



Exercise: Firewall Setup with Ansible-Automation

Here's a complete **Ansible playbook** that configures a basic **UFW firewall** for a Kubernetes cluster with:



Objective

You will learn to:

- Install and enable the UFW firewall via Ansible on:
 - One **control-plane node**
 - One or more **worker nodes**
 - assign roles (control-plane or worker) using **host groups** in your Ansible inventory.
-




Directory structure (recommended)

```
k8s-firewall/  
├─ inventory.ini  
└─ playbook.yml
```



inventory.ini

```
[control_plane]  
master1 ansible_host=192.168.0.10  
  
[worker]  
worker1 ansible_host=192.168.0.11  
worker2 ansible_host=192.168.0.12
```

 playbook.yml

```
---
- name: Configure UFW firewall for Kubernetes nodes
  hosts: all
  become: true
  vars:
    internal_subnet: "192.168.0.0/24"

  tasks:
    - name: Install UFW
      apt:
        name: ufw
        state: present
        update_cache: yes

    - name: Set default policies
      ufw:
        direction: incoming
        policy: deny

    - name: Allow outgoing traffic
      ufw:
        direction: outgoing
        policy: allow

    - name: Allow SSH
      ufw:
        rule: allow
        port: 22
        proto: tcp

- name: Configure control-plane firewall rules
  hosts: control_plane
  become: true
  tasks:
    - name: Allow Kubernetes API server
      ufw:
        rule: allow
        port: 6443
        proto: tcp

    - name: Allow etcd ports
      ufw:
        rule: allow
        port: "{{ item }}"
        proto: tcp
        loop: [2379, 2380]

    - name: Allow kubelet API
      ufw:
        rule: allow
        port: 10250
        proto: tcp
```

```
- name: Allow scheduler and controller-manager
  ufw:
    rule: allow
    port: "{{ item }}"
    proto: tcp
    loop: [10257, 10259]

- name: Enable UFW
  ufw:
    state: enabled


- name: Configure worker node firewall rules
  hosts: worker
  become: true
  tasks:
    - name: Allow kubelet API
      ufw:
        rule: allow
        port: 10250
        proto: tcp

    - name: Allow NodePort range
      ufw:
        rule: allow
        port: "30000:32767"
        proto: tcp

    - name: Enable UFW
      ufw:
        state: enabled
```

Run the playbook

```
ansible-playbook -i inventory.ini playbook.yml
```

 Use `--ask-become-pass` if you don't use passwordless sudo.

Outcome

- UFW will be enabled on all nodes
- Only the necessary Kubernetes ports will be open
- Everything else will be blocked

 August 22, 2025