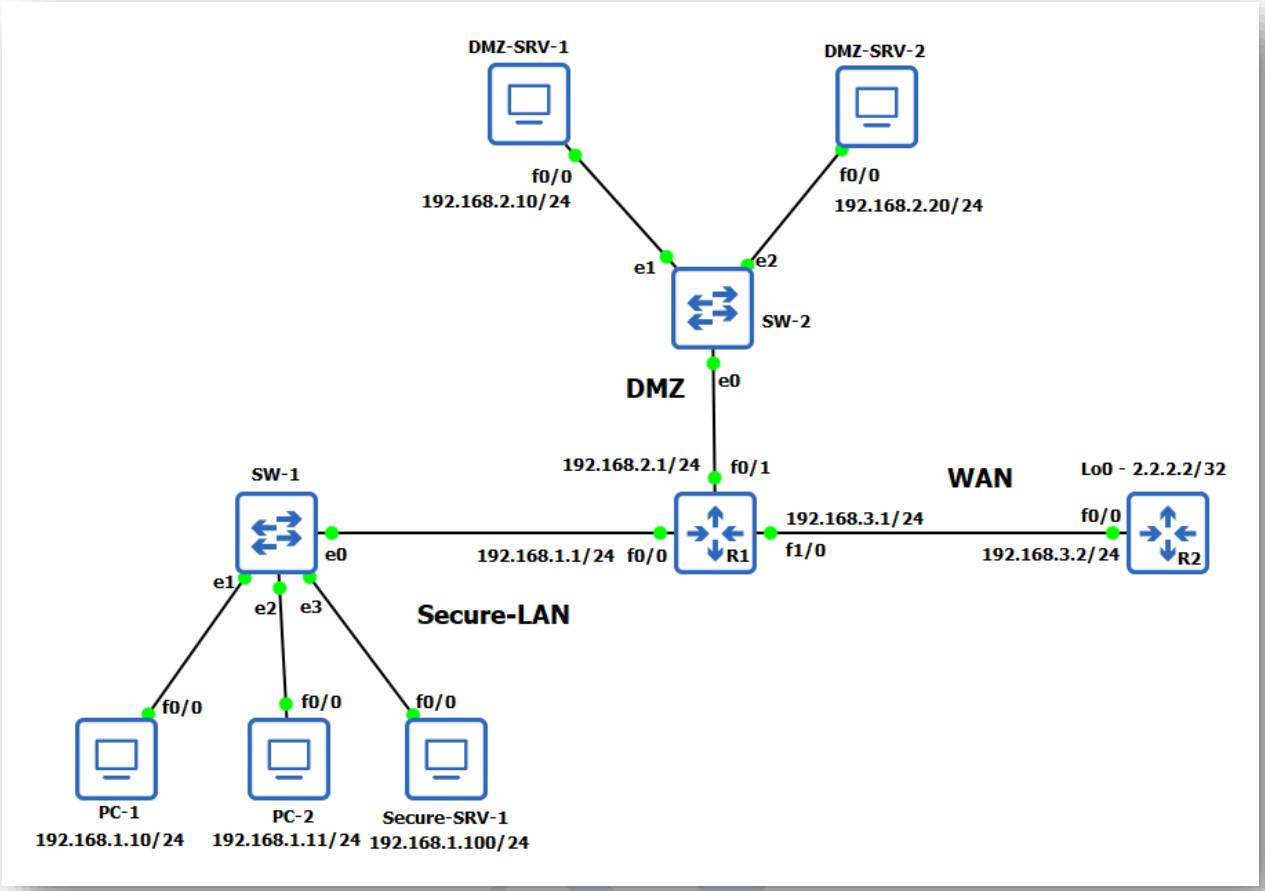
Standard ACL – Number & Named



Task

1. Configure routers R1 & R2 with IP address as shown in topology and configure enable password as **ccna**.
2. Configure routers as Host (PC / Servers)
3. On Secure-SRV-1, enable SSH and HTTPs service on port 1025.
4. On DMZ-SRV-1 & DMZ-SRV-1, enable SSH and HTTP service.
5. Configure default routing to provide connectivity between them.
6. Configure standard number ACL to block access to R2 network from Secure-LAN and DMZ-SRV-2
7. Configure standard name ACL to block access to Secure-LAN from DMZ.

