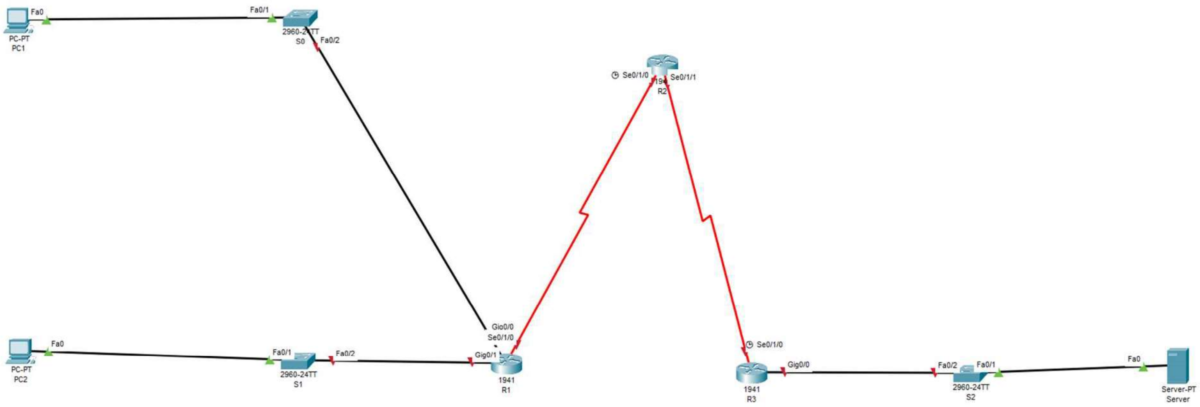
Black – CONFIG line code

Purple – PC Command Prompt line code

Green – Router# command line code

# CONFIGURE IPv6 ACL TO MITIGATE ATTACKS

Topology:



Addressing Table:

| Device | Interface | IP Address | Default Gateway |
|---|---|---|---|
| PC1 | NIC | 2001:DB8:1:10::10/64 | FE80::1 |
| PC2 | NIC | 2001:DB8:1:11::11/64 | FE80::1 |
| R1 | gig 0/0 | 2001:DB8:1:10::1/64 | FE80::1 |
| R1 | se 0/1/0 | 2001:DB8:1:1::1/64 | FE80::1 |
| R1 | gig 0/1 | 2001:DB8:1:11::1/64 | FE80::1 |
| R2 | se 0/1/0 | 2001:DB8:1:1::2/64 | FE80::2 |
| R2 | se 0/1/1 | 2001:DB8:1:2::2/64 | FE80::2 |
| R3 | gig 0/0 | 2001:DB8:1:30::1/64 | FE80::3 |
| R3 | se 0/1/0 | 2001:DB8:1:2::1/64 | FE80::3 |
| Server | NIC | 2001:DB8:1:30::30/64 | FE80::3 |

Objective:

1. Configure, apply and verify an IPv6 ACL
2. Configure, apply and verify a second IPv6 ACL

Black – CONFIG line code
Purple – PC Command Prompt line code
Green – Router# command line code

## Part 1: CONFIGURE ROUTER

(Execute command on all routers)

Step 1: configure secret password on router

```
enable secret enpa55
```

Step 2: Assign static IPv6 Address

R1:

```
int gig0/0
ipv6 address 2001:DB8:1:10::1/64
ipv6 address FE80::1 link-local
no shut

int gig0/1
ipv6 address 2001:DB8:1:11::1/64
ipv6 address FE80::1 link-local
no shut

int se0/1/0
ipv6 address 2001:DB8:1:1::1/64
ipv6 address FE80::1 link-local
no shut
```

R2:

```
int se0/1/0
ipv6 address 2001:DB8:1:1::2/64
ipv6 address FE80::2 link-local
no shut

int se0/1/1
```

```
ipv6 address 2001:DB8:1:2::2/64

ipv6 address FE80::2 link-local

no shut
```

R3:

```
int gig0/0

ipv6 address 2001:DB8:1:30::1/64

ipv6 address FE80::3 link-local

no shut
```

```
int se0/1/0

ipv6 address 2001:DB8:1:2::1/64

ipv6 address FE80::3 link-local

no shut
```

Step 3: Enable IPv6 static routing

R1:

```
ipv6 unicast-routing

ipv6 route 2001:DB8:1:2::0/64 2001:DB8:1:1::2

ipv6 route 2001:DB8:1:30::0/64 2001:DB8:1:1::2
```

R2:

```
ipv6 unicast-routing

ipv6 route 2001:DB8:1:10::0/64 2001:DB8:1:1::1

ipv6 route 2001:DB8:1:11::0/64 2001:DB8:1:1::1

ipv6 route 2001:DB8:1:30::0/64 2001:DB8:1:2::1
```

R3:

```
ipv6 unicast-routing
```

```
ipv6 route 2001:DB8:1:10::0/64 2001:DB8:1:2::2

ipv6 route 2001:DB8:1:11::0/64 2001:DB8:1:2::2

ipv6 route 2001:DB8:1:1::0/64 2001:DB8:1:2::2
```

Step 4:  verify connectivity

```
PC1> ping 2001:DB8:1:30::30
```

(Successful)

```
PC2> ping 2001:DB8:1:30::30
```

(Successful)

---

PART 2: CONFIGURE APPLY AND VERIFY IPv6 ACL

Step 1: configure an ACL that will block HTTP and HTTPS access

R1:

```
ipv6 access-list BLOCK_HTTP

deny tcp any host 2001:DB8:1:30::30 eq www

deny tcp any host 2001:DB8:1:30::30 eq 443

permit ipv6 any any

exit
```

Step 2: Apply the ACL to correct interface

R1:

```
int gig0/1

ipv6 traffic-filter BLOCK_HTTP in
```

Step 3: Verify the ACL implementation

PC1:

Desktop -> Web Browser -> http://2001:DB8:1:30::30

(Successful)

Desktop -> Web Browser -> https://2001:DB8:1:30::30

(Successful)

PC2:

Desktop -> Web Browser -> http://2001:DB8:1:30::30

(Request Timeout)

Desktop -> Web Browser -> https://2001:DB8:1:30::30

(Request Timeout)

```
PC2> ping 2001:DB8:1:30::30
(Successful)
```

---

PART 3: CONFIGURE APPLY AND VERIFY THE SECOND IPv6 ACL

Step 1: Create an access-list to block ICMP

R3:

```
ipv6 access-list BLOCK_ICMP
deny icmp any any
permit ipv6 any any
exit
```

Step 2: Apply the ACL to corrective interface

R3:

```
int gig0/0
ipv6 traffic-filter BLOCK_ICMP out
```

Step 3: Verify the proper access-list functions

```
PC1> ping 2001:DB8:1:30::30
```

(Unsuccessful) – Destination host unreachable

PC2> ping 2001:DB8:1:30::30

(Unsuccessful) – Destination host unreachable

PC1:

Desktop -> Web Browser -> http://2001:DB8:1:30::30

(Successful)

Desktop -> Web Browser -> https://2001:DB8:1:30::30

(Successful)