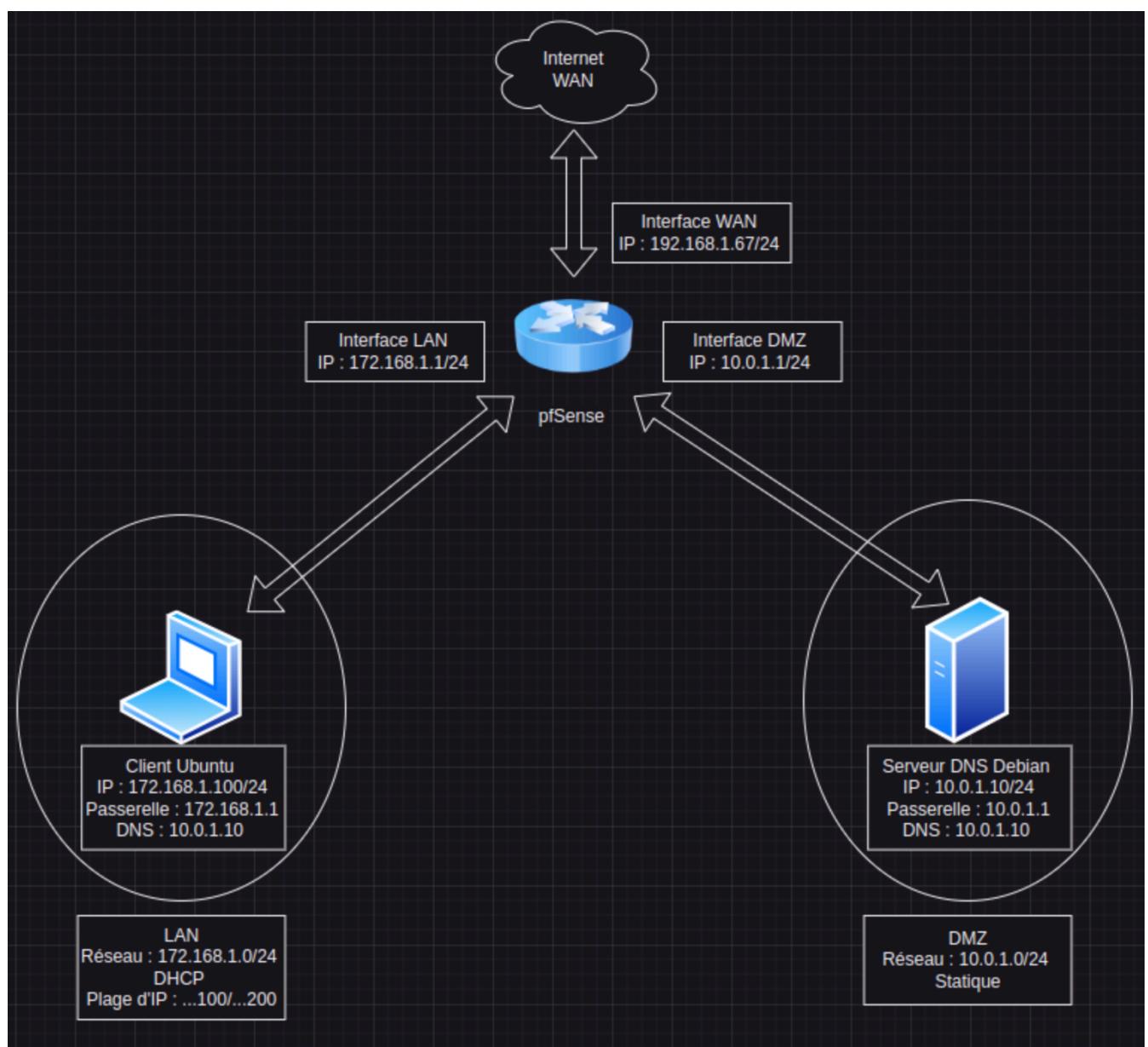


Mise en œuvre pratique d'un système DNS au sein d'une DMZ

Objectif :

1. Mise en place d'un serveur DNS sous Debian
2. Configuration du client
3. Règles de Pare-feu sur pfSense
4. Tests : nslookup/dig et ping

Pour commencer, voyons l'architecture du réseau et des interfaces LAN et DMZ.



Mise en place du serveur DNS sous Debian

Après avoir créé et configuré l'interface DMZ :

Interfaces / DMZ (em2)

Configuration générale

Activer Activer interface

Description: DMZ
Entrez ici une description (nom) pour cette interface.

Type de configuration IPv4: IPv4 statique

Type de configuration IPv6: Aucun

Adresse MAC: XXXXXXXX
Ce champ peut être utilisé pour modifier ("spoof") l'adresse MAC de cette interface.
Entrez une adresse MAC au format suivant : xx:xx:xx:xx:xx ou laissez vide.