Task-1: Configure R1 and R2 with IP address.

R1 Router Configuration:

```
R1#config t
R1(config)#no ip domain-lookup
R1(config)#enable password ccna
R1(config)#int fa0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut
```

```
R1(config-if)#description Link to Secure-LAN
R1(config-if)#exit
R1(config)#int fa0/1
R1(config-if)#ip address 192.168.2.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#description Link to DMZ
R1(config-if)#exit
R1(config)#int fa1/0
R1(config-if)#ip address 192.168.3.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#description Link to R2 on fa0/0
R1(config-if)#exit
R1(config)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exec-timeout 1 0
R1(config-line)#exit
R1(config)#exit
R1#
```

R2 Router Configuration:

```
R2#config t
R2(config)#no ip domain-lookup
R2(config)#enable password ccna
R2(config)#int fa0/0
R2(config-if)#ip address 192.168.3.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#description Link to R1 on fa1/0
R2(config-if)#exit
R2(config)#int lo0
R2(config-if)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#exit
R2(config)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#logging synchronous
R2(config-line)#exec-timeout 1 0
R2(config-line)#exit
R2(config)#exit
R2#
```

Task-2: Configure routers as Host (PC / Servers)

Router as Secure-SRV-1 Configuration:

```
Secure-SRV-1#config t
Secure-SRV-1(config)#no ip domain-lookup
Secure-SRV-1(config)#no ip routing
Secure-SRV-1(config)#ip default-gateway 192.168.1.1
```

We Make Learning Simplified..

```
Secure-SRV-1(config)#int fa0/0
Secure-SRV-1(config-if)#ip address 192.168.1.100 255.255.255.0
Secure-SRV-1(config-if)#no shut
Secure-SRV-1(config-if)#description Secure-SRV-1
Secure-SRV-1(config-if)#exit
Secure-SRV-1(config)#exit
Secure-SRV-1#
```

Router as DMZ-SRV-1 Configuration:

```
DMZ-SRV-1#config t
DMZ-SRV-1(config)#no ip domain-lookup
DMZ-SRV-1(config)#no ip routing
DMZ-SRV-1(config)#ip default-gateway 192.168.2.1
DMZ-SRV-1(config)#int fa0/0
DMZ-SRV-1(config-if)#ip address 192.168.2.10 255.255.255.0
DMZ-SRV-1(config-if)#no shut
DMZ-SRV-1(config-if)#description DMZ-SRV-1
DMZ-SRV-1(config-if)#exit
DMZ-SRV-1(config)#exit
DMZ-SRV-1#
```

Router as DMZ-SRV-2 Configuration:

```
DMZ-SRV-2#config t
DMZ-SRV-2(config)#no ip domain-lookup
DMZ-SRV-2(config)#no ip routing
DMZ-SRV-2(config)#ip default-gateway 192.168.2.1
DMZ-SRV-2(config)#int fa0/0
DMZ-SRV-2(config-if)#ip address 192.168.2.20 255.255.255.0
DMZ-SRV-2(config-if)#no shut
DMZ-SRV-2(config-if)#description DMZ-SRV-2
DMZ-SRV-2(config-if)#exit
DMZ-SRV-2(config)#exit
DMZ-SRV-2#
```

Router as PC-1 Configuration:

```
PC-1#config t
PC-1(config)#no ip domain-lookup
PC-1(config)#no ip routing
PC-1(config)#ip default-gateway 192.168.1.1
PC-1(config)#int fa0/0
PC-1(config-if)#ip address 192.168.1.10 255.255.255.0
PC-1(config-if)#no shut
PC-1(config-if)#description PC-1
PC-1(config-if)#exit
PC-1(config)#exit
PC-1#
```

