Lab 4.1 Network Firewalls 1

In this lab we are going to shut down and then manage traffic between the LAN, DMZ,WAN and MGMT Networks.

The initial configuration of fw01 will be illustrated in detail, but you will need to use that information to configure fw-mgmt.

Prerequisites

Make sure you can do the following before progressing in the lab (this step is extremely important for the success of your lab).
- rw01 can ping web01 via its static route, rw01 can browse to web01
- wks01 can browse web01
- wks01 can browse wazuh
- web01 can ping wazuh

Task 1: Configuring fw01

Create and link firewall zones to interfaces (eth0, eth1, eth2)

```
set zone-policy zone WAN interface eth0
set zone-policy zone DMZ interface eth1
set zone-policy zone LAN interface eth2
commit save
```

Creating default drop and log rules across fw01

Step 1: WAN and DMZ firewalls

Observe and repeat the following commands. In the illustration below, we have created firewalls for WAN to DMZ and DMZ to WAN, we are going to lock them down with a default drop directive, and we will log violations of the firewall rules. We have also assigned firewalls to the respective direction of communication between zones.
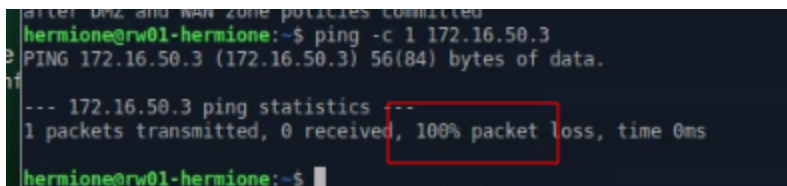
Firewalls for WAN and DMZ

```
set firewall name WAN-to-DMZ default-action drop
set firewall name DMZ-to-WAN default-action drop
set firewall name WAN-to-DMZ enable-default-log
set firewall name DMZ-to-WAN enable-default-log
```

Assigning Firewalls to Zones

```
set zone-policy zone WAN from DMZ firewall name DMZ-to-WAN
set zone-policy zone DMZ from WAN firewall name WAN-to-DMZ
commit
save
```

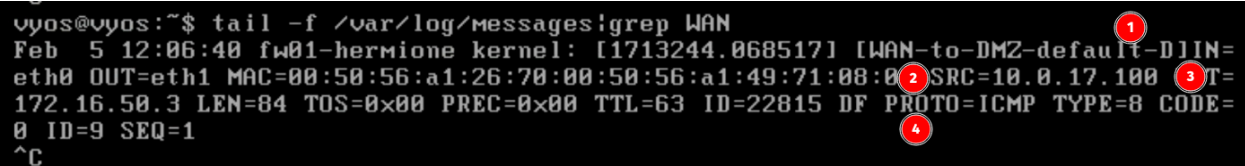Attempt to connect to web01 via rw01, it should fail

On fw01, monitor your firewall logs with the following command:

```
tail -f /var/log/messages | grep WAN
```

Try your failed connection test again, You should observe a failed message similar to this:

There is lots of good troubleshooting data here! This screenshot indicates
1. That the default drop rule for WAN-TO-DMZ via eth0 was invoked.
2. The source ip is rw01
3. The destination ip is web01
4. The protocol was ICMP

Deliverable 1: Provide a screenshot showing a [WAN-TO-DMZ-default-D]
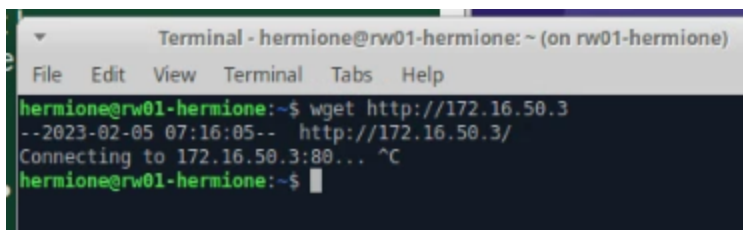log entry similar to the one above.

