state table** tracks the sessions and inspects all packets that pass through the stateful packet filter firewall.
 - CBAC then **uses the state table to build dynamic ACL entries** **that** permit returning traffic through the perimeter router or firewall.

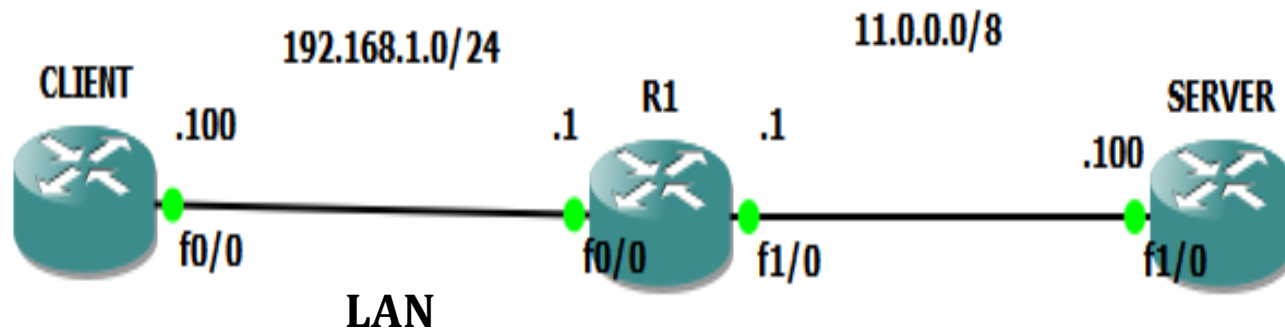


How CBACs Work



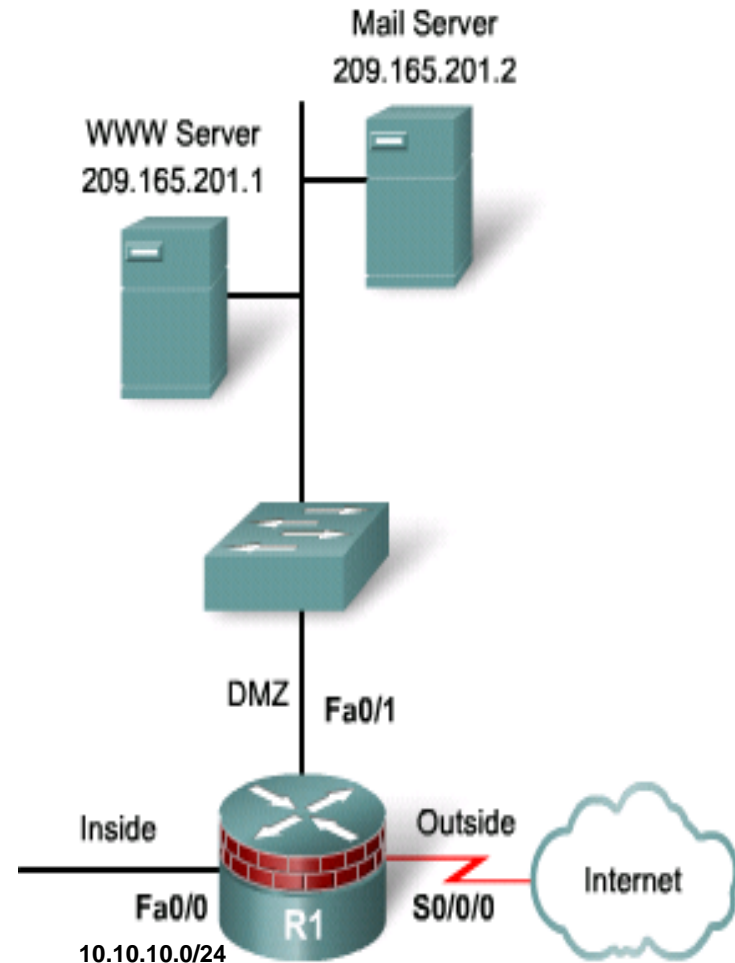
CBAC firewall Lab

- ▶ **Objective:**
- ▶ Configure CBAC firewall on R1 to inspect all TCP, UDP and ICMP traffic sourced from the LAN to the SERVER.



