Exercise Introduction

You will need at least 2 terminal sessions on the head node to do these exercises, with 3 being ideal. If you only are logged in with one, start another one right away.

You will learn to

- Install firewalld
- Write Service files for the services you are using
- Write Zone files
- Setup routing from an internal network to the outside

Contents

Task 1: Set user password on head node (2 min) 1

Task 2: Install required software (3 min) 1

Task 3: Write Service files for those not provided by firewalld (5 min) 2

Task 4: Start a port scan of the head node from a compute node (1 min) 2

Task 5: Creating Zones for the cluster and external networks (10 min) 2

Task 6: Start the firewall and check it (5 min) 3

Task 7: Turn the head node into a gateway for the compute nodes (10 min) 3

Optional Task 8: Extra Task (5 min) 4

Task 1: Set user password on head node (2 min)

It is very easy when configuring the firewall to lock yourself out entirely. In OpenStack, there is the Console for each VM, which can be used to login and stop the firewall if you lock yourself out of SSH. To use that, a password must first be set for the `cloud` username. On the head node as root, change `cloud`'s password with `passwd cloud` to a long secure password and write it down somewhere safe.

Task 2: Install required software (3 min)

Install the following packages on the head node and the warewulf images:

- `firewalld`

- `nmap`

and double check that `firewalld`'s service is disabled by running `systemctl disable firewalld`. Then reboot the compute nodes and proceed to the next Task.

`nmap` will be used to scan open ports to check the firewall.

WARNING: **NEVER** scan a machine or network without permission of its owner. Port scanning is often an indicator of an attack, and will often be reacted to as such.

Task 3: Write Service files for those not provided by firewalld (5 min)

Firewalld has Service files for many services already, but not all. Take a look in the `/usr/lib/firewalld/services` directory and see which of the services in the table below that you have setup in this course that don't have a builtin Service file:

Service	TCP Ports	UDP Ports
DHCP (Warewulf)		67
DNS	53	53
NFS v3	2049	2049
rpc-bind (NFS)	111	111
slurmctld	6817	
slurmdbd	6819	
Squid	3128	
SSH	22	
TFTP (Warewulf)		69
Warewulf	9873	

Write Service files on the head node for each not provided service and put them in `/etc/firewalld/services`. Look at the existing Service files if you get stuck or the documentation at `https://firewalld.org/documentation/man-pages/firewalld.service.html`.

Task 4: Start a port scan of the head node from a compute node (1 min)

From one of the rebooted compute nodes, start a port scan of the head node by

```
nmap -A ADDRESS
```

where `ADDRESS` is the IP address of the head node. The scan takes quite a while, so move onto the next task in your other terminal session/s.

Task 5: Creating Zones for the cluster and external networks (10 min)

On the head node, go to `/etc/firewalld/zones` for setting up the Zones.

The `public` Zone will be repurposed for the external network. Remove all services, forwarding, etc. from it you don't need, remembering to keep SSH (otherwise you will lock yourself out) and important IPv6 items. Notice that the Zone file has no `<interface name="INTERFACE"/>` nor `source address="ADDRESS/PREFIX"/>` entries. It doesn't need them because the `public` Zone is the default, so anything not in another Zone is put into it.

Create a Zone file for the cluster's internal network (the PXE network) adding all the services in the previous table. Make sure to pick a filename that is before `public.xml` when sorted as seen by `ls`. This is important so that `public.xml` is the last one parsed since it is the default Zone that should only include what is not in the other Zones. Remember, if a Service file's name is `foo.xml`, the Service name is `foo`. Add the cluster internal network with `<source address="10.0.0.0/24"/>` line. Add the TCP port you chose for InfluxDB (the suggested port was 8009) with `<port port="PORT" protocol="tcp"/>`.

