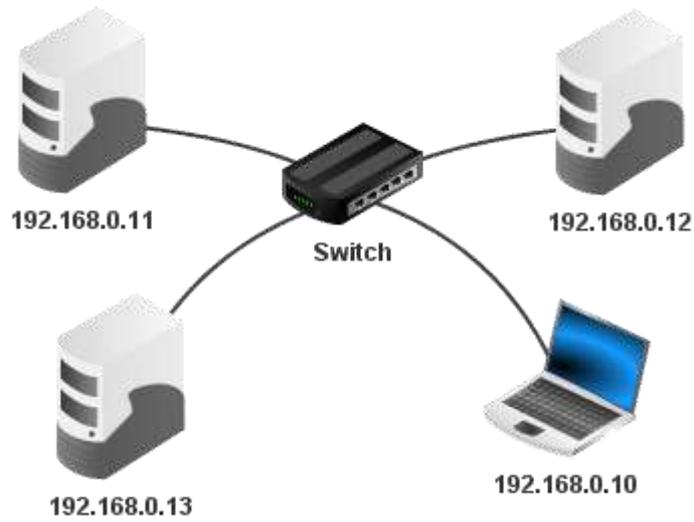


Documentation Technique du Projet de réseau pour l'entreprise Alpy

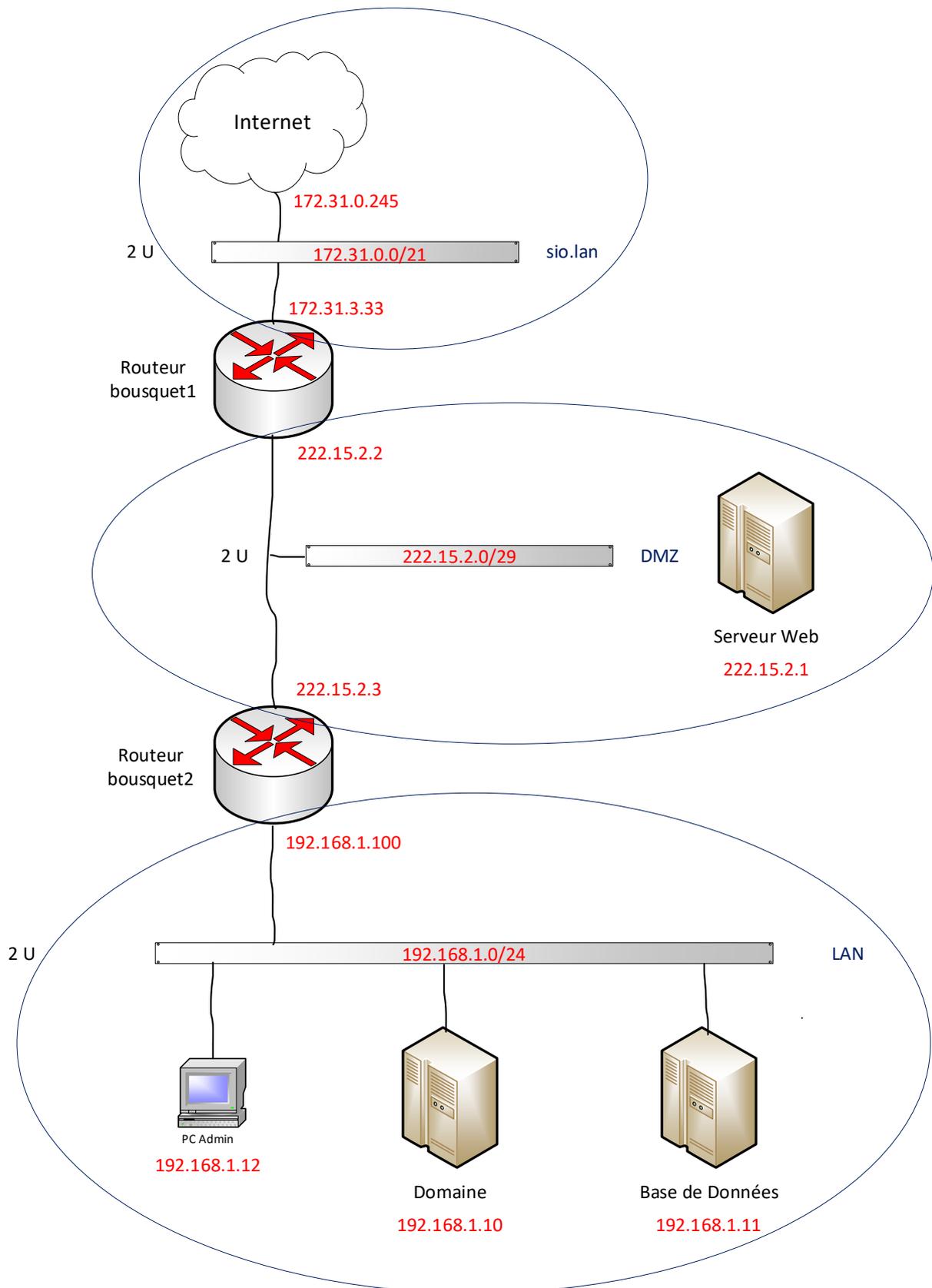


Raphaël Bousquet—Cadena ; SIO1

SOMMAIRE

1. Schéma Réseau	3
2. Plan d'adressage	4
3. Serveur Web	4
4. Serveur Base de Données	5
5. Machine Administrateur	5
6. Routeurs	6
7. Serveur Domaine	8

Shéma Réseau



Plan d'adressage

Machines	Noms	Adresses IP	Masques de sous-réseau	Passerelles	DNS
<u>LAN</u>	<u>bousquet.lan</u>	<u>192.168.1.0/24</u>	<u>255.255.255.0</u>	-	-
PC Admin	bousquetalpyadmin12	192.168.1.12	255.255.255.0	192.168.1.100	192.168.1.100
Samba AD	bousquetalpydomain12	192.168.1.10	255.255.255.0	192.168.1.100	192.168.1.100
Base de Données	bousquetalpybdd12	192.168.1.11	255.255.255.0	192.168.1.100	192.168.1.100
Routeur 2 (LAN)	routeurbousquet2	192.168.1.100	255.255.255.0		
<u>DMZ</u>	<u>bousquet.dmz</u>	<u>222.15.2.0/29</u>	<u>255.255.255.248</u>	-	-
Serveur Web	bousquetalpyweb12	222.15.2.1	255.255.255.248	222.15.2.2	222.15.2.2
Routeur 1 (LAN)	routeurbousquet1	222.15.2.2	255.255.255.248		
Routeur 2 (WAN)	routeurbousquet2	222.15.2.3	255.255.255.248	222.15.2.2	
<u>Internet</u>	<u>sio.lan</u>	<u>172.31.0.0/21</u>	<u>255.255.248.0</u>	-	-
Routeur 1 (WAN)	routeurbousquet1	172.31.3.33	255.255.248.0	172.31.0.245	

Serveur Web

Ip + hostname modifier (`nano /etc/hostname ; nano /etc/network/interfaces`)