CBAC – Example 1

- ▶ Permit inside users to initiate TCP, UDP, and ICMP traffic with all external sources.
 - Outside clients are allowed to communicate with the SMTP server (209.165.201.1) and HTTP server (209.165.201.2) that are located in the enterprise DMZ.
 - Also permit certain ICMP messages to all interfaces.
 - All other traffic from the external network is denied.



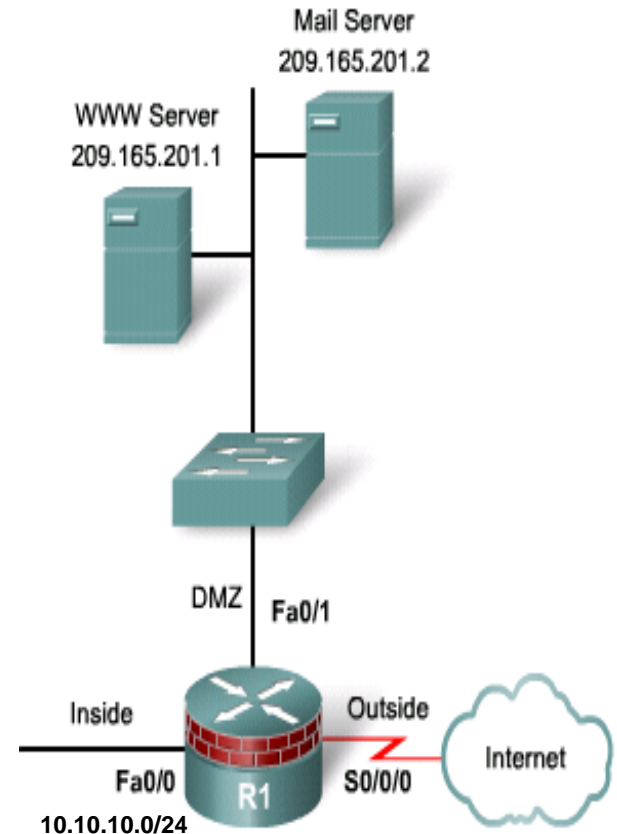
CBAC – Example 1

- ▶ First create an ACL that processes traffic initiating from the internal network prior to leaving the network.
 - Specifically, it allows TCP, UDP, and ICMP sessions and denies all other traffic.

```
R1(config)# access-list 101 permit tcp 10.10.10.0 0.0.0.255 any
R1(config)# access-list 101 permit udp 10.10.10.0 0.0.0.255 any
R1(config)# access-list 101 permit icmp 10.10.10.0 0.0.0.255
any
R1(config)# access-list 101 deny ip any any
```

- ▶ Apply the ACL to the internal interface in the inbound direction.

```
R1(config)# interface Fa0/0
R1(config-if)# ip access-group 101 in
```



CBAC – Example 1

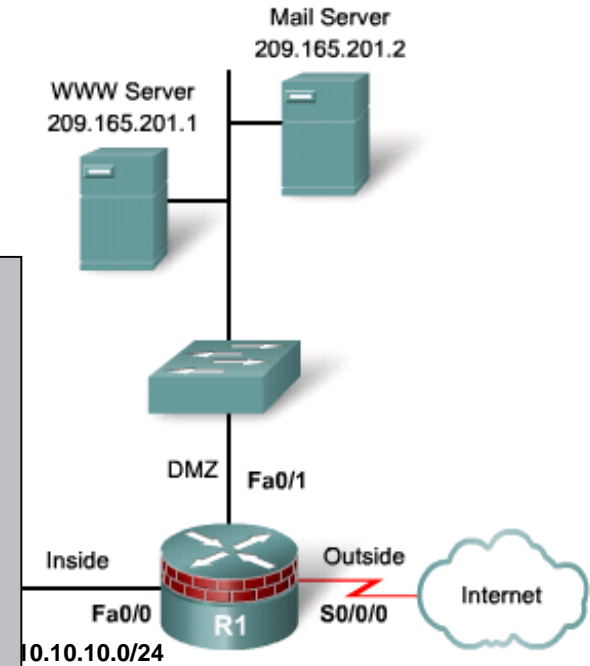
- ▶ Next, create an extended ACL in which SMTP, HTTP, and ICMP traffic is permitted from the external network to the DMZ network only, and all other traffic is denied.

