Topologie

```
vboxuser@MachinerServer:~/secured-network-infrastructure/mininet$ sudo python3 topology.py
*** Démarrage du réseau
*** Configuring hosts
firewall wanclient attacker web1 web2 vpnserver lanclient1 admin
*** Starting controller

*** Starting 5 switches
s1 s2 s3 s4 s5 ...
*** Application des règles Zone-Based Firewall...
✓ Règles de sécurité appliquées avec succès.
```

```
mininet> firewall ifconfig
fwadmin: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.1  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::307e:76ff:fe9d:3eff  prefixlen 64  scopeid 0x20<link>
        ether 32:7e:76:9d:3e:ff  txqueuelen 1000  (Ethernet)
        RX packets 54  bytes 5294 (5.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21  bytes 1566 (1.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

fwdmz: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.1.1  netmask 255.255.255.0  broadcast 172.16.1.255
        inet6 fe80::909d:53ff:fe96:e1c6  prefixlen 64  scopeid 0x20<link>
        ether 92:9d:53:96:e1:c6  txqueuelen 1000  (Ethernet)
        RX packets 74  bytes 6790 (6.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 29  bytes 2294 (2.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

fwlan: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.1  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::4c17:2bff:fe10:74ef  prefixlen 64  scopeid 0x20<link>
        ether 4e:17:2b:10:74:ef  txqueuelen 1000  (Ethernet)
        RX packets 54  bytes 5294 (5.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21  bytes 1566 (1.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

fwvpn: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.8.0.254  netmask 255.255.255.0  broadcast 10.8.0.255
        inet6 fe80::88b7:d9ff:fec7:992d  prefixlen 64  scopeid 0x20<link>
```

iptables

```
mininet> firewall iptables -L -v -n
Chain INPUT (policy DROP 5 packets, 420 bytes)
 pkts bytes target     prot opt in     out     source               destination
    5   420 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
    5   420 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0           LOG flags 0 level 4 prefix "FW-INPUT-DROP: "

Chain FORWARD (policy DROP 16 packets, 1344 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  fwwan  fwdmz   0.0.0.0/0            0.0.0.0/0           tcp dpt:80
    0     0 ACCEPT     tcp  --  fwwan  fwdmz   0.0.0.0/0            0.0.0.0/0           tcp dpt:443
    0     0 ACCEPT     tcp  --  fwlan  fwdmz   0.0.0.0/0            0.0.0.0/0           multiport dports 80,443
    0     0 ACCEPT     tcp  --  fwvpn  fwadmin  0.0.0.0/0            0.0.0.0/0           tcp dpt:22
    1    84 LOG        all  --  fwvpn  fwadmin  0.0.0.0/0            0.0.0.0/0           LOG flags 0 level 4 prefix "FW-VPN-ADMIN-SSH: "
    0     0 ACCEPT     all  --  fwlan  fwwan   0.0.0.0/0            0.0.0.0/0
    2   168 LOG        all  --  fwdmz  fwlan   0.0.0.0/0            0.0.0.0/0           LOG flags 0 level 4 prefix "FW-BLOCK-DMZ-LAN: "
    2   168 REJECT     all  --  fwdmz  fwlan   0.0.0.0/0            0.0.0.0/0           reject-with icmp-port-unreachable
    2   168 LOG        all  --  *      fwlan   0.0.0.0/0            0.0.0.0/0           LOG flags 0 level 4 prefix "FW-REJECT-TO-LAN: "
   16  1344 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0           LOG flags 0 level 4 prefix "FW-FINAL-DROP: "

Chain OUTPUT (policy ACCEPT 17 packets, 1764 bytes)
 pkts bytes target     prot opt in     out     source               destination
mininet>
```

test de qlq ping

```
mininet> web1 ping -c 3 172.16.1.11
PING 172.16.1.11 (172.16.1.11) 56(84) bytes of data.
64 bytes from 172.16.1.11: icmp_seq=1 ttl=64 time=1.00 ms
64 bytes from 172.16.1.11: icmp_seq=2 ttl=64 time=0.072 ms
64 bytes from 172.16.1.11: icmp_seq=3 ttl=64 time=0.094 ms

--- 172.16.1.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2032ms
rtt min/avg/max/mdev = 0.072/0.390/1.004/0.434 ms
mininet> wanclient ping -c 3 192.168.10.10
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data.
From 203.0.113.10 icmp_seq=1 Destination Host Unreachable
From 203.0.113.10 icmp_seq=2 Destination Host Unreachable
From 203.0.113.10 icmp_seq=3 Destination Host Unreachable

--- 192.168.10.10 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2044ms
pipe 3
mininet>
```