Step 2: Allow http inbound

Allow http traffic from the WAN to the DMZ based web01 using the following syntax, remember you use your IP address for web01.

Using what you know about VyOS Syntax, figure out how to append rule 10 to the WAN-to-DMZ firewall

```
vyos@fw01-hermione# show firewall name WAN-to-DMZ
  default-action drop
  enable-default-log
  rule 10 {
      action accept
      description "Allow HTTP from WAN to DMZ"
      destination {
          address 172.16.50.3
          port 80
      }
      protocol tcp
  }
[edit]
```

Try to connect via http, the connection should still fail.

```
Terminal - hermione@rw01-hermione: ~ (on rw01-hermione)
File   Edit   View   Terminal   Tabs   Help
hermione@rw01-hermione:~$ wget http://172.16.50.3
--2023-02-05 07:16:05--  http://172.16.50.3/
Connecting to 172.16.50.3:80... ^C
hermione@rw01-hermione:~$
```

This time the failure is due to another firewall. **The communication was stopped on the way back out, not on the way in. We need to explicitly tell the DMZ-TO-WAN firewall to allow established connections initiated from the WAN back out again**. The following log shows the DMZ-TO-WAN default drop at work here.

```
Feb  5 12:17:57 fw01-hermione kernel: [1713920.91375 1  [DMZ-to-WAN-default-DJIN=
eth1 OUT=eth0 MAC=00:50:56:a1:81:3a:00:50:56:a1:49:ad:08:0 2 SRC=172.16.50.3 DST=
10.0.17.100 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=0 DF PROTO=TC 3 SPT=80 DPT=40262
WINDOW=28960 RES=0x00 ACK SYN URGP=0
```

Updated Sep 15, 2023

1. The rule is DMZ-to-WAN or outbound traffic from the DMZ back to rw01
2. The source ip is web01
3. The source port is port 80/tcp (the web server response to the wget from rw01)

Step 3: Allowing established connections back out again.

The following screenshot shows an updated DMZ-to-WAN firewall rule that will allow connections that were let in the door, back out again.

```
vyos@fw01-hermione# show firewall name DMZ-to-WAN
 default-action drop
 enable-default-log
 rule 1 {
     action accept
     state {
         established enable
     }
 }
}
```

💡 We will reserve rule **1** for two conditions. The first is to allow established connections back out again, the second would be to have an open rule where all connections are allowed. Typically this would be the only rule in such a firewall.