R1(config)#

```
access-list 102 permit tcp any 209.165.201.1 0.0.0.0 eq 80
access-list 102 permit tcp any 209.165.201.2 0.0.0.0 eq smtp
access-list 102 permit icmp any any echo-reply
access-list 102 permit icmp any any unreachable
access-list 102 permit icmp any any administratively-
prohibited
access-list 102 permit icmp any any packet-too-big
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any time-exceeded
access-list 102 deny ip any any
```

- ▶ Apply the ACL to the external interface in the inbound direction.

```
R1(config)# interface S0/0/0
R1(config-if)# ip access-group 102 in
```



CBAC – Example 1

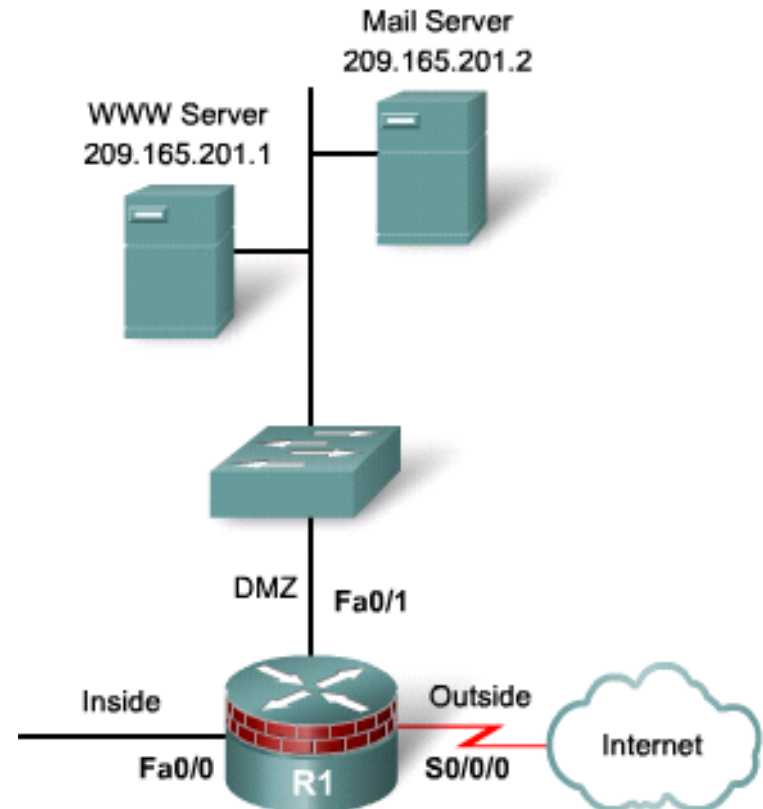
- ▶ Next, create inspection rules for TCP inspection and UDP inspection.
 - Otherwise, all returning traffic, with the exception of ICMP messages, is denied because of the external ACL.

```
R1(config)# ip inspect name MYSITE tcp
R1(config)# ip inspect name MYSITE udp
```

- ▶ Apply the inspection rule in the inbound direction.

```
R1(config)# interface Fa0/0
R1(config-if)# ip inspect MYSITE in
```

- The inspection list automatically creates temporary ACL statements in the inbound ACL applied to the external interface permitting TCP and UDP return traffic.