MTU:
Si ce champ est laissé vide, la valeur MTU par défaut de la carte réseau est utilisée. En général 1 500 octets, mais peut varier dans certaines circonstances.

MSS:
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IP header size) and minus 60 for IPv6 (TCP/IP header size) will be in effect.

Vitesse et Duplex: Par défaut (aucune préférence, habituellement une auto-sélection)
Forcer la vitesse et le mode duplex pour cette interface.
ATTENTION: doit être défini sur autoselect (vitesse négociée automatiquement) à moins que la vitesse et duplex du port auquel cette interface est connectée soit aussi forcé.

Configuration statique IPv4

Adresse IPv4: 10.0.1.1 / 24
Passerelle IPv4 en amont: Aucun + Ajouter une nouvelle passerelle

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".

J'ai commencé par renommer la machine (fichier hosts et hostname) et fixer une adresse IP au serveur pour qu'il se trouve dans le même réseau que l'interface DMZ du routeur. Pour ce faire, je suis allé dans le fichier **/etc/network/interface** comme suit :

```
GNU nano 7.2                                         hostname
#FQDN de la machine
ns1.itic.lan
```

```
GNU nano 7.2                                         hosts
127.0.0.1      localhost
127.0.1.1      ns1.itic.lan

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

```

GNU nano 7.2                               interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
source /etc/network/interfaces/*
#The loopback network interface
auto lo
iface lo inet loopback
auto enp0s3
iface enp0s3 inet static
    address 10.0.1.10/24
    gateway 10.0.1.1

```

J'ai ensuite configuré le fichier /etc/resolvconf/resolv.conf.d/base et les différents fichiers de bind. En commençant par le fichier base pour fixer le nameserver dans le fichier /etc/resolv.conf:

```

GNU nano 7.2                               base
#DNS PRIMAIRE

nameserver 10.0.1.10

```

J'ai ensuite configuré le fichier /etc/bind/named.conf.local pour déclarer le domaine dans lequel se trouve le serveur :

```

GNU nano 7.2                               named.conf.local
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "itic.lan"{
    type master;
    file "/etc/bind/db.itic.lan";
    allow-query {any;};
};

```

Puis le fichier /etc/bind/named.conf.options pour créer les liens et les redirection des requêtes DNS :

```

GNU nano 7.2                                         named.conf.options
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        10.0.1.1;
        8.8.8.8;
    };
}

//=====
// If BIND logs error messages about the root key being expired,
// you will need to update your keys. See https://www.isc.org/bind-keys
//=====
dnssec-validation auto;

listen-on-v6 { any; };

};


```

Pour finir, j'ai configuré la base de données du serveur pour qu'il ait les membres du domaine et puisse résoudre les requêtes DNS pour ces derniers :

```

GNU nano 7.2                                         db.itic.lan
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$TTL    86400
@       IN      SOA     localhost. root.localhost. (
                        1                  ; Serial
                        604800             ; Refresh
                        86400              ; Retry
                        2419200            ; Expire
                        86400 )             ; Negative Cache TTL
;
@       IN      NS      ns1.itic.lan.
ns1    IN      A       10.0.1.10
client IN      A       172.168.1.100

```

Configuration du client

Comme pour le serveur DNS il a fallu renommer la machine client dans ls fichier /etc/hosts et hostname :

```
GNU nano 7.2                                     hosts
127.0.0.1 localhost
127.0.1.1 client.itic.lan
172.168.1.100 client.itic.lan
```

