Redes de Computadores - RECOMP

ACLs

Lab Topology:

The lab network topology is illustrated below:

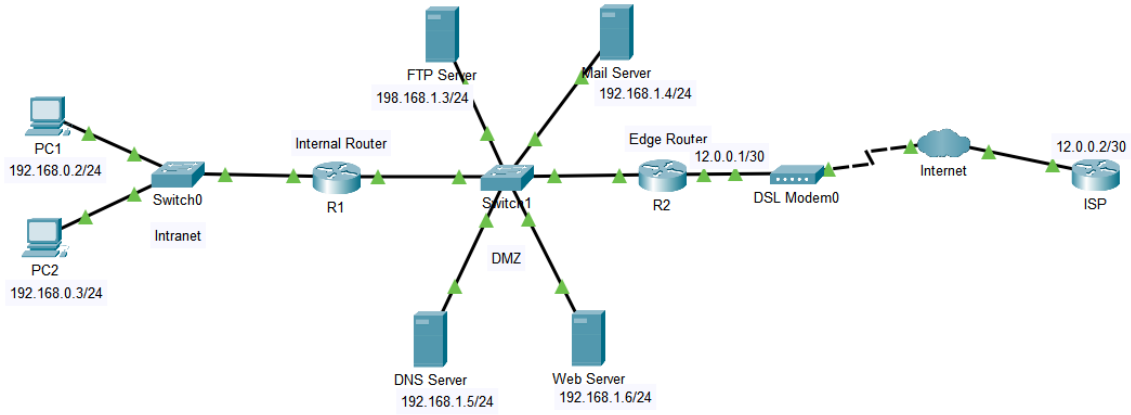

Figure 1- Lab Topology

Objectives

Part 1: Plan an ACL Implementation
Part 2: Configure the ACLs
Part 3: Verify the ACLs

Instructions

Part 1: Plan an ACL Implementation

Step 1: Spoofing

All IP spoofing must be blocked, if possible.

Step 2: The INTRANET

a) All network nodes of the network (192.168.0.0/24) may access HTTP service, the DNS service, the FTP service, and the email service of the DMZ. Response traffic must also be allowed.
b) All network nodes of the network (192.168.0.0/24) may access HTTP service (TCP/80) on every internet node. Response traffic must also be allowed.
c) Nodes 192.168.0.2 and 192.168.0.3 may send ICMP echo requests to every internet node. Response traffic must also be allowed.

Step 3: The INTERNET

a) May access HTTP service (TCP/80) on the Web Server. Response traffic must also be allowed.
b) May access DNS service (UDP/53) on The DNS Server. Response traffic must also be allowed.

c) May access FTP service (FTP/21) on The FTP Server. Response traffic must also be allowed.
d) May access Email service (SMTP/POP3) on The Email Server. Response traffic must also be allowed.
e) May send ICMP echo requests to node 192.168.1.6. Response traffic must also be allowed.

Step 4: The DMZ

a) Node 192.168.1.5 may access the DNS service (UDP/53) on every internet node. Response traffic must also be allowed.
b) All other traffic is to be blocked.

Part 2: Configure the ACLs

Step 1: R1 – Interface Gig0/0 – Inbound (INTRANET)

a) Delete the ACL, if exists.

```
no access-list 100
```

b) All network nodes of the network (192.168.0.0/24) may access HTTP service, the DNS service, the FTP service, and the email service of the DMZ. Response traffic must also be allowed.
c) All network nodes of the network (192.168.0.0/24) may access HTTP service (TCP/80) on every internet node. Response traffic must also be allowed.

```
access-list 100 permit tcp 192.168.0.0 0.0.0.255 host 192.168.1.6 eq 80
access-list 100 deny tcp any 192.168.1.0 0.0.0.255 eq 80
access-list 100 permit tcp 192.168.0.0 0.0.0.255 any eq 80
access-list 100 permit udp 192.168.0.0 0.0.0.255 host 192.168.1.5 eq 53
access-list 100 permit tcp any host 192.168.1.4 eq smtp
access-list 100 permit tcp any host 192.168.1.4 eq pop3
access-list 100 permit tcp any host 192.168.1.3 eq ftp
```

d) Nodes 192.168.0.2 and 192.168.0.3 may send ICMP echo requests to every internet node except to the DMZ. Response traffic must also be allowed.

```
access-list 100 deny icmp any 192.168.1.0 0.0.0.255 echo
access-list 100 permit icmp 192.168.0.2 0.0.0.3 any echo
```

