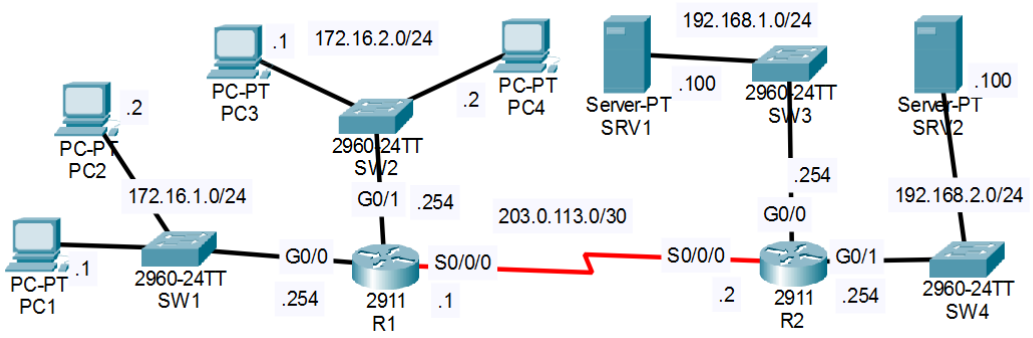
Network Topology:



Instructions and actions:

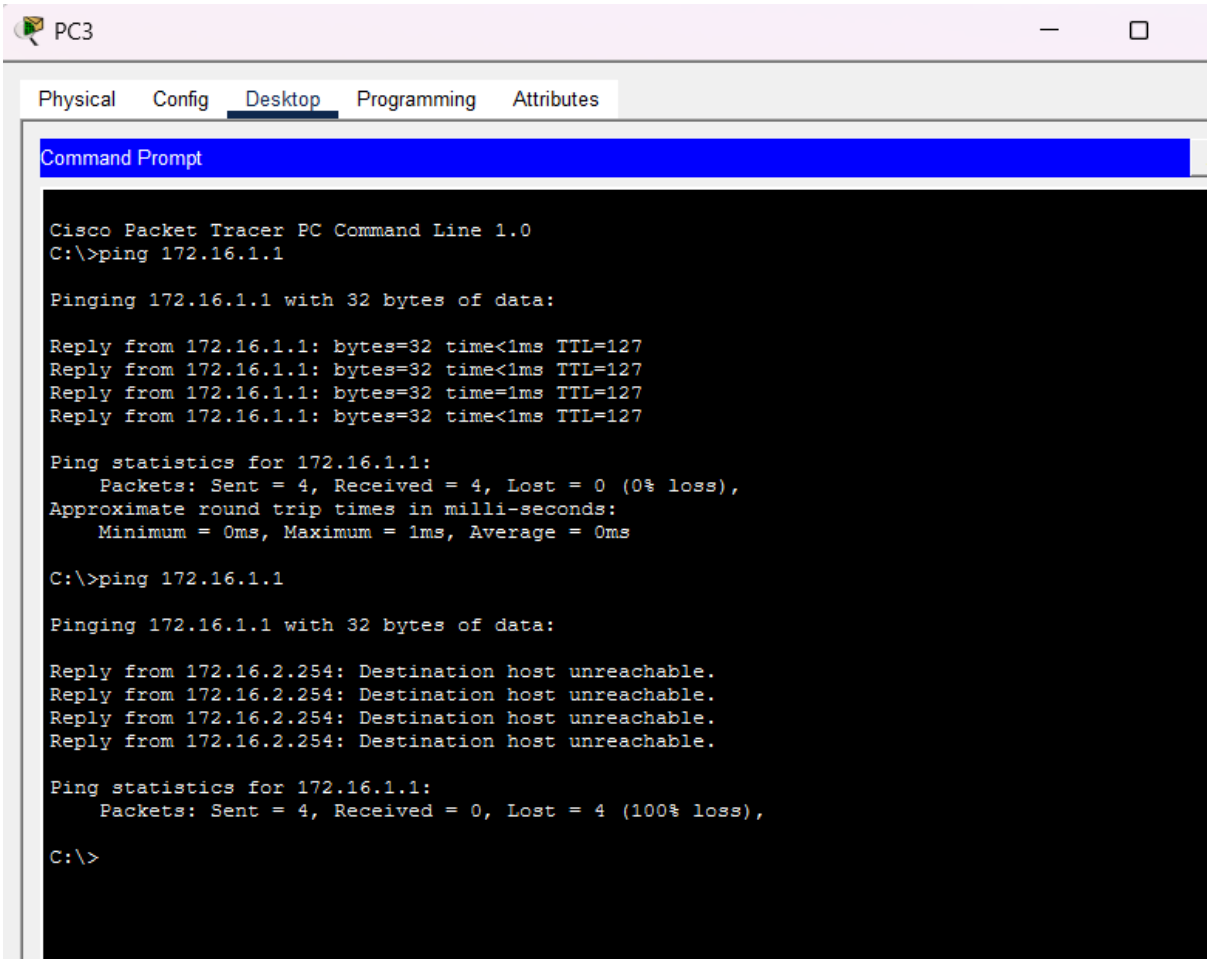
Configure extended ACLS to fulfil the following network policies:

1. Hosts in 172.16.2.0/24 can't communicate with PC1.

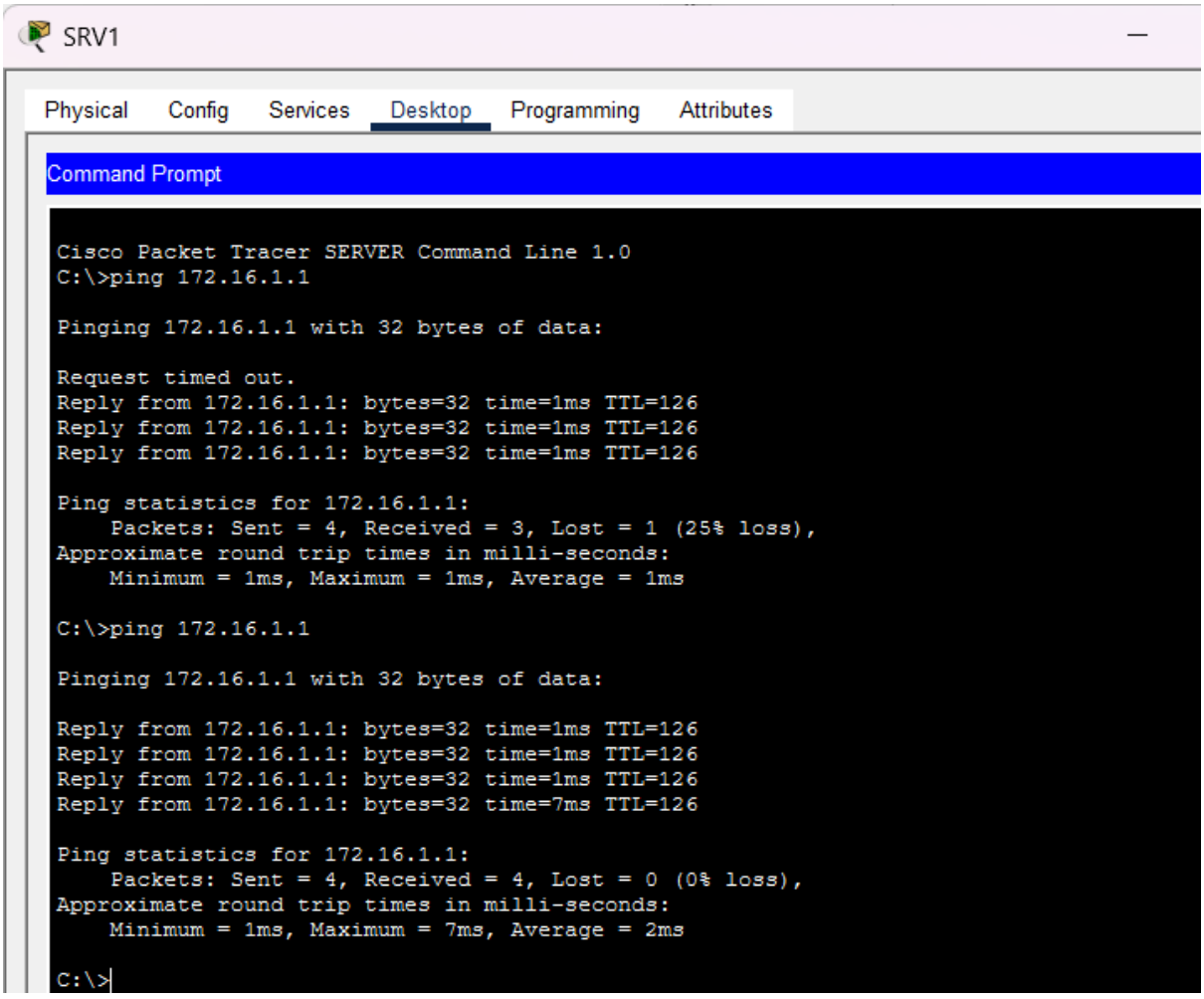
   R1 CLI:

```
R1(config-ext-nacl)#10 deny icmp 172.16.2.0 0.0.0.255 172.16.1.1 0.0.0.0
R1(config-ext-nacl)#do sh access-lists
Extended IP access list 101
    10 deny icmp 172.16.2.0 0.0.0.255 host 172.16.1.1

R1(config-ext-nacl)#exit
R1(config)#int g0/1
R1(config-if)#ip ?
  access-group     Specify access control for packets
  address          Set the IP address of an interface
  authentication   authentication subcommands
  flow             NetFlow Related commands
  hello-interval   Configures IP-EIGRP hello interval
  helper-address   Specify a destination address for UDP broadcasts
  mtu              Set IP Maximum Transmission Unit
  nat              NAT interface commands
  ospf             OSPF interface commands
  proxy-arp        Enable proxy ARP
  split-horizon    Perform split horizon
  summary-address  Perform address summarization
R1(config-if)#ip access-group ?
  <1-199>  IP access list (standard or extended)
  WORD     Access-list name
R1(config-if)#ip access-group 101 ?
  in   inbound packets
  out  outbound packets
R1(config-if)#ip access-group 101 in
R1(config-if)#do sh access-lists
Extended IP access list 101
    10 deny icmp 172.16.2.0 0.0.0.255 host 172.16.1.1

R1(config-if)#
```

