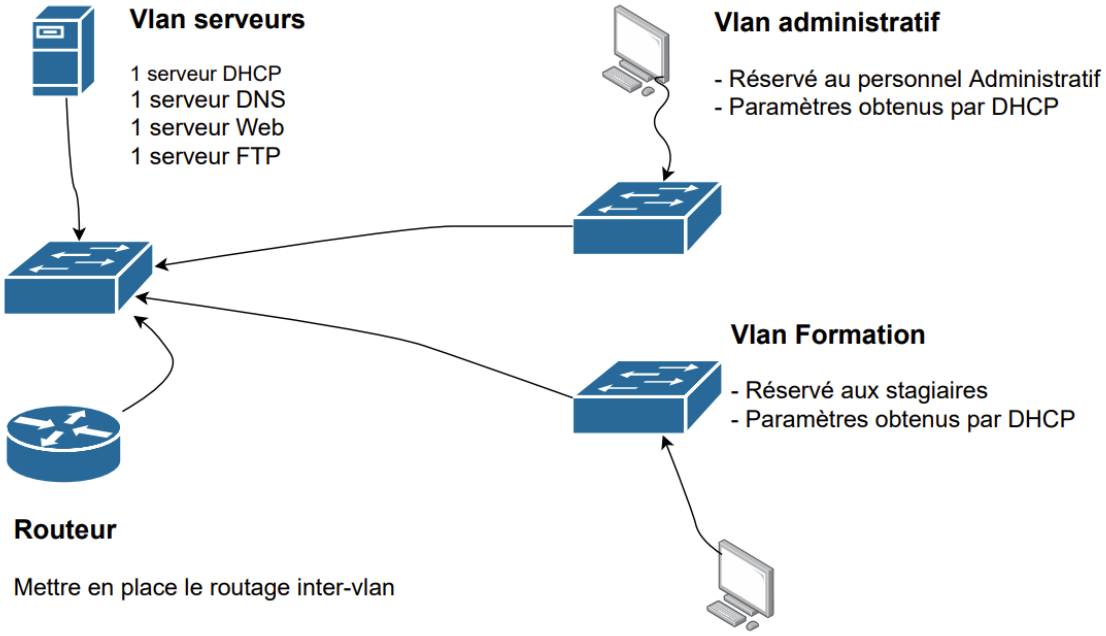
Restructuration d'un réseau

Ershad RAMEZANI

Table des matières

Restructuration d'un réseau

Segmentation par Vlans – déploiement de services



Travail demandé

Situation initiale

- Pour l'ensemble du site Adrar Pole-Numérique, il est prévu un unique réseau global avec l'adresse IP 192.168.100.0/24.
- Le site comprendra 10 salles de formation, chacune équipée pour accueillir 20 ordinateurs. En plus de ces salles, un réseau distinct sera mis en place pour le personnel administratif.

Situation finale souhaitée

Il est nécessaire de créer une structure qui permet de séparer les flux de données entre les diverses salles. Voici les directives pour cette organisation :

- Le sous-réseau 1 sera dédié au personnel administratif, aux postes utilisateurs, aux imprimantes et aux points d'accès Wifi.
- Le sous-réseau 2 sera réservé aux serveurs.
- Les sous-réseaux suivants seront affectés aux salles de formation. Pour représenter le fonctionnement de ces salles, le troisième sous-réseau sera nommé "sous-réseau Formation".

Services accessibles

Les services qui seront accessibles sont les suivants :

- Un serveur Windows, accessible uniquement depuis le sous-réseau administratif.
- Un serveur Web hébergeant deux sites web, www.adrar.lan et www.adrar-form.lan, accessibles à TOUS.
- Un serveur FTP accessible uniquement depuis le poste de l'administrateur du pôle numérique, situé dans le sous-réseau administratif.

- Les salles de formation ne peuvent pas accéder au sous-réseau du personnel administratif. Cependant, l'administrateur du service administratif peut accéder aux postes et équipements des salles.

La mise en place

Pour réaliser ce projet, j'ai utilisé un switch Cisco de niveau 2, un routeur Cisco 1921 et un serveur tour Dell équipé de Windows Server 2012 R2. Toutes les machines sont des machines virtuelles hébergées sur l'hyperviseur Hyper-V. Le cahier des charges initial prévoyait la mise en place de ce projet pour 10 salles de cours, mais j'ai décidé de n'en installer qu'une seule pour la démonstration. Le réseau de cette salle de cours, où le projet a été mis en place, est considéré comme un réseau public, avec une adresse IP publique de 192.168.90.125 et une adresse de passerelle de 192.168.90.254 fournie par mon FAI pour configurer le routage.