```
GNU nano 7.2                                     hostname
client.itic.lan
```

Pour configurer la carte réseau du client, il fallait tout d'abord configurer l'interface pfSense et le service DHCP, j'ai décidé de mettre en place une plage d'adresse IP allant de 172.168.1.100 à 172.168.1.200 comme suit :

Interfaces / LAN (em1)

Configuration générale

Activer	<input checked="" type="checkbox"/> Activer interface
Description	LAN Entrez ici une description (nom) pour cette interface.
Type de configuration IPv4	IPv4 statique
Type de configuration IPv6	Aucun
Adresse MAC	XXXXXXXXXXXXXX Ce champ peut être utilisé pour modifier ("spoof") l'adresse MAC de cette interface. Entrez une adresse MAC au format suivant : xx:xx:xx:xx:xx ou laissez vide.
MTU	 Si ce champ est laissé vide, la valeur MTU par défaut de la carte réseau est utilisée. En général 1 500 octets, mais peut varier dans certaines circonstances.
MSS	 If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPV4 header size) and minus 60 for IPv6 (TCP/IPV6 header size) will be in effect.
Vitesse et Duplex	Par défaut (aucune préférence, habituellement une auto-sélection) Forcer la vitesse et le mode duplex pour cette interface. ATTENTION: doit être défini sur autoselect (vitesse négociée automatiquement) à moins que la vitesse et duplex du port auquel cette interface est connectée soit aussi forcé.

Configuration statique IPv4

Adresse IPv4	172.168.1.1	/ 24
--------------	-------------	------

Activer	<input checked="" type="checkbox"/> Activer le serveur DHCP sur l'interface LAN		
BOOTP	<input type="checkbox"/> Ignorer les requêtes BOOTP		
Rejeter les clients inconnus	<input type="button" value="Allow all clients"/> <small>When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.</small>		
Ignorer les clients inconnus	<input type="checkbox"/> Les clients refusés seront ignorés plutôt que rejetés <small>Cette option n'est pas compatible avec le failover et ne peut pas être activée lorsqu'une adresse Failover Peer IP est configurée.</small>		
Ignorer les identifiants clients	<input type="checkbox"/> Si un client inclue un identifiant unique dans sa requête DHCP, cet UID ne sera pas enregistré dans son bail. <small>Cette option peut être utile lorsqu'un client peut dual boot en utilisant différents identifiants client, mais avec la même adresse matérielle (MAC). Notez que ce comportement du serveur est contraire aux spécifications officielles de DHCP.</small>		
Sous-réseau	172.168.1.0		
Masque de sous-réseau	255.255.255.0		
Plage disponible	172.168.1.1 - 172.168.1.254		
Plage	<input type="text" value="172.168.1.100"/> <small>De</small> <input type="text" value="172.168.1.200"/> <small>À</small>		
Pools additionnels			
Ajouter	<input type="button" value="Add pool"/>		
<small>Si des pools d'adresses supplémentaires sont nécessaires à l'intérieur de ce sous-réseau en dehors de la plage ci-dessus, ils peuvent être spécifiés ici.</small>			
Début du Pool	Fin du Pool	Description	Actions
Serveurs			
Serveurs WINS	<input type="text" value="WINS Server 1"/> <input type="text" value="WINS Server 2"/>		
Serveurs DNS	<input type="text" value="10.0.1.10"/>		

J'ai également lié la pfSense au domaine pour pouvoir configurer le resolv.conf du client en utilisant un lien symbolique entre le resolv.conf du dossier /etc à celui du dossier /run/systemd/resolve/ fourni par le DHCP.

Système			
Nom d'hôte	<input type="text" value="pfSense"/> <small>Nom d'hôte du pare-feu, sans le nom de domaine</small>		
Domaine	<input type="text" value="itic.lan"/> <small>Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternative TLDs such as 'local.lan' or 'mylocal' are safe.</small>		
Paramètres du serveur DNS			
Serveurs DNS	<input type="text" value="10.0.1.10"/>	<input type="text" value="ns1"/>	<input type="button" value="Supprimer"/>
	<input type="text" value="8.8.8.8"/>	<input type="text" value="Google"/>	<input type="button" value="Supprimer"/>

Après l'allumage de la machine cliente, on voit bien qu'elle obtient son IP du DHCP :

```
user@client:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 172.168.1.100 netmask 255.255.255.0 broadcast 172.168.1.255
                ether 08:00:27:92:b7:56 txqueuelen 1000 (Ethernet)
                RX packets 640 bytes 61697 (61.6 KB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 669 bytes 53003 (53.0 KB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Pour créer le lien symbolique, j'ai utilisé la commande suivante :

```
sudo ln -sf /run/systemd/resolve/resolv.conf /etc/resolv.conf
```

On voit ici que les deux fichiers sont bien liés :

```
user@client:~$ ll /etc/resolv.conf
lrwxrwxrwx 1 root root 32 mai 20 20:17 /etc/resolv.conf -> /run/systemd/resolve/resolv.conf
user@client:~$
```

Voici le contenu du fichier resolv.conf :

```
GNU nano 7.2                                     resolv.conf *
nameserver 10.0.1.10
search itic.lan
```

Règles de Pare-feu sur pfSense

- Les différentes règles de firewalling pour l'interface LAN :
 - Les trois premières règles sont celles par défaut, qui en autre permettent l'accès à internet en IPv4 et IPv6
 - La quatrième règle permet l'accès au serveur DNS avec le port 53 (DNS)
 - Les dernières règles permettent quand à elles l'accès au serveur en HTTP et HTTPS

