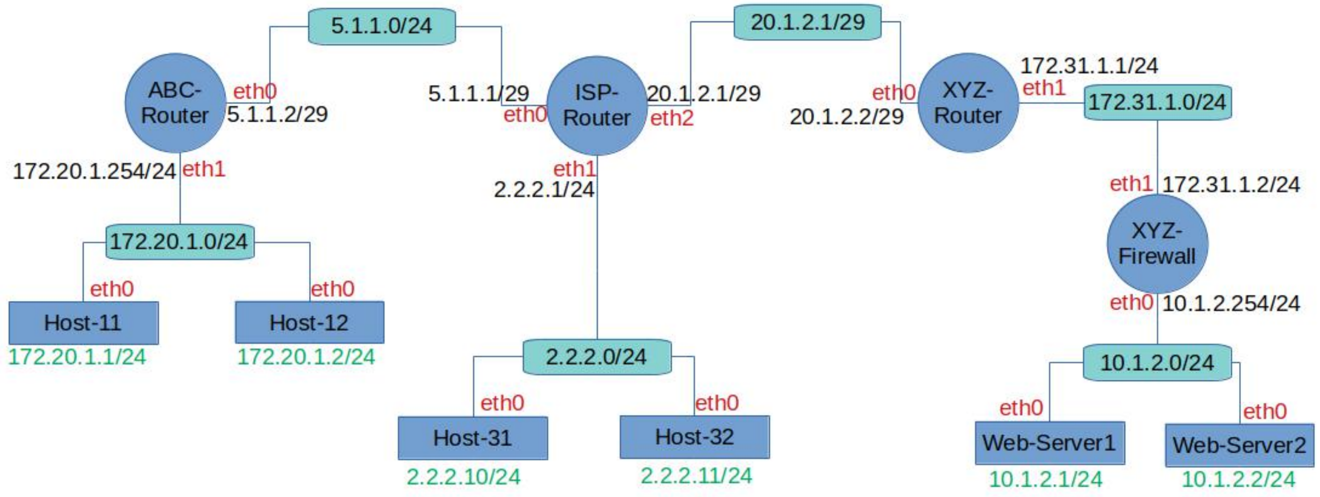
Cyber Security Course - Networking Assessment

1 Background

The objective of this lab is to configure all hosts and routers with their IP addresses. Routers should be configured to route traffic by default to ISP-Router. Private IP addresses should NOT be routed on a public network and routers should use NAT/PAT techniques to allow traffic from/to private networks.



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
ABC-Router	admin	admin
ISP-Router	admin	admin
XYZ-Router	admin	admin
XYZ-Firewall	admin	admin

3 Tasks

1. Configure the IP addresses on all network interfaces
   Note: You have to restart the HTTP services on the HTTP servers after configuring their IP addresses.
   You can use the following command: *sudo systemctl restart httpserver*
2. Configure default route/gateway on ABC-Router to forward traffic to ISP-Router
3. Configure default route/gateway on XYZ-Firewall to forward traffic to XYZ-Router
4. Configure route to 10.1.2.0/24 on XYZ-Router to forward traffic to XYZ-Firewall
5. Configure default route/gateway on XYZ-Router to forward traffic to ISP-Router
6. Add NATing (PAT) on ABC-Router to allow Host-11 and Host-12 to surf simultaneously the Internet using the Public IP address of the ABC-Router
7. Add NATing (Port Forwarding) on XYZ-Router to forward traffic arriving from the Internet based on the following rules:
   a) First Rule:
      1. Packet Destination Port: 8080
      2. Should be Forwarded to: 10.1.2.1:80
   b) Second Rule:
      1. Packet Destination Port: 8081
      2. Should be Forwarded to: 10.1.2.2:80

8. Configure the firewall-xyz to add the following rules
   a) First Rule
      1. Source IP: 0.0.0.0/0 (any)
      2. Destination IP: 10.1.2.1
      3. Protocol: TCP
      4. Port: HTTP
   b) Second Rule
      1. Source IP: 0.0.0.0/0 (any)
      2. Destination IP: 10.1.2.2
      3. Protocol: TCP
      4. Port: HTTP

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.