Installation et configuration de php (+ php-fpm), nginx. (`apt install ; nano /etc/nginx/sites-available/default`)

```

GNU nano 7.2                                wordpress
# Note: You should disable gzip for SSL traffic.
# See: https://bugs.debian.org/773332
#
# Read up on ssl_ciphers to ensure a secure configuration.
# See: https://bugs.debian.org/765782
#
# Self signed certs generated by the ssl-cert package
# Don't use them in a production server!
#
# include snippets/snakeoil.conf;

root /var/www/WordPress;

# Add index.php to the list if you are using PHP
index index.php;

server_name 222.15.2.1;

location / {
    # First attempt to serve request as file, then
    # as directory, then fall back to displaying a 404.
    try_files $uri $uri/ / index.php?$args;
}

# pass PHP scripts to FastCGI server
#
location ~ \.php$ {
    include snippets/fastcgi-php.conf;
    #
    # With php-fpm (or other unix sockets):
    fastcgi_pass unix:/run/php/php8.2-fpm.sock;
    # With php-cgi (or other tcp sockets):
    fastcgi_pass 127.0.0.1:9000;
}

^G Aide      ^O Écrire   ^W Chercher  ^K Couper    ^T Exécuter  ^C EmplacementM-U Annuler
^X Quitter   ^R Lire fich.^N Remplacer ^U Coller    ^J Justifier ^_ Aller ligneM-E Refaire

```

Suppression de Apache2. (Dans etc : `rm -r apache2`)

Modification de la page .html par défaut avec un lien vers info.php.