Ratan

info@rsatechforum.in

Router as PC-2 Configuration:

```
PC-2#config t
PC-2(config)#no ip domain-lookup
PC-2(config)#no ip routing
PC-2(config)#ip default-gateway 192.168.1.1
PC-2(config)#int fa0/0
PC-2(config-if)#ip address 192.168.1.11 255.255.255.0
PC-2(config-if)#no shut
PC-2(config-if)#description PC-2
PC-2(config-if)#exit
PC-2(config)#exit
PC-2#
```

✓ Verification & Testing:

```
R1#sh ip int brief | exclude unassign
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.1.1     YES manual up                    up
FastEthernet0/1        192.168.2.1     YES manual up                    up
FastEthernet1/0        192.168.3.1     YES manual up                    up

R2#sh ip int brief | exclude unassign
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.3.2     YES manual up                    up
Loopback0              2.2.2.2         YES manual up                    up
```

Task-3: On Secure-SRV-1, enable SSH and HTTPs service on port 1025.

```
Secure-SRV-1#config t
Secure-SRV-1(config)#enable password ccna
Secure-SRV-1(config)#username user1 secret pass1
Secure-SRV-1(config)#ip domain-name rsatechforum.in
Secure-SRV-1(config)#crypto key generate rsa modulus 1024
The name for the keys will be: Secure-SRV-1.rsatechforum.in

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)
*Oct 30 12:47:28.587: %SSH-5-ENABLED: SSH 1.99 has been enabled

Secure-SRV-1(config)#ip http secure-server
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)
Failed to generate persistent self-signed certificate.
    Secure server will use temporary self-signed certificate.

Secure-SRV-1(config)#ip http secure-port 1025
Secure-SRV-1(config)#ip http secure-client-auth
Secure-SRV-1(config)#line vty 0 15
Secure-SRV-1(config-line)#login local
Secure-SRV-1(config-line)#transport input ssh
```

We Make Learning Simplified..

```
Secure-SRV-1(config-line)#exit
Secure-SRV-1(config)#exit
Secure-SRV-1#
```

Task-4: On DMZ-SRV-1 & DMZ-SRV-1, enable SSH and HTTP service.

DMZ-SRV-1 configuration:

```
DMZ-SRV-1#config t
DMZ-SRV-1(config)#enable password ccna
DMZ-SRV-1(config)#username user1 secret pass1
DMZ-SRV-1(config)#ip domain-name rsatechforum.in
DMZ-SRV-1(config)#crypto key generate rsa modulus 1024
The name for the keys will be: DMZ-SRV-1.rsatechforum.in

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

*Oct 30 12:51:41.539: %SSH-5-ENABLED: SSH 1.99 has been enabled

DMZ-SRV-1(config)#ip http server
DMZ-SRV-1(config)#ip http secure-client-auth
DMZ-SRV-1(config)#
DMZ-SRV-1(config)#line vty 0 15
DMZ-SRV-1(config-line)#login local
DMZ-SRV-1(config-line)#transport input ssh
DMZ-SRV-1(config-line)#exit
DMZ-SRV-1(config)#exit
DMZ-SRV-1#
```

DMZ-SRV-2 configuration:

```
DMZ-SRV-2#config t
DMZ-SRV-2(config)#enable password ccna
DMZ-SRV-2(config)#username user1 secret pass1
DMZ-SRV-2(config)#ip domain-name rsatechforum.in
DMZ-SRV-2(config)#crypto key generate rsa modulus 1024
The name for the keys will be: DMZ-SRV-2.rsatechforum.in

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

*Oct 30 12:52:28.435: %SSH-5-ENABLED: SSH 1.99 has been enabled

DMZ-SRV-2(config)#ip http secure-server
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)
Failed to generate persistent self-signed certificate.
    Secure server will use temporary self-signed certificate.
DMZ-SRV-2(config)#ip http secure-client-auth
```

Ratan

info@rsatechforum.in

```
DMZ-SRV-2(config)#line vty 0 15
DMZ-SRV-2(config-line)#login local
DMZ-SRV-2(config-line)#transport input ssh
DMZ-SRV-2(config-line)#exit
DMZ-SRV-2(config)#exit
DMZ-SRV-2#
```

Task-5: Configure default routing to provide connectivity between R1 & R2.

