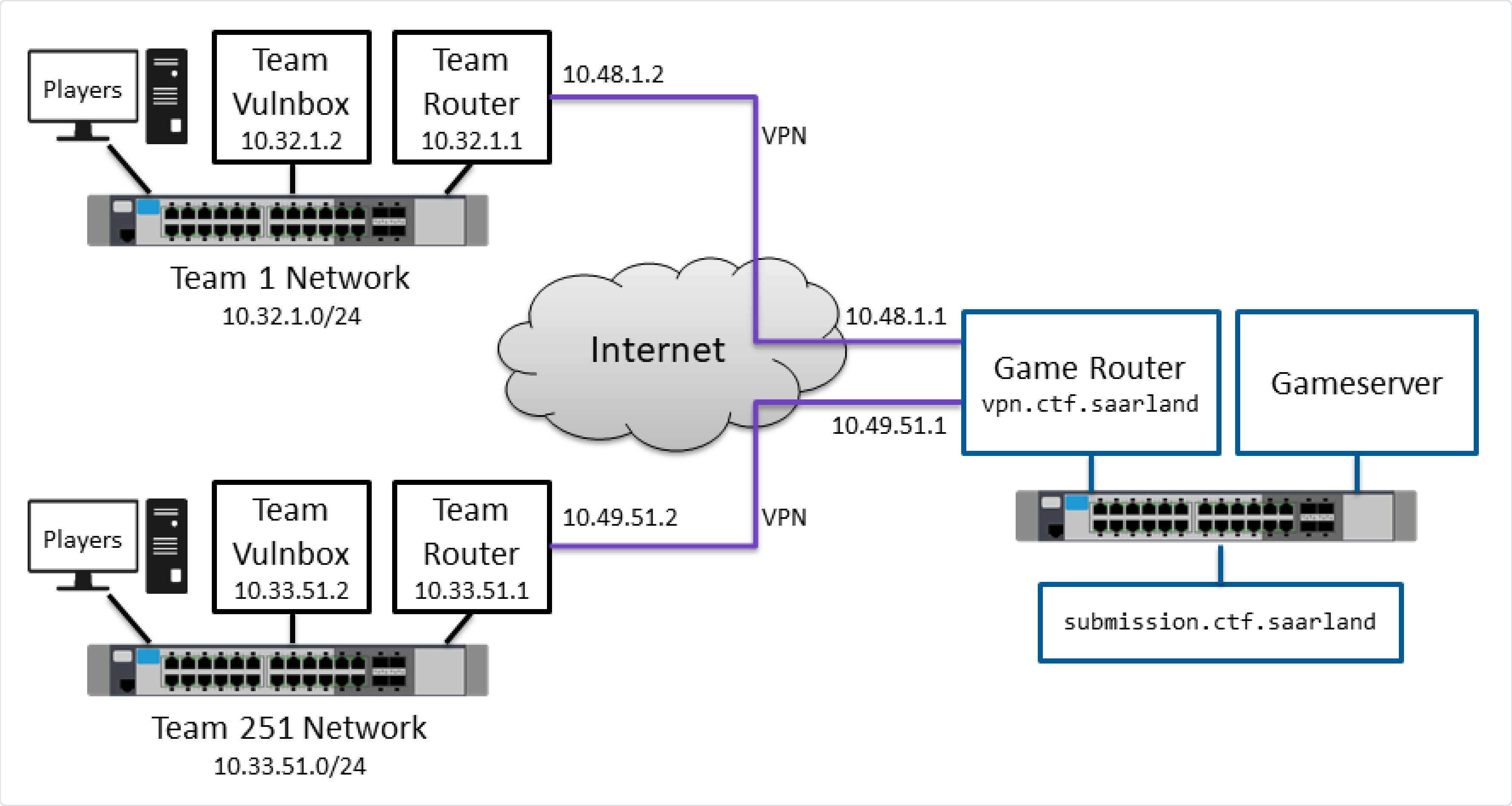
Setup:

Summary

Game network	`10.32.0.0/15` (`10.32.0.0 - 10.33.255.255`)
Team Network	`10.(32+X).Y.0/24` where `X := <team_id> // 200` and `Y := <team_id> % 200`
Router IP	`10.(32+X).Y.1`
Vulnbox IP	`10.(32+X).Y.2`
Testbox IP	`10.(32+X).Y.3`



The Vulnbox

The Vulnbox will be delivered as encrypted VirtualBox image in OVA format. You need at least VirtualBox 5.2, newer is better.

We suggest your host machine has at least 4 CPU cores and 8 GB RAM.

We will provide a router image for your convenience and a test machine before the competition.

Setup VPN and Network

You need one machine to host the Vulnbox and act as VPN gateway (between your team network and our game network). Depending on your infrastructure there are different setups possible. We suggest our pre-configured Router VM image to save you most of the configuration.

1. If you have a machine with two network interfaces (preferrably physical), we suggest setup 1 (Router VM + physical team network).
2. If you do not have a machine with two network interfaces, use setup 2 (Router VM + team-internal VPN).
3. If you know what you're doing, use setup 3 (manual setup).
4. If you want to play online/remote without any hardware, use setup 4 (cloud based)

You can see if your configuration works on vpn.ctf.saarland. To test the other direction `ping submission.ctf.saarland`.

Setup 1: Router VM + physical team network (recommended)

Setup 2: Router VM + team-internal VPN

Setup 3: Manual setup

Setup 4: Cloud Hosting

You can play the game with two machines rented in the cloud. This is especially handy for teams that play together over internet. The following instructions assume you use Hetzner Cloud (where we also host our infrastructure), but in theory other cloud providers might also work out. Costs should be less than 1€ depending on your configuration. The following instructions assume that you already have an activated Hetzner Cloud Account.

1. **Hosting the router**
   The router is the central machine for your team. It connects to Vulnbox and game VPN and hosts its own VPN server for your players.

   1. Create a new "network" with IP range `10.32.0.0/11`. Remove its default subnet and create a new one for your team network (for example `10.32.99.0/24` for team #99).
   2. Create a new server "Router": select location Falkenstein, image "Debian 10", type "CX21", your network from step 1 and your SSH key.
   3. In Hetzner network settings, create a route for your network: `0.0.0.0/0`, gateway is your router server.
   4. SSH to the router server and install all software with our script:
      ```
      wget 'https://ctf.saarland/static/scripts/install_cloud_router.sh'
      chmod +x install_cloud_router.sh
      ./install_cloud_router.sh
      ```
   5. Fix routes to cloud machines (replace `32.99` with your team network):
      ```
      ip route add 10.32.99.2/31 via 10.32.0.1 dev ens10
      ```
   6. Copy the game VPN configuration you received to `/etc/openvpn/saarctf.conf`. Start the VPN with `systemctl start openvpn@saarctf`. Enable permanently with `systemctl enable openvpn@saarctf`.
   7. Open `/root/team-vpn-client.conf`, insert your server's public IP in the first line and distribute to your team. All players can use the same configuration file.
   8. Check if the router and the players can ping `10.32.250.2`.
2. **Hosting the testbox**
   While the testbox is not strictly necessary, you can already try out the setup process you'll need for the vulnbox later.

   1. Create a new server "Testbox": select location Falkenstein, image "Debian 10", type "CX11" and your SSH key. No network!
   2. Attach the new server to your network in the network configurations, manually assign IP `10.X.Y.3`.
   3. Reboot the server into rescue mode ("enable rescue & power cycle, system "linux64")
   4. Download testbox archive and install script:
      ```
      cd /dev/shm
      wget 'https://ctf.saarland/static/scripts/install_cloud_bundle.sh'
      wget 'https://vpn.ctf.saarland/vm/saarctf-testbox.tar.xz'
      chmod +x install_cloud_bundle.sh
      ```
   5. Install the bundle: `./install_cloud_bundle.sh saarctf-testbox.tar.xz`
   6. Edit `/mnt/root/.ssh/authorized_keys` and insert your SSH key again
   7. Reboot
3. **Hosting the vulnbox**
   Hosting the vulnbox is similar to the testbox, only IP, download URL and password differ. The password will be released when the game starts.