Ce projet consiste en une maquette simple visant à illustrer la mise en place de serveurs Linux tels que DHCP, DNS, WEB et FTP, ainsi que la configuration de VLANs, de ports Trunk/Access et de la communication inter-VLAN à l'aide de la technique ROAS. Le réseau est également sécurisé à l'aide de différentes listes ACLs. De plus, la configuration NAT permet au réseau interne d'accéder à Internet et au serveur web d'être accessible depuis Internet.

Pour aller plus loin :

Les configurations suivantes n'ont pas été demandées dans le projet initial et visent à étendre les fonctionnalités du réseau :

1. Deux serveurs Linux distincts seront déployés : l'un pour le DHCP et le DNS, et l'autre pour le Web et le FTP.
2. Le serveur DNS interne sera capable de résoudre les requêtes DNS pour l'accès à Internet.
3. Le serveur FTP sera configuré en mode passif.
4. Une machine physique sera utilisée, et un câble réseau trunk sera établi entre l'hôte et le switch L2.
5. La configuration de NAT surchargé sera mise en place pour permettre l'accès à Internet depuis le réseau interne.
6. Une configuration de NAT statique sera établie pour rendre le site Web interne accessible depuis le réseau externe.
7. Des listes de contrôle d'accès (ACLs) seront mises en place sur l'interface du routeur pour sécuriser le réseau interne contre le réseau externe.
8. Les règles ACLs seront les suivantes :
    a. Le réseau de serveurs sera autorisé à effectuer des pings sur tout le monde, y compris Internet.
    b. Tout le monde aura accès à Internet.
    c. L'administrateur pourra effectuer des pings sur le réseau de formation (ce qui implique que tous les protocoles ne seront pas autorisés).
    d. La passerelle de la salle de formation effectuera la résolution de noms secondaires.

Schéma Réseau :

Schéma Réseau ADRAR

avec une salle de formation pour la démonstration

Router

ROAS sur Interface Gigabit 0/0:
Sub-int 0/0.10 : .101.142 ACL 110 OUT
Sub-int 0/0.20 : .100.62 ACL 120 OUT
Sub-int 0/0.30 : .100.94 ACL 130 OUT
ip-helper on each Sub-int: 192.168.101.129
Interface Gigabit 0/1
IP: 192.168.90.125 – ACL 101 IN, 102 OUT
NAT overload for 192.168.0.0/16
NAT Static P.443 for server web interne
Route par défaut vers FAI (192.168.90.254)
Configuration SSH OK

Internet

Router Cisco 1900 Series

Switch Cisco 3750 Series

Switch

Int FastEth. 1/0/1: Taggé Vlan 10,20,30
Int FastEth. 1/0/2: Taggé Vlan 10,20,30
Int vlan 20 : 192.168.100.60 pour SSH
Configuration SSH OK

VLAN 10 Servers

WEB_FTP
192.168.101.130

DHCP_DNS
192.168.101.129

VLAN 20 Administration

Admin
192.168.100.1

PC-administration
DHCP

VLAN 30 Formation (Salle 1)

Stagiaire 1
DHCP

Stagiaire 2
DHCP

Servers

WEB_FTP : Debian 10
Apache2 et Proftpd
DHCP_DNS : Debian 10
Isc-dhcp-server et Bind9
IDSR: 192.168.101.128/28
MSR: 255.255.255.240
Passerelle : 192.168.101.142
DNS: 192.168.101.129

Administration

Admin : Win 10
Win SCP, MobaXterm, Firefox
PC-administration: Win 10
Firefox
IDSR: 192.168.100.0/26
MSR: 255.255.255.192
Passerelle : 192.168.100.62
DNS: 192.168.101.129

Formation (Salle 1)

PC-stagiaire : Win 10, Firefox
IDSR: 192.168.100.64/27
MSR: 255.255.255.224
Passerelle : 192.168.100.94
DNS: 192.168.101.129

Rôles et fonctionnalités

Serveur	machine	IP	OS	Rôles
HOST1	Physique	-	Windows Server 2012	Hyperviseur Hyper V
DHCP_DNS	VM	192.168.101.129	Debian 10	DHCP, BIND9
WEB_FTP	VM	192.168.101.130	Debian 10	Apache2, proftpd
PC-administration	VM	DHCP	Windows 10	Utilisateur
Admin	VM	192.168.100.1	Windows 10	Admin du réseau
PC-stagiaire	VM	DHCP	Windows 10	Utilisateur

Segmentation et VLANs

Adresse IP principale du réseau :

IDR	CIDR	MSR
192.168.100.0	/24	255.255.255.0

Calcul par nombre d'hôte :

Réseau	N° poste fixe	N° portable (wifi)	N° périphérique	IDSR/BRD/ PASS/SSH	IP Réservé	Totale IP	Calcul pas
Serveurs	2	-	-	3	5	10	2^4=16
Administration	20	20	1	4	5	50	2^6=64
Formation par salle (10 salles)	20	-	-	3	5	28	2^5=32

