**Bachelier en informatique et Systèmes**

**Informatique industrielle**

**3ème année**



**Catégorie technique**

**Charleroi**

**EXAMEN LABO**

**MODIFICATION maquette**

**2017 – 2018 Haveaux Valentin**

Table des matières

[1) Maquette avant modification 4](#_Toc504599166)

[2) Fichier de configuration départ de la maquette 4](#_Toc504599167)

[2.1) /etc/named.conf du serveur DHCP 4](#_Toc504599168)

[2.2) /etc/sysconfig/dhcrelay du routeur R2 5](#_Toc504599169)

[3) Modification désirée : adressage dynamique rezo DMZ 5](#_Toc504599170)

[3.1) Taches à réaliser 5](#_Toc504599171)

[3.1.1) Sur R1 5](#_Toc504599172)

[3.1.2) Sur le serveur DHCP 5](#_Toc504599173)

[3.1.3) Sur le serveur WEB 6](#_Toc504599174)

[3.2) Maquette après modification 6](#_Toc504599175)

[4) Modification désirée : Ajout d’un serveur DNS redondant 6](#_Toc504599176)

[4.1) Taches à réaliser 7](#_Toc504599177)

[4.1.1) Sur le serveur DHCP 7](#_Toc504599178)

[4.1.2) Sur le serveur DNS1 7](#_Toc504599179)

[4.1.3) Sur le serveur DNS3 8](#_Toc504599180)

[4.2) Maquette après modification 9](#_Toc504599181)

[5) Modification désirée : Délégation et sous domaine DNS2 9](#_Toc504599182)

[5.1) Taches à réaliser 10](#_Toc504599183)

[5.1.1) Sur le serveur DHCP 10](#_Toc504599184)

[5.1.2) Sur le serveur DNS1 10](#_Toc504599185)

[5.1.3) Sur le serveur DNS2 11](#_Toc504599186)

[5.2) Maquette après modification 12](#_Toc504599187)

[6) Modification désirée : Ajout d’un site web privé au machine du réseau lan 13](#_Toc504599188)

[6.1) Taches à réaliser 13](#_Toc504599189)

[6.1.1) Sur le serveur web 13](#_Toc504599190)

[7) Modification désirée : ajout de virtualhost sur le web 13](#_Toc504599191)

[7.1) Taches à réaliser 14](#_Toc504599192)

[7.1.1) Sur le serveur WEB 14](#_Toc504599193)

[7.1.2) Sur le serveur DNS 16](#_Toc504599194)

[8) Arborescence et fichier de conf des serveurs 18](#_Toc504599195)

[8.1) Serveur DHCP 18](#_Toc504599196)

[8.1.1) Fichier /etc/sysconfig/network-scripts/ifcfg-eth0 18](#_Toc504599197)

[8.1.2) Fichier /etc/resolf.conf 18](#_Toc504599198)

[8.1.3) Fichier /etc/dhcp/dhcp.conf 18](#_Toc504599199)

[8.2) Serveur DNS1 20](#_Toc504599200)

[8.2.1) Fichier /etc/named.conf 20](#_Toc504599201)

[8.2.2) Fichier /etc/resolv.conf 20](#_Toc504599202)

[8.2.3) Fichier /var/named/db.exam.men 21](#_Toc504599203)

[8.2.4) Fichier /var/named/db.exam.men.rev 21](#_Toc504599204)

[8.3) Sur le serveur DNS2 22](#_Toc504599205)

[8.3.1) Fichier /etc/named.conf 22](#_Toc504599206)

[8.3.2) Fichier /var/named/db.work.exam.men 22](#_Toc504599207)

[8.3.3) Fichier /var/named/db.work.exam.men.rev 23](#_Toc504599208)

[8.4) Sur le serveur DNS3 23](#_Toc504599209)

[8.4.1) Fichier /etc/named.conf 23](#_Toc504599210)

[8.4.2) Fichier /var/named/slaves/db.exam.men 24](#_Toc504599211)

[8.4.3) Fichier /var/named/slaves/db.exam.men.rev 24](#_Toc504599212)

[8.5) Sur le serveur WEB 25](#_Toc504599213)

[8.5.1) Fichier /etc/http/httpd.conf 25](#_Toc504599214)

[8.5.2) Fichier /etc/httpd/conf.d/00-main.conf 25](#_Toc504599215)

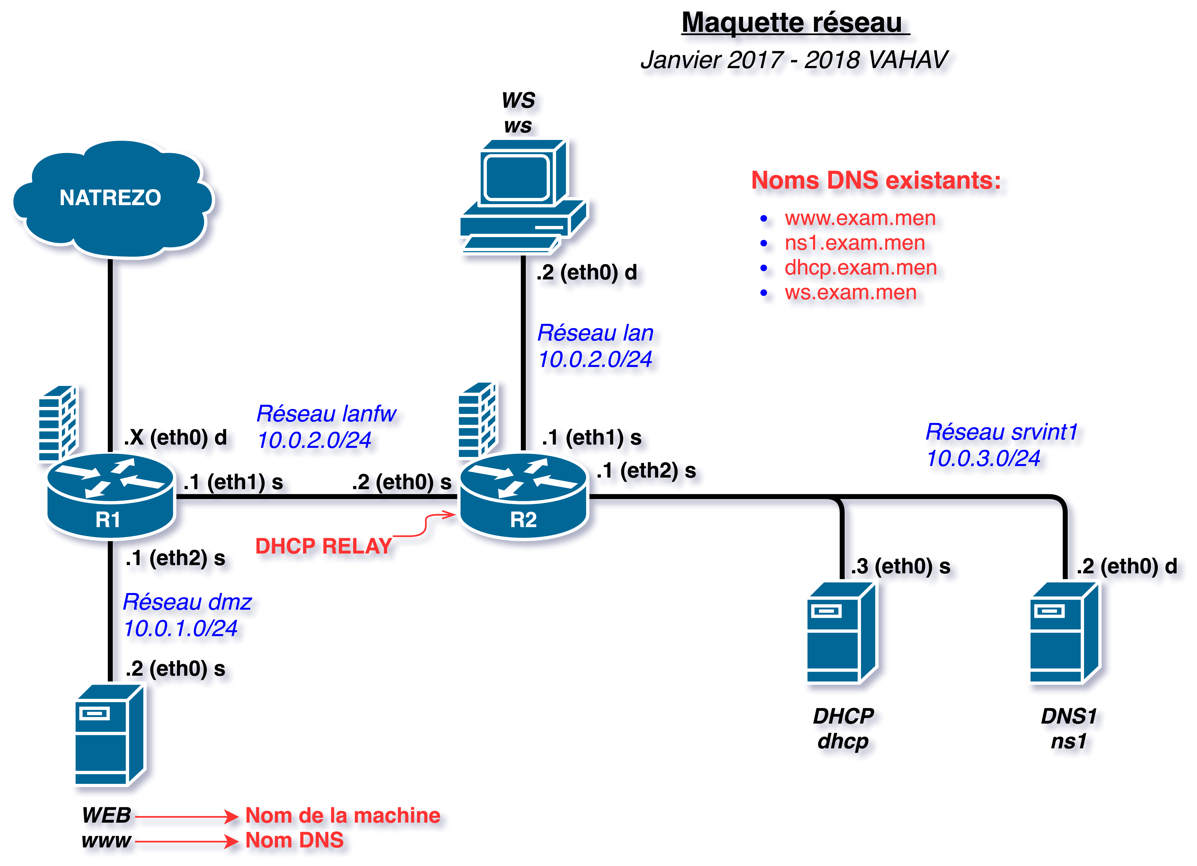
[8.5.3) Fichier /etc/httpd/conf.d/00-server.conf 25](#_Toc504599216)

[8.5.4) Fichier /etc/httpd/conf.d/0-userdir.conf 26](#_Toc504599217)

[8.5.5) Arborescence /var/www 27](#_Toc504599218)

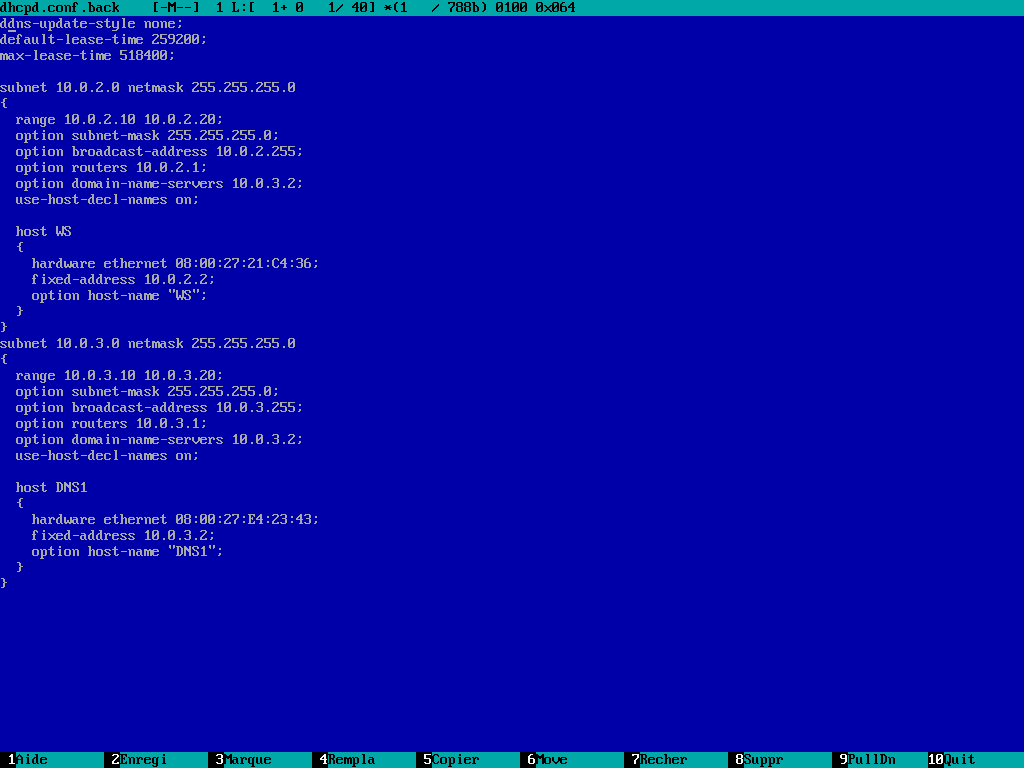
[9) Maquette finale 27](#_Toc504599219)