   The change on PC3:



While others:



2. Hosts in 172.16.1.0/24 can't access the DNS service on SRV1.

   R1 CLI:

```
R1(config)#do sh access-lists
Extended IP access list 101
    10 deny icmp 172.16.2.0 0.0.0.255 host 172.16.1.1 (4 match(es))
    20 permit ip any any
Extended IP access list 103
    10 deny tcp 172.16.1.0 0.0.0.255 host 192.168.1.100 eq domain
    20 deny udp 172.16.1.0 0.0.0.255 host 192.168.1.100 eq domain
    30 permit ip any any

R1(config)#
```

   PC1 and PC2: (As in DNS, we use hostnames instead of IPs)

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping srv1
Ping request could not find host srv1. Please check the name and try again.
C:\>
```

   PC3 and PC4:

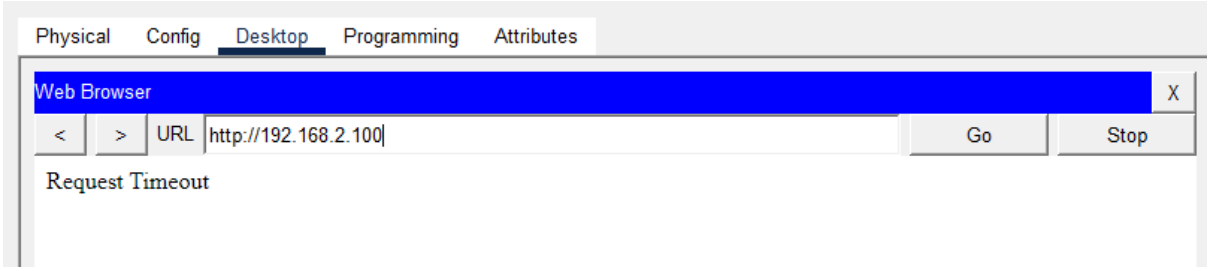
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping srv1

Pinging 192.168.1.100 with 32 bytes of data:

Reply from 192.168.1.100: bytes=32 time=15ms TTL=126
Reply from 192.168.1.100: bytes=32 time=1ms TTL=126
Reply from 192.168.1.100: bytes=32 time=1ms TTL=126
Reply from 192.168.1.100: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 15ms, Average = 4ms

C:\>
```

   Mistake – I forgot to give the “permit ip any any” command for the first instruction, which can lead to problems later on that interface. Therefore, we know that ACLs can be edited, so I just entered the access-list ID again and gave the command.

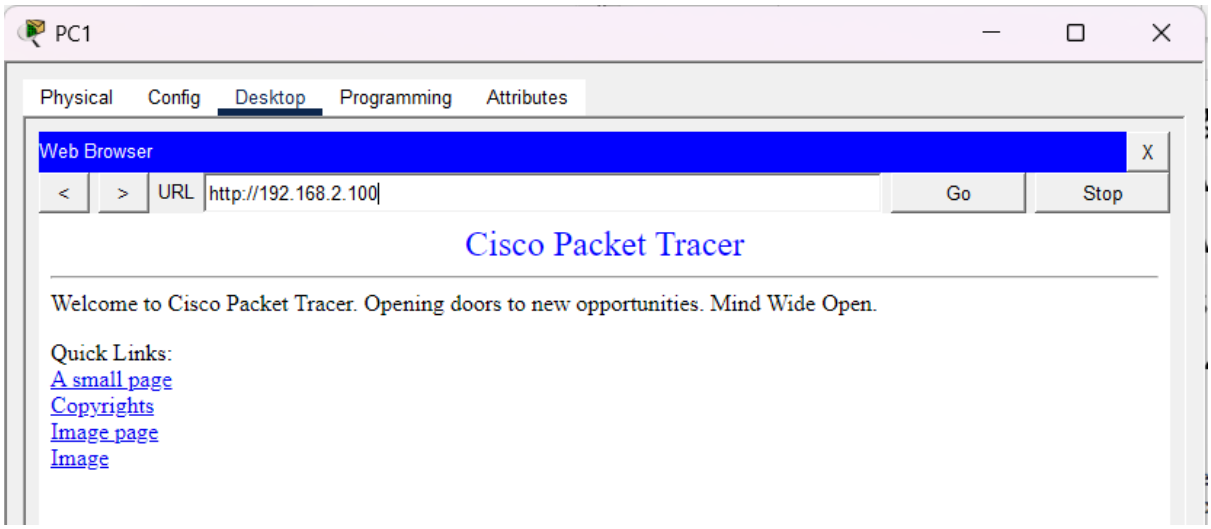
3. Hosts in 172.16.2.0/24 can't access the HTTP or HTTPS services on SRV2.

```
R1(config)#ip access-list extended 104
R1(config-ext-nacl)#deny tcp 172.16.2.0 0.0.0.255 host 192.168.2.100 eq 80
R1(config-ext-nacl)#deny tcp 172.16.2.0 0.0.0.255 host 192.168.2.100 eq 443
R1(config-ext-nacl)#permit ip any any
R1(config-ext-nacl)#exit
R1(config)#int g0/1
R1(config-if)#ip access-group 104 in
R1(config-if)#
```

   PC3 and PC4:



PC1 and PC2:



I will try to use the DNS hostnames instead of IP and add that later*