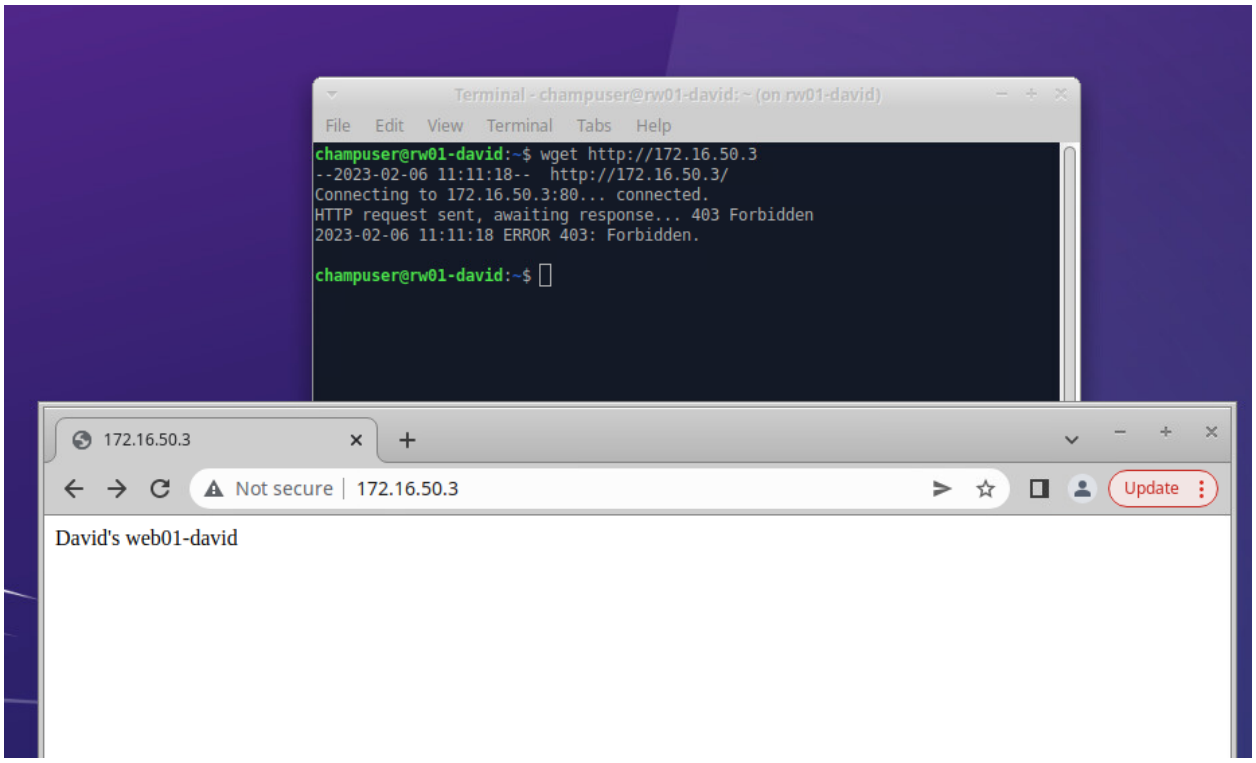
Deliverable 1: Provide a screenshot showing a [WAN-TO-DMZ-default-D] log entry similar to the one above.