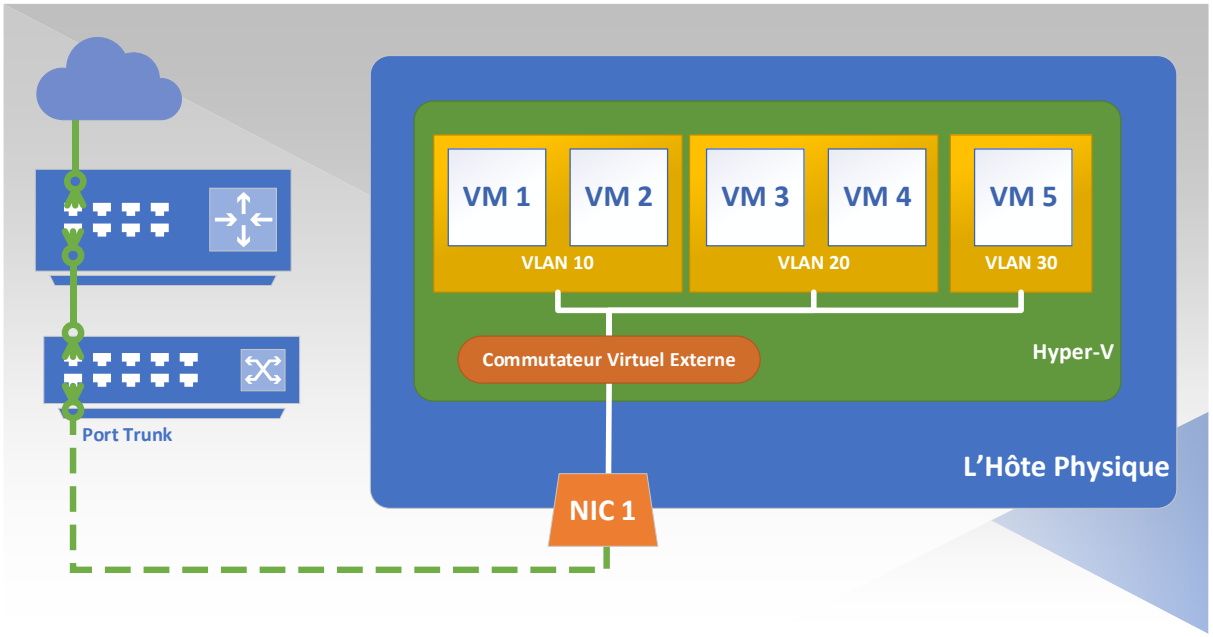
Les sous-réseaux et VLANs :

VLAN ID	VLAN NOM	IDSR	CIDR	MSR	Premier addr	Passerelle
20	**Admin**	**192.168.100.0**	**26**	**255.255.255.192**	**192.168.100.1**	**192.168.100.62**
30	**Formation**	**192.168.100.64**	**27**	**255.255.255.224**	**192.168.100.65**	**192.168.100.94**
-	Salle 2	192.168.100.96	27	255.255.255.224	192.168.100.97	192.168.100.126
-	Salle 3	192.168.100.128	27	255.255.255.224	192.168.100.129	192.168.100.158
-	Salle 4	192.168.100.160	27	255.255.255.224	192.168.100.161	192.168.100.190
-	Salle 5	192.168.100.192	27	255.255.255.224	192.168.100.193	192.168.100.222
-	Salle 6	192.168.100.224	27	255.255.255.224	192.168.100.225	192.168.100.254
-	Salle 7	192.168.101.0	27	255.255.255.224	192.168.101.1	192.168.101.30
-	Salle 8	192.168.101.32	27	255.255.255.224	192.168.101.33	192.168.101.62
-	Salle 9	192.168.101.64	27	255.255.255.224	192.168.101.65	192.168.101.94
-	Salle 10	192.168.101.96	27	255.255.255.224	192.168.101.97	192.168.101.126
10	**Serveurs**	**192.168.101.128**	**28**	**255.255.255.240**	**192.168.101.129**	**192.168.101.142**

Commutateurs Réseaux Virtuel :

En ce qui concerne le commutateur réseau virtuel, étant donné que je disposais d'une seule carte réseau, j'ai créé un commutateur virtuel externe pour toutes mes machines virtuelles, mais j'ai défini des VLANs différents dans les paramètres de chacune de mes machines individuellement.

Pour le côté switch, j'ai configuré une interface en mode trunk pour connecter mes machines virtuelles au réseau. (Cependant, dans la théorie de ce projet, on considère qu'il y a une carte réseau par machine virtuelle, et donc chacune est connectée à une interface non marquée du switch.)



