VALIDATION COMPETENCES

Elève : RUGGERI Anthony
Projet : **Infra-Site**
Chef de projet : Jules HATCHUEL
Date : 14/11/2019
Objectifs du projet : Mise en place de l'infrastructure pour l'entreprise GSB permettant le cloisonnement LAN/DMZ/Internet.

A1.2.4 Détermination des tests nécessaires à la validation d'un service

C1.2.4.1
Recenser les tests d'acceptation nécessaires à la validation du service et les résultats attendus

+

C1.2.4.2
Préparer les jeux d'essai et les procédures pour la réalisation des tests

1 Accès des différents services aux serveurs de la zone LAN :
- Ping des services vers le serveur AD
  - **Résultat attendu :** le ping passe

2 Les services ne doivent pas communiquer entre eux sauf les serveurs
- Ping entre postes, connectés à des ports appartenant à des VLAN de différents services
  - **Résultat attendu :** le ping ne passe pas sauf pour les serveurs entre eux

3 Le parefeu autorise les connexions entrantes vers le serveur web en DMZ
- Requête http et HTTPS via navigateur vers le serveur web applifrais.gsb.com (10.5.10.11)
  - **Résultat attendu :** la page du site s'affiche avec cadenas vert par nom ou IP
- Requêtes DNS vers 10.5.10.11 (lui-même étant web et dns)
  - **Résultat attendu :** la page du site s'affiche avec cadenas vert par son nom

4 Le parefeu autorise les connexions des services VLAN vers Internet
- DNS primaire : 10.5.10.11 secondaire : 8.8.8.8, puis ping 8.8.8.8 des postes connectés sur les VLAN
  - **Résultat attendu :** le ping passe

5 Limiter au strict nécessaire l'accès aux éléments se trouvant dans la DMZ
- Accès HTTPS (affichage de page web) / DNS (url sans IP) / (S)FTP (connexion filezilla)
  - **Résultats attendus :** Page web affichée par le nom de domaine, accès ftp fonctionnel

6 Administration de l'ensemble des éléments d'interconnexion depuis le LAN
- Accès Telnet ou SSH (invite de commande ou putty)
  - **Résultats attendus :** Connexion établie

7 Zone LAN au complet + DMZ ont accès à Internet
- Ping 8.8.8.8 + requête http google.com depuis zone LAN + DMZ
  - **Résultats attendus :** Internet OK

A1.2.5 Définition des niveaux d'habilitation associés à un service

C1.2.5.2
Recenser les ressources liées à l'utilisation du service

- Les différents services devront pouvoir accéder à l'ensemble des serveurs de la zone LAN dont l'AD
- Les services ne devront pas communiquer entre eux à l'exception des serveurs
- Le parefeu doit permettre l'entrée des connexions vers le serveur Web situé dans la DMZ
- Le parefeu doit permettre aux utilisateurs situés dans la zone LAN d'accéder à internet
- Limiter au strict nécessaire l'accès aux éléments se trouvant dans la DMZ
- L'administrateur devra pouvoir depuis le LAN administrer l'ensemble des éléments d'interconnexion
- Les différents services et serveurs côté LAN ainsi que la zone DMZ devront pouvoir accéder à internet sachant qu'il est impossible d'accéder à la configuration du routeur principal de connexion internet (routeur du BTS : 125.125.0.25)

