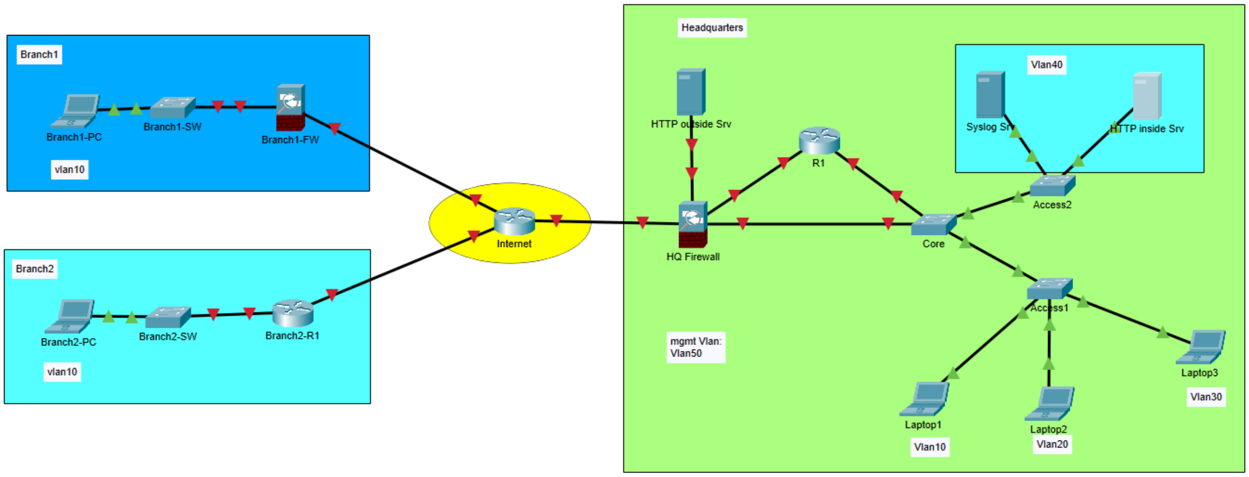
## How to pass the laboratory classes in network security systems

*In order to pass the laboratories, the following tasks must be performed based on the attached topology (open the file in the Cisco Packet Tracer program). Please document all steps: the final configuration from the devices can be copied and pasted into a Word file, and the results of individual tasks should be documented by taking screenshots. Please also provide a brief description of what was done at each step.*

The topology represents a company consisting of a headquarters (Headquarters) and two other locations (Branch1 and Branch2) connected to each other via the Internet. Attached is a file with the topology below.



*Task 1*

Assign private addressing (fill in the table below) for Vlan10, Vlan 20, Vlan 30, Vlan 40, and Vlan 50, and address the devices in the respective Vlans. The default gateway for the above Vlans is Router R1.

| ***Device Name*** | ***vlan*** | ***Assigned IP Address*** | ***Network Mask*** | ***Default Gateway IP Address*** |
|---|---|---|---|---|
| Laptop1 | 10 | 192.168.10.10 | 255.255.255.0 | 192.168.10.1 |
| Laptop2 | 20 | 192.168.20.10 | 255.255.255.0 | 192.168.20.1 |
| Laptop3 | 30 | 192.168.30.10 | 255.255.255.0 | 192.168.30.1 |
| Syslog Srv | 40 | 192.168.40.10 | 255.255.255.0 | 192.168.40.1 |
| HTTP inside Srv | 40 | 192.168.40.11 | 255.255.255.0 | 192.168.50.1 |
| HTTP outside Srv | - | 192.168.100.10 | 255.255.255.0 | 192.168.100.1 |
| Branch1-PC | 10 | 190.16.19.10 | 255.255.255.0 | 190.16.19.1 |
| Branch2-PC | 10 | 190.16.18.10 | 255.255.255.0 | 190.16.18.1 |
| R1 | 50 | 192.168.50.1 | 255.255.255.0 | n/a |
| Core | 50 | 192.168.50.12 | 255.255.255.0 | 192.168.50.1 |
| Access1 | 50 | 192.168.50.10 | 255.255.255.0 | 192.168.50.1 |
| Access2 | 50 | 192.168.50.11 | 255.255.255.0 | 192.168.50.1 |
| HQ Firewall | 50 | 192.168.50.3 | 255.255.255.0 | 192.168.50.1 |

Vlan 50 is known as the management vlan. Every network device at the Headquarters (switches, router, and firewall) should have an address assigned from this Vlan. Ideally, these addresses should be accessible for logging in, for example, using ssh.