DMZ web1 bash
/home/vboxuser/secured-network-infrastructure/configs/dmz_web_config.sh

```
mininet> web1 bash /home/vboxuser/secured-network-infrastructure/configs/dmz_web_config.sh
=== Configuration HTTPS sur MachinerServer ===
....+.......+...+.........+.....+...++++++++++++++++++++++++++++++++++++++++++.+.....+....+...+........+....+...+..+.+............+...+..+...+++++++++++++++++
++++++++++++++++++++x.......+.....+....+..+...+......+.+...+..+.........+...+...+...+.........+.+.....++++++
............+..+.+.....++++++++++++++++++++++++++++++++++++++++++.....+...+....+..+...+..........++++++++++++++++++++++++++++++++++++++++.+....+...+.........
...+........+.+..+............+...+.............+..+...+.......+............+...........+.........+.........+.....+.........+.......
.....+.............+.+.................+.+..+....+...+.....+.+..+.....................+.....+....+.+.........+..+.....+.........+...........+.+...+..+..
..+.....+...+.+....+.+........+.+..+...+.....................+.....+...+....+..+........+...........+...+.....+.........+...+.....+.............+.+
.....+....+...+.............+...+...+....+.....+..........+...........+.........+....+.....+...+..+..+.....+...+...+..+..+...+.....+.+..+.......+....
..........+...+.........+.........+....+.............+...+......+........+.........+.....+...+.......+..+.........+....+.+.+.+.....+.+...+..........+...
.+........+.........+...+.+......+.....+....+.........+....+...........+.+...+...........+.+.............+.+.....+.......+...+.............+......+.....
..+.+....+..+....+......+..+...+.......+..................+...+.....+....+...........+.....................+...+.................+...+.......+.+.........
...+..........+.....+...+.....+...+........+....+.....+.+.....+...+.........+...+....+.....+.....+...+...................+......+..............+......+.
....+.+..+.............+...+..+.......+..++++++
-----
Certificats générés:
total 8.0K
-rw-r--r-- 1 root root 1.3K Jan  3 01:46 MachinerServer.crt
-rw------- 1 root root 1.7K Jan  3 01:46 MachinerServer.key
Processus lancés: HTTPS=22400, HTTP=22402
✓ Processus HTTPS actif (PID: 22400)
✓ Serveur HTTPS démarré sur https://172.16.1.10:443
✓ Processus HTTP actif (PID: 22402)
✓ Redirection HTTP démarrée sur http://172.16.1.10:80
tcp        0      0 172.16.1.10:443         0.0.0.0:*               LISTEN      22400/python3
tcp        0      0 172.16.1.10:80          0.0.0.0:*               LISTEN      22402/python3
```

```
mininet> web1 curl -k https://172.16.1.10
<!DOCTYPE html>
<html>
<head><title>MachinerServer</title></head>
<body>
<h1>Serveur MachinerServer (172.16.1.10)</h1>
<p>HTTPS Actif - Infrastructure Zero Trust</p>
</body>
</html>
mininet> web1 curl -I http://172.16.1.10
HTTP/1.0 301 Moved Permanently
Server: BaseHTTP/0.6 Python/3.13.5
Date: Sat, 03 Jan 2026 00:47:04 GMT
Location: https://172.16.1.10/

mininet> lanclient1 curl -k https://172.16.1.10
<!DOCTYPE html>
<html>
<head><title>MachinerServer</title></head>
<body>
<h1>Serveur MachinerServer (172.16.1.10)</h1>
<p>HTTPS Actif - Infrastructure Zero Trust</p>
</body>
</html>
mininet>
```

SSH

Phase 1 - Configuration manuelle SSH

on a travailler sur le port 2222 car je suis deja en utilisation du port 22

```
Generating public/private rsa key pair.
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:7nqMtKb03DWvXa0ghpVBMc4X80mn5BL7x7sqsKyI09c root@MachinerServer
The key's randomart image is:
+---[RSA 2048]----+
|          +.+ o .|
|         + . X + |
|          + + =  |
|           + o . |
|        S o   . o|
|      .. +     o.|
|    o. += B . ...|
|   o.+=+oE * o ..|
|   .o+=++ ..+.o. |
+----[SHA256]-----+
mininet> admin ls -la /root/.ssh/
total 16
drwx------ 2 root root 4096 Jan  3 15:23 .
drwx------ 7 root root 4096 Jan  3 01:44 ..
-rw------- 1 root root 1823 Jan  3 15:23 id_rsa
-rw-r--r-- 1 root root  401 Jan  3 15:23 id_rsa.pub
```