Installation et configuration de phpMyAdmin en ssh (`mv -i phpMyAdmin /var/www/html` puis sur `default info.php`)

Modification du propriétaire et du groupe (`chown/chgrp -R www-data * ls -la`)

Installation et configuration de WordPress en ssh pour ensuite le déplacer pour la mettre en page par défaut (`mv -i wordpress /var/www/html`)

Modification du propriétaire et du groupe (`chown/chgrp -R www-data * ls -la`)

Serveur Base de Données

Ip + hostname modifier (`nano /etc/hostname ; nano /etc/network/interfaces`)

Suppression de Apache2. (Dans etc : `rm -r apache2`)

Installation et configuration de mariaDB, mysql, wget, zip. (`apt install ; nano /etc/mysql/mariadb.conf.d/50-server.cnf`)

```

GNU nano 7.2                               50-server.cnf
#
# These groups are read by MariaDB server.
# Use it for options that only the server (but not clients) should see
#
# this is read by the standalone daemon and embedded servers
[server]
#
# this is only for the mysqld standalone daemon
[mysqld]
#
# * Basic Settings
#
#user                               = mysql
pid-file                             = /run/mysqld/mysqld.pid
basedir                              = /usr
#datadir                            = /var/lib/mysql
#tmpdir                              = /tmp
#
# Broken reverse DNS slows down connections considerably and name resolve is
# safe to skip if there are no "host by domain name" access grants
#skip-name-resolve
#
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address                         = 192.168.1.11
#
# * Fine Tuning
#
#key_buffer_size                     = 128M

```

[Lecture de 119 lignes]

Ⓜ Aide	Ⓜ Écrire	Ⓜ Chercher	Ⓜ Couper	Ⓜ Exécuter	Ⓜ Emplacement	Ⓜ Annuler
Ⓜ Quitter	Ⓜ Lire fich.	Ⓜ Remplacer	Ⓜ Coller	Ⓜ Justifier	Ⓜ Aller ligne	Ⓜ Refaire

Connexion (`mysql -u root -p`) Création de la BDD (`CREATE DATABASES wordpress`) et d'un utilisateur (`CREATE USER 'root'@'%' IDENTIFIED BY 'sio';`) (`GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY 'sio';`)

Machine Administrateur

installation sur Virtual Box...

Configuration de l'IP en fonction du schéma réseau (*panneau de configuration > Réseau et Internet > Centre réseau et partage > Modifier les paramètres de la carte > Propriétés*)

Lorsque le serveur Domain sera installé et configuré, raccorder le domain.lan

Routeurs

Création de nouvelles machines avec l'iso de pfsense...

Configuration sur l'iso puis lors du *reboot*, détacher l'iso du disque de la VM (*Périphériques > Lecteurs Optiques > éjecter le disque du lecteur virtuelle*)

Dans VirtualBox, pour le routeur 1, configurer la première carte réseau en « accès par pont » puis la deuxième en « réseau interne ». Pour le routeur 2, configurer les deux cartes réseau en « réseau interne » (*VirtualBox > Réseau > Adapter 1 et Adapter 2*)

Après le reboot, mettre les IP des cartes réseau selon le schéma réseau.

Se connecter à pfsense avec la Machine Administrateur à pfsense (*mettre les adresses des routeurs dans un navigateur web pour accéder à pfsense, avec l'utilisateur admin et le mot de passe pfsense*)

Configurer les règles NAT selon le tableau suivant (*pfsense > Pare-feu > NAT*)

Routeur WAN / DMZ	Interface Web PFSENSE	4431
Routeur DMZ / LAN	Interface Web PFSENSE	4432
WEB / WORDPRESS	HTTP	80
WEB / WORDPRESS	HTTPS	443
WEB / WORDPRESS	SSH	22
ADMIN WINDOWS	RDP	3389
SGBD	SQL	3306

pfSense.bousquetJan - Pare-feu x pfSense.bousquet.dmz - Pare-feu x

Non sécurisé | https://222.15.2.3/firewall_nat.php

Systeme Interfaces Pare-feu Service VPN État Diagnostica Aide

Pare-feu / NAT / Transfert de port

Transfert de port 1:1 Sortant NPt

Règles

<input type="checkbox"/>	Interface	Protocole	Adresse source	Ports source	Adresse de destination	Ports dest.	IP NAT	Ports NAT	Description	Actions
<input type="checkbox"/>	DMZ	TCP/UDP	*	*	DMZ address	4432	192.168.1.100	443 (HTTPS)	Routeur WAN / DMZ	
<input type="checkbox"/>	DMZ	TCP/UDP	*	*	DMZ address	3389 (MS RDP)	192.168.1.12	3389 (MS RDP)	Bureau à distance	
<input type="checkbox"/>	DMZ	TCP/UDP	*	*	DMZ address	3306	192.168.1.11	3306	WEB - BDD	