# Maquette avant modification



# Fichier de configuration départ de la maquette

## 2.1) /etc/named.conf du serveur DHCP

ddns-update-style none ;

default-lease-time 259200 ;

max-lease-time 518400 ;

subnet 10.0.2.0 netmask 255.255.255.0

{

range 10.0.2.10 10.0.2.20 ;

option subnet-mask 255.255.255.0 ;

option broadcast-address 10.0.2.255 ;

option domain-name-servers 10.0.3.2 ;

use-host-decl-names on ;

host WS

{

hardware ethernet 08:00:27:21:C4:36 ;

fixed-address 10.0.2.2 ;

option host-name « WS » ;

}

}

subnet 10.0.3.0 netmask 255.255.255.0

{

range 10.0.3.10 10.0.3.20 ;

option subnet-mask 255.255.255.0 ;

option broadcast-address 10.0.3.255 ;

option domain-name-servers 10.0.3.2 ;

use-host-decl-names on ;

host DNS1

{

hardware ethernet 08:00:27:E4:23:43;

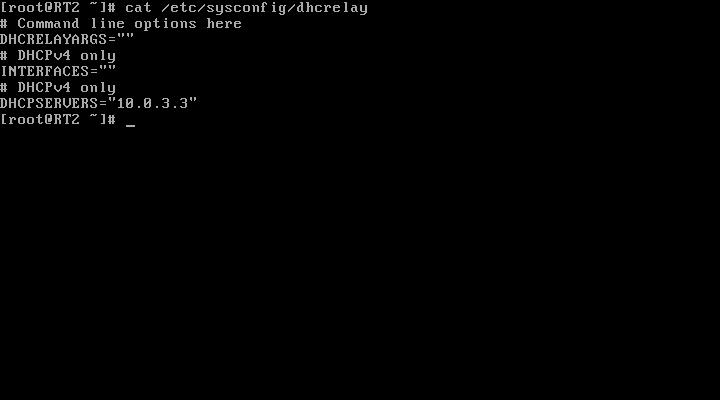
fixed-address 10.0.2.2 ;

option host-name « WS » ;

}

}

## 2.2) /etc/sysconfig/dhcrelay du routeur R2



# Modification désirée : adressage dynamique rezo DMZ

On souhaite modifier la maquette réseau, afin que le serveur WEB se trouvant dans le réseau *dmz* puisse obtenir sa configuration de sa carte Ethernet via le serveur DHCP.

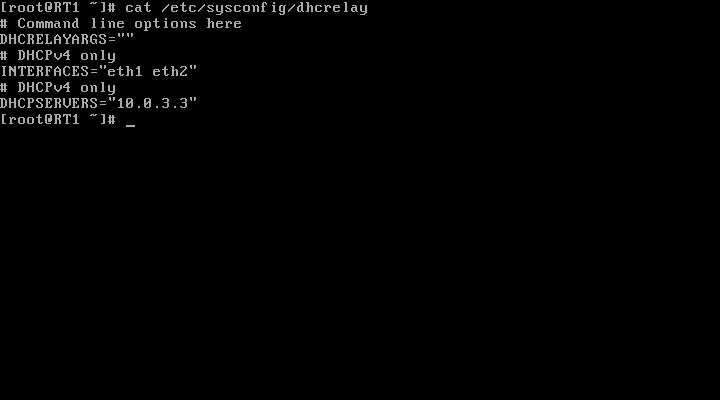
Pour cela, il va falloir installer dhcprelay sur le serveur R1. Il va falloir également configurer le serveur DHCP pour que celui-ci attribue des adresses dans le réseau dmz et plus précisément pour le serveurs WEB.

## 3.1) Taches à réaliser

### 3.1.1) Sur R1

La première chose à faire sur R1 est d’installer dhcp via la commande 🡪 # yum install dhcp –y

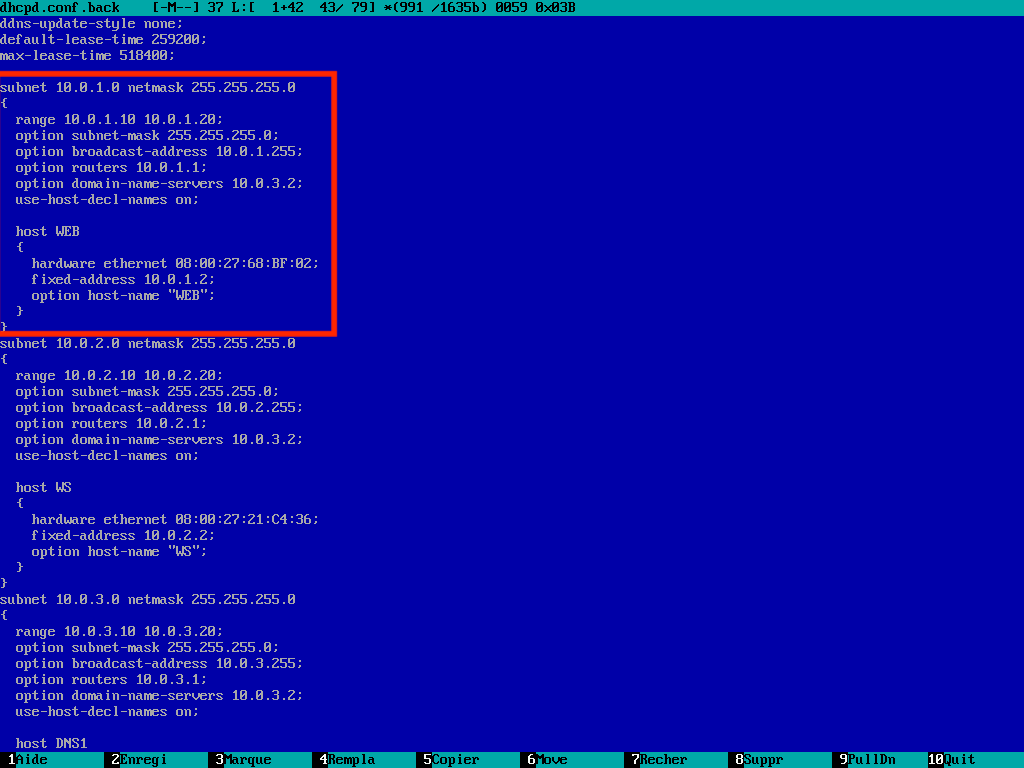
Ensuite, il vaudra modifier le fichier /etc/sysconfig/dhcrelay afin d’y ajouter les interfaces de relais et l’adresse ip du serveur DHCP. Le fichier devait ressembler à ça :



Et pour finir, il faudra lancer le service dhcrelay via la commande 🡪 #service dhcrelay start

### 3.1.2) Sur le serveur DHCP

Sur le serveur dhcp, il faudra modifier le fichier de configuration /etc/dhcp/dhcpd.conf afin d’y ajouter le subnet dmz ainsi que le host WEB. La syntaxe devra ressembler à ça :

 subnet 10.0.2.0 netmask 255.255.255.0

{

range 10.0.2.10 10.0.2.20 ;

option subnet-mask 255.255.255.0 ;

option broadcast-address 10.0.2.255 ;

option domain-name-servers 10.0.3.2 ;

use-host-decl-names on ;

host WS

{

hardware ethernet 08:00:27:21:C4:36 ;

fixed-address 10.0.2.2 ;

option host-name « WS » ;

}

}

Il faudra alors relancer le serveur DHCP via la commande 🡪 #service dhcpd restart

### 3.1.3) Sur le serveur WEB

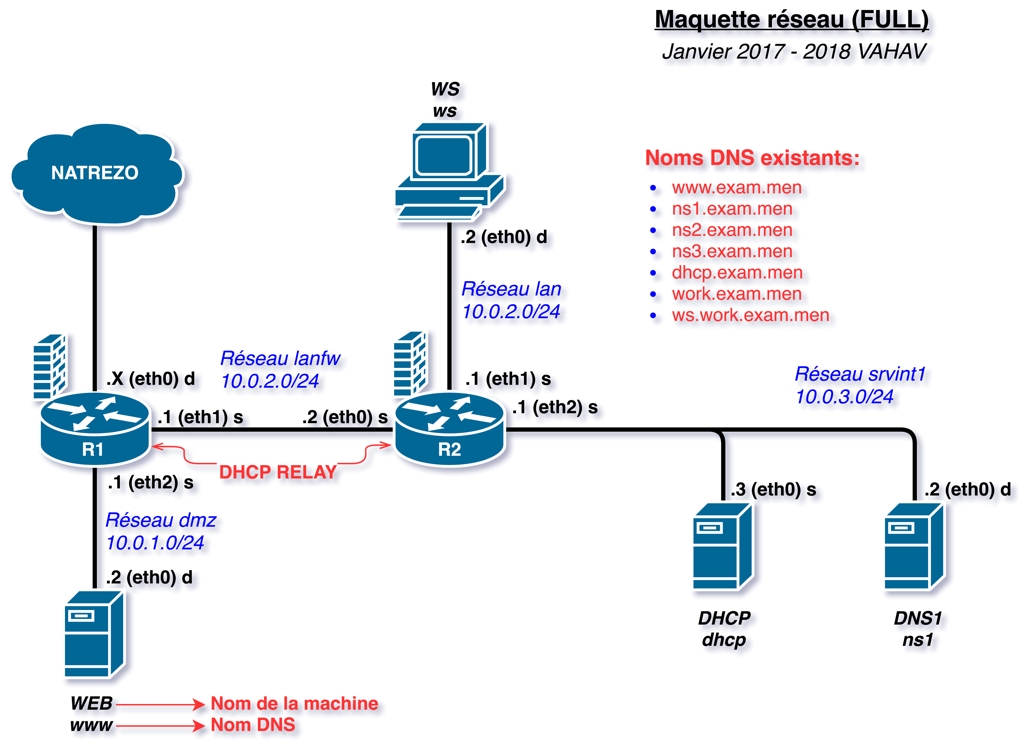
Sur le serveur WEB, il faudra modifier le fichier /etc/sysconfig/network-scipts/ifcfg-eth0 afin que sa configuration soit via DHCP et non plus static.