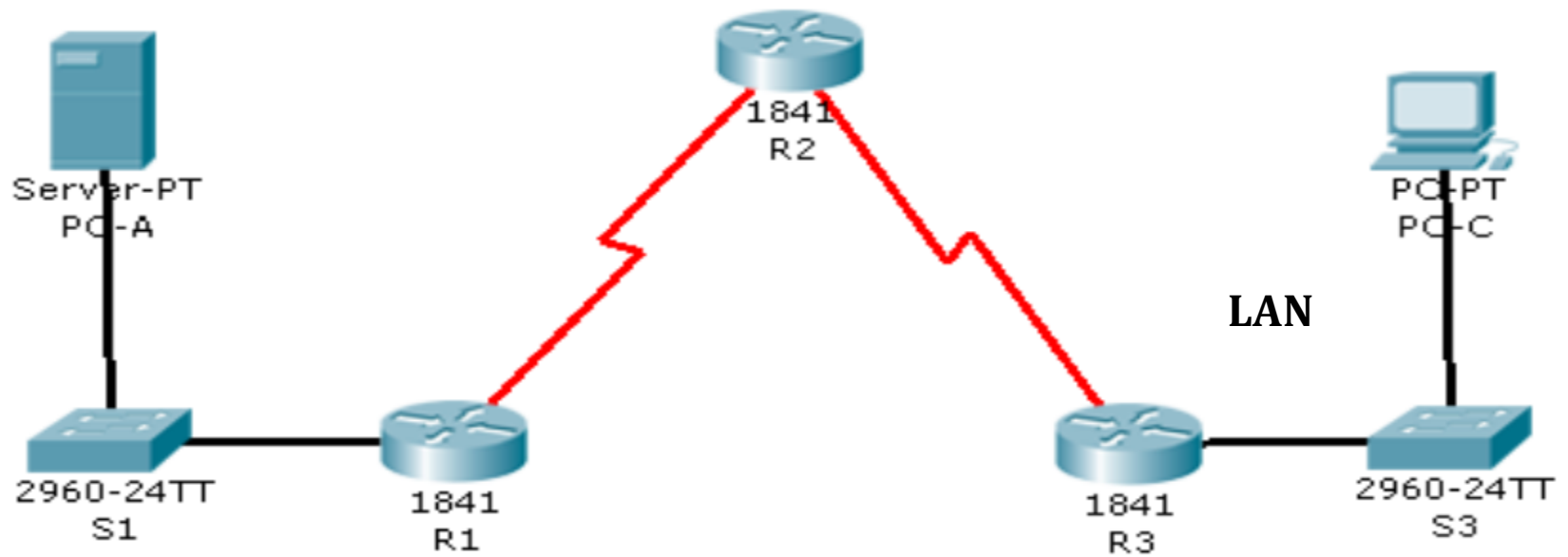


CBAC firewall example Lab2

▶ **Objective:**

- ▶ Apply rip routing.
- ▶ Verify connectivity among devices before firewall configuration.
- ▶ Configure an IOS firewall with CBAC on router R3 so that all traffic from outside is denied expect ping, Telnet and HTTP.
- ▶ Turn on time-stamped logging and CBAC audit trail messages.
- ▶ Verify that audit trail messages are being logged on the syslog SERVER
- ▶ Verify CBAC functionality using ping, Telnet, and HTTP.

CBAC firewall example Lab2



TCP intercept

- ▶ TCP Intercept enables you to deal with **DoS attacks that attempt to take advantage of the weakness in** the way that TCP connections establish a session with the three-way handshake.
- ▶ The attacker sends a flood of TCP SYN segments with **no intention of completing the three-way** handshake for each of these connections.