A1.3.1 Test d'intégration et d'acceptation d'un service

C1.3.1.1
Mettre en place l'environnement de test du service

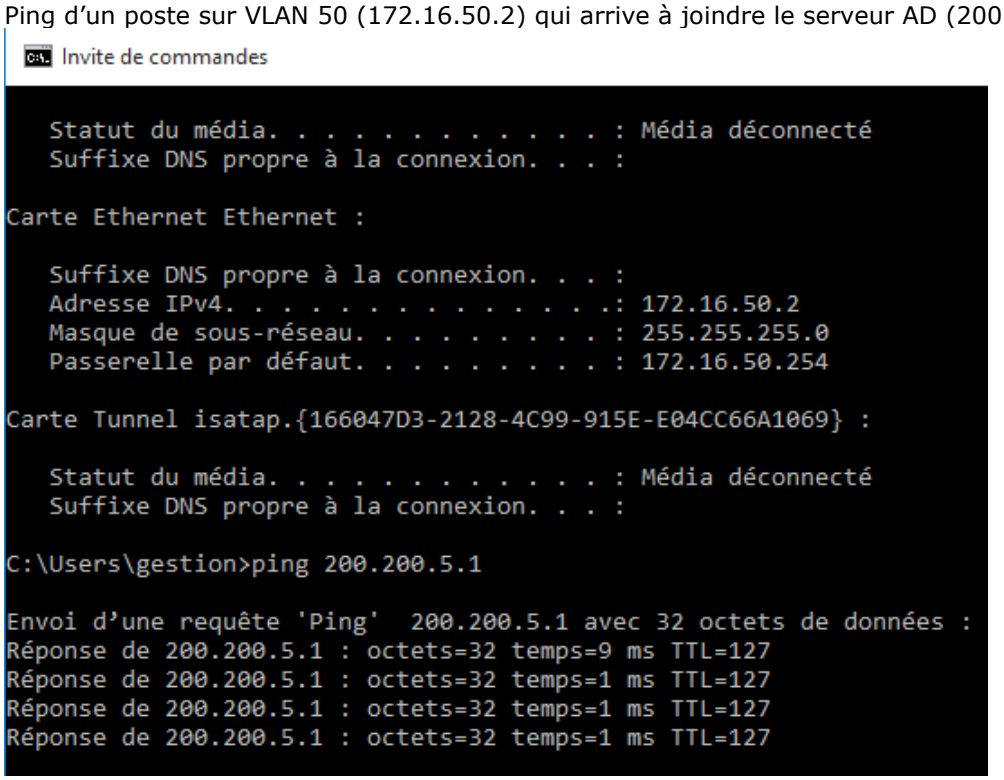
Un poste dédié aux tests + les 2 postes de travail, connexion wifi pour documentation éventuelle, connexion par câble Ethernet aux ports voulus pour les tests avec paramétrages IP correspondants

C1.3.1.2
Tester le service

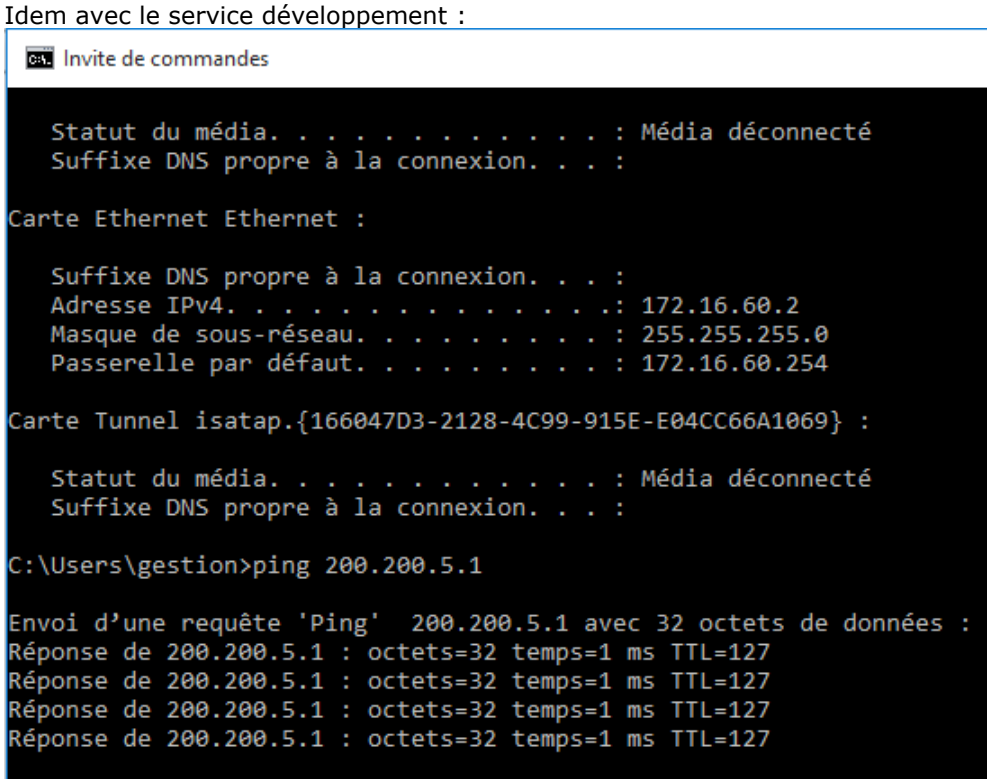
+

C1.3.1.3
Rédiger le rapport de test

Ping d'un poste sur VLAN 50 (172.16.50.2) qui arrive à joindre le serveur AD (200.200.5.1)