Pour terminer il faudra relancer la demande d’adressage via la commande 🡪 #service network restart

## 3.2) Maquette après modification

Après cette modification, la maquette ressemblera à ceci :



On peut voir que les deux routeurs R1 et R2 sont en DHCP RELAY et que le serveur WEB n’a plus une adresse statique (s) mais dynamique (d).

# Modification désirée : Ajout d’un serveur DNS redondant

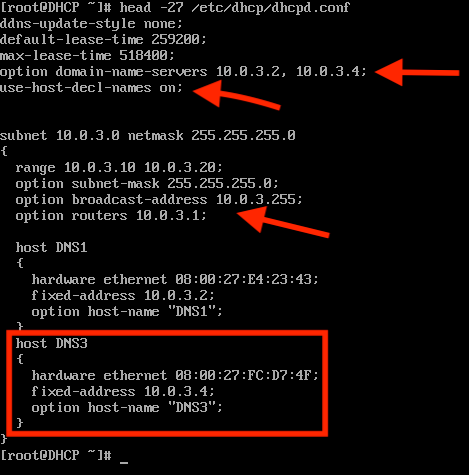
On souhaite ajouter un serveur DNS esclave du serveur DNS1. Ce serveur DNS3 sera placé sur le réseau srvint1. Ce serveur aura pour objectif d’assurer la résolution de noms si jamais le serveurs DNS1 maitre venait à cracher. Si l’on souhaite que la maquette soit fonctionnelle, il faudra également modifier le serveur DHCP afin que celui-ci indique le serveur esclave dans la configuration.

## 4.1) Taches à réaliser

### 4.1.1) Sur le serveur DHCP

Sur le serveur DHCP, nous allons modifier le fichier de configuration afin que celui-ci attribue une adresse fixe à notre nouveau serveur DNS3.

Nous allons aussi modifier le fichier afin que le paramètre *option domain-name-servers* (en y ajoutant le nouveau serveur 10.0.3.4) ainsi que le paramètre *use-host-decl-names* soient en global vu que ces paramètres sont communs à tous nos subnets, par besoin de les recopier.



Après il faudra relancer le serveur DHCP et lancer la machine serveur DNS3.

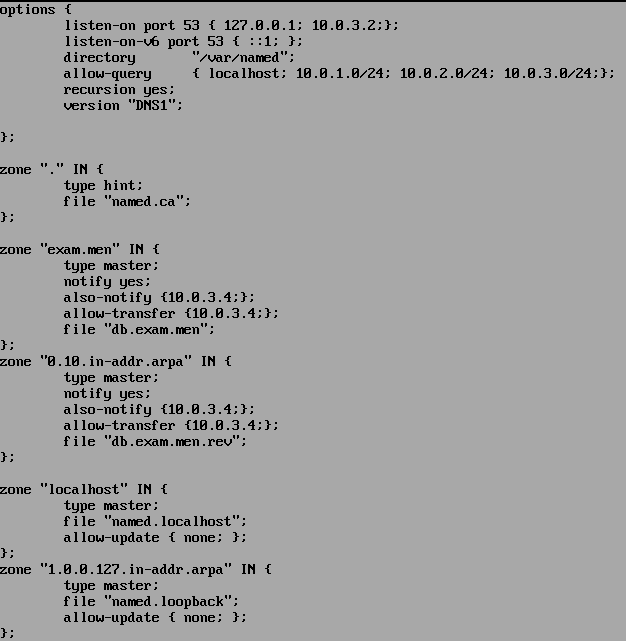
### 4.1.2) Sur le serveur DNS1

Sur le serveur DNS1, il va falloir modifier le fichier /etc/named.conf afin d’y indiquer qu’il doit transférer les fichiers de zone via 10.0.3.4 ainsi que d’activer les notify. Il faudra donc ajouter les paramètres : notify yes;

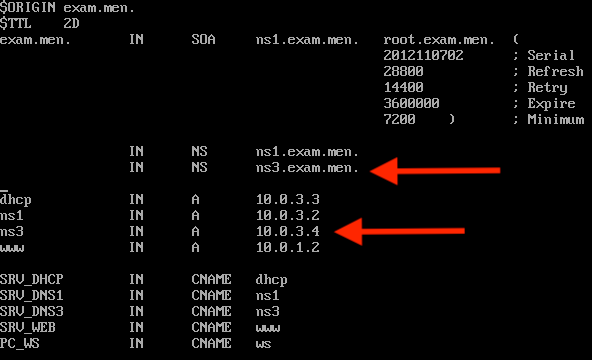
Also-notify {10.0.3.4;};

Allow-transfer {10.0.3.4;};

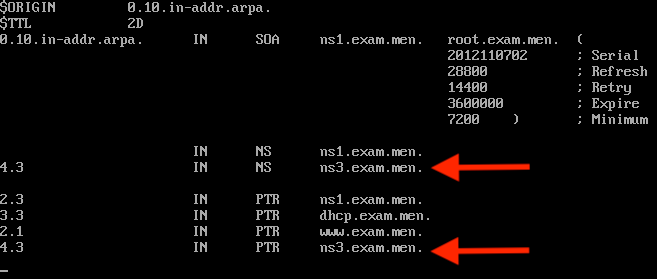
Dans chaque la zone exam.men et la zone 0.10.in-addr.arpa



Ensuite, il faudra modifier les fichiers de zone /var/named/db.exam.men et /var/named/db.exam.men.rev afin d’y indique le nouveau serveur DNS3 et ajouter un RR de type name server (NS).

Attention aux permissions

#chgrp named /var/named/db.exam.men\*

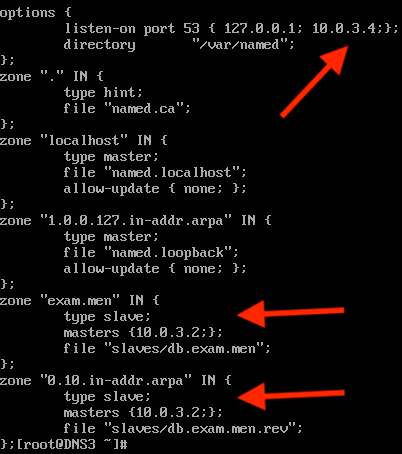


### 4.1.3) Sur le serveur DNS3

Sur le serveur DNS3, il faut d’abord installer bind via la commande :

#yum install bind bind-utils bind-libs .

Ensuite, il faut modifier le fichier /etc/named.conf afin de lui indiquer qu’il est esclave du serveur DNS1 et que ses fichiers de zone se trouvent dans /var/named/slaves/



Dans listen-on port 53, on ajoute l’adresse ip du serveur DNS3.

Dans les zones exam.men et rev on mets les paramètres : type slave ;

masters {10.0.3.2;};

file «slaves/db.exam.men(.rev)»;

Une fois ceci fait, il faut relancer le serveurs DNS1 suivi du serveurs DNS3 via la commande : #service named restart.

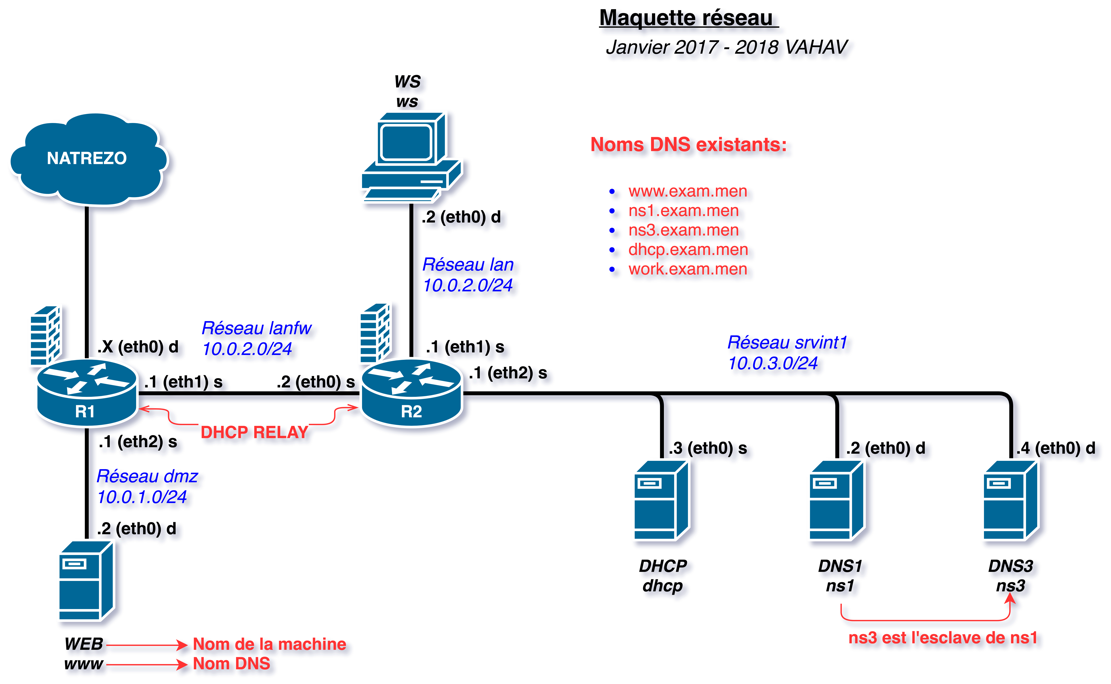
Si tout s’est bien déroulé, les fichiers /var/named/slaves/db.exam.men et /var/named/slaves/db.exam.men.rev ont dû être créés sur le serveur DNS3.