1. Créer le dossier nécessaire pour le démon
SSH mininet> admin mkdir -p /run/sshd #

2. Lancer le serveur SSH uniquement sur admin et sur le port 2222
mininet> admin /usr/sbin/sshd -p 2222 #
3. Vérifier que le port est ouvert localement dans admin mininet> admin netstat -tlnp | grep :2222

```
mininet> admin mkdir -p /run/sshd
mininet> admin /usr/sbin/sshd -p 2222
mininet> admin netstat -tlnp | grep :2222
tcp        0      0 0.0.0.0:2222            0.0.0.0:*               LISTEN
    30120/sshd: /usr/sb
tcp6       0      0 :::2222                 :::*                    LISTEN
    30120/sshd: /usr/sb
```

3. Tests de validation (Pour tes captures d'écran)

Test 1 : Connexion réussie (depuis admin lui-même)

```
mininet> admin ssh -p 2222 root@192.168.100.10
The authenticity of host '[192.168.100.10]:2222 ([192.168.100.10]:2222)' can
't be established.
ED25519 key fingerprint is SHA256:iU649Tr0R0nMpFW3KTIqNnJY0oOdZ0K2QlwBUPz938
M.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

Warning: Permanently added '[192.168.100.10]:2222' (ED25519) to the list of
known hosts.
Linux MachinerServer 6.12.57+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.
57-1 (2025-11-05) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@MachinerServer:~# exit
```

Test 2 : Blocage par le Firewall (depuis l'attaquant)

```
mininet> attacker ssh -p 2222 root@192.168.100.10
ssh: connect to host 192.168.100.10 port 2222: No route to host
mininet>
```

Automatisation finale dans [topology.py]

vpnserver

Phase 1 : Initialisation de la PKI (Sur vpnserver)

```
mininet> vpnserver mkdir -p /etc/openvpn/easy-rsa
mininet> vpnserver cp -r /usr/share/easy-rsa/* /etc/openvpn/easy-rsa/
mininet> vpnserver cd /etc/openvpn/easy-rsa/
mininet> vpnserver ./easyrsa init-pki

Notice
------
'init-pki' complete; you may now create a CA or requests.

Your newly created PKI dir is:
* /etc/openvpn/easy-rsa/pki

Using Easy-RSA configuration:
* undefined
mininet>
```

Création du CA (Autorité de Certification)

```
mininet> vpnserver ./easyrsa build-ca nopass
.......+++++++++++++++++++++++++++++++++++*...+.+.....+.+......+...+....
..+...+..+...+...+...+++++++++++++++++++++++++++++++++++*....+.....+....
..+.......+..+.................+...+..+.........+.....+.........+.........+.
...+.....+.+..+...+....+..+.+...+.............+......+.............+....+
...+........+......+.+...+..+.............+.............+......+.........+
......+......+..+...+.............+....+.....+....+..+...+....+..+...+....
......+.....+.........+......+..+...+......+.+...+.............+.........
..+......+.................+....+........+.........+....+.............+.+.
..........+....+......+..........+.........+.+...........+...........+....
..+...+.+..+.......+.................+..+.+..+.........+.+..+.......+......
.......................+...+......+..+...........+.+..+....+........+...+.
...+...+.....+.............+.+.....+.+.....+.+...+..+...+.+...+..........
.+.....+...........+..+.+.................+.+..+...+.+......+..+.+........
............+.........+...+....+.............+......+.+.....+...+.......+..
.+......+...+........+...+.+.....................+.........+......+.........+
.+...+..+...+.......+.....+....+..........+.........+.........+.....+.++++
++
..+.............+.................+..+...+.+........+...+...++++++++++
++++++++++++++++++++++++*...+....++++++++++++++++++++++++++++++++++++*
..........+..........+.........+...+........+...+....+......+.........+.....
+......+.............+....+..+.+..+.+......+........+.......+......+......
..+.+.....+....+.............+..........+...+..........+.....+...+.......
...+........+......+.+...+..+....+...+.....................+..............
..........+....+.........+......+......+........+.+.....+.......+..+......+.
..............+....+......+.....+............+....+.....+......+....+...+...
..+..........+..+.+........+.+.........+..+...........+.......+.........+..
+.........+...+.+..+............+...+.......+.....+......+.+...+...+..+.....
..+......+..+.+.....+....+...+.........+.....+....+.............+......+++
+++
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:
```