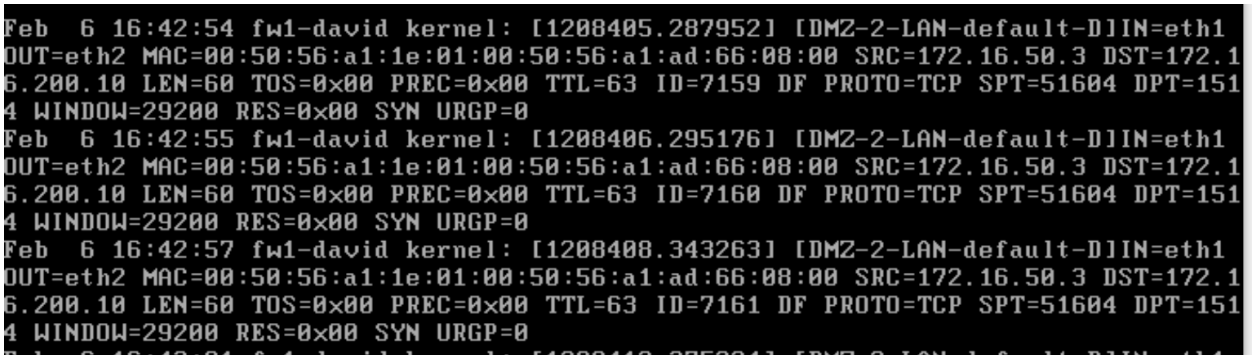
```
vyos@fw1-david# show firewall name W
WAN-2-DMZ  WAN-2-LAN
[edit]
vyos@fw1-david# show firewall name WAN-2-DMZ
 default-action drop
 enable-default-log
 rule 10 {
     action accept
     description "Allow HTTP from WAN to DMZ"
     destination {
         address 172.16.50.3
         port 80
     }
     protocol tcp
 }
[edit]
vyos@fw1-david#
```

```
vyos@fw1-david:~$ cat /var/log/messages | grep WAN
Feb  6 15:45:35 fw1-david kernel: [1204966.443314] [WAN-2-DMZ-default-D]IN=eth0
OUT=eth1 MAC=00:50:56:a1:c9:2c:00:50:56:a1:28:7a:08:00 SRC=10.0.17.15 DST=172.16
.50.3 LEN=84 TOS=0x00 PREC=0x00 TTL=63 ID=43180 DF PROTO=ICMP TYPE=8 CODE=0 ID=4
 SEQ=1
```

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).