Très important : echo « nameserver 127.0.0.1 » > /etc/resolf.conf

Si maintenant nous arrêtions le serveurs DNS1, ce serait le serveur DNS3 qui prendrait le relais pour la résolution de noms.

## 4.2) Maquette après modification

Après cette modification, la maquette ressemblera à ceci :



On peut y voir l’ajout du serveur DNS3 qui est esclave du serveur DNS1. On peut voir également que son adressage est dynamique (d).

# Modification désirée : Délégation et sous domaine DNS2

On souhaite ajouter un serveur DNS2 sur un nouveau réseau srvint2 connecter avec l’interface eth3 du routeur R2 qui aura pour rôle de superviser un sous domaine de examen.men. Pour ce faire, il faudra faire ceci:

🡪 modifier le serveur DHCP afin qu’il configure le serveur DNS2.

🡪 modifier les fichiers de zones sur le serveur DNS1.

🡪 Relancer le serveur bind DNS1.

🡪 Relancer le serveur bind DNS3.

🡪 Installer bind sur DNS2.

🡪 Configurer le fichier de configuration bind et les fichiers de zones du serveur DNS2.

🡪 Lancer le serveur bind DNS2.

## 5.1) Taches à réaliser

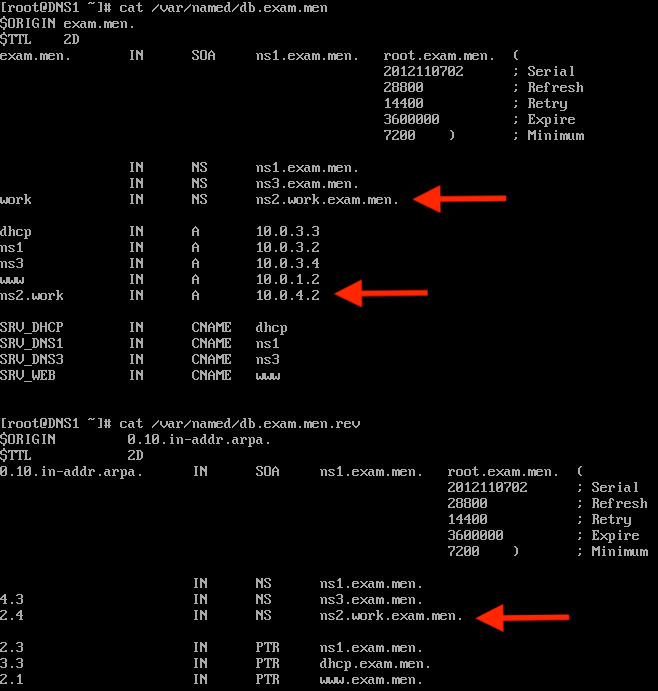
### 5.1.1) Sur le serveur DHCP

Sur le serveur DHCP, nous allons modifier le fichier de configuration afin que celui-ci est autorité sur le subnet 10.0.4.0/24 et que l’on attribue l’adresse 10.0.4.2 au nouveau serveur DNS2 qui sera sur ce subnet avec comme passerelle la nouvelle carte ajoutée au routeur R2.



### 5.1.2) Sur le serveur DNS1

Sur le serveur DNS1 nous allons modifier le fichier de zone exam.men et son fichier .rev afin d’y déléguer le sous domaine work au serveurs DNS2.



Une fois que ces modifications sont faites, nous pouvons relancer le serveur DNS1 via la commande : #service named restart.

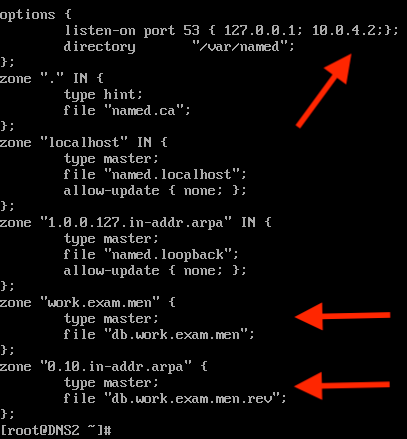
Nous devons aussi effacer les fichiers slaves/ sur le serveur DNS3 et le relancer afin qu’il reçoive les modifications faites sur le serveurs DNS1.

### 5.1.3) Sur le serveur DNS2

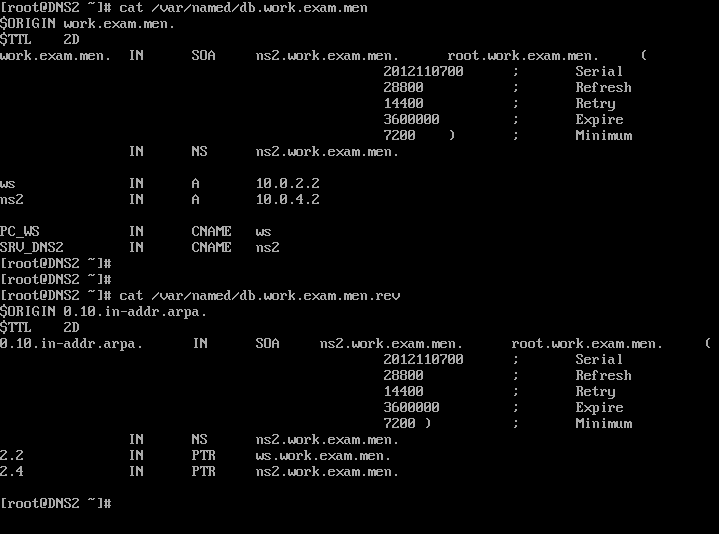
Sur le serveur DNS2 il faut d’abord installer bind via la commande :

#yum install bind bind-utils bind-libs

Ensuite il faut configurer le fichier /etc/named.conf afin que celui-ci écoute le serveur DNS1 (10.0.3.2) et qu’il possède deux fichiers de zone pour le domaine work.exam.men



Après cela, il faudra créer le fichier de zone work.exam.men ainsi que le fichier reverse dans /var/named afin que le serveur DNS2 puisse résoudre les requêtes du domain work.exam.men.

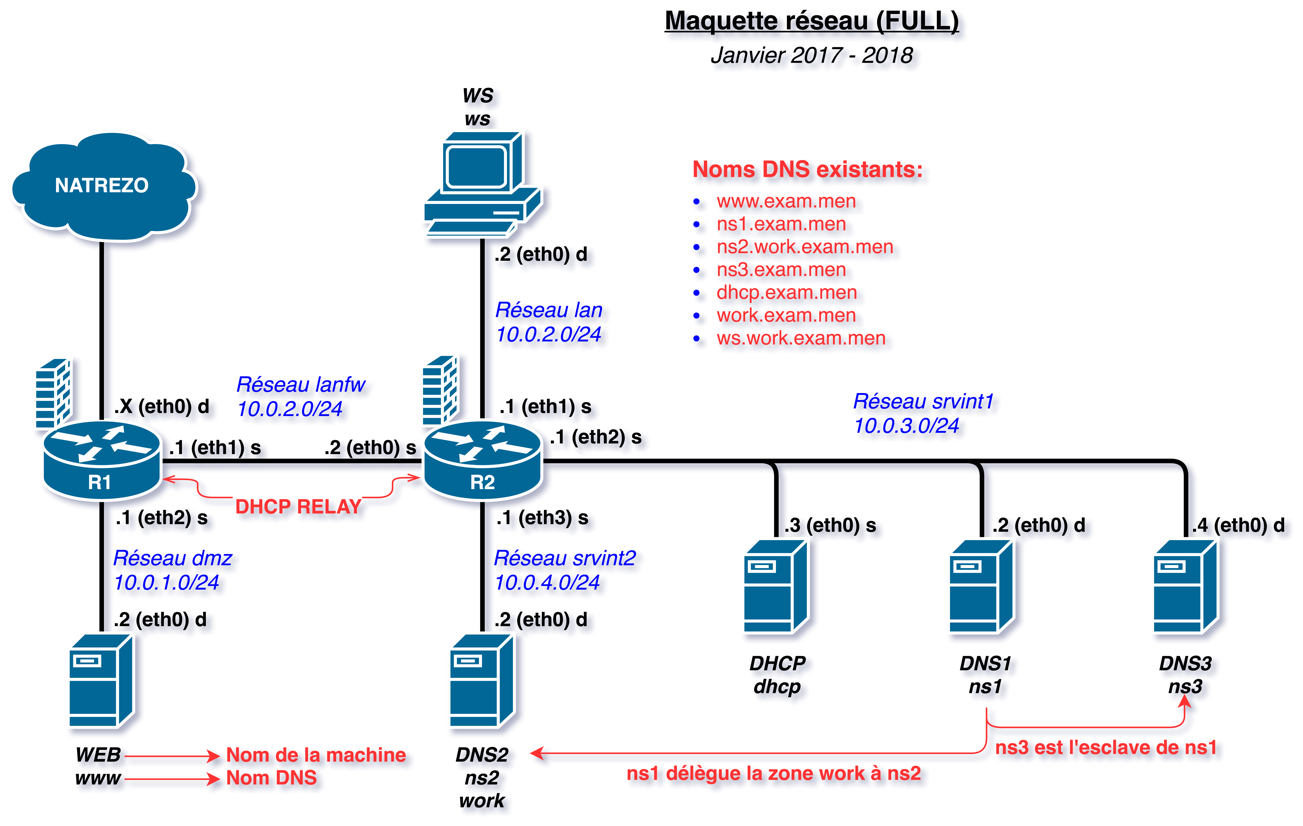


Ensuite, il ne faut pas oublier de faire un #chgrp named /var/named/db.work.exam\* afin que le service named puisse accéder aux fichiers de zone.

