NETSEC: TP2 Firewalls and tunnels

Jacopo Bufalino, Pengwenlong GU

October 2025

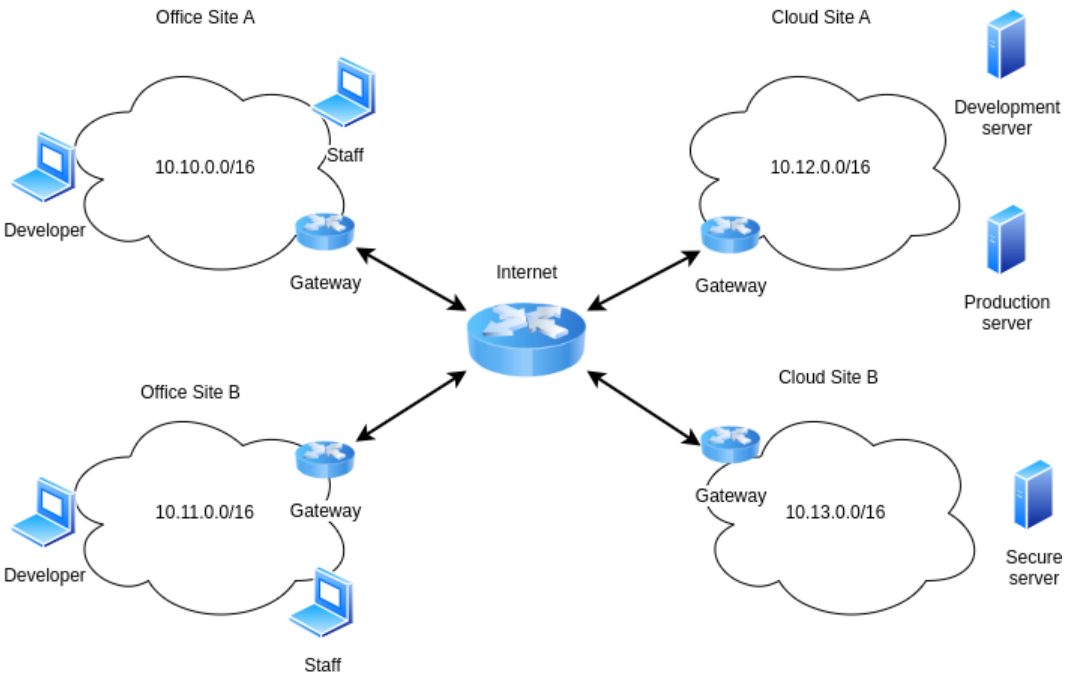

Figure 1: Topology

You are responsible of securing the network of AI-Coorp, a leading AI video-editing company. AI-Coorp has two physical offices (Site A and Site B). In each office there is a developer and a staff member. AI-Coorp rents servers from a cloud provider which has two locations, called Cloud Site A and Cloud Site B. As a system administrator, **you can only make changes to the gateway of each subnet**.

The current network configuration allows access from every office to every Cloud Site. This is not secure therefore, the management has requested you to make some changes divided in two parts.

Part 1

1. **Everyone** in the office can access the **Production server**
2. **Developers** can access the **Secure Server** no matter their location
3. **Staff** members on the office B can access the **Production server** and the **Secure Server**
4. **Developers** on the office A can also access the **Development server**

Part 2

Management has been told that the communication to Cloud Site A is unencrypted. So they want you to setup IPSec tunnels from Office A to Cloud Site A and Office B to Cloud Site A.

Start the lab

Run `docker compose up --build -d` from the **lab** folder of the project. This may take up to a minute to complete.

Stop the lab

Run `docker compose down` from the **lab** folder of the project. This command will destroy all the containers and you will not be able to access their history.

Useful commands

- `docker compose ps` to show all running containers
- `docker compose exec -it <service_name> bash` to get a shell in a container
- `docker compose restart <service_name> -d` to restart a single container
- `iptables` is the tool you will use to add firewall rules
- `strongswan` is the tool you will use to implement IPSec tunnels

Once inside the container you can run:

- `bash /scripts/check_reachability.sh` to check if the container can reach the other targets
- `exit` to exit from a container.
- `tcpdump` to analyze the network traffic. You are encouraged to look the manual online. [1]. You can store locally the results of tcpdump by saving them in `/exports` folder of every container. You can then analyze the traffic using Wireshark.

Submission instructions

- Part 1: For a correct submission of the first part of the report, provide the list of iptables rules for each host: **one file per host in the form surname_gateway (e.g., doe_gwcloudA.txt**. You can optionally attach screenshots of the rules.
- Part 2: Provide the commands and outputs used to generate the IPSec tunnel: **one file per host in the form surname_gateway (e.g., doe_gwcloudA.txt**. Also, upload a screenshot **from the router** showing that the connection between the offices and clouds is encrypted.

[1] https://www.tcpdump.org/manpages/tcpdump.1.html