12.6.2 Configure firewalld

Click one of the buttons to take you to that part of the video.

Configure firewalld 0:00-0:10

In this demonstration, we're going to show firewall technologies and firewall rule sets.

Firewall Status and Start 0:11-1:37

The first thing that we need to ensure when we are manipulating or changing firewall rules, is we need to make sure that the firewall process is running. To do that, we run firewall -cmd followed by the keyword - -state and that tells us whether or not it's running. Of course, now tells us that it's not running, so we need to start that with systemctl.

Before we do that, notice that the user that I'm logged in is just a normal user. We really need to be the superuser to do this. We can use sudo on all of our commands, but for this demonstration we're going to go ahead and ‘sudo su –‘ to our root user. The prompt has changed, whoam I shows that I am root, so we are good to go.

Let's go ahead and start the process, so it's ‘systemctl start firewalld', firewalld is the daemon, so that started. Just to be sure that it starts every time that are system boots, we need to ‘enable' the firewalld process, so we'll put in that keyword, firewalld. Now every time our system boots, the firewall process will also run. Just to check, ‘firewall -cmd --state' shows that the firewall is running, so we're ready to go forward.

Firewall Commands 1:38-2:38

There are many, many, many command line parameters that are available for the firewall process.

Just to show you, if we do, the ‘firewall -cmd --help', I'll go ahead and filter that through ‘more' just because there are so many screens, you're going to see that there are several different command-line parameters that we can add and use for the firewall process.

Now one bit of warning. The firewall is the first line of defense for most organizations, so when manipulating the firewall and changing firewall rules and parameters, it's really important that the person doing it understands and knows what he or she is doing. So, this is something that should not be taken lightly and really should have a bit of knowledge before attempting to do anything. If it's a test system, and you really don't care, then find, a go ahead and use this for experimentation. But be sure and understand what it is you're doing if this is a production machine.

Configuration files 2:39-3:30

All right, so moving forward. There are a couple of configuration files to look at, the first one is in the /etc directory. We'll go ahead and use the ‘less' program here so we can scroll up and down. We'll go to the /etc/firewall directory and we will go ahead and look at the firewalld.conf file.

The configuration file has the ‘DefaultZone', the ‘Minimal mark', ‘Clean up on exit', ‘Lockdown', basically, all of the defaults that we want for our firewalld process. For the most part, we're going to leave these at defaults. Again, if we know were doing and we feel the change is needed, we can do that, or if someone in support tells us, "hey you need to make this change", go ahead and do that. Otherwise, you probably want to leave that file alone.

Set Zones 3:31-5:47

In the /usr/lib/firewalld directory, there are many other directories within there. The ‘zones' file, the ‘services' file, that's where all of our zones are kept and that's where all of our services are kept. So, changing directories to the zones and doing a directory listing, you see those are all of our zones. We have the block.xml, dmz.xml, drop.xml, external.xml, home.xml, all of our zones, and their all XML files. If you are an XML programmer and understand XML, go ahead and make changes if you wish. Otherwise, again, probably want to leave these alone.

If we look at the services directory, you're going to see that there are many, many different services that we have here. Again, all XML files.

All right, so I'll change back to our home directory clear the screen, and we're going to do a couple of things.

First thing we want to do is we want to see what our default zone is, always wanted to make sure. So, we want to do this to find out what our default zone is before we start making any changes.

To do that, we run the firewall -cmd again and we --get-default-zone.

So, it tells us it's public, which is great but let's just say we want to make a change and let's make it the internal zone. So, we run the firewall-cmd again and we --set-default-zone and that equals internal. So, we've just changed it and if we go ahead and run the --get-default-zone again, you'll see that indeed the default zone has changed.

If I want to see all the settings for that zone, I can do that by specifying the zone, which in this case, is ‘internal' and I want to list all of the parameters for this zone. So, you can see that for services I have ssh, I have an mdns, samba, DHCP. These are all internal services that are available for the internal zone.

I can go ahead and add services and remove services. I can do them on the fly. I can change the parameters. Let's go ahead and add the service HTTP.

Add a service to a zone 5:48-7:35

To do that, ‘firewall -cmd --zone=internal' and what we want to do is add a service and we'll say the services is http. Again, successful. That's good. Now, if we do the --list-all for this internal zone. You'll see that http in now at the end. That's great. That's fantastic, but that happened at run time, but once the system reboots or the firewall is reloaded, that will go away.

Let's go ahead and do that. Just so you can see it; ‘firewall -cmd --reload'.

All this does is restart the demon, basically reload the configuration files. So now I'm doing the same command, ‘firewall -cmd --zone=internal --list-all', and you'll see that http is not there.

If we want to make it so that it will be there the next time, we boot we can add the parameter --permanent.

Okay, so that's been successful, but here's the catch. I changed the configuration file. I did not add it to the run time list. So, when I look at the services that are running. Notice http is not there. Now I can add it. Just like I did before without the permanent flag and that'll change the runtime environment, or I can go ahead and I can reload the command again, which will reload the configuration files, and now the http is there, and this will now be there from this point forward.

I can also add or remove ports by port number, or I can add services as well.

Summary 7:36-7:38

In this demonstration, we showed the firewall technologies firewall commands and dynamic rule sets.