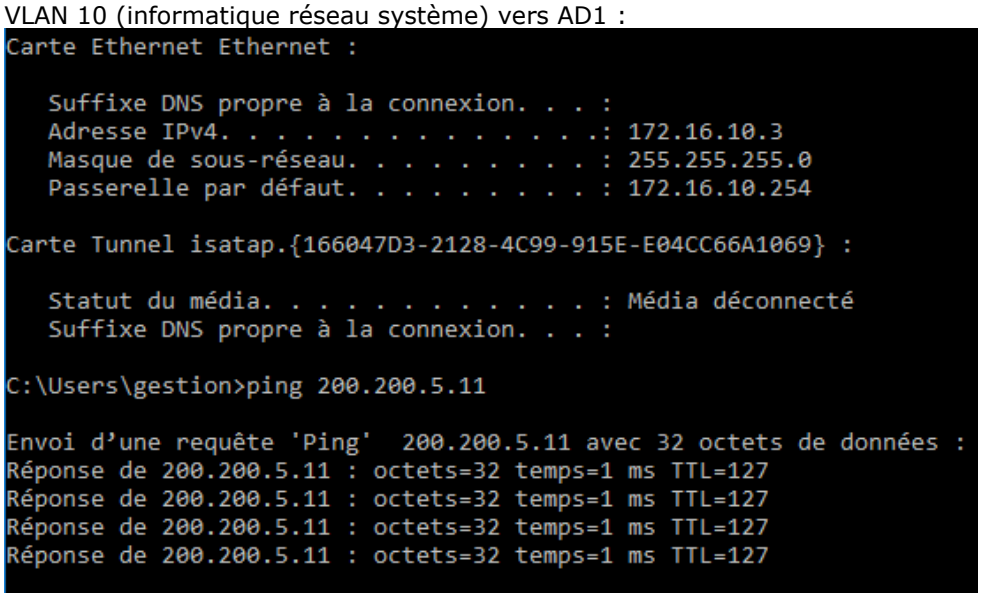


Idem avec le service développement :

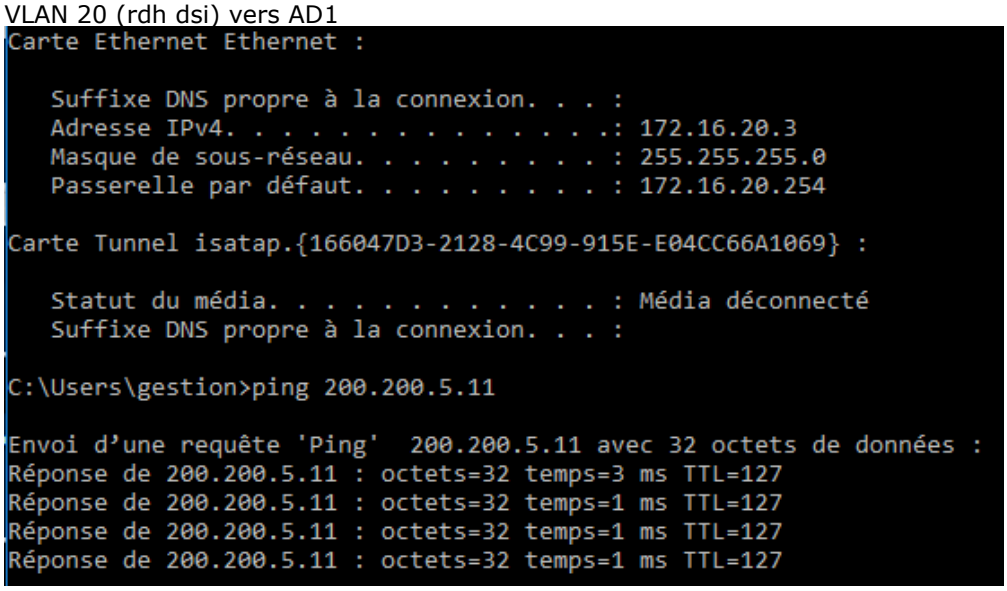


Salle de réunion vers serveur AD :