NOM	TYPE	VLAN	NIC
Externe	Externe	10	Realtek USB GbE
Externe	Externe	20	Realtek USB GbE
Externe	Externe	30	Realtek USB GbE

Configuration de Switch

Les interfaces :

Interface	Trunk (Tagged)	Access (Untagged)	Encapsulation	VLANs
FastEth. 1/0/1	*		Dot1Q	10, 20, 30
FastEth. 1/0/2	*		Dot1Q	10, 20, 30

Configuration SSH :

SSH		
Username	Admin	-
Password	Admin	-
Port	22	-
Adresse IP	192.168.100.60	Interface vlan 20
Default-gateway	-	-

Configuration routeur

Les interfaces :

Interface	Adresse IP	MSR	VLAN	IP helper	Encapsulation
Fast Ethernet 0/1	192.168.90.125	255.255.255.0	-	-	-
Fast Ethernet 0/0	-	-	-	-	-

Fast Ethernet 0/0.10	192.168.101.142	255.255.255.240	10	192.168.101.129	Dot1Q
Fast Ethernet 0/0.20	192.168.100.62	255.255.255.192	20	192.168.101.129	Dot1Q
Fast Ethernet 0/0.30	192.168.100.94	255.255.255.224	30	192.168.101.129	Dot1Q

Configuration SSH :

SSH		
Username	Admin	-
Password	Admin	-
Port	22	-
Adresse IP	192.168.100.62	Interface Fast Eth. 0/0.20
Default-gateway	-	-

NAT (Surchargé et Static) :

Afin de permettre l'accès à Internet à mon réseau, j'ai configuré le NAT surchargé sur l'adresse IP publique (192.168.90.125) de l'interface Gigabit 0/1 de mon routeur. De plus, j'ai mis en place la configuration NAT statique pour le port 443, afin que mon serveur web puisse être accessible depuis l'extérieur du réseau.

NAT Surchargé
Access-list 1 permit 192.168.0.0 0.0.255.255
Ip nat inside source list 1 interface gigabit ethernet 0/1 overload

NAT Statique
Ip nat inside source static tcp 192.168.101.130 443 192.168.90.125 443

Les ACLs :

Pour sécuriser mon réseau, j'ai mis en place plusieurs ACL sur les interfaces de mon routeur. Afin d'assurer une précision maximale et de limiter le nombre de règles à ajouter pour le moment et à l'avenir, j'ai décidé de placer les ACL aussi près que possible des destinations. J'ai donc configuré trois ACL en direction OUT sur les sous-interfaces du Gigabit 0/0. De plus, pour garantir la sécurité de l'accès au serveur web depuis l'extérieur de mon réseau, j'ai configuré deux ACL en direction IN et OUT sur l'interface Gigabit 0/1.

Les principes visent à permettre à l'administrateur d'accéder à tous les services du réseau et d'Internet, y compris le web en HTTP et HTTPS, le service FTP, DHCP et DNS, ainsi que la possibilité de faire des pings et des connexions SSH sur l'ensemble du réseau.

Le sous-réseau Serveurs est capable de répondre à une variété de demandes provenant de différents utilisateurs et sources au sein du réseau interne. Il peut répondre aux demandes HTTPS, DNS et DHCP de tous les utilisateurs du réseau interne. En outre, il est en mesure de répondre aux demandes ICMP et FTP émanant de l'administrateur du réseau, ainsi qu'aux demandes HTTPS provenant d'utilisateurs externes.

Le sous-réseau Serveurs est également connecté à Internet, ce qui lui permet de télécharger des paquets et d'effectuer des tests d'exploitation. Il a la possibilité de faire le ping sur le réseau interne et externe à des fins de tests. Enfin, le serveur DNS situé dans ce sous-réseau est capable d'envoyer et de

recevoir des requêtes DNS sur le réseau externe, notamment sur le routeur de la salle de cours, qui est situé à l'adresse IP 192.168.90.254.

Le sous-réseau formation a la capacité d'accéder au serveur web interne en HTTPS ainsi qu'à Internet, et peut aussi échanger des informations avec le serveur DHCP.

