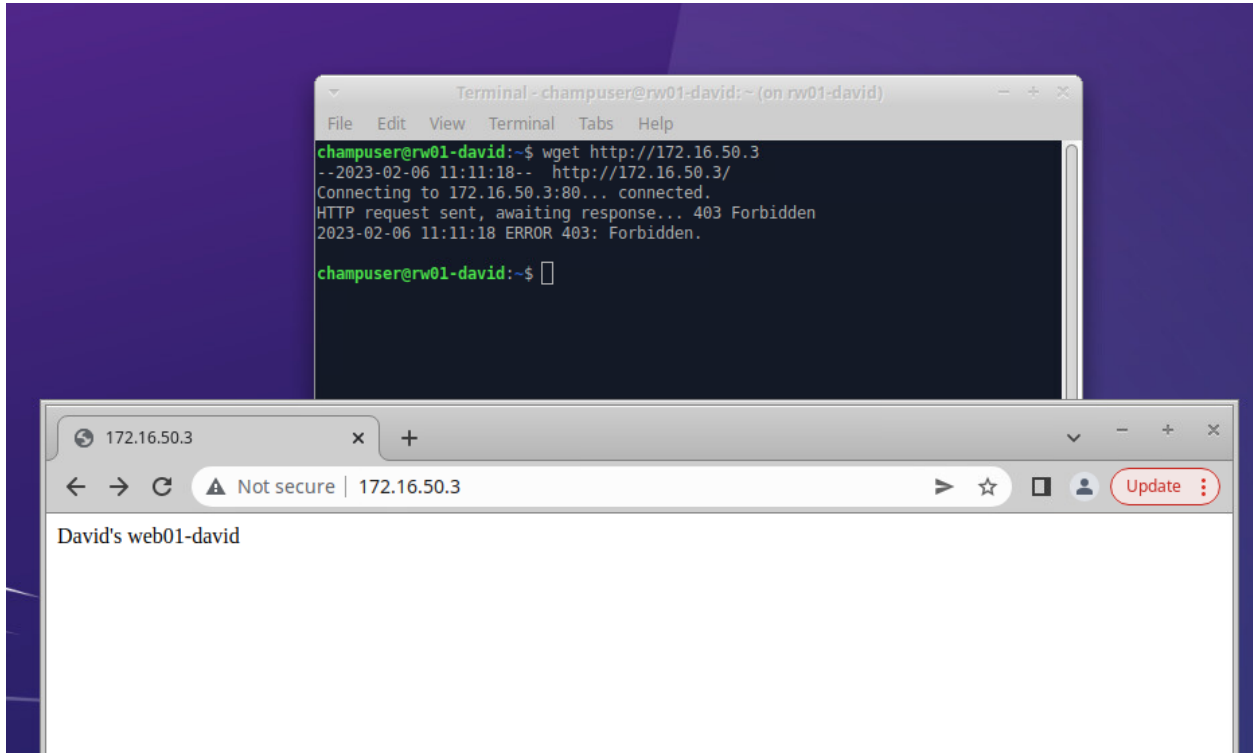


Deliverable 1: Provide a screenshot showing a [WAN-TO-DMZ-default-D] log entry similar to the one above.

```
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

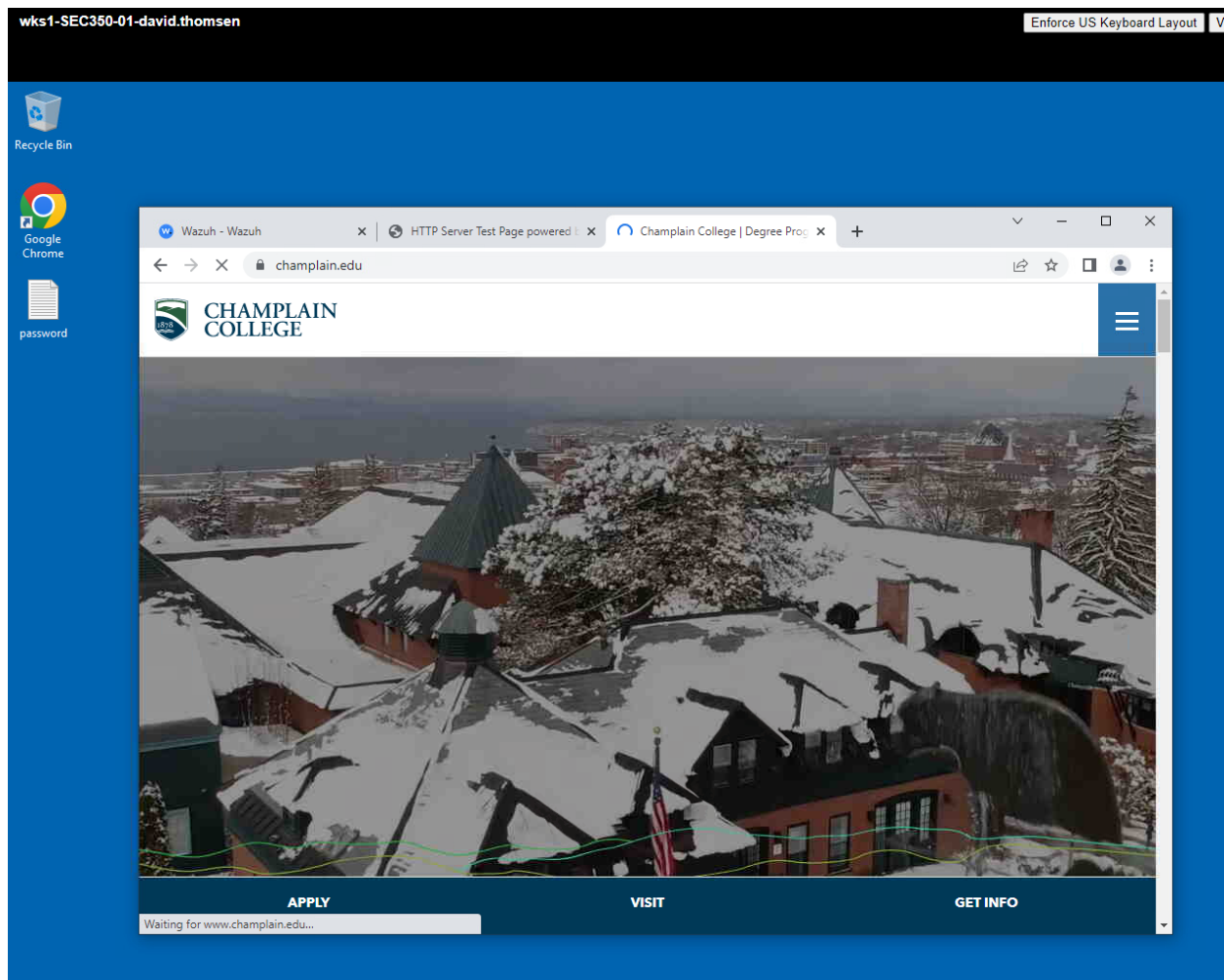
```
Feb  6 16:42:54 fw1-david kernel: [1208405.287952] [DMZ-2-LAN-default-DIIN=eth1
OUT=eth2 MAC=00:50:56:a1:1e:01:00:50:56:a1:ad:66:08:00 SRC=172.16.50.3 DST=172.1
6.200.10 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=7159 DF PROTO=TCP SPT=51604 DPT=151
4 WINDOW=29200 RES=0x00 SYN URG=0
Feb  6 16:42:55 fw1-david kernel: [1208406.295176] [DMZ-2-LAN-default-DIIN=eth1
OUT=eth2 MAC=00:50:56:a1:1e:01:00:50:56:a1:ad:66:08:00 SRC=172.16.50.3 DST=172.1