VLAN 10 (informatique réseau système) vers AD1 :



VLAN 20 (rdh dsi) vers AD1



VLAN 30 (comptabilité) vers AD1 :

```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv4. . . . . . . . . . . . . .: 172.16.30.3
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 172.16.30.254

Carte Tunnel Teredo Tunneling Pseudo-Interface :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte Tunnel isatap.{166047D3-2128-4C99-915E-E04CC66A1069} :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

C:\Users\gestion>ping 200.200.5.11

Envoi d'une requête 'Ping'  200.200.5.11 avec 32 octets de données :
Réponse de 200.200.5.11 : octets=32 temps=1 ms TTL=127
Réponse de 200.200.5.11 : octets=32 temps=1 ms TTL=127
Réponse de 200.200.5.11 : octets=32 temps=1 ms TTL=127
Réponse de 200.200.5.11 : octets=32 temps=1 ms TTL=127
```

VLAN 100 (administration) vers AD1 :

```
   Suffixe DNS propre à la connexion. . . :
   Adresse IPv4. . . . . . . . . . . . . .: 172.16.100.3
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 172.16.100.254

Carte Tunnel Teredo Tunneling Pseudo-Interface :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte Tunnel isatap.{166047D3-2128-4C99-915E-E04CC66A1069} :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

C:\Users\gestion>ping 200.200.5.11

Envoi d'une requête 'Ping'  200.200.5.11 avec 32 octets de données :
Réponse de 200.200.5.11 : octets=32 temps=1 ms TTL=127
Réponse de 200.200.5.11 : octets=32 temps=1 ms TTL=127
Réponse de 200.200.5.11 : octets=32 temps=1 ms TTL=127
Réponse de 200.200.5.11 : octets=32 temps=1 ms TTL=127
```

Connexion au VLAN d'administration 1er étage :

```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::4ce9:2cfb:8c2d:b79%7
   Adresse IPv4. . . . . . . . . . . . . .: 172.16.100.3
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 172.16.100.254

Carte réseau sans fil Wi-Fi :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . : domadj.fr
```

172.16.100.250 - PuTTY

```
User Access Verification

Username:
Username: admin
Password:
SW1E>en
Password:
SW1E#
```

Connexion au VLAN d'administration 2e étage :

```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::4ce9:2cfb:8c2d:b79%7
   Adresse IPv4. . . . . . . . . . . . . .: 172.16.100.3
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 172.16.100.254

Carte réseau sans fil Wi-Fi :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . : domadj.fr
```

```
172.16.100.251 - PuTTY

User Access Verification

Username: admin
Password:
SW2ESERV>en
Password:
SW2ESERV#
```

Connexion au VLAN d'administration rez de chaussée :

```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::4ce9:2cfb:8c2d:b79%7
   Adresse IPv4. . . . . . . . . . . . . .: 172.16.100.3
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 172.16.100.254

Carte réseau sans fil Wi-Fi :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . : domadj.fr
```

