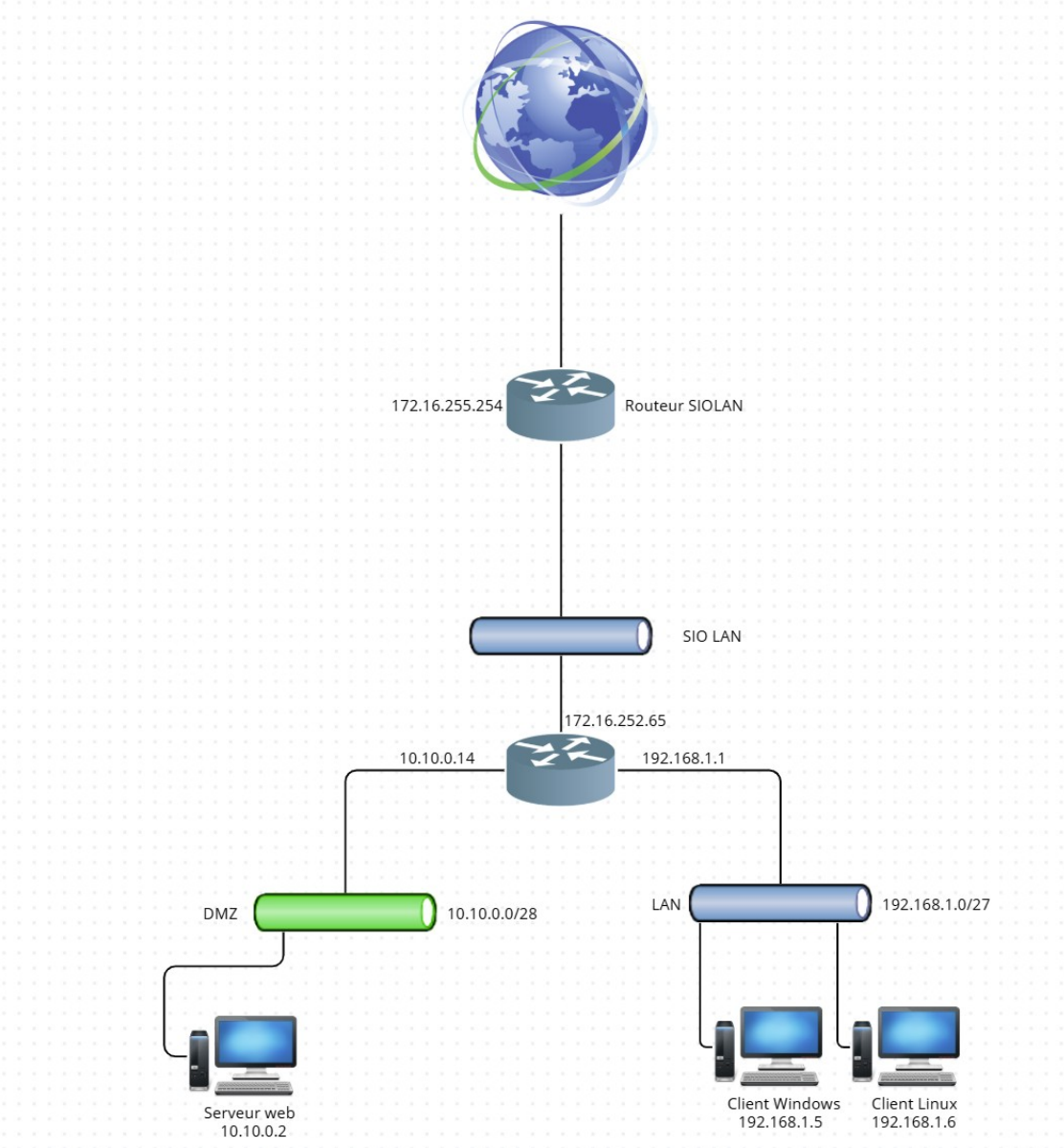
Documentation projet ProxMox

Objectif du projet

Mettre en place une infrastructure virtualisée sous Proxmox intégrant :