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

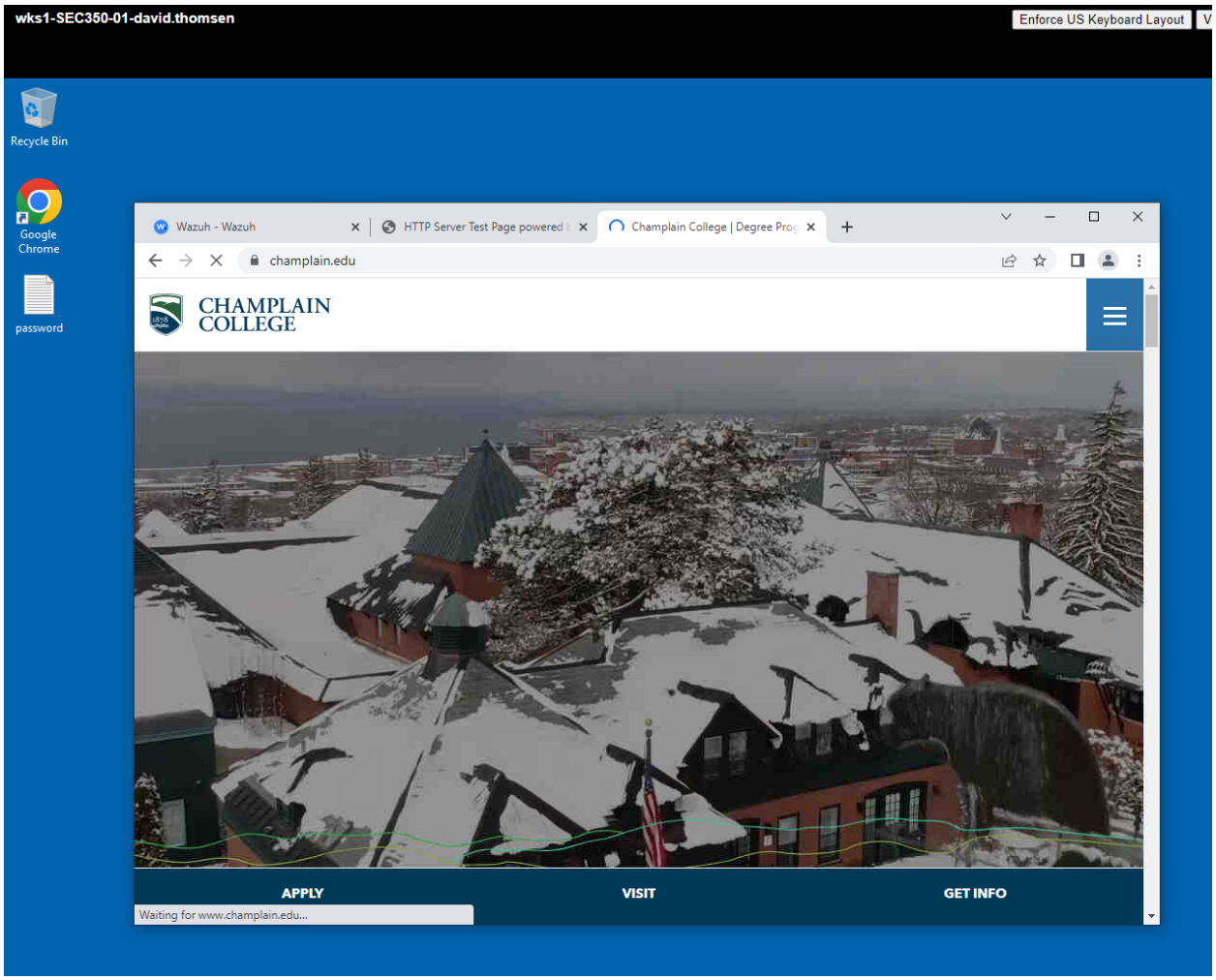


Deliverable 4. Provide a screenshot of your new LAN-to-DMZ rule 1 that allows established connections back through the LAN-to-DMZ firewall.

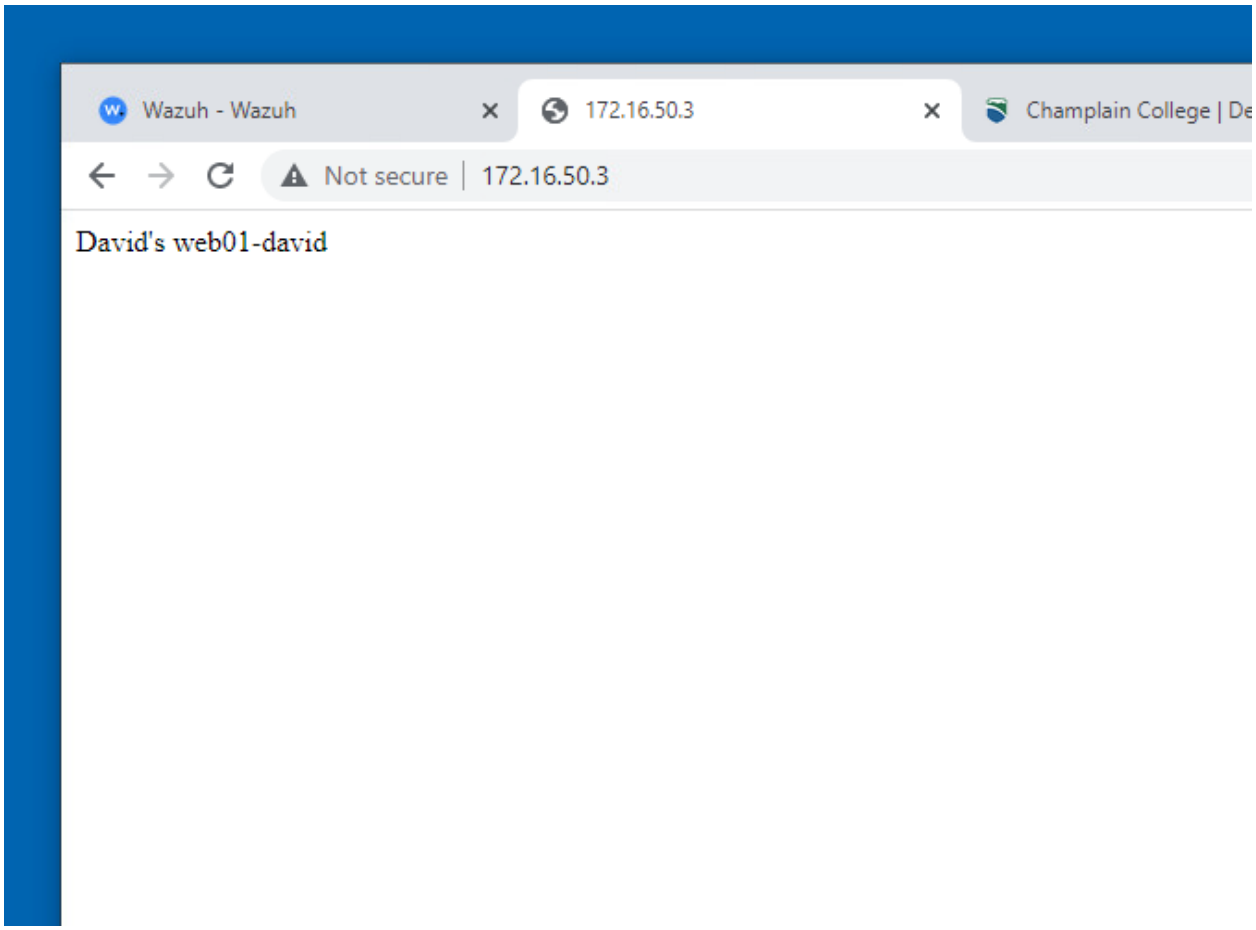
```
[edit]
vyos@fw1-david# cat /var/log/messages | grep "SPT=151" | head -n 1
Feb  6 16:36:12 fw1-david kernel: [1208002.774207] [LAN-2-DMZ-default-D]IN=eth2
OUT=eth1 MAC=00:50:56:a1:e1:dc:00:50:56:a1:6c:a3:08:00 SRC=172.16.200.10 DST=172
.16.50.3 LEN=60 TOS=0x00 PREC=0x00 TTL=62 ID=0 DF PROTO=TCP SPT=1514 DPT=51598 W
INDOW=65160 RES=0x00 ACK SYN URGP=0
[edit]
vyos@fw1-david# _
```

```
vyos@fw1-david# show firewall  name LAN-2-DMZ
 default-action drop
 enable-default-log
 rule 420 {
     action accept
     description "The LAN-2-DMZ Stamp of approval"
     state {
         established enable
     }
 }
[edit]
```