   1. Create a new server "Vulnbox": select location Falkenstein, image "Debian 10", type "CX21" or "CX41" and your SSH key. No network!
   2. Attach the new server to your network in the network configurations, manually assign IP `10.X.Y.2`.
   3. Reboot the server into rescue mode ("enable rescue & power cycle, system "linux64")
   4. Download vulnbox archive and install script once it is released:
      ```
      cd /dev/shm
      wget 'https://ctf.saarland/static/scripts/install_cloud_bundle.sh'
      wget 'https://vpn.ctf.saarland/vm/saarctf-vulnbox.tar.xz.gpg'
      chmod +x install_cloud_bundle.sh
      ```
   5. Install the bundle: `./install_cloud_bundle.sh saarctf-vulnbox.tar.xz.gpg <PASSWORD>`
   6. Edit `/mnt/root/.ssh/authorized_keys` and insert your SSH key again
   7. Reboot

7. Reboot

Hints:

- Hetzner Cloud charges you for offline servers. After the game you must delete all machines.
- We advertise against using AWS: traffic is expensive there, we can't estimate your final costs
- To get better performance, you could run your exploits on the Router machine
- If team VPN performance is too bad, you can create multiple VPN servers on the router: Clone the configs and change the server port.

Service status

Every tick the Gameserver connects to your services and rates them in one of these categories:

- UP — Service is working, you receive SLA points
- Flag missing — Service is working, but flags from last tick could not be retrieved. No SLA points.
- Mumble — Service is accessible but non-functional.
- Offline — Service can't be accessed, error on network layer.
- Not checked — If your VPN connection is terminated, your service will not be checked.

If your service is broken, you can see more details in the scoreboard.

Flag submission

You can submit flags in a plain TCP connection to `submission.ctf.saarland` port 31337 from your team network. Each flag must be submitted in a single line terminated by a line feed (`\n`). For each submitted line, the submission server answers with one line that starts either with `[OK]` if the flag was accepted, `[ERR]` if the flag is permanently invalid or `[OFFLINE]` if submission is currently disabled. This status is possibly followed by a more detailed description.

A non-complete list of possible responses:

- `[OK]`
- `[ERR] Invalid format`
- `[ERR] Invalid flag`
- `[ERR] Expired`
- `[ERR] Already submitted`
- `[ERR] Can't submit flag from NOP team`
- `[ERR] This is your own flag`
- `[OFFLINE] CTF not running`

Status endpoints

The endpoint `https://scoreboard.ctf.saarland/attack.json` gives you a JSON with all information you need during the competition. It is updated at the beginning of each tick. Format:

```
{
    "teams": [
        {
            "id": 1,
            "name": "NOP",
            "ip": "10.32.1.2"
        },
        {
            "id": 2,
            "name": "saarsec",
            "ip": "10.32.2.2"
        }
    ],
    "flag_ids": {
        "service_1": {
            "10.32.1.2": {
                "15": ["username1", "username1.2"],
                "16": ["username2", "username2.2"]
            },
            "10.32.2.2": {
                "15": ["username3", "username3.2"],
                "16": ["username4", "username4.2"]
            }
        }
    }
}
```

`"teams"` contains a list of all teams that are online, including the IP of their Vulnbox. If you limit your attacks to these IPs you can safe yourself some bandwidth.

Some services have `"flag_ids"`, additional information that you might need for an exploit. Usually this is the username of the Gameserver's account that you should attack. The flag ids are only given for flags that are still valid.