# 01\_Secure Remote Access

## Backgrounds

Make a base configuration (00\_Baseline) or use the base file you made earlier. Below is a link to a file that has a baseline pre-made:

<https://www.dropbox.com/s/ps8c57jv7z15hic/netw_sec_base_v3_00_done.pkt?dl=0>

<https://www.dropbox.com/s/ps8c57jv7z15hic/netw_sec_base_v3_00_done.pkt?dl=0>

# Task

At this point, imagine that you are responsible for the information networks of an A company and therefore only target the networks and equipment of that company (Note: of course, you are responsible for both the head office HQ and the branch BR).

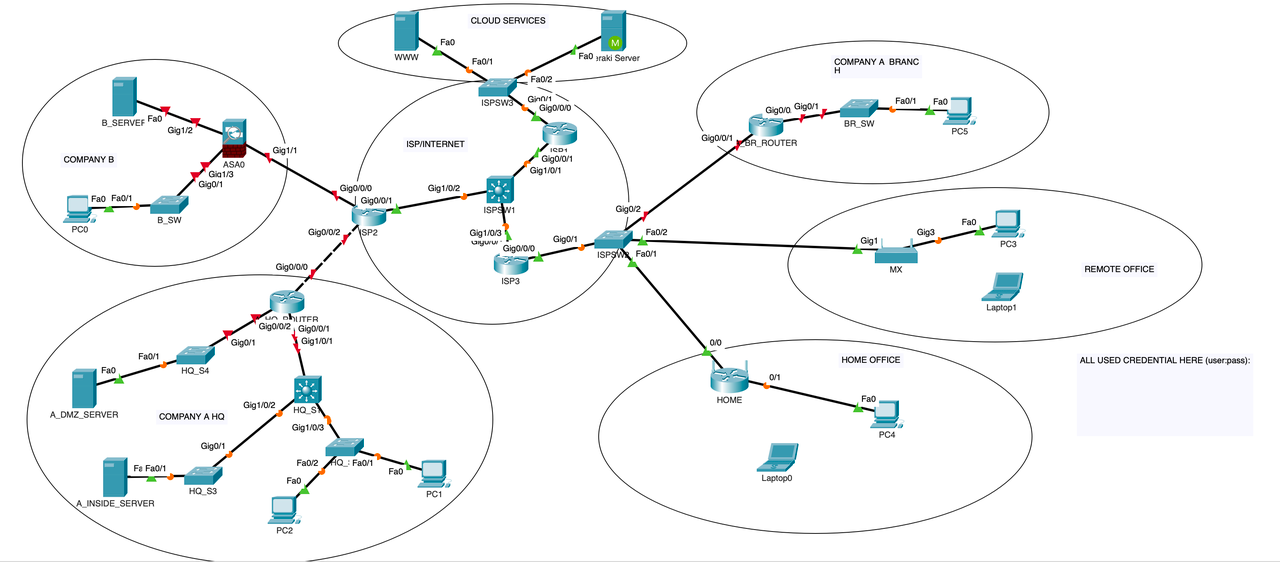
The goal is to create a secure remote management connection for all corporate A network devices. First, do remote management for routable devices (HQ\_ROUTER, HQ\_S1, and BR\_ROUTER).

See parts 2, 3 and 4 of Cisco Lab 4.4.7, applying them as needed. N.B. Be careful never to lock yourself away from the devices so that you can no longer establish a configuration connection!

A couple of observations:

1. *Set passwords for console connections only last, after you have already tested, that you will definitely be able to access the devices and enable mode even remotely (if the console password setting goes wrong). Always make sure that you have one, tested and verified, way to get to configure the equipment!*

1. *Make a sticky note of usernames and passwords in the pt file and fill in all the IDs you use, e.g. bottom right corner of the image:*



Test:

|  |  |  |
| --- | --- | --- |
| SOURCE | DESTINATION | TEST |
| PC1 | HQ\_ROUTER | SSH |
| PC1 | HQ\_S1 | SSH |
| PC1 | BR\_ROUTER | SSH |

## Extra

If you have the time and enthusiasm, make the HQ and BR switches remotely manageable. To do this, you should set IP settings for the switches. Document and you'll remember what you've done!

To test remote control of switches:

|  |  |  |
| --- | --- | --- |
| SOURCE | DESTINATION | TEST |
| PC1 | HQ\_S2 | SSH |
| PC1 | HQ\_S3 | SSH |
| PC1 | HQ\_S4 | SSH |
| PC5 | BR\_SW | SSH |

END