R1 Configuration:

```
R1#config t
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.3.2
R1(config)#exit
R1#
```

R2 Configuration:

```
R2#config t
R2(config)#ip route 0.0.0.0 0.0.0.0 192.168.3.1
R2(config)#exit
R2#
```

✓ Verification & Testing:

R1#sh ip route static

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.3.2 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.3.2
R1#
```

R2#sh ip route static

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.3.1 to network 0.0.0.0
```

We Make Learning Simplified..

S* 0.0.0.0/0 [1/0] via 192.168.3.1
R2#

Ping R2's Loopback IP from R1

R1#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/16/20 ms

Ping all PCs and Servers IP from R2

R2#ping 192.168.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 28/40/64 ms

R2#ping 192.168.1.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.11, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 20/27/32 ms

R2#ping 192.168.1.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.100, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 12/35/56 ms

R2#ping 192.168.2.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 28/34/44 ms

R2#ping 192.168.2.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.20, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 12/31/40 ms

Ping DMZ servers and R2's loopback from PC-1

PC-1#ping 192.168.2.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/40/40 ms

Ratan

info@rsatechforum.in

PC-1#ping 192.168.2.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/40/44 ms

PC-1#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/39/40 ms

Ping DMZ servers and R2's loopback from PC-2

PC-2#ping 192.168.2.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/18/24 ms

PC-2#ping 192.168.2.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/40/64 ms

PC-2#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/40/44 ms

Ping DMZ servers and R2's loopback from Secure-SRV-1

Secure-SRV-1#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/40/40 ms

Secure-SRV-1#ping 192.168.2.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/39/44 ms

Secure-SRV-1#ping 192.168.2.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/40/64 ms

We Make Learning Simplified..

Ping Secure-LAN PCs, Server R2's loopback from DMZ-SRV-1

DMZ-SRV-1#ping 192.168.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/40/44 ms

DMZ-SRV-1#ping 192.168.1.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/40/44 ms

DMZ-SRV-1#ping 192.168.1.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/39/44 ms

DMZ-SRV-1#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/40/44 ms

Ping Secure-LAN PCs, Server R2's loopback from DMZ-SRV-2

DMZ-SRV-2#ping 192.168.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/27/40 ms

DMZ-SRV-2#ping 192.168.1.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/25/32 ms

DMZ-SRV-2#ping 192.168.1.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/40/44 ms

DMZ-SRV-2#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!

Ratan

info@rsatechforum.in

Success rate is 100 percent (5/5), round-trip min/avg/max = 40/40/44 ms
DMZ-SRV-2#

Test the HTTP and HTTPs services of Servers from R2

R2#telnet 192.168.1.100 443
Trying 192.168.1.100, 443 ...
% Connection refused by remote host

R2#telnet 192.168.1.100 1025
Trying 192.168.1.100, 1025 ... Open

R2#telnet 192.168.2.10 443
Trying 192.168.2.10, 443 ...
% Connection refused by remote host

R2#telnet 192.168.2.10 80
Trying 192.168.2.10, 80 ... Open

R2#telnet 192.168.2.20 80
Trying 192.168.2.20, 80 ...
% Connection refused by remote host

R2#telnet 192.168.2.20 443
Trying 192.168.2.20, 443 ... Open

Test the HTTP and HTTPs services of Servers from Secure-SRV-1

Secure-SRV-1#telnet 192.168.2.10 443
Trying 192.168.2.10, 443 ...
% Connection refused by remote host