Ajouter Ajouter Supprimer Toggle Enregistrer Séparateur

Légende
 Autoriser
 Règle liée

Afficher les icônes cachées

15° Rechercher 15:53 15/05/2024

pfSense.bousquetJan - Pare-feu x pfSense.bousquet.dmz - Pare-feu x

Non sécurisé | https://222.15.2.2/firewall_nat.php

Systeme Interfaces Pare-feu Service VPN État Diagnostica Aide

Transfert de port 1:1 Sortant NPt

Règles

<input type="checkbox"/>	Interface	Protocole	Adresse source	Ports source	Adresse de destination	Ports dest.	IP NAT	Ports NAT	Description	Actions
<input type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	4431	222.15.2.2	443 (HTTPS)	Routeur WAN / DMZ	
<input type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	4432	222.15.2.3	4432	Routeur DMZ / LAN	
<input type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	3389 (MS RDP)	222.15.2.3	3389 (MS RDP)	Bureau à distance	
<input type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	22 (SSH)	222.15.2.1	22 (SSH)	SSH	
<input type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	80 (HTTP)	222.15.2.1	80 (HTTP)	HTTP	
<input type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	443 (HTTPS)	222.15.2.1	443 (HTTPS)	HTTPS	

Ajouter Ajouter Supprimer Toggle Enregistrer Séparateur

Légende
 Autoriser
 Règle liée

https://222.15.2.2/firewall_nat_out.php

15° Rechercher 15:57 15/05/2024

Serveur Domaine

Dans VirtualBox, mettre la carte réseau en réseau interne.

Installation de samba AD (`apt install samba-ad-dc`)

Commande pour avoir tout les fichiers de configuration : `apt-get install samba winbind krb5-user smbclient python3-cryptography`

Retirer le fichier de configuration de samba (`rm -f /etc/samba/smb.conf`) puis tapez cette commande pour en créer un nouveau : `samba-tool domain provision --realm=MYDOMAIN.LAN --domain MYDOMAIN --server-role=dc`

Modifier le fichier `hosts` dans `etc`, rajouter une ligne l'IP de la machine, le nom de la machine collé au domain puis le nom de la machine seul.

```
GNU nano 7.2          etc/hosts          S
127.0.0.1    localhost
192.168.1.10 dombouquet.bousquet.lan bousquet.lan
# The following lines are desirable for IPv6 capable hosts
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters
```

Dans `etc/resolv.conf`, mettre son domain.lan puis l'IP du routeur et de la machine.

```
GNU nano 7.2          etc/resolv.conf
domain bousquet.lan
search bousquet.lan
nameserver 192.168.1.100
nameserver 192.168.1.10
nameserver 8.8.8.8
```

Dans `etc/samba/smb.conf` :

- DNS = IP Routeur
- Netbiosname = Nom de la Machine
- Realm = nom de domaine
- WorkGroup = DOMAIN

```

GNU nano 7.2 /etc/samba/smb.conf
# Global parameters
[global]
  dns forwarder = 192.168.1.100
  netbios name = DOMBOUSQUET
  realm = BOUSQUET.LAN
  server role = active directory domain controller
  workgroup = BOUSQUET

[sysvol]
  path = /var/lib/samba/sysvol
  read only = No

[netlogon]
  path = /var/lib/samba/sysvol/bousquet.lan/scripts
  read only = No

```

Dans *etc/krb5.conf* :

- Dns_lookup_Realm FALSE
- Dns_lookup_Kdc TRUE
- REALM Domain.lan

```

GNU nano 7.2 etc/krb5.conf
[libdefaults]
  default_realm = BOUSQUET.LAN
  dns_lookup_kdc = true
  dns_lookup_realm = false

  kdc_timesync = 1
  ccache_type = 4
  forwardable = true
  proxiable = true
  rdnc = false

  fcc-mit-ticketflags = true

[realms]
  BOUSQUET.LAN = {
    kdc = BOUSQUET.LAN
    admin_server = BOUSQUET.LAN
  }

```

Ainsi que le hostname :

```

GNU nano 7.2 etc/hostname
dombousquet.bousquet.lan

```