Deliverable 2: Take a screenshot similar to the one below that shows a failed wget or curl (1) followed by a successful connection to your web server. **Make sure you've deleted the default welcome.conf file, you've restarted httpd and have added a simple index.html banner as shown in (2).**
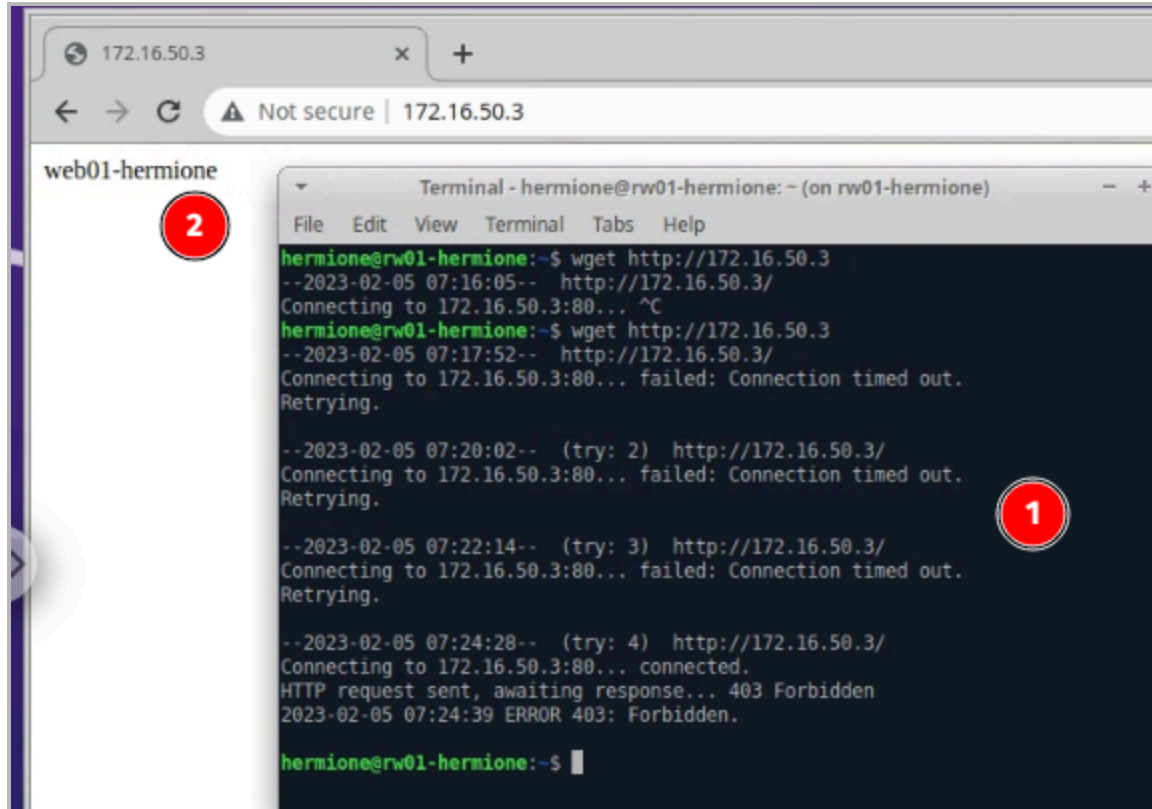
Step 4: DMZ and LAN Traffic Firewalls

We are going to continue our firewalling by creating default firewalls for LAN and DMZ and link them to zone policies. The completed DMZ and LAN zones should look like this.

Firewalls

```
vyos@fw01-hermione# show firewall name LAN-to-DMZ
 default-action drop
 enable-default-log
[edit]
vyos@fw01-hermione# show firewall name DMZ-to-LAN
 default-action drop
 enable-default-log
[edit]
```

Zones

```
vyos@fw01-hermione# show zone-policy zone DMZ
 from LAN {
     firewall {
         name LAN-to-DMZ
     }
 }
 from WAN {
     firewall {
         name WAN-to-DMZ
     }
 }
 interface eth1
```

```
vyos@fw01-hermione# show zone-policy zone LAN
 from DMZ {
     firewall {
         name DMZ-to-LAN
     }
 }
 interface eth2
[edit]
```

💡Whenever you set something you should **commit** it. If you want that setting to survive a reboot, you better **save** it too.⌷

Step 5: Wassup with Wazuh?

Right now we have firewalls whose only rules are to <u>drop</u> everything (except port 80 to web01 from the WAN). We are now going to use debugging techniques shown earlier to find out why our wazuh traffic doesn't work between DMZ and LAN (actually MGMT, but fw01 does not know about the MGMT network, just the LAN).

The Wazuh server expects clients to connect to it via tcp/1514 and tcp/1515, this is a good connection to start with. We will examine or logs to see if there are any drop messages for these ports.