Pour finir, il faudra lancer le service sur DNS2 via la commande : #service named start

## 5.2) Maquette après modification

Après ces modifications sur la maquette, nous pouvons voir l’ajout du serveur DNS2 se trouvant dans le réseau srvint2 avec comme passerelle le routeur R2.



# Modification désirée : Ajout d’un site web privé au machine du réseau lan

On souhaite modifier le serveur WEB afin que seul les machines se trouvant dans le réseau lan aient accès à un intranetWS.

## 6.1) Taches à réaliser

### 6.1.1) Sur le serveur web

* Tout d’abord il va falloir créer la directory : #mkdir /var/www/html/intranetWS
* Ensuite il va falloir écrire un index.html dans cette directory :

#vi /var/www/html/intranetWS/index.html

<html>

<head>

<title> INTRANET LAN </title>

</head>

<body>

INTRANET DU LAN

</body>

</html>

* Puis dans le fichier /etc/httpd/conf.d/00-\*main.conf il va falloir ajouter cette directory :

<Directory /var/www/html/intranetWS>

<RequireAny>

Require ip 10.0.2.0/24

</RequireAny>

</Directory>

* Après il faut relancer le serveur WEB pour qu’il prenne en compte les modifications :

#service httpd restart

Une fois tout ceci fait, les machines se trouvant dans le réseau lan pourront accéder à leur intranet via #lynx [www.exam.men/intranetWS](http://www.exam.men/intranetWS)

# Modification désirée : ajout de virtualhost sur le web

On souhaite modifier la maquette afin que le serveur WEB héberge plusieurs virtualhost sur son interface d’écoute. Pour cela, il faudra donc :

🡪 Créer les alias de la carte Ethernet enp0s3 du serveur WEB

🡪 Créer les fichiers index.html dans /var/www/vh/\*

🡪 Créer les virtualhost dans le fichier /etc/httpd/conf.d/00-server.conf

🡪 Relancer le serveur WEB

🡪 Modifier le serveur DNS pour la résolution de noms

🡪 Relancer le serveur DNS

## 7.1) Taches à réaliser

### 7.1.1) Sur le serveur WEB

Tout d’abord il va falloir écrire les alias de la carte Ethernet enp0s3 (enp0s3:0, enp0s3:1, enp0s3:2, enp0s3:3, enp0s3:4).

Exemple : #vi /etc/sysconfig/network-scripts/ifcfg-enp0s3:0

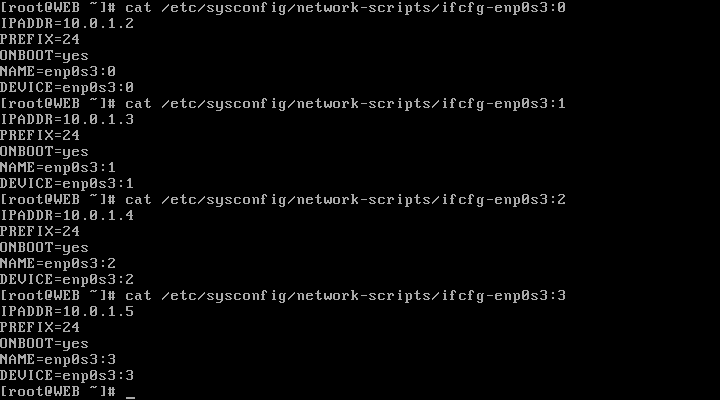
IPADDR=10.0.1.3

PREFIX=24

ONBOOT=yes

NAME=enp0s3:0

DEVICE=enp0s3:0



Ensuite, il faut créer les dossiers hébergent les hôtes virtuels :

#mkdir /var/www/vh/jean

#mkdir /var/www/vh/louis

#mkdir /var/www/vh/vh1

#mkdir /var/www/vh/vh2

#mkdir /var/www/vh/vh3

Puis pour chaque dossier, il faut écrire un fichier index.html comme par exemple :

#vi /var/www/vh/jean/index.html

<html>

<head>

<title> Site vh jean </title>

</head>

<body>

SITE VH DE JEAN

</body>

</html>

Après cela, il faut ajouter les virtualhost dans le fichier /etc/httpd/conf.d/00-server.conf :

ServerName www.exam.men

ServerAdmin moi@exam.men

ErrorDocument 404 /erreur/erreur\_404.html

<IfModule prefork.c>

MinSpareServers 3

MaxSpareServers 1O

StartServers 7

MaxRequestWorkers 20

ServerLimit 20

</IfModule>

<IfModule dir\_module>

DirectoryIndex index.html accueil.html

</IfModule>

**#PAR IP**

**<VirtualHost 10.0.1.4>**

**ServerName jean.www.exam.men**

**DocumentRoot /var/www/vh/jean**

**</VirtualHost>**

**<VirtualHost 10.0.1.5>**

**ServerName louis.exam.men**

**DocumentRoot /var/www/vh/louis**

**</VirtualHost>**

**#PAR NOMS**

**<VirtualHost 10.0.1.2>**

**ServerName www.exam.men**

**DocumentRoot /var/www/html**

**</VirtualHost>**

**<VirtualHost 10.0.1.2>**

**ServerName vh1.exam.men**

**DocumentRoot /var/www/vh/vh1**

**</VirtualHost>**

**<VirtualHost 10.0.1.3>**

**ServerName vh2.exam.men**

**DocumentRoot /var/www/vh/vh2**

**<Directory /var/www/vh/vh2>**

**AuthName "Acces au site vh2"**

**AuthType Basic**

**AuthUserFile /var/www/securite/pwd**

**Require valid-user**

**</Directory>**

**</VirtualHost>**

**<VirtualHost 10.0.1.3>**

**ServerName vh3.exam.men**

**DocumentRoot /var/www/vh/vh3**

**</VirtualHost>**

Pour le serveur WEB, il ne reste plus maintenant qu’à relancer le service network pour attribuer les nouvelles adresses au alias et relancer le serveur httpd pour qu’il reçoivent les modifications faites dans le fichier 00-server.conf :

#service network restart

#service httpd restart

### 7.1.2) Sur le serveur DNS

Sur le serveur DNS, nous allons modifier le fichier de zone exam.men et son reverse afin qu’il puisse résoudre les noms que nous allons lier au alias du serveur WEB

[root@DNS1 ~]# cat /var/named/db.exam.men

$ORIGIN exam.men.

$TTL 2D

exam.men. IN SOA ns1.exam.men. root.exam.men. (

2012110702 ; Serial

28800 ; Refresh

14400 ; Retry

3600000 ; Expire

7200 ) ; Minimum

IN NS ns1.exam.men.

IN NS ns3.exam.men.

work IN NS ns2.work.exam.men.

dhcp IN A 10.0.3.3

ns1 IN A 10.0.3.2

ns3 IN A 10.0.3.4

ns2.work IN A 10.0.4.2

www IN A 10.0.1.2

**vh1 IN A 10.0.1.2**

**vh2 IN A 10.0.1.3**

**vh3 IN A 10.0.1.3**

**jean.www IN A 10.0.1.4**

**louis IN A 10.0.1.5**

SRV\_DHCP IN CNAME dhcp

SRV\_DNS1 IN CNAME ns1

SRV\_DNS3 IN CNAME ns3

SRV\_WEB IN CNAME www

[root@DNS1 ~]# cat /var/tmp/db.exam.men.rev

$ORIGIN 0.10.in-addr.arpa.

$TTL 2D

0.10.in-addr.arpa. IN SOA ns1.exam.men. root.exam.men. (

2012110702 ; Serial

28800 ; Refresh

14400 ; Retry

3600000 ; Expire

7200 ) ; Minimum

IN NS ns1.exam.men.

4.3 IN NS ns3.exam.men.

2.4 IN NS ns2.work.exam.men.

2.3 IN PTR ns1.exam.men.

3.3 IN PTR dhcp.exam.men.

2.1 IN PTR www.exam.men.

**2.1 IN PTR vh1.exam.men.**

**3.1 IN PTR vh2.exam.men.**

**3.1 IN PTR vh3.exam.men.**

**4.1 IN PTR jean.www.exam.men.**

**5.1 IN PTR louis.exam.men.**

Une fois les fichiers de zone modifier, il faut relancer le serveur DNS1 ainsi que le DNS3 qui est l’esclave afin qu’ils prennent en compte les modifications.

Les machines peuvent désormais avoir accès au différent hôtes virtuels.