Créer le certificat du Serveur VPN

```
mininet> vpnserver ./easyrsa gen-req vpnserver nopass
...+...+..+.+...+..............+......+.....+...+.+..+..........+..+++++++
++++++++++++++++++++++++++++++++*........+.........++++++++++++++++++++++++
+++++++++++++++*.................+.+...+......+...........+...+.+.....+.....
...........+...+..+.........+...+.+.........+.....+......................+..
........+............+..+............+.+.........+...........+..........+..
.+......+.....+....+.....+.+...........+.........+...+.+.....+.+.....+...+.
+.....+.+.....+.+................+.....+...+....+...+.................+.....
..+...+......+.....+.++++++
.+......+++++++++++++++++++++++++++++++++++*...+...+..+...+....+.......
..+..+....+...+........+.........+..........+.........+.........+...+.....+
...+....+++++++++++++++++++++++++++++++++++*.....+..........+...+......
..............+.........+.+...+......................+..................++++
++
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [10.8.0.1]:aya
```

Signer le certificat du serveur

```
mininet> vpnserver ./easyrsa sign-req server 10.8.0.1
Please check over the details shown below for accuracy. Note that this requ
est
has not been cryptographically verified. Please be sure it came from a trus
ted
source or that you have verified the request checksum with the sender.
You are about to sign the following certificate:

  Requested CN:     'aya'
  Requested type:   'server'
  Valid for:        '825' days


subject=
    commonName                = aya

Type the word 'yes' to continue, or any other input to abort.
  Confirm requested details: yes

Using configuration from /etc/openvpn/easy-rsa/pki/e03f349f/temp.1.1
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'aya'
Certificate is to be certified until Apr  7 15:35:26 2028 GMT (825 days)
```

Générer les paramètres Diffie-Hellman (DH)

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++
DH parameters appear to be ok.

Notice
------

DH parameters of size 2048 created at:
* /etc/openvpn/easy-rsa/pki/dh.pem
```

Générer le certificat du Client (wanclient) et la signer

```
You are about to sign the following certificate:

  Requested CN:     'client1'
  Requested type:   'client'
  Valid for:        '825' days


subject=
    commonName                = client1

Type the word 'yes' to continue, or any other input to abort.
  Confirm requested details: yes

Using configuration from /etc/openvpn/easy-rsa/pki/3939a6aa/temp.1.1
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'client1'
Certificate is to be certified until Apr  7 15:38:01 2028 GMT (825 days)

Write out database with 1 new entries
Database updated
```

Création du fichier de configuration Serveur

```
mininet> vpnserver mkdir -p /etc/openvpn/server
mininet> vpnserver cp /etc/openvpn/easy-rsa/pki/ca.crt /etc/openvpn/server/
mininet> vpnserver cp /etc/openvpn/easy-rsa/pki/dh.pem /etc/openvpn/server/
mininet> vpnserver cp /etc/openvpn/easy-rsa/pki/issued/10.8.0.1.crt /etc/op
envpn/server/server.crt
mininet> vpnserver cp /etc/openvpn/easy-rsa/pki/private/10.8.0.1.key /etc/o
penvpn/server/server.key
mininet> vpnserver cat > /etc/openvpn/server/server.conf << 'EOF'
> b 3
EOF> > > > > > > > > > > > > >
> mininet>
```

lancer le serveur