ACL : 110		Interface : Gigabit 0/0.10		Direction : OUT			
ACE	**Règle**	**Protocole**	**IP Source**	**Port Sour**	**IP Destination**	**Port Dest**	**Comment**
10	permit	TCP	any		host 192.168.101.130	eq 443	Tout le monde accès web interne
20	permit	TCP	any	eq 443	192.168.101.128 0.0.0.15		Sous-réseau serveurs accès internet
30	permit	TCP	any	eq 80	192.168.101.128 0.0.0.15		Sous-réseau serveurs accès internet
40	permit	UDP	192.168.0.0 0.0.255.255		host 192.168.101.129	eq 53	Tous réseau interne accès DNS interne
50	permit	UDP	host 192.168.90.254	eq 53	host 192.168.101.129		DNS interne reçois paquets DNS externe
60	permit	ICMP	host 192.168.100.1		192.168.101.128 0.0.0.15	echo	Que admin peut faire ping sur serveurs
70	permit	ICMP	any		192.168.101.128 0.0.0.15	echo-reply	Serveurs peut pinger tout le monde
80	permit	TCP	host 192.168.100.1		192.168.101.128 0.0.0.15	eq 22	Que admin peut faire ssh sur serveurs
90	permit	TCP	host 192.168.100.1		host 192.168.101.130	eq 21	Que admin peut faire ftp (passif) - connexion
100	permit	TCP	host 192.168.100.1		host 192.168.101.130	range 49152 65534	Que admin puisse faire ftp (passif) - data

ACL : 120		interface : Gigabit 0/0.20		direction : OUT			
ACE	**règle**	**protocole**	**IP Source**	**Port Sour**	**IP Destination**	**Port Dest**	**comment**
10	permit	TCP	any	eq 443	192.168.100.0 0.0.0.63		Administratif accès internet et web interne
20	permit	TCP	any	eq 80	192.168.100.0 0.0.0.63		Administratif a accès internet
30	permit	UDP	host 192.168.101.129	eq 53	192.168.100.0 0.0.0.63		Administratif reçois depuis DNS interne
40	permit	ICMP	any		host 192.168.100.1	echo-reply	L'admin reçois réponse ping
50	permit	ICMP	192.168.101.128 0.0.0.15		192.168.100.0 0.0.0.63	echo	Serveurs peut faire ping sur administratif
60	permit	TCP	192.168.101.128 0.0.0.15	eq 22	host 192.168.100.1		Admin peut faire SSH sur serveurs
70	permit	TCP	host 192.168.101.130	eq 21	host 192.168.100.1		Admin reçois réponse ftp (passif) -connexion
80	permit	TCP	host 192.168.101.130	range 49152 65534	host 192.168.100.1		Admin reçois réponse ftp (passif) - data

ACL : 130		interface : Gigabit 0/0.30		direction : OUT			
ACE	**règle**	**protocole**	**IP Source**	**Port Sour**	**IP Destination**	**Port Dest**	**comment**
10	permit	TCP	any	eq 443	192.168.100.64 0.0.0.31		Formation a accès internet et web interne
20	permit	TCP	any	eq 80	192.168.100.64 0.0.0.31		Formation a accès internet et web interne
30	permit	UDP	host 192.168.101.129	eq 53	192.168.100.64 0.0.0.31		formation reçois paquets serveur DNS interne
40	permit	ICMP	host 192.168.100.1		192.168.100.64 0.0.0.31	echo	admin peut faire le ping sur formation
50	permit	ICMP	192.168.101.128 0.0.0.15		192.168.100.64 0.0.0.31	echo	serveurs peut faire ping sur formation

ACL : 101		interface : Gigabit 0/1		direction : IN			
ACE	**règle**	**protocole**	**IP Source**	**Port Sour**	**IP Destination**	**Port Dest**	**comment**
10	permit	TCP	any	eq 443	host 192.168.90.125		le réseau interne a accès internet
20	permit	TCP	any	eq 80	host 192.168.90.125		le réseau interne a accès internet
30	permit	TCP	any		host 192.168.90.125	eq 443	le réseau externe a accès web interne
40	permit	ICMP	any		host 192.168.90.125	echo-reply	le réseau externe répond au ping interne
50	permit	UDP	host 192.168.90.254	eq 53	host 192.168.90.125		réponse DNS peut passer vers DNS interne

ACL : 102		interface : Gigabit 0/1		direction : OUT			
ACE	**règle**	**protocole**	**IP Source**	**Port Sour**	**IP Destination**	**Port Dest**	**comment**
10	permit	ICMP	host 192.168.90.125		any	echo	admin et serveurs peuvent pinger internet
20	permit	UDP	host 192.168.90.125		host 192.168.90.254	eq 53	serveur DNS interne peut envoyer DNS req.
30	permit	TCP	host 192.168.90.125		any	443	Réseau interne a accès internet https
40	permit	TCP	host 192.168.90.125		any	80	Réseau interne a accès internet http

Serveur WEB :

Les deux sites web adrar.lan et adrar-form.lan sont hébergé sur un serveur web apache2. Ce serveur web est installé sur un machine virtuelle linux Debian 10 nommé WEB_FTP. Tous les deux sites sont configurés en https et pour cela un certificat SSL a été créé grâce au paquet openssl et en construisant d'un CA locale.

L'adresse IP de serveur WEB_FTP est 192.168.101.130 et il est accessible par SSH depuis le poste admin.