# Arborescence et fichier de conf des serveurs

## 8.1) Serveur DHCP

### 8.1.1) Fichier /etc/sysconfig/network-scripts/ifcfg-eth0

DEVICE=eth0

ONBOOT=yes

BOOTPROTO=static

IPADDR=10.0.3.3

PREFIX=24

GATEWAY=10.0.3.1

### 8.1.2) Fichier /etc/resolf.conf

; generated by /sbin/dhclient-script

search google.be

nameserver 8.8.8.8

nameserver 212.71.0.33

nameserver 212.71.8.10

### 8.1.3) Fichier /etc/dhcp/dhcp.conf

ddns-update-style none;

default-lease-time 259200;

max-lease-time 518400;

option domain-name-servers 10.0.3.2, 10.0.3.4;

use-host-decl-names on;

subnet 10.0.3.0 netmask 255.255.255.0

{

range 10.0.3.10 10.0.3.20;

option subnet-mask 255.255.255.0;

option broadcast-address 10.0.3.255;

option routers 10.0.3.1;

host DNS1

{

hardware ethernet 08:00:27:E4:23:43;

fixed-address 10.0.3.2;

option host-name "DNS1";

}

host DNS3

{

hardware ethernet 08:00:27:FC:D7:4F;

fixed-address 10.0.3.4;

option host-name "DNS3";

}

}

subnet 10.0.1.0 netmask 255.255.255.0

{

range 10.0.1.10 10.0.1.20;

option subnet-mask 255.255.255.0;

option broadcast-address 10.0.1.255;

option routers 10.0.1.1;

host WEB

{

hardware ethernet 08:00:27:39:c6:8c;

fixed-address 10.0.1.2;

option host-name "WEB";

}

}

subnet 10.0.2.0 netmask 255.255.255.0

{

range 10.0.2.10 10.0.2.20;

option subnet-mask 255.255.255.0;

option broadcast-address 10.0.2.255;

option routers 10.0.2.1;

host WS

{

hardware ethernet 08:00:27:21:C4:36;

fixed-address 10.0.2.2;

option host-name "WS";

}

}

subnet 10.0.4.0 netmask 255.255.255.0

{

range 10.0.4.10 10.0.4.20;

option subnet-mask 255.255.255.0;

option broadcast-address 10.0.4.255;

option routers 10.0.4.1;

host DNS2

{

hardware ethernet 08:00:27:7C:0D:9E;

fixed-address 10.0.4.2;

option host-name "DNS2";

}

}

## 8.2) Serveur DNS1

### 8.2.1) Fichier /etc/named.conf

options {

listen-on port 53 { 127.0.0.1; 10.0.3.2;};

listen-on-v6 port 53 { ::1; };

directory "/var/named";

allow-query { localhost; 10.0.1.0/24; 10.0.2.0/24; 10.0.3.0/24; 10.0.4.0/24;};

recursion yes;

version "DNS1";

};

zone "." IN {

type hint;

file "named.ca";

};

zone "exam.men" IN {

type master;

notify yes;

also-notify {10.0.3.4;};

allow-transfer {10.0.3.4;};

file "db.exam.men";

};

zone "0.10.in-addr.arpa" IN {

type master;

notify yes;

also-notify {10.0.3.4;};

allow-transfer {10.0.3.4;};

file "db.exam.men.rev";

};

zone "localhost" IN {

type master;

file "named.localhost";

allow-update { none; };

};

zone "1.0.0.127.in-addr.arpa" IN {

type master;

file "named.loopback";

allow-update { none; };

};

### 8.2.2) Fichier /etc/resolv.conf

; generated by /sbin/dhclient-script

nameserver 127.0.0.1

### 8.2.3) Fichier /var/named/db.exam.men

$ORIGIN exam.men.

$TTL 2D

exam.men. IN SOA ns1.exam.men. root.exam.men. (

2012110702 ; Serial

28800 ; Refresh

14400 ; Retry

3600000 ; Expire

7200 ) ; Minimum

IN NS ns1.exam.men.

IN NS ns3.exam.men.

work IN NS ns2.work.exam.men.

dhcp IN A 10.0.3.3

ns1 IN A 10.0.3.2

ns3 IN A 10.0.3.4

ns2.work IN A 10.0.4.2

www IN A 10.0.1.2

vh1 IN A 10.0.1.2

vh2 IN A 10.0.1.3

vh3 IN A 10.0.1.3

jean.www IN A 10.0.1.4

louis IN A 10.0.1.5

SRV\_DHCP IN CNAME dhcp

SRV\_DNS1 IN CNAME ns1

SRV\_DNS3 IN CNAME ns3

SRV\_WEB IN CNAME www

### 8.2.4) Fichier /var/named/db.exam.men.rev

$ORIGIN 0.10.in-addr.arpa.

$TTL 2D

0.10.in-addr.arpa. IN SOA ns1.exam.men. root.exam.men. (

2012110702 ; Serial

28800 ; Refresh

14400 ; Retry

3600000 ; Expire

7200 ) ; Minimum

IN NS ns1.exam.men.

4.3 IN NS ns3.exam.men.

2.4 IN NS ns2.work.exam.men.

2.3 IN PTR ns1.exam.men.

3.3 IN PTR dhcp.exam.men.

2.1 IN PTR www.exam.men.

2.1 IN PTR vh1.exam.men.

3.1 IN PTR vh2.exam.men.

3.1 IN PTR vh3.exam.men.

4.1 IN PTR jean.www.exam.men.

5.1 IN PTR louis.exam.men.

## 8.3) Sur le serveur DNS2

### 8.3.1) Fichier /etc/named.conf

options {

listen-on port 53 { 127.0.0.1; **10.0.4.2**;};

directory "/var/named";

};

zone "." IN {

type hint;

file "named.ca";

};

zone "localhost" IN {

type master;

file "named.localhost";

allow-update { none; };

};

zone "1.0.0.127.in-addr.arpa" IN {

type master;

file "named.loopback";

allow-update { none; };

};

zone "work.exam.men" {

type master;

file "db.work.exam.men";

};

zone "0.10.in-addr.arpa" {

type master;

file "db.work.exam.men.rev";

};

### 8.3.2) Fichier /var/named/db.work.exam.men

$ORIGIN work.exam.men.

$TTL 2D

work.exam.men. IN SOA ns2.work.exam.men. root.work.exam.men. (

2012110700 ; Serial

28800 ; Refresh

14400 ; Retry

3600000 ; Expire

7200 ) ; Minimum

IN NS ns2.work.exam.men.

ws IN A 10.0.2.2

ns2 IN A 10.0.4.2

PC\_WS IN CNAME ws

SRV\_DNS2 IN CNAME ns2

### 8.3.3) Fichier /var/named/db.work.exam.men.rev

$ORIGIN 0.10.in-addr.arpa.

$TTL 2D

0.10.in-addr.arpa. IN SOA ns2.work.exam.men. root.work.exam.men. (

2012110700 ; Serial

28800 ; Refresh

14400 ; Retry

3600000 ; Expire

7200 ) ; Minimum

IN NS ns2.work.exam.men.

2.2 IN PTR ws.work.exam.men.

2.4 IN PTR ns2.work.exam.men.

## 8.4) Sur le serveur DNS3

### 8.4.1) Fichier /etc/named.conf

options {

listen-on port 53 { 127.0.0.1; 10.0.3.4;};

directory "/var/named";

};

zone "." IN {

type hint;

file "named.ca";

};

zone "localhost" IN {

type master;

file "named.localhost";

allow-update { none; };

};

zone "1.0.0.127.in-addr.arpa" IN {

type master;

file "named.loopback";

allow-update { none; };

};

zone "exam.men" IN {

type slave;

masters {10.0.3.2;};

file "slaves/db.exam.men";

};

zone "0.10.in-addr.arpa" IN {

type slave;

masters {10.0.3.2;};

file "slaves/db.exam.men.rev";

### 8.4.2) Fichier /var/named/slaves/db.exam.men

$ORIGIN .

$TTL 172800 ; 2 days

exam.men IN SOA ns1.exam.men. root.exam.men. (

2012110702 ; serial

28800 ; refresh (8 hours)

14400 ; retry (4 hours)

3600000 ; expire (5 weeks 6 days 16 hours)

7200 ; minimum (2 hours) )

NS ns1.exam.men.

NS ns3.exam.men.

$ORIGIN exam.men.

dhcp A 10.0.3.3

louis A 10.0.1.5

ns1 A 10.0.3.2

ns3 A 10.0.3.4

SRV\_DHCP CNAME dhcp

SRV\_DNS1 CNAME ns1

SRV\_DNS3 CNAME ns3

SRV\_WEB CNAME www

vh1 A 10.0.1.2

vh2 A 10.0.1.3

vh3 A 10.0.1.3

work NS ns2.work

$ORIGIN work.exam.men.

ns2 A 10.0.4.2

$ORIGIN exam.men.

www A 10.0.1.2

$ORIGIN www.exam.men.

jean A 10.0.1.4

### 8.4.3) Fichier /var/named/slaves/db.exam.men.rev

$ORIGIN .

$TTL 172800 ; 2 days

0.10.in-addr.arpa IN SOA ns1.exam.men. root.exam.men. (

2012110702 ; serial

28800 ; refresh (8 hours)

14400 ; retry (4 hours)

3600000 ; expire (5 weeks 6 days 16 hours)

7200 ; minimum (2 hours)

)

NS ns1.exam.men.

$ORIGIN 1.0.10.in-addr.arpa.

2 PTR www.exam.men.

PTR vh1.exam.men.

3 PTR vh2.exam.men.

PTR vh3.exam.men.

4 PTR jean.www.exam.men.

5 PTR louis.exam.men.

$ORIGIN 3.0.10.in-addr.arpa.

2 PTR ns1.exam.men.

3 PTR dhcp.exam.men.

4 NS ns3.exam.men.

$ORIGIN 0.10.in-addr.arpa.

