### **Part 2: "Drop Zone" Lab**

#### **Log into the Azure firewall machine**

Log in using the following credentials:

* Username: sysadmin
* Password: cybersecurity

#### **Uninstall ufw**

Before getting started, you should verify that you do not have any instances of [ufw] running. This will avoid conflicts with your firewalld service. This also ensures that firewalld will be your default firewall.

* Run the command that removes any running instance of [ufw].
  + [$ sudo ufw disable]
  + [$ sudo apt remove ufw]

#### **Enable and start firewalld**

By default, these services should be running. If not, then run the following commands:

* Run the commands that enable and start firewalld upon boots and reboots.
  + [$ sudo systemctl start firewalld]
  + -$ sudo systemctl enable firewalld]

Note: This will ensure that firewalld remains active after each reboot.

Confirm that the service is running.

* Run the command that checks whether or not the firewalld service is up and running.
  + [$ systemctl status firewalld]

#### **List all firewall rules currently configured.**

Next, lists all currently configured firewall rules. This will give you a good idea of what's currently configured and save you time in the long run by not doing double work.

* Run the command that lists all currently configured firewall rules:
  + [$ sudo firewall-cmd --list-all]

Take note of what Zones and settings are configured. You may need to remove unneeded services and settings.

**List all supported service types that can be enabled.**

* Run the command that lists all currently supported services to see if the service you need is available
  + [$ sudo firewall-cmd --get-services]
* We can see that the Home and Drop Zones are created by default.

#### **Zone Views**

* Run the command that lists all currently configured zones.
  + [$ sudo firewall-cmd --get-zones]
* We can see that the Public and Drop Zones are created by default. Therefore, we will need to create Zones for Web, Sales, and Mail.

#### **Create Zones for Web, Sales, and Mail.**

Run the commands that create Web, Sales, and Mail zones.

[$ sudo firewall-cmd --permanent --new-zone=web]

[$ sudo firewall-cmd --permanent --new-zone=sale]

[$ sudo firewall-cmd --permanent --new-zone=mail]

**Set the zones to their designated interfaces:**

Run the commands that set your eth interfaces to your zones.  
 [$ sudo firewall-cmd --reload]

[$ sudo firewall-cmd --zone=web --add-interface=eth1]

[$ sudo firewall-cmd --zone=sale --add-interface=eth2]

[$ sudo firewall-cmd --zone=mail --add-interface=eth3]

#### **Add services to the active zones:**

* Run the commands that add services to the **public** zone, the **web** zone, the **sales** zone, and the **main** zone.
* Public:
  + [$ sudo firewall-cmd --zone=public --add-service=http]
  + [$ sudo firewall-cmd --zone=public --add-service=https]
  + [$ sudo firewall-cmd --zone=public --add-service=pop3]
  + [$ sudo firewall-cmd --zone=public --add-service=smtp]
* Web
  + [$ sudo firewall-cmd --zone=web --add-service=http]
* Sales
  + [$ sudo firewall-cmd --zone=sales --add-service=https]
* Mail
  + [$ sudo firewall-cmd --zone=mail --add-service=smtp]
  + [$ sudo firewall-cmd --zone=mail --add-service=pop3]
* What is the status of http, https, smtp, and pop3?
  + Active

#### **Add your adversaries to the Drop Zone.**

Run the command that will add all current and any future blacklisted IPs to the Drop Zone.  
 [$ sudo firewall-cmd --zone=drop --add-source=10.208.56.23]

[$ sudo firewall-cmd --zone=drop --add-source=135.95.103.76]

[$ sudo firewall-cmd --zone=drop --add-source=76.34.169.118]

#### **Make rules permanent then reload them:**

It's good practice to ensure that your firewalld installation remains nailed up and retains its services across reboots. This ensures that the network remains secured after unplanned outages such as power failures.

* Run the command that reloads the firewalld configurations and writes it to memory
  + [$ sudo firewall-cmd --runtime-to-permanent]

#### **View active Zones**

Now, we'll want to provide truncated listings of all currently **active** zones. This is a good time to verify your zone settings.

* Run the command that displays all zone services.
  + [$ sudo firewall-cmd --get-active-zones]

#### **Block an IP address**

* Use a “rich-rule” that blocks the IP address 138.138.0.3.
  + [$ sudo firewall-cmd --add-rich-rule='rule family="ipv4" source address="138.138.0.3" reject' ]

#### **Block Ping/ICMP Requests**

Harden your network against ping scans by blocking icmp ehco replies.

* Run the command that blocks pings and icmp requests in your public zone.
  + [$ sudo firewall-cmd --permanent --add-icmp-block=echo-request --add-icmp-block=echo-reply]

#### **Rule Check**

Now that you've set up your brand new firewalld installation, it's time to verify that all of the settings have taken effect.

* Run the command that lists all of the rule settings. Do one command at a time for each zone.
  + [$ sudo firewall-cmd --info-zone=public]
  + [$ sudo firewall-cmd --info-zone=web]
  + [$ sudo firewall-cmd --info-zone=sales]
  + [$ sudo firewall-cmd --info-zone=mail]
  + [$ sudo firewall-cmd --info-zone=drop]
* Are all of our rules in place? If not, then go back and make the necessary modifications before checking again.

Congratulations! You have successfully configured and deployed a fully comprehensive firewalld installation.