6.200.10 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=7160 DF PROTO=TCP SPT=51604 DPT=151
4 WINDOW=29200 RES=0x00 SYN URG=0
Feb  6 16:42:57 fw1-david kernel: [1208408.343263] [DMZ-2-LAN-default-DIIN=eth1
OUT=eth2 MAC=00:50:56:a1:1e:01:00:50:56:a1:ad:66:08:00 SRC=172.16.50.3 DST=172.1
6.200.10 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=7161 DF PROTO=TCP SPT=51604 DPT=151
4 WINDOW=29200 RES=0x00 SYN URG=0
```

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

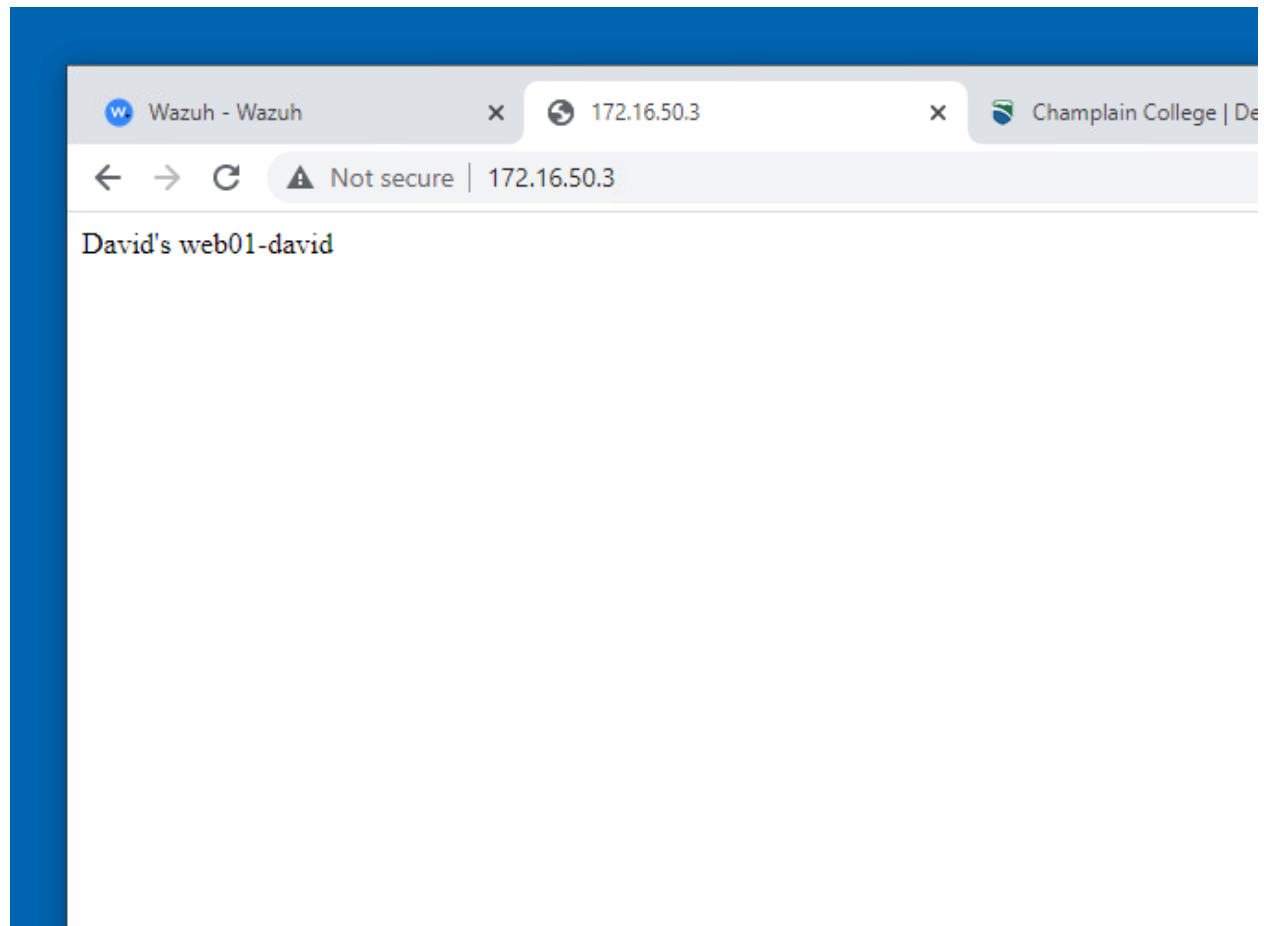
```
[edit]
vyos@fw1-david# cat /var/log/messages | grep "SPT=151" | head -n 1
Feb  6 16:36:12 fw1-david kernel: [1208002.774207] [LAN-2-DMZ-default-DIIN=eth2
OUT=eth1 MAC=00:50:56:a1:e1:dc:00:50:56:a1:6c:a3:08:00 SRC=172.16.200.10 DST=172
.16.50.3 LEN=60 TOS=0x00 PREC=0x00 TTL=62 ID=0 DF PROTO=TCP SPT=1514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

```
SSH: connect to host 172.16.150.3 port 22: connection timed out
champuser@mgmt01-david:~$ ssh testwazuhafterfirewall@172.16.50.3
testwazuhafterfirewall@172.16.50.3's password:
aPermission denied, please try again.
testwazuhafterfirewall@172.16.50.3's password:
Permission denied, please try again.
testwazuhafterfirewall@172.16.50.3's password:
testwazuhafterfirewall@172.16.50.3: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
champuser@mgmt01-david:~$
```