SSH (serveur WEB_FTP)			
Username	**Password**	**Port**	**Adresse IP**
ershad	Ershad	2230	192.168.101.130

Chemin d'accès au répertoire web sont les suivants :

/var/www/html/adrar/index.html

/var/www/html/adrar-form/index.html

Deux fichiers VirtualHost sont créé, un par site. Le chemin d'accès è ces fichiers est le suivant :

/etc/apache2/sites-available/adrar.conf

/etc/apache2/sites-available/adrar-form.conf

Chaque fichier VirtualHost contient les éléments suivants :

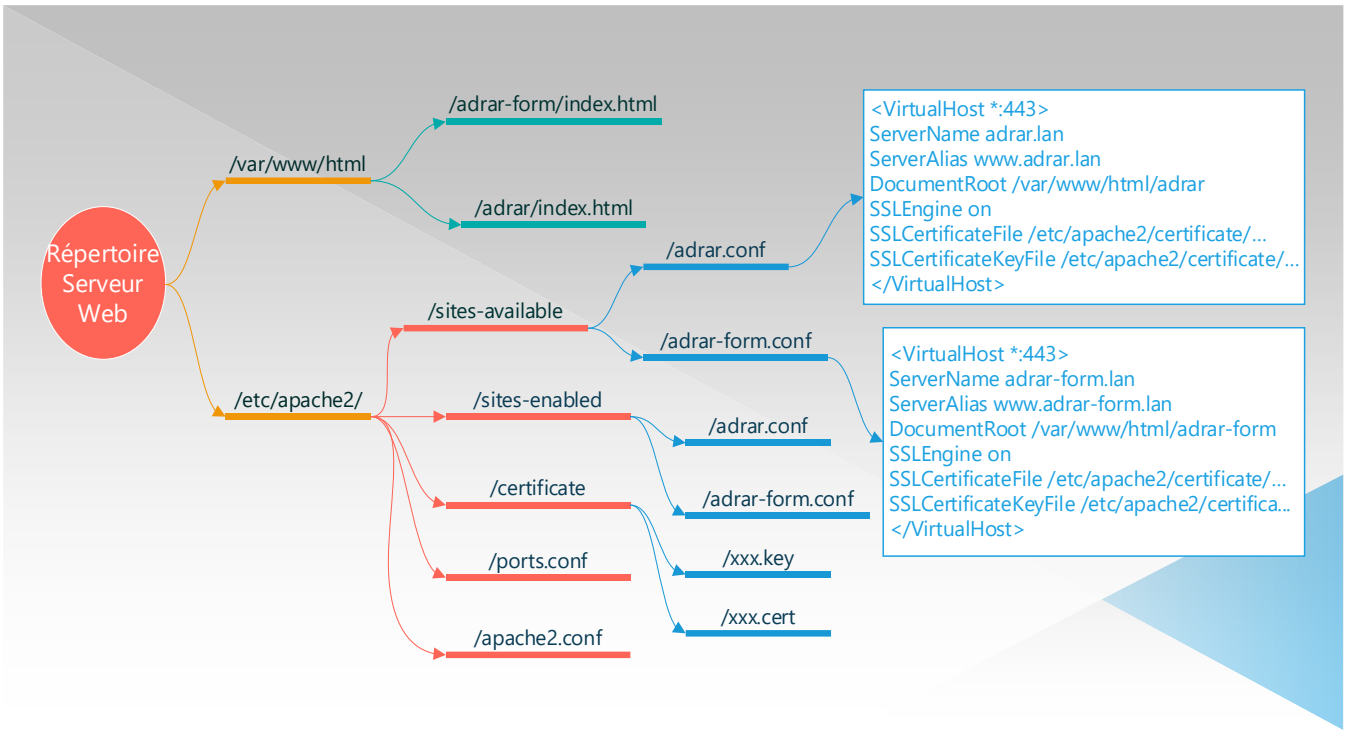
ServerName, ServerAlias, DocumentRoot, SSLCertificateFile

Le ServerAlias est defini le www. suivi par le nom du domaine de site web :

www.adrar.lan et ***www.adrar-form.lan***

Le certificat est accessible dans le répertoire suivant :

/etc/apache2/certificat



Serveur FTP :

Le serveur FTP est installé et configuré par le paquet proftpd. Il est accessible par le protocole SSH et depuis le poste admin. Selon les ACLs configuré sur le routeur c'est juste depuis le poste admin que les utilisateurs peuvent accéder au serveur FTP. En plus, l'utilisateur admin a accès au répertoire web et les autres utilisateurs ont accès que à leurs répertoires personnels. Le chemin d'accès est le suivant :

/etc/proftpd/

La configuration de serveur proftpd est le suivant :