DMZ-to-LAN

Deliverable 3: Provide a screenshot similar to the one above of /var/log/messages on fw01 that shows a drop message like the one below, make sure you select the message that indicated PROTO=TCP and DPT=1514 or 1515

Step 6: Allow Wazuh agent communications

```
vyos@fw01-hermione# cat /var/log/messages;grep 1514 ; head -1
Feb  5 12:41:43 fw01-hermione kernel: [1715346.976832] [DMZ-to-LAN-default-D]IN=
eth1 OUT=eth2 MAC=00:50:56:a1:81:3a:00:50:56:a1:49:ad:08:00 SRC=172.16.50.3 DST=
172.16.200.10 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=18313 DF PROTO=TCP SPT=33850 D
PT=1514 WINDOW=29200 RES=0x00 SYN URGP=0
[edit]
vyos@fw01-hermione# cat /var/log/messages;grep 1515 ; head -1
Feb  5 12:39:22 fw01-hermione kernel: [1715205.904873] [DMZ-to-LAN-default-D]IN=
eth1 OUT=eth2 MAC=00:50:56:a1:81:3a:00:50:56:a1:49:ad:08:00 SRC=172.16.50.3 DST=
172.16.200.10 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=4239 DF PROTO=TCP SPT=45958 DP
T=1515 WINDOW=29200 RES=0x00 SYN URGP=0
[edit]
```

The following firewall rule allows 1514,1515 TCP through the DMZ-to-LAN firewall.

```
vyos@fw01-hermione# show firewall name DMZ-to-LAN rule 10
 action accept
 description "wazuh agent communications with wazuh server"
 destination {
     address 172.16.200.10
     port 1514,1515
 }
 protocol tcp
```

Step 7: Allowing established wazuh traffic back

Try finding LAN-to-DMZ traffic that has been dropped that has a SPT=1514,1515. This is a tcp connection, so we need to allow established back through the related firewall (LAN-to-DMZ)

```
vyos@fw01-hermione# cat /var/log/messages | grep "SPT=151" | head -n 1
Feb  5 12:49:45 fw01-hermione kernel: [1715829.007674①[LAN-to-DMZ-default-D]IN=
eth2 OUT=eth1 MAC=00:50:56:a1:b2:6c:00:50:56:a1:6b:af:08:00 SRC=172.16.200.10 DS
T=172.16.50.3 LEN=60 TOS=0x00 PREC=0x00 TTL=62 ID=0 DF PROTO=T② SPT=1514 DPT=33
856 WINDOW=65160 RES=0x00 ACK SYN URGP=0
[edit]
```

Deliverable 4. Provide a screenshot of your new LAN-to-DMZ rule 1 that allows established connections back through the LAN-to-DMZ firewall.

Step 8: Configure LAN-TO-WAN Firewall

We are receiving complaints from our Burlington-based employees because they cannot surf the internet or listen to Spotify. It is also likely that CRD is no longer working. We need to allow clients to initiate <u>any</u> connections to the WAN. This <u>one</u> requirement can be the [Achilles Heel](#) of network security. Clients in this zone typically need to initiate connections in a very permissive manner to do their jobs. We may need to look at supplementary host based controls and restrictive web proxies later.

Create a default LAN to WAN firewall and associate it with the appropriate zone policy. This firewall will have only one rule allowing LAN clients to initiate WAN connections.

The completed LAN-TO-WAN firewall looks like:

```
vyos@fw1-hermione# show firewall name LAN-to-WAN
 default-action drop
 enable-default-log
 rule 1 {
     action accept
 }
```

Step 9: Configure WAN-TO-LAN Firewall

Create the WAN-TO-LAN firewall, link it to the appropriate zones and allow established connections back from WAN to LAN