- Une séparation LAN / DMZ
- Un routeur MikroTik assurant le routage, le NAT et le firewall
- Un conteneur Apache dans la DMZ
- Des clients Windows et Linux dans le LAN

Schéma Réseau



Infrastructure Proxmox

- VM et conteneurs

Nom	Type	Rôle	IP	Zone
MikroTik	VM	Routeur	192.168.1.1 / 10.10.0.14 / 172.16.252.65	LAN / DMZ / WAN
Apache	Conteneur	Serveur Web	10.10.0.2	DMZ
Client Linux	VM	Test LAN	192.168.1.6	LAN
Client Windows	VM	Test LAN	192.168.1.5	LAN

- Bridges Proxmox

- vmbr10 → WAN (vers SIO)
- vmbr300 → DMZ et LAN

Plan d’adressage

Zone	Réseau	Passerelle	Rôle
LAN	192.168.1.0/27	192.168.1.1	Clients
DMZ	10.10.0.0/28	10.10.0.14	Serveurs (Web)
WAN	172.16.0.0/22	172.16.0.254	Sortie vers Internet par le SIO

Configuration MikroTik

Interfaces

- ether1 = WAN
- ether2 = LAN
- ether3 = DMZ

IP

/ip address add address=10.10.0.14/28 interface=ether3
/ip address add address=172.16./22 interface=ether

/ip address add address=192.168.1.1/24 interface=ether2

Comment	Address	Network	Interface
Interface DMZ	10.10.0.14/28	10.10.0.0	ether3
interface sortie vers SIO	172.16.252.65/22	172.16.252.0	ether1
Interface LAN	192.168.1.1/27	192.168.1.0	ether2

Route par défaut

	Comment	Dst. Address	Gateway	Distance	Routing Ta...	Pref. Source
AS	Default route	0.0.0.0/0	172.16.255.254	1	main	

NAT

/ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade

#	Comment	Action	Chain	Src. Addr...	Dst. Addr...	Src. A...	Dst. A...	Pro...	Src. Port	Dst. Port	Any. Port	In. Int...	Out. Interface	In. Int...	Out. I...
0		masquerade	srcnat										ether1		

DNS

/ip dns set servers=172.16.255.254 allow-remote-requests=yes

Firewall MikroTik

Règles actives

add chain=forward src-address=10.10.0.0/28 dst-address=192.168.1.0/24 connection-state=new action=drop comment="Bloque DMZ to LAN"

add chain=forward src-address=10.10.0.0/28 action=accept comment="Autorise DMZ to Internet"

add chain=forward src-address=192.168.1.0/24 dst-address=10.10.0.0/28 action=accept comment="Autorise LAN to DMZ"

#	Comment	Action	Chain	Src. Address	Dst. Address	Src. A...	Dst. A...	Pro...	Src. Port	Dst. Port	Any. Port	In. Int...	Out. I...	In. Int...	Out. I...
0	Bloque DMZ to LAN	drop	forward	10.10.0.0/28	192.168.1.0/27										
1	Autorise DMZ to I...	accept	forward	10.10.0.0/28									ether1		
2	Autorise LAN to D...	accept	forward	192.168.1.0/24	10.10.0.0/28										

Tests de validation

Numéro de test	Test	Commande
1	LAN → MikroTik	ping 192.168.1.1
2	LAN → Internet	Ping 8.8.8.8 + ping perdu.com pour tester la résolution de noms
3	LAN → Apache	curl http://10.10.0.2 ou accès sur internet avec ce lien
4	DMZ → Internet	Ping 8.8.8.8 + ping perdu.com (pour tester la résolution de noms)
5	DMZ → LAN	ping 192.168.1.6
6	Windows ↔ Linux	Ping
7	Test du NAT	Côté client : ping 8.8.8.8 Côté Mikrotik : table NAT