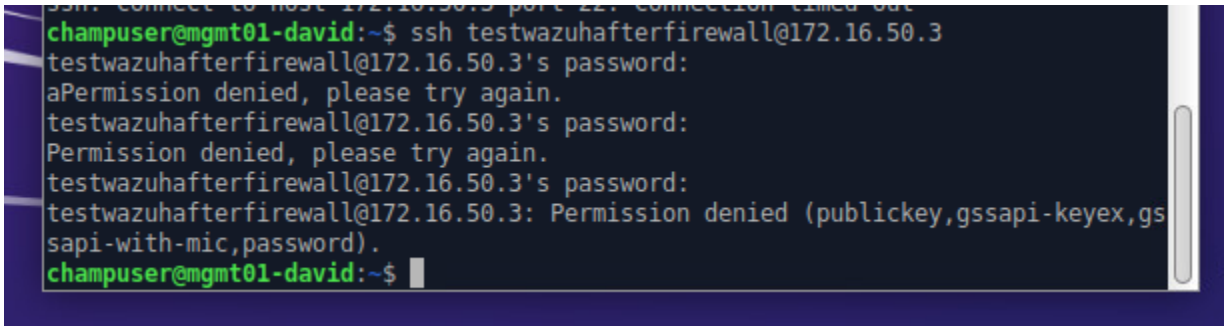
Deliverable 5: Submit a screenshot showing a LAN-TO-WAN browsing session between wks01 and champlain.edu

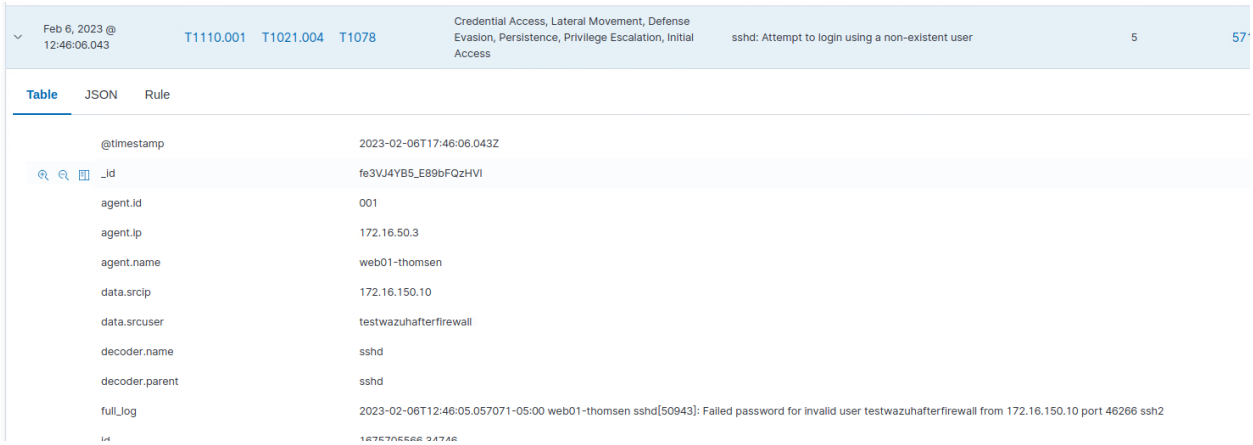


Deliverable 6: Screenshot showing web session between wks01 and web01.