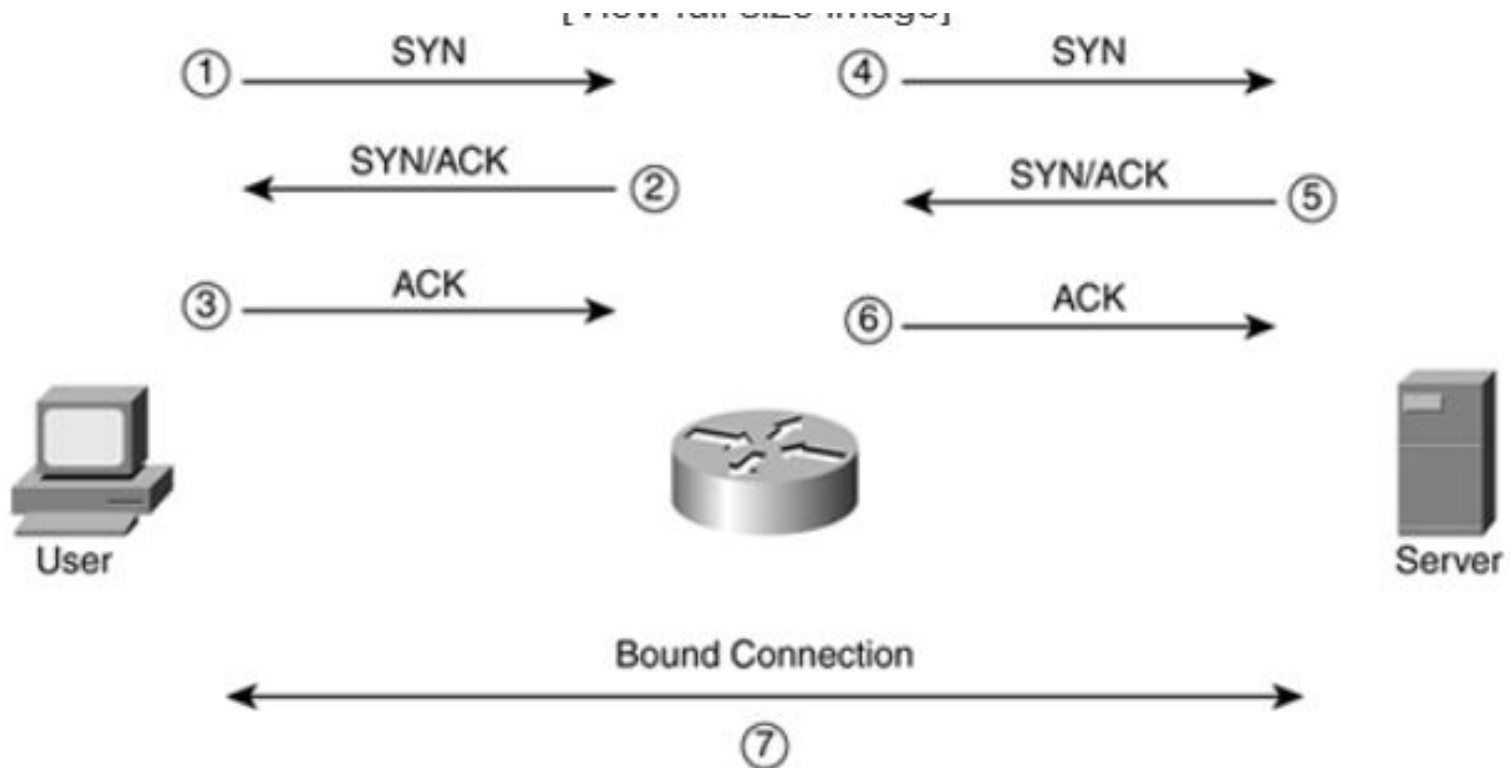
TCP intercept

- ▶ The hacker combines this with **an IP spoofing attack in which the source addresses in the packet are either invalid or someone else's address.**
- ▶ TCP server being attacked hangs in limbo with these **half-open connections.**
- ▶ The server must **wait until the TCP timeout expires** for the connection before removing the connection from its local connection table.

TCP intercept Modes

- ▶ TCP Intercept Modes
- ▶ Intercept Mode:
 - ▶ The router intercepts **all TCP connection requests**
 - ▶ The router pretends to be the internal server, completing the connection to the external user.
 - ▶ Only upon a successful three-way handshake with the external user

TCP intercept Modes



TCP intercept Modes

- ▶ This process is **transparent** to the two devices that make up the final TCP connection.
- ▶ The router using TCP because **provides a buffer to the internal servers.**
- ▶ The router deals with the half-open connections, which **time out and are removed from the router's TCP connection table.**
- ▶ The router sends an **RST** to the requesting source device.