Test 1 & 2: Client Linux

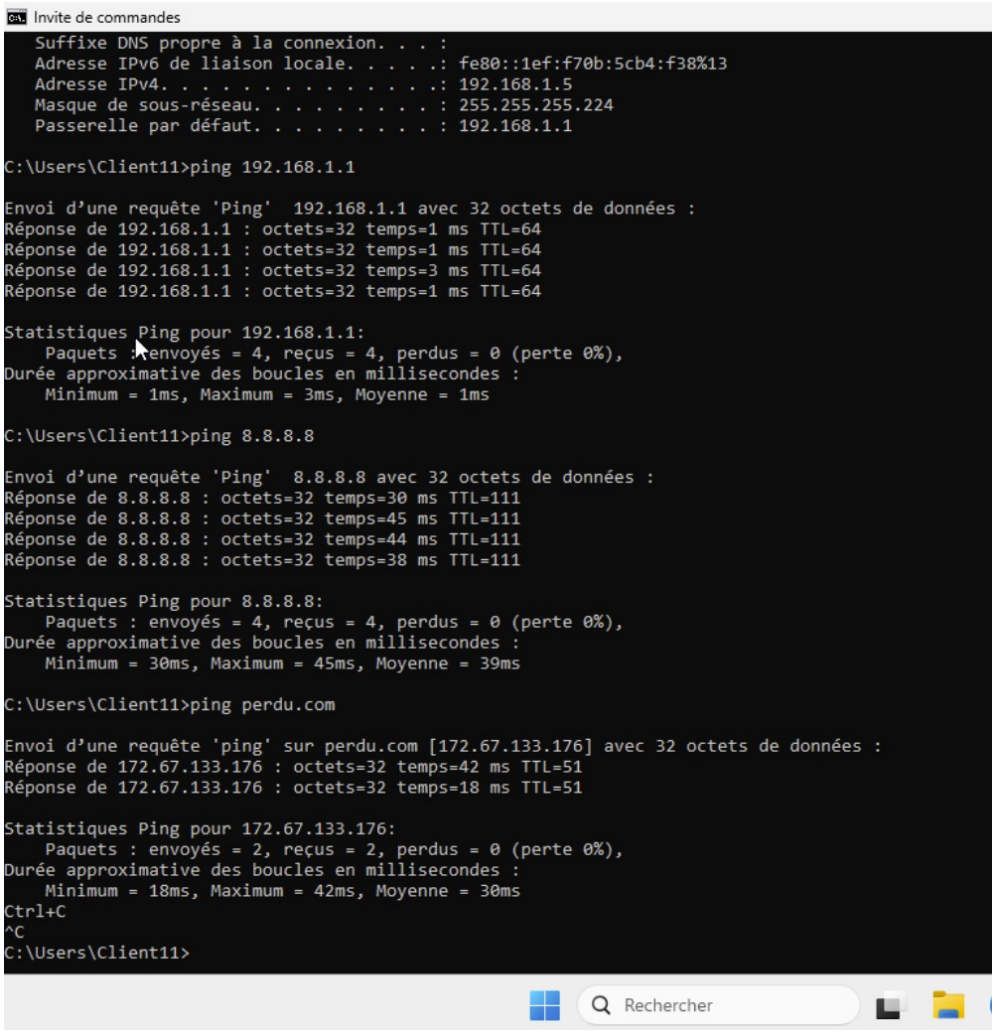
```
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
    link/ether bc:24:11:bd:2d:ae brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    altname enxbc2411bd2dae
    inet 192.168.1.6/27 brd 192.168.1.31 scope global noprefixroute ens18
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:febd:2dae/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
user@CL-LAN:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.895 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.803 ms
^C
--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.803/0.849/0.895/0.046 ms
user@CL-LAN:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=111 time=17.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=111 time=16.5 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 16.476/17.139/17.802/0.663 ms
user@CL-LAN:~$ ping perdu.com
PING perdu.com (172.67.133.176) 56(84) bytes of data.
64 bytes from 172.67.133.176: icmp_seq=1 ttl=51 time=17.5 ms
64 bytes from 172.67.133.176: icmp_seq=2 ttl=51 time=17.5 ms
^C
--- perdu.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 17.452/17.487/17.522/0.035 ms
```