```
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel
state UNKNOWN group default qlen 500
    link/none
    inet 10.8.0.1 peer 10.8.0.2/32 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::101f:b655:a1b1:53ce/64 scope link stable-privacy proto kern
el_ll
```

Tes tests sont **parfaits** et montrent exactement ce qu'il faut :

- **vpnserver ping 10.8.0.1 (Succès)** : Le service est "vivant". L'interface virtuelle est créée. La porte d'entrée du tunnel existe.
- **wanclient nc -u -z -v 10.8.0.1 1194 (Open):**Ton firewall laisse passer le trafic VPN.
- **attacker nc -u -z -v 10.8.0.1 1194 (Open) :**

    La **PKI (Easy-RSA)** intervient : même si l'attaquant voit le port, il ne peut pas entrer car il n'a pas le certificat client1.crt signé par toi. C'est l'authentificat **(Host Unreachable) :**

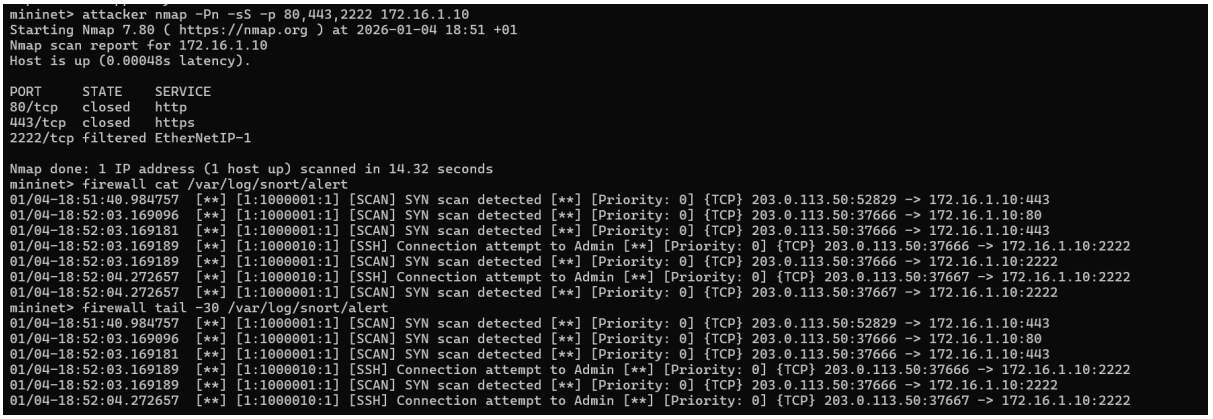
C'est le test le plus important. Cela prouve que le réseau est Zero Trust. Le WAN peut voir le service VPN (port 1194), mais il ne peut pas "pinguer"

```
mininet> vpnserver ping -c 3 10.8.0.1
PING 10.8.0.1 (10.8.0.1) 56(84) bytes of data.
64 bytes from 10.8.0.1: icmp_seq=1 ttl=64 time=0.969 ms
64 bytes from 10.8.0.1: icmp_seq=2 ttl=64 time=0.039 ms
64 bytes from 10.8.0.1: icmp_seq=3 ttl=64 time=0.030 ms

--- 10.8.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.030/0.346/0.969/0.440 ms
mininet> wanclient nc -u -z -v 10.8.0.1 1194
10.8.0.1: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [10.8.0.1] 1194 (openvpn) open
mininet> attacker nc -u -z -v 10.8.0.1 1194
10.8.0.1: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [10.8.0.1] 1194 (openvpn) open
mininet> wanclient ping -c 3 10.8.0.1
PING 10.8.0.1 (10.8.0.1) 56(84) bytes of data.
From 203.0.113.10 icmp_seq=1 Destination Host Unreachable
From 203.0.113.10 icmp_seq=2 Destination Host Unreachable
From 203.0.113.10 icmp_seq=3 Destination Host Unreachable

--- 10.8.0.1 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2035ms
pipe 3
```

Snort IDS

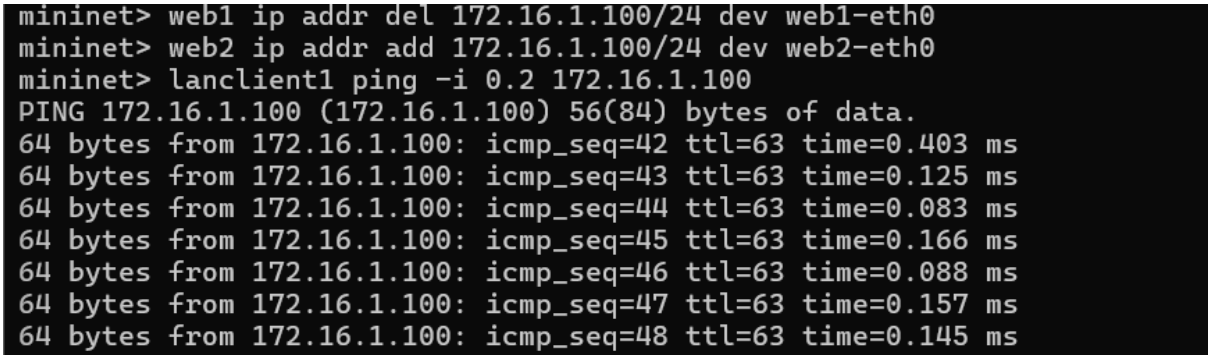


```
mininet> attacker nmap -Pn -sS -p 80,443,2222 172.16.1.10
Starting Nmap 7.80 ( https://nmap.org ) at 2026-01-04 18:51 +01
Nmap scan report for 172.16.1.10
Host is up (0.00048s latency).