Feb 6, 2023 @ 12:46:06.043	T1110.001 T1021.004 T1078	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: Attempt to login using a non-existent user	5	57
Table JSON Rule					
@timestamp	2023-02-06T17:46:06.043Z				
_id	fe3VJ4YB5_E80bFQzHVI				
agent.id	001				
agent.ip	172.16.50.3				
agent.name	web01-thomsen				
data.scrip	172.16.150.10				
data.srcuser	testwazuhafterfirewall				
decoder.name	sshd				
decoder.parent	sshd				
full_log	2023-02-06T12:46:05.057071-05:00 web01-thomsen sshd[50943]: Failed password for invalid user testwazuhafterfirewall from 172.16.150.10 port 46266 ssh2				
14	127E70EE68 3A7A8				

Deliverable 8. Provide a screenshot similar to the one below

```
Windows PowerShell

StatusCode      : 200
ReStatusDescription : OK
Content         : David's web01-david

RawContent      : HTTP/1.1 200 OK
                  Keep-Alive: timeout=5, max=100
                  Connection: Keep-Alive
                  Accept-Ranges: bytes
                  Content-Length: 20
                  Content-Type: text/html; charset=UTF-8
                  Date: Mon, 06 Feb 2023 20:06:16 GMT
                  ETag: "1..."
Forms           : {}
Headers         : {[Keep-Alive, timeout=5, max=100], [Connection, Keep-Alive], [Accept-Ranges, bytes],
                  [Content-Length, 20]...}
Images          : {}
InputFields     : {}
Links           : {}
ParsedHtml      : System.__ComObject
RawContentLength : 20

PS C:\Users\david-adm> ping 172.16.150.10

Pinging 172.16.150.10 with 32 bytes of data:
Reply from 172.16.150.10: bytes=32 time=1ms TTL=62
Reply from 172.16.150.10: bytes=32 time<1ms TTL=63
Reply from 172.16.150.10: bytes=32 time<1ms TTL=63
Reply from 172.16.150.10: bytes=32 time<1ms TTL=63

Ping statistics for 172.16.150.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Users\david-adm> ping champlain.edu

Pinging champlain.edu [208.115.107.132] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 208.115.107.132:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\david-adm> 
```


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

```
vyos@fw-mgmt-david# show firewall name MGMT-2-LAN
default-action drop
enable-default-log
rule 1 {
    action accept
    state {
        established enable
    }
}
rule 10 {
    action accept
    description "MGMT to DMZ"
    destination {
        address 172.16.150.0/24
    }
}
rule 20 {
    action accept
    description "MGMT to LAN"
    destination {
        address 172.16.50.0/29
    }
}
[edit]
vyos@fw-mgmt-david# _
```

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.

The image shows a terminal window and a Wazuh web interface. The terminal window displays the command `ssh fw-mgmt-test@172.16.50.3` being executed from the `mgmt01-david` host. The output shows three password prompts, all resulting in "Permission denied". The Wazuh web interface shows the "Security events" page, displaying a list of events. The event details for the failed SSH connection are as follows:

Field	Value
@timestamp	2023-02-06T20:24:13.234Z
_id	001mKIYB5_E89bFQkHVd
agent.id	001
agent.ip	172.16.50.3
agent.name	web01-thomsen
data.srcip	172.16.150.10
data.srcuser	fw-mgmt-test
decoder.name	sshd
decoder.parent	sshd
full_log	2023-02-06T15:24:11.971807-05:00 web01-thomsen sshd[51657]: Failed password for invalid user fw-mgmt-test from 172.16.150.10 port 46268 ssh2
id	1675715053.40198