Step 2: R1 – Interface Gig0/1 – Inbound (DMZ)

a) Delete the ACL, if exists.

```
no access-list 105
```

b) Block external spoofing.

```
access-list 105 deny ip 192.168.0.0 0.0.0.255 any
```

c) Allows response traffic for every HTTP, DNS, FTP and Email access.

```
access-list 105 permit tcp any eq 80 192.168.0.0 0.0.0.255 established
access-list 105 permit udp host 192.168.1.5 eq 53 192.168.0.0 0.0.0.255
access-list 105 permit tcp any eq smtp any established
access-list 105 permit tcp any eq pop3 any established
access-list 105 permit tcp any host 192.168.1.4 eq pop3
access-list 105 permit tcp any host 192.168.1.3 eq ftp
access-list 105 permit tcp host 192.168.1.3 eq ftp any established
```

d) Block all other traffic from DMZ.

```
access-list 105 deny ip 192.168.1.0 0.0.0.255 any
```

e) Allow ICMP echo replies to nodes 192.168.0.2 and 192.168.0.3

```
access-list 105 permit icmp any 192.168.0.2 0.0.0.3 echo-reply
```

Step 3: R2 – Interface Gig0/0 – Inbound (DMZ)

a) Delete the ACL, if exists.

```
no access-list 100
```

b) Allows response traffic for every HTTP, DNS (responses and requests), FTP and Email access.

```
access-list 100 permit tcp 192.168.0.0 0.0.1.255 eq 80 any established
access-list 100 permit udp host 192.168.1.5 eq 53 any
access-list 100 permit udp host 192.168.1.5 any eq 53
access-list 100 permit tcp any eq smtp any established
access-list 100 permit tcp any eq pop3 any established
access-list 100 permit tcp host 192.168.1.3 eq ftp any established
```

c) Allow ICMP echo replies from nodes

```
access-list 100 permit icmp 192.168.0.2 0.0.0.3 any echo-reply
```

d) Block all other traffic from DMZ

```
access-list 100 deny ip 192.168.1.0 0.0.0.255 any
```

e) Allow HTTP access from intranet

```
access-list 100 permit tcp 192.168.0.0 0.0.0.255 any eq 80
```

f) Allow ICMP echo requests from nodes 192.168.0.2 and 192.168.0.3.

```
access-list 100 permit icmp 192.168.0.2 0.0.0.3 any echo
```

Step 4: Router 2 – Interface Gig0/1 – Inbound (INTERNET)

a) Delete the ACL, if exists.

```
no access-list 110
```

b) Block external spoofing.

```
access-list 110 deny ip 192.168.0.0 0.0.1.255 any
```

g) Allow HTTP access to HTTP, DNS (responses and requests), FTP and Email access.

```
access-list 110 permit tcp any host 192.168.1.6 eq 80
access-list 110 permit udp any host 192.168.1.5 eq 53
access-list 110 permit udp any eq 53 host 192.168.1.5
access-list 110 permit tcp any host 192.168.1.4 eq smtp
access-list 110 permit tcp any eq smtp any established
access-list 110 permit tcp any host 192.168.1.4 eq pop3
access-list 110 permit tcp any eq pop3 any established
access-list 110 permit tcp any host 192.168.1.3 eq ftp
```

c) Allow ICMP echo requests to Web server

```
access-list 110 permit icmp any host 192.168.1.6 echo
```

d) Block all other traffic to the DMZ.

```
access-list 110 deny ip any 192.168.1.0 0.0.0.255
```

e) Allow HTTP response traffic to all INTRANET nodes

```
access-list 110 permit tcp any eq 80 192.168.0.0 0.0.0.255 established
```

f) Allow ICMP echo replies to nodes 192.168.0.2 and 192.168.0.3.

```
access-list 110 permit icmp any 192.168.0.2 0.0.0.3 echo-reply
```

Step 5: Deploy defined access lists.

R1:

```
interface Gig0/0
ip access-group 100 in
interface Gig0/1
ip access-group 105 in
```

R2:

```
interface Gig0/0
ip access-group 100 in
interface Gig0/1
ip access-group 110 in
```

Part 3: Verify the ACLs

Step 1: Access services from PCs

a) Try to access FTP, open the command prompt, and type ftp 192.168.1.3. There is a login and password by default (login: cisco, password: cisco).
b) Try to access the email. Both PCs have an email account configured. PC1 (email: admin@mail.com, password: admin), PC2 (email: user1@mail.com, password: user1) and PC0 (email: user1@mail.com, password: user1). Try to send an email from one account and receive it in the other.
c) If the Email worked the DNS was also tested, because email uses the DNS to discover the domain (mail.com)
d) Open a browser and try to access the web server http://192.168.1.6
e) Try to ping PC0, and the DMZ.