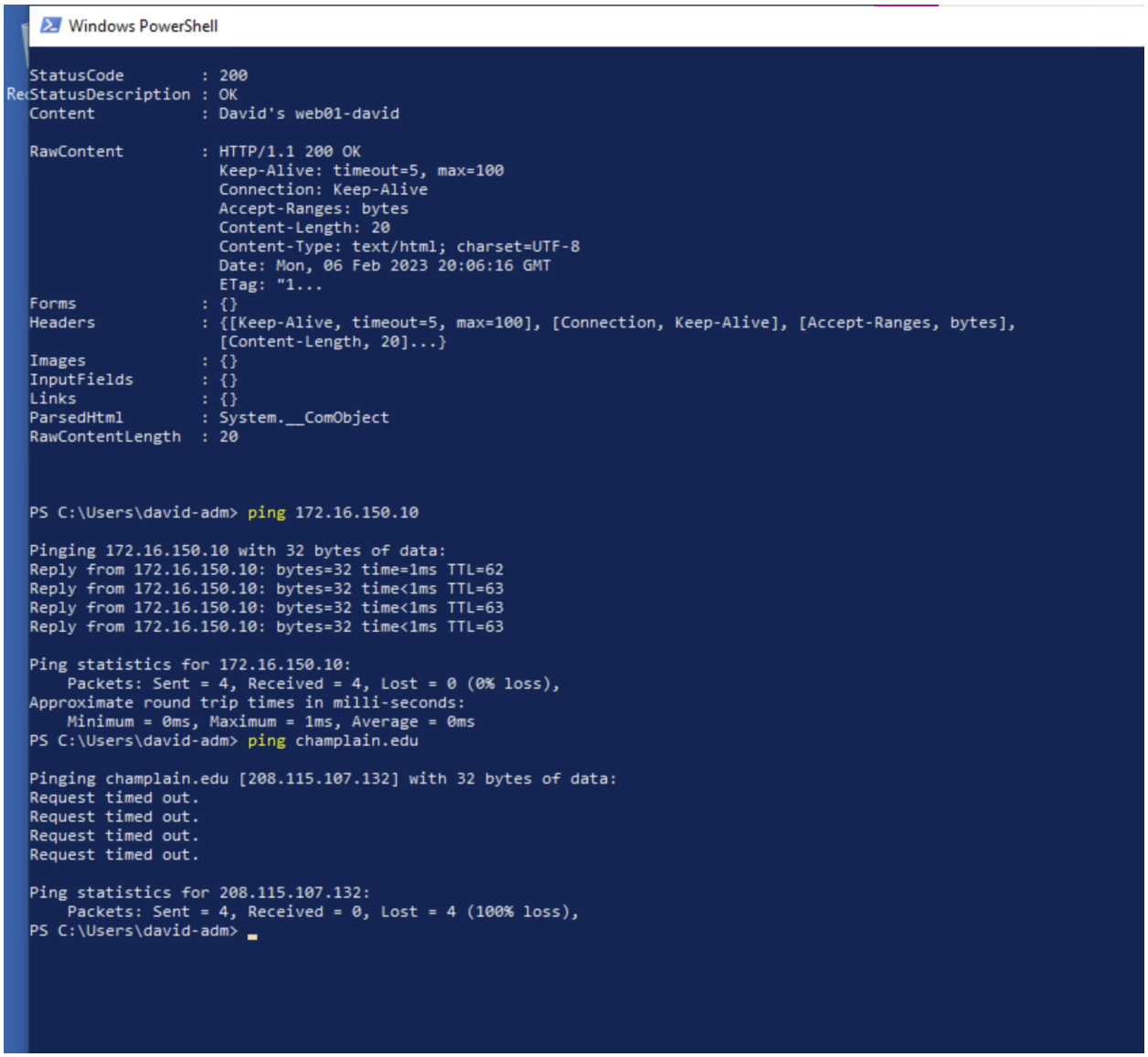


Deliverable 7. ssh into web01 from using the username testwazuhafterfirewall. Attempt this until the session is closed by web01. Provide a screenshot similar to the one below that shows a related security event in wazuh, after fw1 was configured.