2.4 NS ns2.work.exam.men.

## 8.5) Sur le serveur WEB

### 8.5.1) Fichier /etc/http/httpd.conf

ServerRoot "/etc/httpd"

Listen 80

Include conf.modules.d/\*.conf

User apache

Group apache

ServerAdmin root@localhost

…

### 8.5.2) Fichier /etc/httpd/conf.d/00-main.conf

Alias /pamauthor "/usr/share/doc/pam/html/sag-author.html"

<Directory "/usr/share/doc/pam/html">

Require all granted

</Directory>

<Directory /var/www/html/intranet>

<RequireAny>

Require ip 10.0.1.0/24

</RequireAny>

</Directory>

<Directory /var/www/html/intranetWS>

<RequireAny>

Require ip 10.0.2.0/24

</RequireAny>

</Directory>

### 8.5.3) Fichier /etc/httpd/conf.d/00-server.conf

ServerName www.exam.men

ServerAdmin moi@exam.men

ErrorDocument 404 /erreur/erreur\_404.html

<IfModule prefork.c>

MinSpareServers 3

MaxSpareServers 1O

StartServers 7

MaxRequestWorkers 20

ServerLimit 20

</IfModule>

<IfModule dir\_module>

DirectoryIndex index.html accueil.html

</IfModule>

#PAR IP

<VirtualHost 10.0.1.4>

ServerName jean.www.exam.men

DocumentRoot /var/www/vh/jean

</VirtualHost>

<VirtualHost 10.0.1.5>

ServerName louis.exam.men

DocumentRoot /var/www/vh/louis

</VirtualHost>

#PAR NOMS

<VirtualHost 10.0.1.2>

ServerName www.exam.men

DocumentRoot /var/www/html

</VirtualHost>

<VirtualHost 10.0.1.2>

ServerName vh1.exam.men

DocumentRoot /var/www/vh/vh1

</VirtualHost>

<VirtualHost 10.0.1.3>

ServerName vh2.exam.men

DocumentRoot /var/www/vh/vh2

<Directory /var/www/vh/vh2>

AuthName "Acces au site vh2"

AuthType Basic

AuthUserFile /var/www/securite/pwd

Require valid-user

</Directory>

</VirtualHost>

<VirtualHost 10.0.1.3>

ServerName vh3.exam.men

DocumentRoot /var/www/vh/vh3

</VirtualHost>

### 8.5.4) Fichier /etc/httpd/conf.d/0-userdir.conf

<IfModule mod\_userdir.c>

UserDir disabled bernard

UserDir public\_html

</IfModule>

<Directory "/home/\*/public\_html">

AllowOverride FileInfo AuthConfig Limit Indexes

Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec

Require method GET POST OPTIONS

</Directory>

### 8.5.5) Arborescence /var/www

/var/www/

├── cgi-bin

├── html

│   ├── cours

│   │   ├── f1.txt

│   │   ├── f2.3.2.tar.gz

│   │   ├── f2.3.3.tar.gz

│   │   └── f3.jpg

│   ├── erreur

│   │   └── erreur\_404.html

│   ├── index.html

│   ├── intranet

│   │   └── index.html

│   └── intranetWS

│   └── index.html

├── securite

│   └── pwd

└── vh

├── jean

│   └── index.html

├── louis

│   └── index.html

├── vh1

│   └── index.html

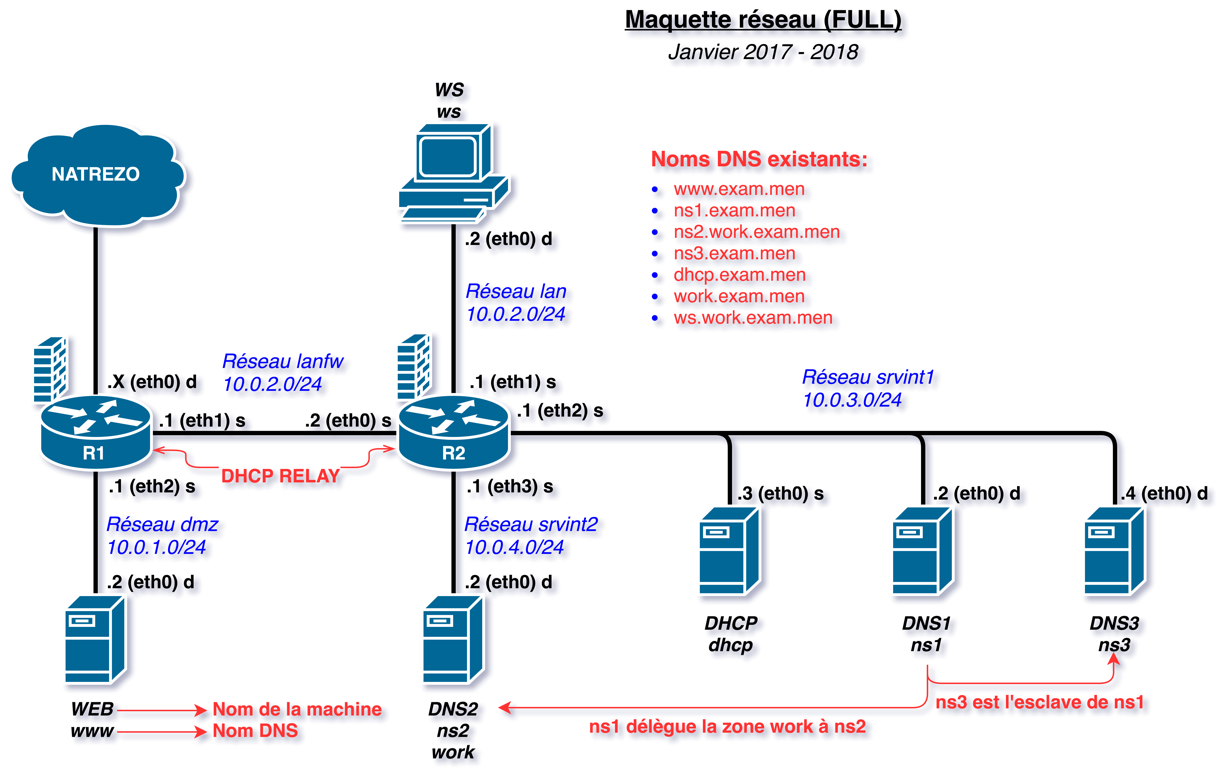
├── vh2

│   └── index.html

└── vh3

└── index.html

# Maquette finale



# SECURITE

# Modification désirée : rendre le VH vh3 sécurisé (https)

On souhaite modifier le serveur web pour que lors d’une requête sur vh3.exam.men, la requête soit sécurisée (https). Pour ce faire nous devrons :

🡪 Installer openssl

🡪 Créer une clé, un CSR et un certificat auto-signé

🡪 Déplacer la clé et les certificats

🡪 Modifier le VH dans /etc/httpd/con.f/00-server.conf pour être redirigé en https

🡪 Créer le VH dans /etc/httpd/conf.d/ssl.conf

🡪 Relancer le serveur apache

🡪 Tester

## 11.1) Tache à faire

### 11.1.1) Sur le serveur apache

La première chose à faire, est d’installer openssl :

#yum install openssl mod\_ssl –y

Ensuite, il faut créer la clé et les certificats

Création de la clé privée du serveur

#cd /tmp

#openssl genrsa –out vh3.exam.men.key 2048

Création du CSR

#openssl req –new –key vh3.exam.men.key –out vh3.exam.men.csr

Remplir les champs d’information…

Création du certificat auto-signé

#openssl x509 –in vh3.exam.men.csr –out vh3.exam.men.crt –req

–signkey vh3.exam.men.key –days 3650

Copier la clé et certificats au bon endroit

#cp vh3.exam.men.crt /etc/pki/tls/certs

#cp vh3.exam.men.csr /etc/pki/tls/private

#cp vh3.exam.men.key /etc/pki/tls/private

Suppression des clés et certificats

#rm –f /tmp/vh3.exam.men.\*

Ajout du VH dans /etc/httpd/conf.d/ssl.conf

#vi /etc/httpd/conf.d/ssl.conf

…

<VirtualHost 10.0.1.3 :443>

ServerName vh3.exam.men

DocumentRoot /var/www/vh/vh3

SSLEngine on

SSLCertificateFile /etc/pki/tls/certs/vh3.exam.men.crt

SSLCertificateKeyFile /etc/pki/tls/private/vh3.exam.men.key

</VirtualHost>

Après cela, nous allons modifier le VH dans /etc/httpd/conf.d/00-server.conf afin qu’il redirige vers le site vh3 https :

#vi /etc/httpd/conf.d/00-server.conf

…

<VirtualHost 10.0.1.3>

ServerName vh3.exam.men

DocumentRoot /var/www/vh/vh3

Redirect permanent "/" "https://vh3.exam.men"

</VirtualHost>

Maintenant il faut créer le VH vh3 securisé dans /etc/httpd/conf.d/ssl.conf :

#vi /etc/httpd/conf.d/ssl.conf

…

<VirtualHost 10.0.1.3:443>

ServerName vh3.exam.men

DocumentRoot /var/www/vh/vh3

SSLEngine on

SSLCertificateFile /etc/pki/tls/certs/vh3.exam.men.crt

SSLCertificateKeyFile /etc/pki/tls/private/vh3.exam.men.key

</VirtualHost>

Pour finir il faut relancer le serveur apache :

#service httpd restart

Maintenant lorsque l’on fait un #lynx vh3.exam.men, l’utilisateur est averti qu’il doit signer un certificat pour accéder au site.