Dans le LAN → OK

Ping vers la passerelle mikrotik → OK

Test de sortie vers Internet → OK

Test 1 & 2 : Client Windows

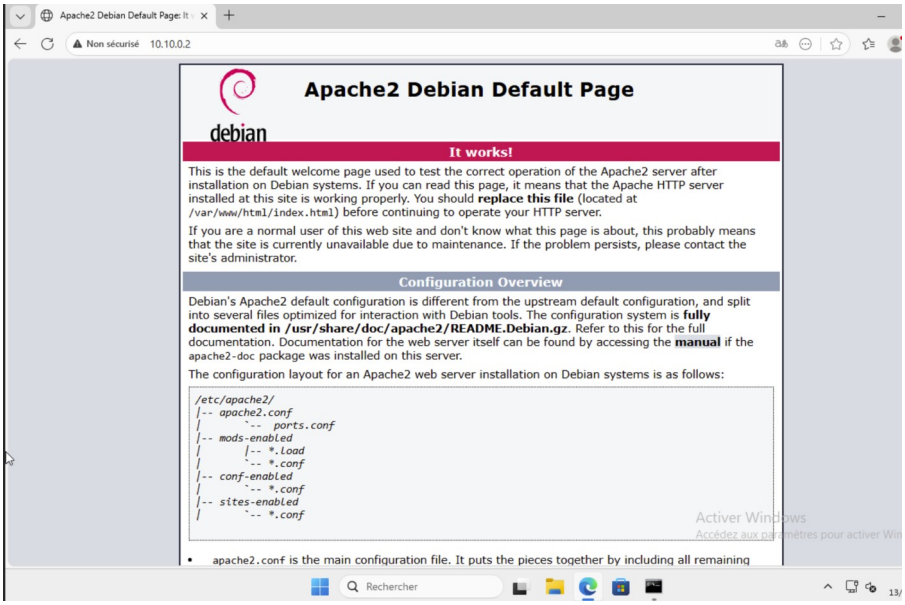


Dans le LAN → OK

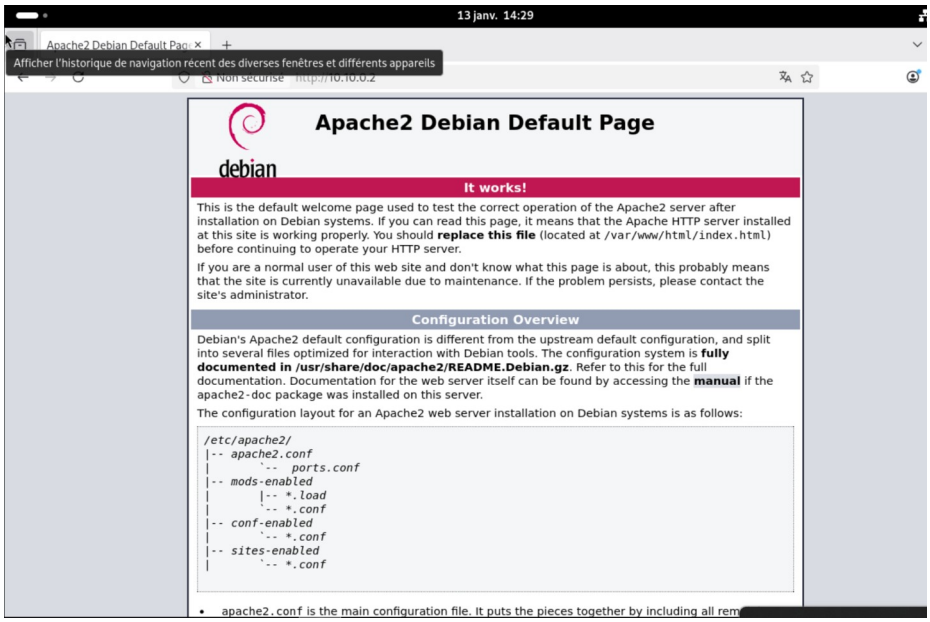
Ping vers la passerelle Mikrotik → OK

test de sortie vers Internet → OK

Test 3 : Accès au serveur Apache depuis le LAN (depuis Windows) Test réussi



Test 3 : Accès au serveur Apache depuis le LAN (depuis Linux)