Now, look at the results of your port scan of the head node in the other terminal session. If you look through it, you will see the most of the services you are using, but not all (to see the others, run `netstat -tulpn` on the headnode to see the open sockets). You will also likely notice the MariaDB used as the backend for slurmdbd, which is something you definitely want to block access to (don't add it to the Zone). But for rpc (part of NFS), you will notice many ports that were not included in the table nor the `nfs3.xml` and `rpc-bind.xml` Service files.

NFS v3 uses a lot of extra ports, which must be added too or else the compute nodes won't be able to mount the head node's NFS shares. Specifically, you will need to open the firewall for lockd, mountd, and statd. NFS by default chooses whatever port it feels like for lockd and statd, but these can be chosen. Modify `/etc/nfs.conf` and set the mountd port to 20048 (the typical value), lockd ports 32001 (somewhat arbitrary), and the statd port to 32002 (somewhat arbitrary). Then restart the NFS services to use the new ports with

```
systemctl restart rpc-statd
systemctl restart nfs-server
```

In the Zone file for the cluster's internal network, add the `mountd` service (firewalld provides it) and add the lockd and statd ports (both TCP and UDP) like `<port port="PORT" protocol="tcp"/>`.

For future reference, the documentation for Zone files is at https://firewalld.org/documentation/man-pages/firewalld.zone.html.

Task 6: Start the firewall and check it (5 min)

Start the firewall on the head node with `systemctl start firewalld` and then check that your SSH session still works. If your SSH session doesn't work, it means you have locked yourself out and you will need to use the Console interface in OpenStack to login and turn off the firewall so you can fix it. Check that your Service and Zone files didn't have any bugs by running `systemctl status firewalld` and fix any bugs you find.

On the compute node you ran the port scan, do the following tests:

- Use the squid proxy with `curl https://zenquotes.io/api/random`
- Can still talk to the slurm controller with `sinfo`
- Use the NFS share with `ls /nfs/home`

If everything is successful, enable the firewall on the head node permanently with `systemctl enable firewalld`

Run the port scan of the head node again and check it later while working on the next taskand see if you successfully blocked access to MariaDB.

Task 7: Turn the head node into a gateway for the compute nodes (10 min)

Since the cluster internal network and the external network are in different Zones, routing must be configured in a Policy file. Create the Policy file `/etc/firewalld/policies/cluster_to_public.xml` (name is arbitrary, but descriptive names like this are a good idea). Set the ingress zone to the name of your internal network's

Zone with `<ingress-zone name="NAME"/>`, and the egress to `<egress-zone name="public"/>`. Enable NAT with `<masquerade/>`. Then restart the firewall to add the Policy and run `systemctl status firewalld` to check and fix any bugs you find.

Now, the Warewulf profile for the nodes has to be changed to use the head node as a gateway and disable setting the environment variables for the squid proxy. Add the gateway with

```
wwctl profile set --netname lan0 --gateway HEADNODEADDRESS default
```

where `HEADNODEADDRESS` is the IP address of the headnode on the PXE network. Then, edit `/etc/warewulf/nodes.con` to remove the overlay where you setup the squid proxy environmental variables from the profile. Rebuild the overlays with `wwctl overlay build` and reboot the compute nodes. When a node has rebooted, login and do the following:

1. Check that no proxy environment variables are set by running `printenv | grep -i proxy`
2. Check that the gateway is set as the default route looking at the output of `ip route`
3. Check that you can access a web server on the internet with `curl https://zenquotes.io/api/random`
4. Check that `ping -c 3 gwdg.de` succeeds

For future reference, the documentation for Policy files is at `https://firewalld.org/documentation/man-pages/firewalld.policy.html`.

Optional Task 8: Extra Task (5 min)

This is a difficult **additional** task that will support your understanding in the topic.

So far, you have worked exclusively with the high-level firewall tool firewalld. Under the hood, firewalld uses the low-level nftables firewall system. Print the nftables firewall rules with

```
nft list ruleset
```

and look through them. You will find several chains with labels like INPUT, FORWARD, etc. See if you can find the rules for the Zones and Policies you made and the Services you enabled.