Deliverable 8. Provide a screenshot similar to the one below



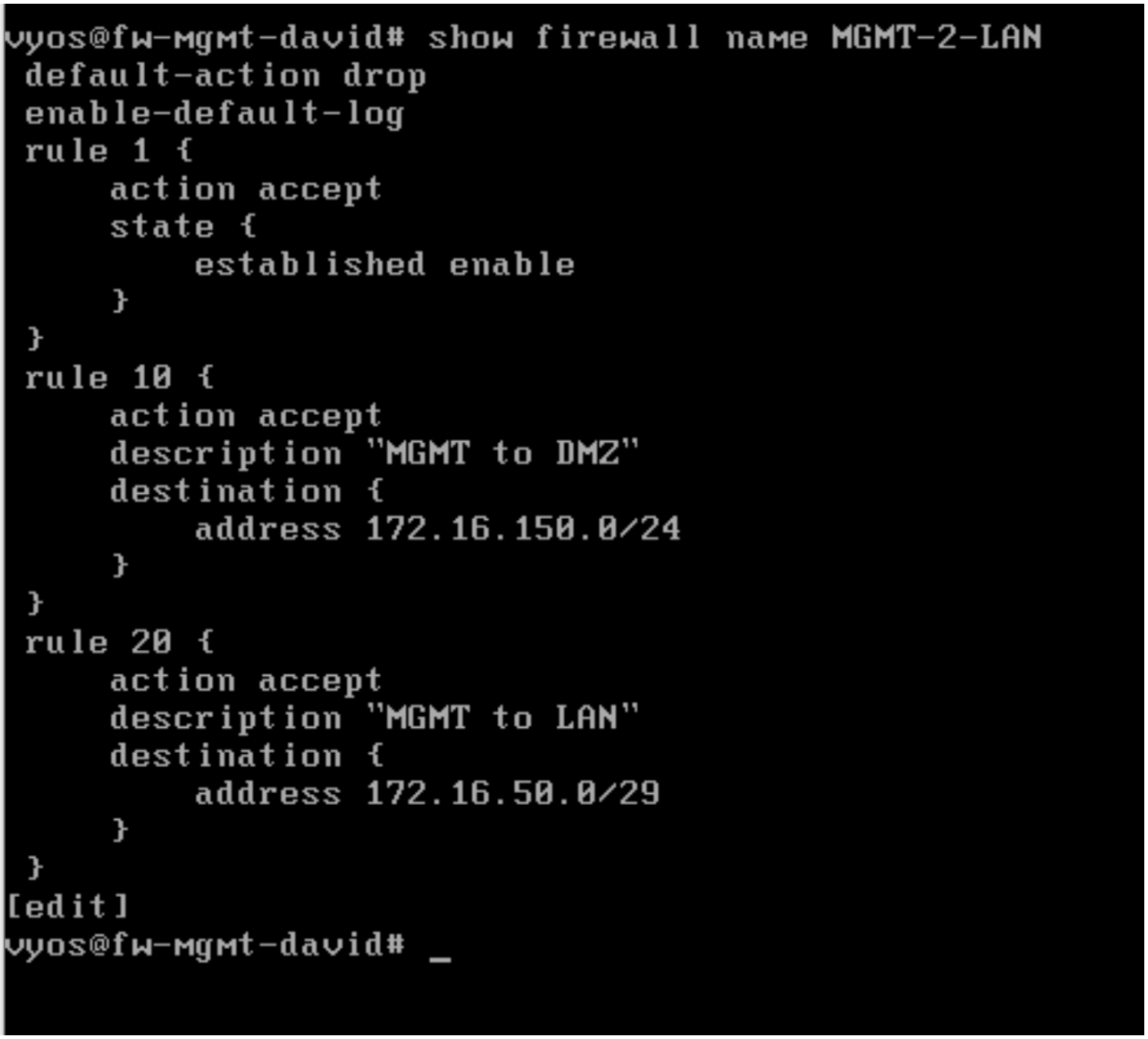
Deliverable 9. Provide the output of:
show zone on fw-mgmt

```
vyos@fw-mgmt-david:~$ show zone
vyos@fw-mgmt-david:~$
```

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

```
default-action drop
enable-default-log
rule 10 {
    action accept
    destination {
        address 172.16.200.10
        port 1514,1515
    }
    protocol tcp
    state {
        established enable
    }
}
rule 20 {
    action accept
    destination {
        address 172.16.200.10
        port 22,443
    }
    protocol tcp
    source {
        address 172.16.150.10
    }
    state {
```

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.