TCP intercept Modes

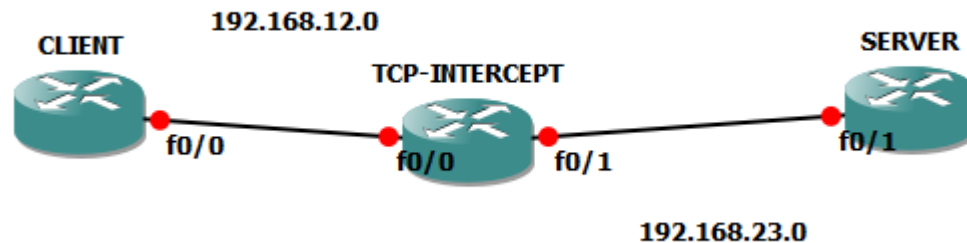
- ▶ **Watch Mode**
- ▶ Intercept Mode → **removes the processing load of TCP SYN floods from the internal server.**
- ▶ The router still is performing the intercept process, **placing a heavy burden on it.**
- ▶ *In watch mode*, the router **passively** watches the setup of TCP connections **from users to servers.**
- ▶ It monitors these connections, **keeping track of** embryonic connections that remain in this limbo state.

TCP intercept Modes

- ▶ Router compares this value to a **preconfigured timeout value** (which defaults to 30 seconds).
- ▶ If a TCP connection does not complete the three-way handshake in this period, the Cisco IOS sends a **TCP reset to the server to remove the connection.**

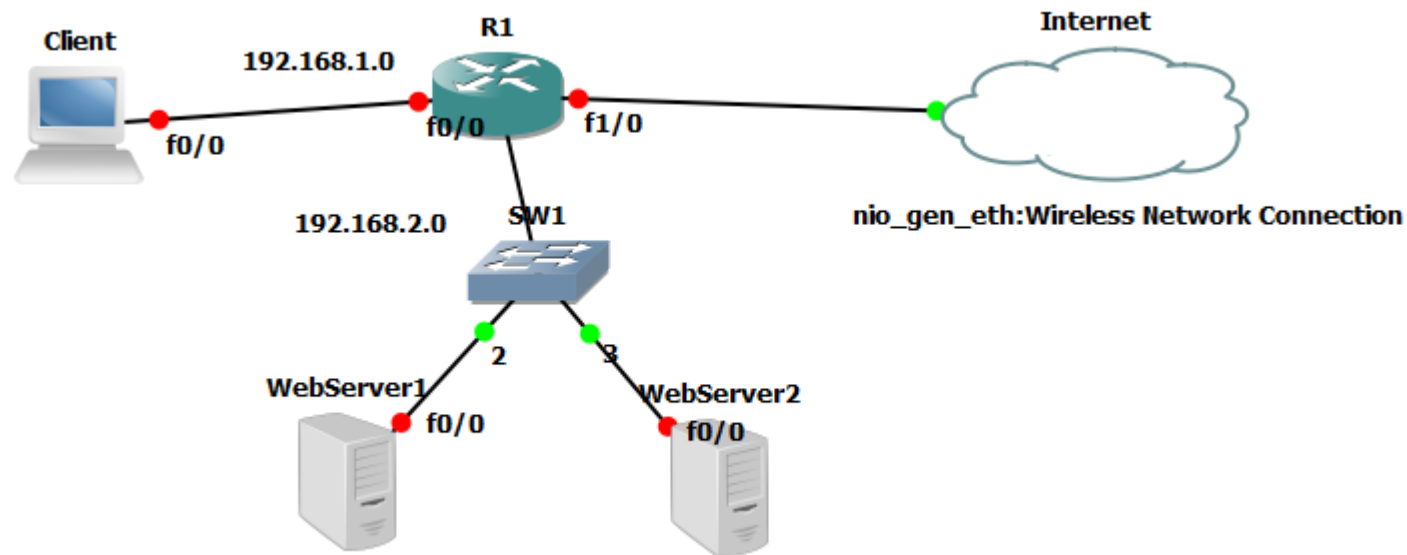
TCP intercept Lab

- ▶ OSPF has been preconfigured for you on all routers.
- ▶ Configure router **TCP-INTERCEPT** so it resets all connections that don't finish the TCP 3 way handshake within 10 seconds by sending a RST to router SERVER.



TCP intercept Lab2

- ▶ In this network, the administrator is concerned about TCP SYN flood attacks against the web servers located in the DMZ. To deal with TCP SYN flood attacks, the administrator has decided to use TCP Intercept in watch mode to monitor connections.



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>