Flottant(e)	WAN	LAN	DMZ							
Règles (Faire glisser pour changer l'ordre)										
	États	Protocole	Source	Port	Destination	Port	File d'attente	Ordonnancement	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	*	*	*	LAN Address	80	*	*	Règle anti-bloquage	
<input type="checkbox"/>	0/0 B	IPv4 *	LAN net	*	*	*	*	aucun	Default allow LAN to any rule	
<input type="checkbox"/>	0/0 B	IPv6 *	LAN net	*	*	*	*	aucun	Default allow LAN IPv6 to any rule	
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	*	*	10.0.1.10	53 (DNS)	*	aucun	Allow protocol DNS LAN-DMZ	
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	*	*	10.0.1.10	80 (HTTP)	*	aucun	Autoriser le protocole HTTP entre le LAN et la DMZ	
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	*	*	10.0.1.10	443 (HTTPS)	*	aucun	Autoriser le protocole HTTPS entre le LAN et la DMZ	

2. Les différentes règles de firewalling pour l'interface DMZ

- La première permet au membre de la DMZ l'accès à internet
- La deuxième autorise le flux de requêtes DNS sur le serveur uniquement
- La troisième autorise le ping au sein de la DMZ
- Les deux dernières autorisent le protocole HTTP et HTTPS

Flottant(e)	WAN	LAN	DMZ								
Règles (Faire glisser pour changer l'ordre)											
	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
<input type="checkbox"/>	✓ 0 /0 B	IPv4 *	DMZ net	*	*	*	*	aucun		Accès de la DMZ vers WAN	
<input type="checkbox"/>	✓ 0 /0 B	IPv4 TCP/UDP	10.0.1.10	*	*	53 (DNS)	*	aucun		Allow protocol DNS	
<input type="checkbox"/>	✓ 0 /0 B	IPv4 ICMP any	*	*	Ce pare- feu	*	*	aucun		Allow ping to this firewall since PC- DMZ	
<input type="checkbox"/>	✓ 0 /0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	aucun		Allow protocol HTTP	
<input type="checkbox"/>	✓ 0 /0 B	IPv4 TCP	*	*	*	443 (HTTPS)	*	aucun		Allow protocol HTTPS	

Tests : nslookup/dig et ping

1. Tests internet (ping et nslookup)

```
Debian_12.0.0_VBM_LinuxVMImages.COM (Instantané 3) [En fonction] - Oracle VM VirtualBox - □ ×
Fichier Machine Écran Entrée Périphériques Aide
root@ns1:/# 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=118 time=14.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=8.65 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=13.9 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=9.85 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=118 time=14.9 ms
^X64 bytes from 8.8.8.8: icmp_seq=6 ttl=118 time=10.3 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5258ms
rtt min/avg/max/mdev = 8.650/12.077/14.889/2.557 ms

root@ns1:/# nslookup amazon.com
Server:          10.0.1.10
Address:         10.0.1.10#53

Non-authoritative answer:
Name:  amazon.com
Address: 52.94.236.248
Name:  amazon.com
Address: 54.239.28.85
Name:  amazon.com
Address: 205.251.242.103
```

```
root@client:/# 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=118 time=12.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=11.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=14.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=8.64 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=118 time=6.84 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 6.839/10.766/14.265/2.703 ms
```

```
root@client:/# nslookup amazon.com
Server:          10.0.1.10
Address:         10.0.1.10#53

** server can't find amazon.com: REFUSED
```

2. Test réseau interne (ping et dig/nslookup)

```
root@client:/# nslookup ns1
Server:          10.0.1.10
Address:         10.0.1.10#53

Name:  ns1.itic.lan
Address: 10.0.1.10
```

```
root@client:/# ping ns1
PING ns1.itic.lan (10.0.1.10) 56(84) bytes of data.
64 bytes from 10.0.1.10 (10.0.1.10): icmp_seq=1 ttl=63 time=1.01 ms
64 bytes from 10.0.1.10 (10.0.1.10): icmp_seq=2 ttl=63 time=0.954 ms
64 bytes from 10.0.1.10 (10.0.1.10): icmp_seq=3 ttl=63 time=0.635 ms
^C
--- ns1.itic.lan ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.635/0.867/1.013/0.166 ms
```

```
root@ns1:/# nslookup client.itic.lan
Server:          10.0.1.10
Address:         10.0.1.10#53
Name:   client.itic.lan
Address: 172.168.1.100
```

```
root@ns1:/# ping client
PING client.itic.lan (172.168.1.100) 56(84) bytes of data.
64 bytes from 172.168.1.100 (172.168.1.100): icmp_seq=1 ttl=63 time=2.05 ms
64 bytes from 172.168.1.100 (172.168.1.100): icmp_seq=2 ttl=63 time=0.563 ms
64 bytes from 172.168.1.100 (172.168.1.100): icmp_seq=3 ttl=63 time=0.676 ms
64 bytes from 172.168.1.100 (172.168.1.100): icmp_seq=4 ttl=63 time=0.700 ms
^C
--- client.itic.lan ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 4964ms
rtt min/avg/max/mdev = 0.563/0.997/2.052/0.610 ms
```