Test réussi

Test 4 : DMZ to Internet

```
    inet 10.10.0.2/28 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe3f:b891/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
root@AB-serveur-web:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=111 time=17.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=111 time=16.6 ms

--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 16.574/16.987/17.401/0.413 ms
root@AB-serveur-web:~# ping perdu.com
PING perdu.com (172.67.133.176) 56(84) bytes of data.
64 bytes from 172.67.133.176: icmp_seq=1 ttl=51 time=19.2 ms
64 bytes from 172.67.133.176: icmp_seq=2 ttl=51 time=17.3 ms

--- perdu.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 17.253/18.221/19.189/0.968 ms
root@AB-serveur-web:~#
```

Test réussi

Test 5 : Bloquer l’accès DMZ to LAN

```
root@AB-serveur-web:~# ping 192.168.1.6
PING 192.168.1.6 (192.168.1.6) 56(84) bytes of data.




--- 192.168.1.6 ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 8223ms
```

Test réussi, la DMZ n’accède pas au LAN

Test 6 : ping dans le LAN entre clients

```
C:\Users\Client11>ping 192.168.1.6

Envoi d'une requête 'Ping'  192.168.1.6 avec 32 octets de données :
Réponse de 192.168.1.6 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.6 : octets=32 temps=3 ms TTL=64
Réponse de 192.168.1.6 : octets=32 temps=6 ms TTL=64
Réponse de 192.168.1.6 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.1.6:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 6ms, Moyenne = 2ms
```

Test réussi

Test 7 : Preuve du bon fonctionnement du NAT

```
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
    link/ether bc:24:11:bd:2d:ae brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    altname enxbc2411bd2dae
    inet 192.168.1.6/27 brd 192.168.1.31 scope global noprefixroute ens18
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:febd:2dae/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
user@CL-LAN:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.895 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.803 ms
^C
--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.803/0.849/0.895/0.046 ms
user@CL-LAN:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=111 time=17.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=111 time=16.5 ms
^C
```

```
[admin@MikroTik] > /ip firewall connection print where src-address~"192.168.1"
Flags: S - SEEN-REPLY; A - ASSURED; C - CONFIRMED; s - SRCNAT
Columns: PROTOCOL, SRC-ADDRESS, SRC-PORT, DST-ADDRESS, DST-PORT, TCP-STATE, TIMEOUT, ORIG-RATE, REPL-RATE, ORIG-PAC>
#      PRO  SRC-ADDRESS  SRC-PORT  DST-ADDRESS      DST-  TCP-STATE    TIMEOUT    ORIG  REPL  ORI  RE  ORIG-B  REPL>
0   C  udp  192.168.1.1      5678  255.255.255.255  5678              22s        0bps  0bps    1   0     181      >
1 SACs tcp  192.168.1.5     56668  98.66.133.185     443  established  23h59m49s  0bps  0bps  166  91  17 419  24 0>
2 SACs tcp  192.168.1.6     58312  34.107.243.93     443  established  23h55m23s  0bps  0bps   10   9   2 646   1 7>
```

Ces commandes montrent que les clients LAN établissent des connexions vers Internet. Les adresses source sont bien réécrites par le NAT (masquerade), les connexions sont actives (established), et les paquets de réponse sont reçus. Cela prouve que le NAT fonctionne correctement.

Conclusion

L'infrastructure est fonctionnelle, sécurisée et conforme aux objectifs du TP. La séparation LAN/DMZ est assurée par le firewall MikroTik, le NAT permet l'accès Internet, et les clients accèdent au serveur Apache dans la DMZ. Tous les tests ont été validés.