Deliverable 5: Submit a screenshot showing a LAN-TO-WAN browsing session between wks01 and champlain.edu
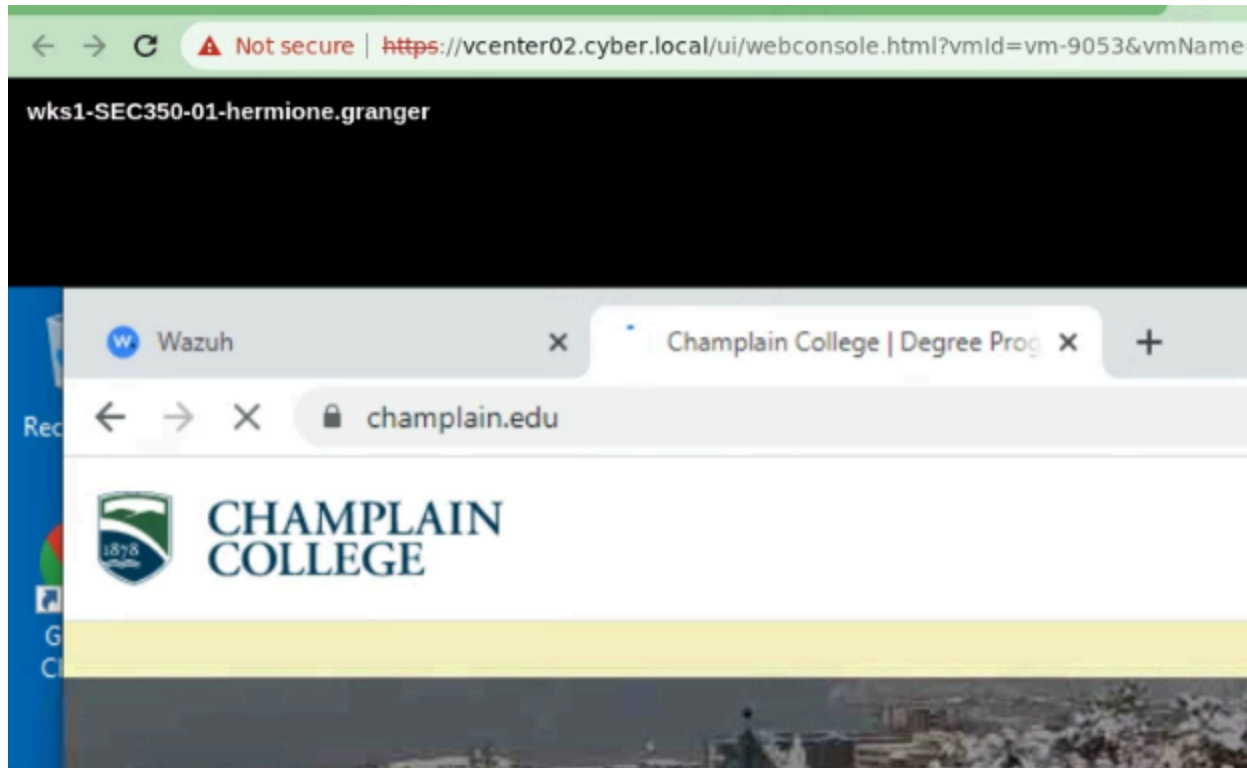
Step 10: Configure LAN to DMZ Firewall

As communication between LAN and DMZ is currently broken, we need to create a firewall, assign to the appropriate zone policy and adjust it to only allow the traffic we want to go through. We want wks01 to be able to browse to web01 and we want mgmt01 to ssh into anything on the DMZ.

With that in mind, create firewall rules on LAN-TO-DMZ that allows
- 80/tcp from LAN to web01.
- 22/tcp from mgmt01 to the DMZ