ServerName	WEB_FTP
ServerType	standalone
Port de connexion	21
PassivePorts	49152 65534
DefaultRoot - admin	Activé (/var/www/html)
DefaultRoot – autres utilisateurs	Activé (répertoire personnel ~)
Configuration utilisateurs Anonymous	désactivé

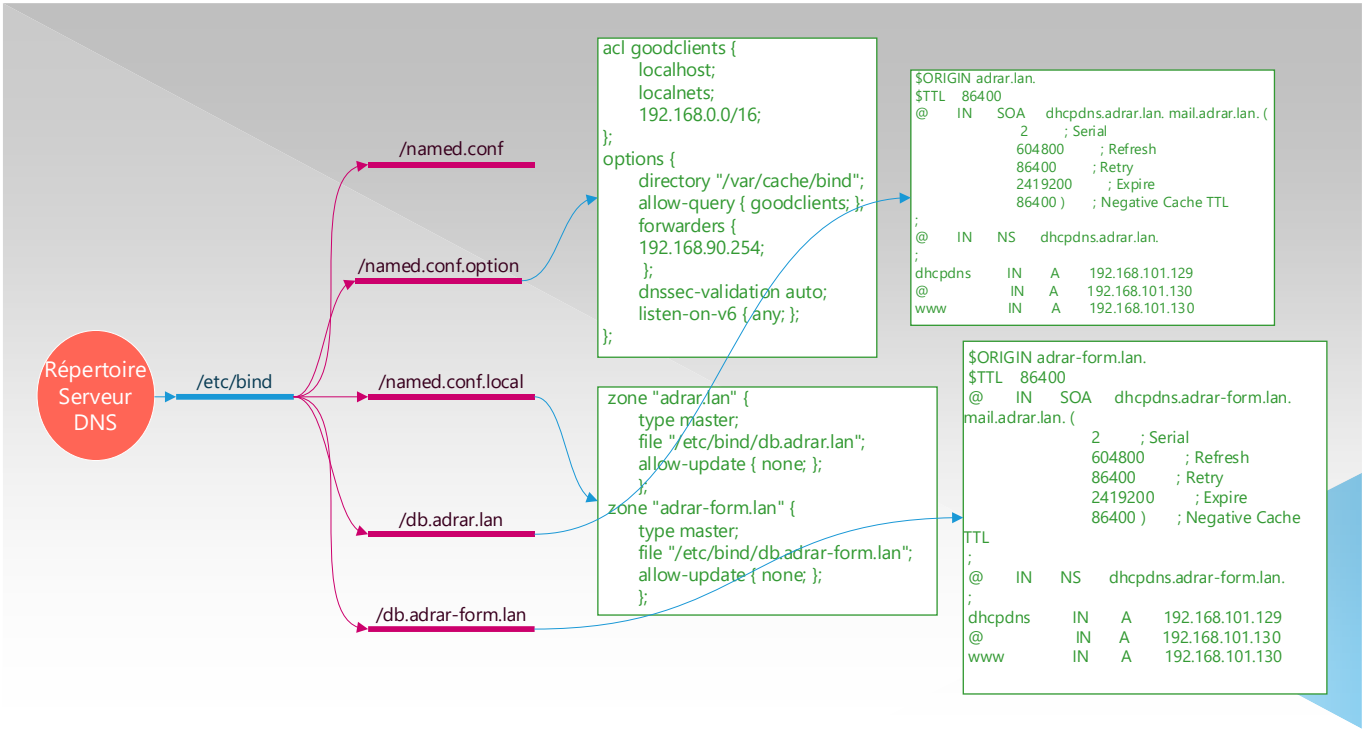
Serveur DNS :

Il y a un serveur DNS installé et configuré par le paquet BIND9. Il est accessible par le protocole SSH et depuis le poste admin. Selon les ACLs configuré sur le routeur c'est juste depuis le poste admin que les utilisateurs peuvent accéder au serveur DHCP_DNS. Il fournit la résolution de nom uniquement pour le réseau interne. S'il

n’a pas un enregistrement pour les noms de domaine demandés, il va transmettre le requête vers le serveur DNS externe (192.168.90.254) configuré dans le fichiers named.conf.options.