Secure-SRV-1#telnet 192.168.2.10 80
Trying 192.168.2.10, 80 ... Open

Secure-SRV-1#telnet 192.168.2.20 80
Trying 192.168.2.20, 80 ...
% Connection refused by remote host

Secure-SRV-1#telnet 192.168.2.20 443
Trying 192.168.2.20, 443 ... Open

Task-6: Configure standard number ACL to block access to R2 network from Secure-LAN and DMZ-SRV-2

Source: Secure-LAN & DMZ-SRV-2
Destination: R2 network
Implementation: R2 (Close to destination)
Traffic inspection: Inbound traffic

We Make Learning Simplified..

```
R2#config t
R2(config)#access-list 10 deny 192.168.1.0 0.0.0.255 log
R2(config)#access-list 10 deny host 192.168.2.20 log
R2(config)#access-list 10 permit any
R2(config)#int fa0/0
R2(config-if)#ip access-group 10 in
R2(config-if)#exit
R2(config)#exit
R2#
```

✓ Verification & Testing:

R2#sh access-lists

```
Standard IP access list 10
    20 deny   192.168.2.20 log (5 matches)
    10 deny   192.168.1.0, wildcard bits 0.0.0.255 log (17 matches)
    30 permit any (10 matches)
R2#
```

Ping the R2's loopback IP from PCs and servers of Secure-LAN & DMZ network

PC-1#ping 2.2.2.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
```

PC-2#ping 2.2.2.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
```

Secure-SRV-1#ping 2.2.2.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
```

DMZ-SRV-1#ping 2.2.2.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/27/32 ms
```

DMZ-SRV-2#ping 2.2.2.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
```

Ratan

info@rsatechforum.in

R2#
*Oct 30 13:34:21.255: %SYS-5-CONFIG_I: Configured from console by console
*Oct 30 13:34:59.319: %SEC-6-IPACCESSLOGNP: list 10 denied 0 192.168.1.10 -> 2.2.2.2, 1 packet
*Oct 30 13:35:14.839: %SEC-6-IPACCESSLOGNP: list 10 denied 0 192.168.1.11 -> 2.2.2.2, 1 packet
*Oct 30 13:35:22.479: %SEC-6-IPACCESSLOGNP: list 10 denied 0 192.168.1.100 -> 2.2.2.2, 1 packet
*Oct 30 13:35:36.479: %SEC-6-IPACCESSLOGNP: list 10 denied 0 192.168.2.20 -> 2.2.2.2, 1 packet

Ping IP of PCs and servers of Secure-LAN & DMZ network from R2

R2#ping 192.168.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:

*Oct 30 20:02:27.603: %SEC-6-IPACCESSLOGNP: list 10 denied 0 192.168.1.10 -> 192.168.3.2, 1 packet
.....
Success rate is 0 percent (0/5)

R2#ping 192.168.1.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.11, timeout is 2 seconds:

*Oct 30 20:03:01.299: %SEC-6-IPACCESSLOGNP: list 10 denied 0 192.168.1.11 -> 192.168.3.2, 1 packet
.....
Success rate is 0 percent (0/5)

R2#ping 192.168.1.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.100, timeout is 2 seconds:
*Oct 30 20:03:50.039: %SEC-6-IPACCESSLOGNP: list 10 denied 0 192.168.1.100 -> 192.168.3.2, 5 packets
.....
Success rate is 0 percent (0/5)

R2#ping 192.168.2.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/34/56 ms

R2#ping 192.168.2.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.20, timeout is 2 seconds:
*Oct 30 20:04:50.039: %SEC-6-IPACCESSLOGNP: list 10 denied 0 192.168.2.20 -> 192.168.3.2, 5 packets
.....
Success rate is 0 percent (0/5)
R2#

To remove the ACL:

R2#config t
R2(config)#no access-list 10

We Make Learning Simplified..