# Modification désirée : faire un script pour push key et créer un nouvel utilisateur sur DNS3

On souhaite faire un scipt pour envoyer la clé publique de root de DNS3 à toutes les machines des différents réseaux et par la suite un script qui ajoute un nouveau user dans ces machines. Il faudra donc :

🡪 Activer les clauses RSAAuthentification et PubkeyAuthentification dans /etc/sshd/sshd\_config

🡪 Relancer les serveurs sshd sur toutes les machines

🡪 Générer la clé privée de root sur DNS3

🡪 Créer un dossier /root/admin, un dossier /root/admin/log, un dossier /root/admin/sh

🡪 Créer un fichier ip.txt dans /root/admin pour renseigner les ip à contacter.

🡪 Ecrire le script fessant un push de la clé

🡪 Ecrire le script fessant le adduser sur toutes les machines

🡪 Rendre les scripts exécutables

🡪 Lancer les scripts

## 12.1) Taches à réaliser

### 12.1.1) Sur toutes les machines

#vi /etc/ssh/sshd\_config

…

RSAAuthentication yes

PubkeyAuthentication yes

…

#service sshd restart

### 12.1.2) Sur le serveur DNS3

Créer la clé publique de root

#cd /root

#ssh-keygen –t rsa

Créer les dossiers

#mkdir /root/admin

#mkdir /root/admin/sh

#mkdir /root/admin/log

Créer le fichier ip.txt contenant les adresses IP à contacter

#vi /root/admin/ip.txt

10.0.1.2

10.0.2.2

10.0.3.2

10.0.3.3

10.0.4.2

Ecrire le script copiant la clé de root du serveur DNS3 vers les autres machines

#vi /root/admin/sh/pushkey.sh

#!/bin/bash

PUBKEYDIR="/root/.ssh"

SHDIR="/root/admin/sh"

LOGDIR="/root/admin/log"

IPFILE="/root/admin/ip.txt"

NAMELOG=`basename $0`

cd $SHDIR

date > $LOGDIR/$NAMELOG.log

date > $LOGDIR/$NAMELOG.errors.log

for IP in `cat $IPFILE`

do

if ping -c 2 $IP > /dev/null 2>&1

then

ssh-copy-id -i $PUBKEYDIR/id\_rsa.pub root@$IP

echo "Copie vers $IP...OK" >> $LOGDIR/$NAMELOG.log

else

echo "$0: $IP ne repond pas" >> $LOGDIR/$NAMELOG.log

fi

done

exit 0

Ecrire le script créant sur chaque machine, un user reçu en paramètre du script

#vi /root/admin/sh/alladduser.sh

#!/bin/bash

PUBKEYDIR="/root/.ssh"

SHDIR="/root/admin/sh"

LOGDIR="/root/admin/log"

IPFILE="/root/admin/ip.txt"

NAMELOG=`basename $0`

if [ $# -eq 1 ]

then

echo $LOGDIR/$NAMELOG

cd $SHDIR

date > $LOGDIR/$NAMELOG.log

date > $LOGDIR/$NAMELOG.errors.log

for IP in `cat $IPFILE`

do

if ping -c 2 $IP > /dev/null 2>&1

then

ssh root@$IP "adduser $1 > /dev/null 2>&1"

ssh root@$IP "echo $1 | passwd --stdin $1 > /dev/null 2>&1"

echo "Ajout de l'utilisateur $1 sur $IP... OK" >> $LOGDIR/$NAMELOG.log

else

echo "$0: $IP ne repond pas" >> $LOGDIR/$NAMELOG.log

fi

done

else

echo "Erreur: Un et un seul argument"

exit 1

fi

exit 0

Il faut maintenant rendre les scripts exécutables

#chmod +x /root/admin/sh/pushkey.sh

#chmod +x /root/admin/sh/alladduser.sh

On peut maintenant exécuter les scripts un à un

#bash /root/admin/sh/pushkey.sh

…

#bash /root/admin/sh/alladduser.sh valentin

# Modification désirée : FW sur le routeur R2

#!/bin/bash

#Demarrage automatique du firewall

# chkconfig 3 98 99

# --> a condition d'avoir ajouter le lien du demon dans le runlevel de demarrage

# --> chkconfig --add fwfull

#

# OU

# Ajouter "/etc/init.d/fwfull start" dans /etc/rc.local

# pour demarrer le firewall automatiquement au lancement de la machine

#

# DEBUG: iptables -L

# iptables -L -v

# itpables -S

#

########################################

### VARIABLES ###

########################################

lanws=10.0.2.0/24

lanfw=10.0.5.0/24

dmz=10.0.1.0/24

srvint1=10.0.3.0/24

srvint2=10.0.4.0/24

WEB=10.0.1.2

DNS1=10.0.3.2

DNS2=10.0.4.2

DNS3=10.0.3.4

DHCP=10.0.3.3

WS=10.0.2.2

RT1=10.0.5.1

dnsfai1=109.8.203.3

dnsfai2=62.197.111.140

dnsfai3=8.8.8.8

####################################

### NETTOYAGE DES REGLES ###

####################################

clean()

{

#On nettoye toutes les regles des tables filter et nat

iptables -F

iptables -X #Pour les regles utilisateurs

iptables -t nat -F

iptables -t nat -X #Pour les regles utilisateurs

}

###################################################################

### ARRET (TOUT OUVERT) MEME L'ACCES AU SERVICE INTERNS ###

###################################################################

stop()

{

#On nettoye les regles

clean

#On ouvre tout

for chaine in INPUT OUTPUT FORWARD

do

iptables -P $chaine ACCEPT

done

for chaine in PREROUTING POSTROUTING OUTPUT

do

iptables -t nat -P $chaine ACCEPT

done

echo "[Done.]"

}

start()

{

#On nettoye les regles

clean

#On ferme tout

for chaine in INPUT OUTPUT FORWARD

do

iptables -P $chaine DROP

done

#Les services locaux doivent pouvoir communiquer entre eux

iptables -A INPUT -i lo -j ACCEPT

iptables -A OUTPUT -o lo -j ACCEPT

#on ouvre pour le protocole ICMP sinon lors du demande DHCP

# Le ping request ne pourra pas marcher

# iptables -A OUTPUT -p icmp -m conntrack --ctstate NEW,ESTABLISHED,RELATED -j ACCEPT

# iptables -A INPUT -p icmp -j ACCEPT

#On ouvre la translation d'adresse (on aurait pu travailler avec MASQUERADE

#(Sinon il n'y aurait pas de nating et l'acces à l'extérieur de l'intérieur

#serait tout simplement impossible

#iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 10.103.0.X

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

#Ouvre l'attribution DHCP vers lan srvint2 lanfw et dmz

#Ouvre l'attribution DHCP vers lan srvint2 lanfw OK

for lan in $lanws

do

iptables -A FORWARD -p udp --sport 67 --dport 68 -s $lan -d $DHCP -j ACCEPT

iptables -A FORWARD -p udp --sport 68 --dport 67 -s $DHCP -d $lan -j ACCEPT

iptables -A INPUT -p icmp --icmp-type 8 -s $lan -d 1.0.2.1 -j ACCEPT

iptables -A OUTPUT -p icmp --icmp-type 0 -s 10.0.2.1 -d $lan -j ACCEPT

done

#Resolution dns vers DNS1 pour tout les hosts dans le reseau lanws et srvint2 OK

for lan in $lanws $srvint2 $dmz

do

iptables -A FORWARD -p udp --dport 53 -s $lan -d $DNS1 -j ACCEPT

iptables -A FORWARD -p udp --sport 53 -s $DNS1 -d $lan -j ACCEPT

done

#Resolution dns vers DNS3 pour tout les hosts dans le reseau lanws et srvint2 OK

for lan in $lanws $srvint2 $dmz

do

iptables -A FORWARD -p udp --dport 53 -s $lan -d $DNS3 -j ACCEPT

iptables -A FORWARD -p udp --sport 53 -s $DNS3 -d $lan -j ACCEPT

done

#

# for dnsint in $DNS1 $DNS3

# do

for dnsfai in $dnsfai1 $dnsfai2 $dnsfai3

do

iptables -A FORWARD -i eth2 -o eth0 -p udp --dport 53 -s $DNS1 -d $dnsfai -j ACCEPT

iptables -A FORWARD -i eth0 -o eth2 -p udp --dport 53 -s $dnsfai -d $DNS1 -j ACCEPT

done

# done

#Autoriser l'acces http du serveur WEB uniquement à partir du lanfw OK

iptables -A FORWARD -i eth1 -o eth0 -p tcp --dport 80 --sport 1024: -s $lanws -d $WEB -j ACCEPT

iptables -A FORWARD -i eth0 -o eth1 -p tcp --dport 1024: --sport 80 -s $WEB -d $lanws -j ACCEPT

#Autoriser l'acces https du serveur WEB uniquement à partir du lan srvint2

iptables -A FORWARD -i eth3 -o eth0 -p tcp --dport 443 -s $srvint2 -d $WEB -j ACCEPT

iptables -A FORWARD -i eth0 -o eth3 -p tcp --dport 443 -s $WEB -d $srvint2 -j ACCEPT

#Autoriser l'acces ssh sur RT2 des hosts sur lanws OK

iptables -A INPUT -i eth1 -s $lanws -p tcp --dport 22 -j ACCEPT

iptables -A OUTPUT -o eth1 -d $lanws -p tcp --sport 22 -j ACCEPT

echo "[Done.]"

}

#########################################################

### GESTION DU PASSAGE DE PARAMETRE AU SCRIPT ###

#########################################################

case "$1" in

start) echo "FIREWALL is starting ..."

start;;

stop) echo "FIREWALL is stopping ..."

stop;;

restart) echo "FIREWALL is stopping ..."

stop

echo "FIREWALL is starting ..."

start;;

status) iptables -L

iptables -t nat -L;;

\*) echo "Usage: $0 {start|stop|restart|status}";;

esac