SSH (serveur DHCP_DNS)			
Username	**Password**	**Port**	**Adresse IP**
ershad	Ershad	2229	192.168.101.129

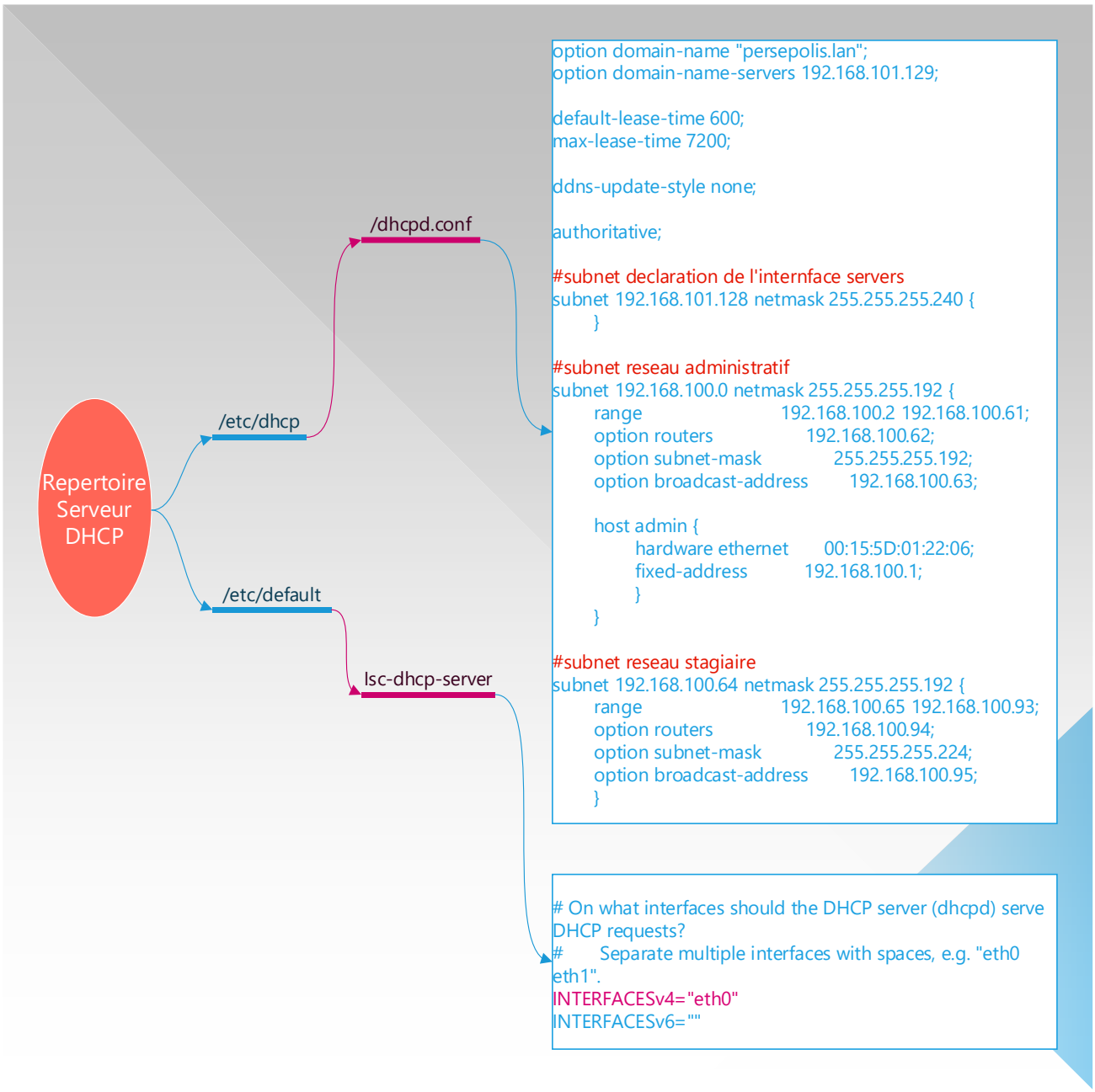
Deux zones sont créés dans le fichier named.conf.local. L’un pour le domaine adrar.lan et l’autre pour adrar-form.lan. Pareil pour les fichiers paramétrages de domaine. (db.adrar.lan et db.adrar-form.lan).



Serveur DHCP :

Le serveur DHCP est installé par le paquet isc-dhcp-server. Le serveur DHCP est accessible pour la configuration par SSH et seulement depuis le poste admin. Tous les réseaux internes ont accès au serveur DHCP. Les serveurs sont configurés en adresse IP statique. et il y a une réservation d’adresse IP pour le poste admin fait par serveur DHCP.

Configuration du serveur DHCP se fait dans le fichier dhcpd.conf (le répertoire dans le schéma au-dessous). Trois étendues sont créées pour trois réseaux. L’étendue pour le réseau serveur est obligatoire pour que le serveur connaisse son interface sur lequel il écoute.



Des axes d'amélioration :

Les autres services qui pourraient mettre en place sont l'agrégation des liens (LACP), la haute disponibilité (HSRP), DMZ avec un ou deux pares-feux, des bornes wifi, mise en pile des switches, VTP pour synchronisation des Vlans, VPN, etc. et dans le system on pourrait améliorer la sécurité du réseau grâce aux techniques comme DDNS, DNS Sec, SFTP, etc.

FIN