```
R2(config)#int fa0/0
R2(config-if)#no ip access-group 10 in
R2(config-if)#exit
R2(config)#exit
R2#
```

Task-7: Configure standard name ACL to block access to Secure-LAN from DMZ.

Source: DMZ network
Destination: Secure-LAN network
Implementation: R1 (Close to destination)
Traffic inspection: Outbound traffic

```
R1#config t
R1(config)#ip access-list standard MyACL
R1(config-std-nacl)#deny 192.168.2.0 0.0.0.255 log
R1(config-std-nacl)#permit any
R1(config-std-nacl)#exit
R1(config)#int fa0/0
R1(config-if)#ip access-group MyACL out
R1(config-if)#exit
R1(config)#exit
R1#
```

✓ Verification & Testing:

R1#sh access-lists

```
Standard IP access list MyACL
    10 deny   192.168.2.0, wildcard bits 0.0.0.255 log
    20 permit any
R1#
```

Ping R2's loopback IP and Secure-LAN's PCs & Server from DMZ's servers

DMZ-SRV-1#ping 2.2.2.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/40/44 ms
```

DMZ-SRV-1#ping 192.168.1.10

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
```

DMZ-SRV-1#ping 192.168.1.11

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.11, timeout is 2 seconds:
```

UUUUU
Success rate is 0 percent (0/5)

DMZ-SRV-1#ping 192.168.1.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.100, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)

*Oct 30 20:52:47.055: %SEC-6-IPACCESSLOGNP: list MyACL denied 0 192.168.2.10 -> 192.168.1.10, 5 packets
*Oct 30 20:52:47.055: %SEC-6-IPACCESSLOGNP: list MyACL denied 0 192.168.2.10 -> 192.168.1.11, 5 packets
*Oct 30 20:52:47.059: %SEC-6-IPACCESSLOGNP: list MyACL denied 0 192.168.2.10 -> 192.168.1.100, 5 packets

DMZ-SRV-2#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/40/44 ms

DMZ-SRV-2#ping 192.168.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)

DMZ-SRV-2#ping 192.168.1.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.11, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)

DMZ-SRV-2#ping 192.168.1.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.100, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)

*Oct 30 20:53:51.003: %SEC-6-IPACCESSLOGNP: list MyACL denied 0 192.168.2.20 -> 192.168.1.10, 1 packet
*Oct 30 20:53:53.763: %SEC-6-IPACCESSLOGNP: list MyACL denied 0 192.168.2.20 -> 192.168.1.11, 1 packet
*Oct 30 20:53:57.171: %SEC-6-IPACCESSLOGNP: list MyACL denied 0 192.168.2.20 -> 192.168.1.100, 1 packet

Test HTTPs and telnet access to Secure-LAN network from DMZ-SRV-1

DMZ-SRV-1#telnet 192.168.1.100 1025
Trying 192.168.1.100, 1025 ...
% Destination unreachable; gateway or host down

We Make Learning Simplified..

DMZ-SRV-1#
DMZ-SRV-1#telnet 192.168.1.10
Trying 192.168.1.10 ...
% Destination unreachable; gateway or host down

DMZ-SRV-1#telnet 192.168.1.11
Trying 192.168.1.11 ...
% Destination unreachable; gateway or host down

Test HTTPs and telnet access to Secure-LAN network from DMZ-SRV-2

DMZ-SRV-2#telnet 192.168.1.100 1025
Trying 192.168.1.100, 1025 ...
% Destination unreachable; gateway or host down

DMZ-SRV-2#telnet 192.168.1.10
Trying 192.168.1.10 ...
% Destination unreachable; gateway or host down

DMZ-SRV-2#telnet 192.168.1.11
Trying 192.168.1.11 ...
% Destination unreachable; gateway or host down

To Remove ACL

R1#config t
R1(config)#no ip access-list standard MyACL
R1(config)#int fa0/0
R1(config-if)#no ip access-group MyACL out
R1(config-if)#exit
R1#

Ratan

info@rsatechforum.in

Important Commands:

sh access-lists
sh ip access-lists

Ratan