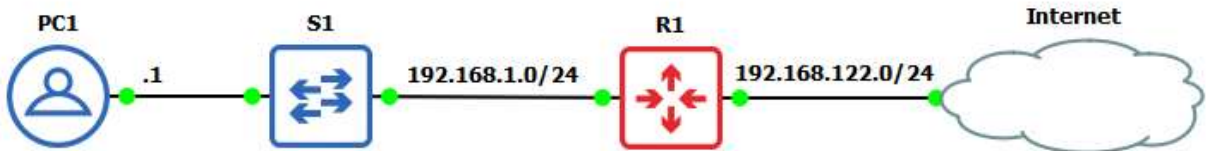


Infrastructure ACL (iACLs):

- o Using Infrastructure iACLs is a technique that was developed by ISPs.
- o It is now a common practice by enterprises and other organizations.
- o iACLs involves use of ACLs that prevent direct attacks to infrastructure devices.
- o Configure these ACLs to specifically allow only authorized traffic to infrastructure.



Infrastructure ACL

R1(config)#!--CMP Packet Filtering

```
R1(config)#ip access-list extended INF
R1(config-ext-nacl)#permit icmp any any echo-reply
R1(config-ext-nacl)#permit icmp any any unreachable
R1(config-ext-nacl)#permit icmp any any time-exceeded
R1(config-ext-nacl)#deny icmp any any
```

R1(config-ext-nacl)#!--Deny Special-Use Address Sources

```
R1(config-ext-nacl)#deny ip host 0.0.0.0 any
R1(config-ext-nacl)#deny ip 127.0.0.0 0.255.255.255 any
R1(config-ext-nacl)#deny ip 192.0.2.0 0.0.0.255 any
R1(config-ext-nacl)#deny ip 224.0.0.0 15.255.255.255 any
```

R1(config-ext-nacl)#!--Filter Private Space.

```
R1(config-ext-nacl)#deny ip 10.0.0.0 0.255.255.255 any
R1(config-ext-nacl)#deny ip 172.16.0.0 0.15.255.255 any
R1(config-ext-nacl)#deny ip 192.168.0.0 0.0.255.255 any
```

R1(config-ext-nacl)#!--Deny Access to Internal infrastructure Addresses.

```
R1(config-ext-nacl)#deny ip any 192.168.122.0 0.0.0.255
```

R1(config-ext-nacl)#!--Permit Transit Traffic.

```
R1(config-ext-nacl)#permit ip any any
```