PORT     STATE    SERVICE
80/tcp   closed   http
443/tcp  closed   https
2222/tcp filtered EtherNetIP-1

Nmap done: 1 IP address (1 host up) scanned in 14.32 seconds
mininet> firewall cat /var/log/snort/alert
01/04-18:51:40.984757  [**] [1:1000001:1] [SCAN] SYN scan detected [**] [Priority: 0] {TCP} 203.0.113.50:52829 -> 172.16.1.10:443
01/04-18:52:03.169096  [**] [1:1000001:1] [SCAN] SYN scan detected [**] [Priority: 0] {TCP} 203.0.113.50:37666 -> 172.16.1.10:80
01/04-18:52:03.169181  [**] [1:1000001:1] [SCAN] SYN scan detected [**] [Priority: 0] {TCP} 203.0.113.50:37666 -> 172.16.1.10:443
01/04-18:52:03.169189  [**] [1:1000010:1] [SSH] Connection attempt to Admin [**] [Priority: 0] {TCP} 203.0.113.50:37666 -> 172.16.1.10:2222
01/04-18:52:03.169189  [**] [1:1000001:1] [SCAN] SYN scan detected [**] [Priority: 0] {TCP} 203.0.113.50:37666 -> 172.16.1.10:2222
01/04-18:52:04.272657  [**] [1:1000010:1] [SSH] Connection attempt to Admin [**] [Priority: 0] {TCP} 203.0.113.50:37667 -> 172.16.1.10:2222
01/04-18:52:04.272657  [**] [1:1000001:1] [SCAN] SYN scan detected [**] [Priority: 0] {TCP} 203.0.113.50:37667 -> 172.16.1.10:2222
mininet> firewall tail -30 /var/log/snort/alert
01/04-18:51:40.984757  [**] [1:1000001:1] [SCAN] SYN scan detected [**] [Priority: 0] {TCP} 203.0.113.50:52829 -> 172.16.1.10:443
01/04-18:52:03.169096  [**] [1:1000001:1] [SCAN] SYN scan detected [**] [Priority: 0] {TCP} 203.0.113.50:37666 -> 172.16.1.10:80
01/04-18:52:03.169181  [**] [1:1000001:1] [SCAN] SYN scan detected [**] [Priority: 0] {TCP} 203.0.113.50:37666 -> 172.16.1.10:443
01/04-18:52:03.169189  [**] [1:1000010:1] [SSH] Connection attempt to Admin [**] [Priority: 0] {TCP} 203.0.113.50:37666 -> 172.16.1.10:2222
01/04-18:52:03.169189  [**] [1:1000001:1] [SCAN] SYN scan detected [**] [Priority: 0] {TCP} 203.0.113.50:37666 -> 172.16.1.10:2222
01/04-18:52:04.272657  [**] [1:1000010:1] [SSH] Connection attempt to Admin [**] [Priority: 0] {TCP} 203.0.113.50:37667 -> 172.16.1.10:2222
```

Haute disponibilité (Heartbeat)



```
mininet> web1 ip addr del 172.16.1.100/24 dev web1-eth0
mininet> web2 ip addr add 172.16.1.100/24 dev web2-eth0
mininet> lanclient1 ping -i 0.2 172.16.1.100
PING 172.16.1.100 (172.16.1.100) 56(84) bytes of data.
64 bytes from 172.16.1.100: icmp_seq=42 ttl=63 time=0.403 ms
64 bytes from 172.16.1.100: icmp_seq=43 ttl=63 time=0.125 ms
64 bytes from 172.16.1.100: icmp_seq=44 ttl=63 time=0.083 ms
64 bytes from 172.16.1.100: icmp_seq=45 ttl=63 time=0.166 ms
64 bytes from 172.16.1.100: icmp_seq=46 ttl=63 time=0.088 ms
64 bytes from 172.16.1.100: icmp_seq=47 ttl=63 time=0.157 ms
64 bytes from 172.16.1.100: icmp_seq=48 ttl=63 time=0.145 ms
```