Step 11: DMZ to LAN Firewall

Make sure to allow established traffic back through

Deliverable 6: Screenshot showing web session between wks01 and web01.
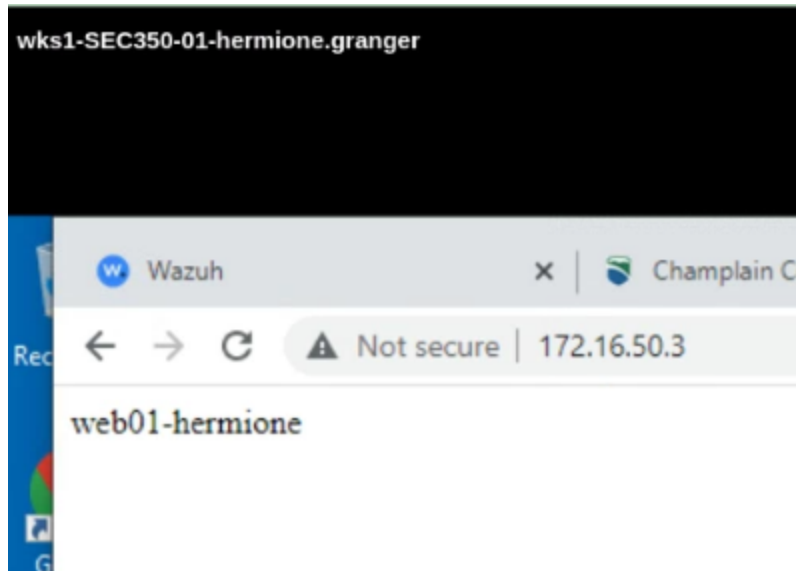
Deliverable 7. ssh into web01 from using the username testwazuhafterfirewall. Attempt this until the session is closed by web01. Provide a screenshot similar to the one below that shows a related security event in wazuh, after fw1 was configured.

Task 2: Configuring fw-mgmt

Now that you have the basics of zone and firewall configuration under your belt, you are going to use the techniques shown above in configuration of fw-mgmt.

Create LAN and MGMT zones on fw-mgmt

Create both zones and assign the correct interfaces and firewalls.

LAN-to-MGMT

Create a LAN-to-MGMT firewall that:
- Allows 1514,1515/tcp from LAN to wazuh
- Allows 443/tcp from mgmt01 on LAN to wazuh
- Allows 22/tcp from mgmt01 on LAN to wazuh
- Allows established traffic back through the related firewall

MGMT-to-LAN

Create a MGMT-TO-LAN firewall that:
- Allows MGMT to initiate any connection to the LAN
- Allows MGMT to initiate any connection to the DMZ
- Allows established traffic back again

If you do this right, you should be able to connect from mgmt02 to the DMZ like so.
1. wget to web01
2. ping to mgmt01
3. ping outside will fail because you didn't explicitly allow MGMT to go anywhere but LAN and DMZ.

Deliverable 8. Provide a screenshot similar to the one below

Deliverable 9. Provide the output of:
show zone on fw-mgmt

Deliverable 10. Provide the output of:
show firewall name LAN-TO-MGMT

Deliverable 11. Provide the output of:
show firewall name MGMT-TO-LAN

Deliverable 12. From mgmt01, Run an ssh test on web01 with a tag that indicates that this is a test of fw-mgmt. Take a screenshot of the resulting log within wazuh.

```
hermione@mgmt01-hermione:~$ ssh fw-mgmt-test@172.16.50.3
fw-mgmt-test@172.16.50.3's password:
Permission denied, please try again.
fw-mgmt-test@172.16.50.3's password:
Permission denied, please try again.
fw-mgmt-test@172.16.50.3's password:
fw-mgmt-test@172.16.50.3: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
hermione@mgmt01-hermione:~$
```

```
0
        12:00                        15:00                    1
```

Time ▾	rule.description
Feb 5, 2023 @ 11:01:59.624	sshd: Attempt to login using a non-existent user

🗁 Expanded document

Table   JSON

ᵗ _index	wazuh-alerts-4.x-2023.02.05
ᵗ agent.id	001
ᵗ agent.ip	172.16.50.3
ᵗ agent.name	web01-hermione
ᵗ data.srcip	172.16.150.10
ᵗ data.srcuser	fw-mgmt-test
ᵗ decoder.name	sshd
ᵗ decoder.parent	sshd

Updated Sep 15, 2023

Deliverable 13. You have a good deal to reflect on and document this week (including the last lab). Make sure you clearly document your week's technical work which includes:
- Updating vyos
- Configuring RIP
- Firewall Zones creation
- Firewall Rule creation
- Debugging Firewall Blocks
- Exporting vyos configurations

See the following video for expectations. Make sure you generate a reflection that discusses what you did (link to articles). You should also export your week 4 vyos configurations for fw01 and fw-mgmt.