Assign private addressing for the connection from Router R1 to the HQ Firewall by filling in the table below, and then configure these addresses on the device interfaces::

| ***Connection from Router R1 to HQ Firewall*** | |
|---|---|
| Ip address of Routera R1 / network mask | IP adress of HQ Firewall / network mask |
| 170.160.30.1/30 | 170.160.30.2/30 |

Assign public addressing (by filling in the table below) for the internet connections, and then configure/address the network devices: HQ Firewall, Branch1-FW, and Branch2-R1.

| ***Connection between HQ Firewall and Internet Router*** | |
|---|---|
| Ip address of HQ Firewall / network mask | IP adress of Router Internet / network mask |
| 2.2.2.1/255.255.255.252 | 2.2.2.2/255.255.255.252 |
| ***Connection from Branch1-FW to Internet Router*** | |
| Ip address of Branch1-FW / network mask | IP address of Router Internet / network mask |
| 3.3.3.1/255.255.255.252 | 3.3.3.2/255.255.255.252 |
| ***Connection from Branch2-R1 to Internet Router*** | |
| Ip address of Branch2-R1 / network mask | IP address of Router Internet / network mask |
| 4.4.4.1/255.255.255.252 | 4.4.4.2/255.255.255.252 |

The task is completed if, after configuring the devices, the "ping" command works:

- from Laptop1 to the address of Laptop2, Laptop3, SyslogSrv, HTTP inside Srv, to the addresses in Vlan 50, and to the HQ Firewall address from the "inside",
- from Branch1-PC to the address of the default gateway,
- from Branch2-PC to the address of the default gateway.

*Task 2*

At the Headquarters location, configure a local user account on devices R1, Core, Access1, Access2, and HQ Firewall, which will be used to log into these devices via SSH. Also, configure the ability to log in to these devices via SSH.

The task is completed if you can log in using an SSH client from Laptop1, Laptop2, and Laptop3 to the devices R1, Core, Access1, Access2, and HQ Firewall.

*Task 3*

Limit the ability to log in via SSH to R1 only from Laptop3.

The task is completed if attempts to log in to R1 from Laptop1 and Laptop2 are blocked, and access from Laptop3 via SSH works correctly.

*Task 4*

Communication to the HTTP inside Srv server on port 80 should only be allowed from Laptop2.

The task is completed if attempts to connect to port 80 (HTTP) from Laptop1 and Laptop3 are blocked, while access from Laptop2 works correctly..

*Task 5*

Configure NAT (Network Address Translation) for the "HTTP outside Srv" server, which is located at Headquarters, so that its private address is converted to a public address, making it accessible from the internet. This configuration should allow computers "Branch1-PC" and "Branch2-PC" to reach the server, and their private addresses should also be translated to public addresses during communication with HTTP outside Srv.

The task is completed if, after starting the HTTP service on the server, you can open a web page from this server using a web browser on Branch1-PC and Branch2-PC.

**IP translated to 15.15.15.15**

*Task 6*

Configure IPSec tunnels between the HQ Firewall and Branch1-FW, as well as between the HQ Firewall and Branch2-R1. These tunnels should enable secure communication between Branch1-PC and the HTTP inside Srv, and between Branch2-PC and the HTTP inside Srv.

The task is completed if you can successfully connect to the private address of the HTTP inside Srv using a web browser from Branch1-PC and Branch2-PC.

*Task 7*

Launch Wireshark and start capturing traffic on the network card that has Internet access.
Type into your browser:
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html
Your browser should display a very simple message in HTML code.
Stop capturing packets in Wireshark.

Answer the questions:

1. Does your browser use HTTP version 1.0 or 1.1? What version of HTTP does the server use?
**Browser**: HTTP/1.1 **Server**: HTTP/1.1

2. What languages (if any) does your browser indicate it can accept from the server?
**Languages**: `en-US, en;q=0.9`

3. What is the IP address of your computer? What is the address of the server gaia.cs.umass.edu?
**MY Computer's IP**: `192.168.1.100` **Server (`gaia.cs.umass.edu`) IP**: `128.119.245.12`

4. What status code does the server return to your browser?
**Status Code**: `200 OK`

5. When was the HTML file you are downloading last modified on the server?
**Last Modified**: Sat, `15 Jun 2024 20:29:21 GMT`

6. How many bytes of content are returned to your browser?
**Content Length**: `4520` bytes

Finally, try visiting a password-protected website and investigate the sequence of HTTP message exchanges for such a site. URL:
http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html

It is password-protected. The username is "wireshark-students" (without quotes), and the password is "network" (again without quotes).

Before you attempt to connect, do the following:

- Make sure your browser's cache is cleared, and close the browser. Then, restart the browser.
- Start the packet capturing program Wireshark.
- Enter the above URL into your browser. Type the requested username and password in the pop-up window.
- Stop capturing packets in Wireshark and type "http" in the display filter specification window of Wireshark, so that only captured HTTP messages will be displayed in the packet list window later.

Answer the questions:

1. What is the server's response (status code and phrase) to the initial HTTP GET message sent by your browser?
**Status Code**: `40` Phrase: `Unauthorized`

2. When your browser sends an HTTP GET message a second time, what new field is included in the HTTP GET message?
Field: `Authorization` Value: `Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=`