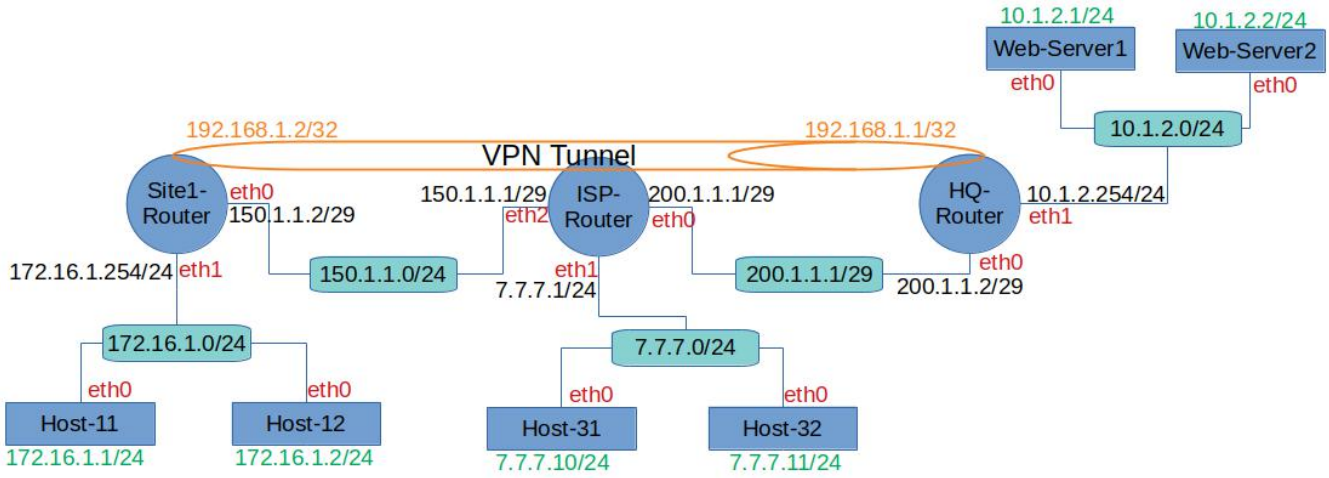
Cyber Security Course- Networking Assessment

1 Background

The objective of this lab is to configure all hosts and routers with their IP addresses. Routers should be configured to route only PUBLIC IP addresses. Private IP addresses should NOT be routed on a public network.



2 Credentials

Device	Username	Password
Host-11	user-11	user-11
Host-12	user-12	user-12
Host-31	user-31	user-31
Host-32	user-32	user-32
Web-Server1	web-admin	web-admin
Web-Server2	web-admin	web-admin
Site1-Router	admin	admin
ISP-Router	admin	admin
HQ-Router	admin	admin

3 Tasks

1. Configure the IP addresses on all network interfaces
2. Configure the routing for all routers to route public IP networks
3. Establish the VPN between the Site1-Router and HQ-Router
4. Configure the firewall on Webs-Server1 to accept Only
   a) First Rule
      1. Source IP: 172.16.1.1
      2. Destination IP: 10.1.2.1
      3. Protocol: TCP
      4. Port: HTTP

   b) Second Rule
      1. Source IP: 172.16.1.1
      2. Destination IP: 10.1.2.1
      3. Protocol: ICMP

   Note: You should configure the INPUT and OUTPUT chains instead of the FORWARD chain

Stop the labtainer

When the lab is completed, or you'd like to stop working for a while, run:

```
stoplab
```

from the host labtainer working directory. You can always restart the lab to continue your work. When the labtainer is stopped, a zip file is created and copied to a location displayed by the stoplab command. When the lab is complete, send that zip file to the instructor.

This lab was developed by Sparta Global for Cybersecurity courses. It was built based on the original lab that was developed for the Labtainer framework by the Naval Postgraduate School, Center for Cybersecurity and Cyber Operations under National Science Foundation Award No. 1438893. This work is in the public domain, and cannot be copyrighted.