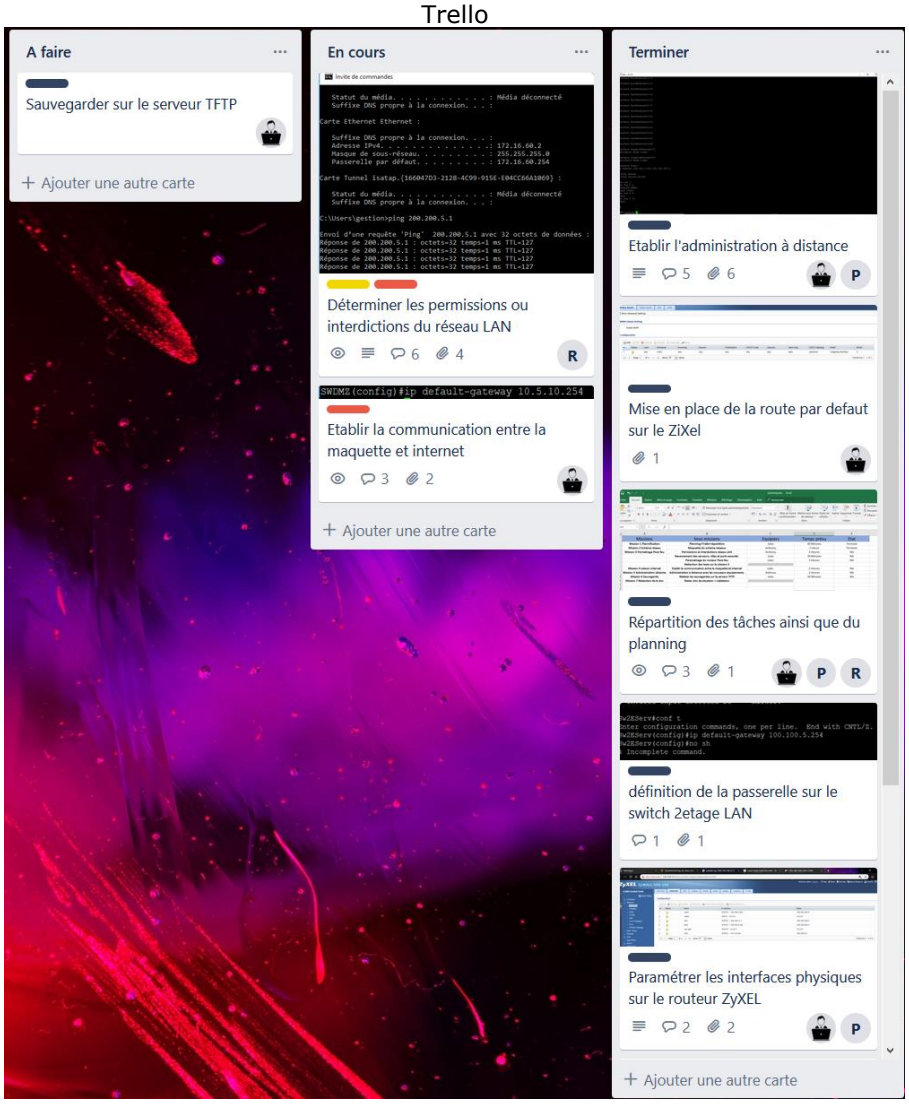
```
User Access Verification

Username: admin
Password:
SWRdc>en
Password:
SWRdc#
```

A1.4.1 Participation à un projet

C1.4.1.2

Rendre compte de son activité

Trello



A1.4.2 Évaluation des indicateurs de suivi d'un projet et justification des écarts

C1.4.2.1
Suivre l'exécution du projet
C1.4.2.2
Analyser les écarts entre temps prévu et temps consommé
C1.4.2.3
Contribuer à l'évaluation du projet

Missions	Sous missions	Equipiers	Temps prévu	Etat
Mission 1 Plannification	Planning+Trello+répartition	Jules	40 Minutes	Terminer
Mission 2 Schéma réseau	Maquette du schéma réseaux	Anthony	1 Heure	Terminer
Mission 3 Parmétrage Pare-feu	Permissions et interdictions réseau LAN	Anthony	3 Heures	NA
	Recensement des serveurs, rôles et ports associés	Jules	30 Minutes	NA
	Paramétrage du routeur Pare-feu	Jules	3 Heures	NA
	Rédaction des tests sur la mission 3	////////////////////////////////////		
Mission 4 Liaison Internet	Etablir la communication entre la maquette et internet	Jules	2 Heures	NA
Mission 5 Administration distante	Administration à distance avec les nouveaux équipements	Anthony	2 Heures	NA
Mission 6 Sauvegarde	Réaliser les sauvegardes sur le serveur TFTP	Jules	30 Minutes	NA
Mission 7 Rédaction de la doc	Rédac doc de situation + validation	////////////////////////////////////		

A3.1.3 Prise en compte du niveau de sécurité nécessaire à une infrastructure

C3.1.3.2
Proposer une solution de sécurité compatible avec les contraintes techniques, financières, juridiques et organisationnelles

L'administration des équipements ne peut plus se faire uniquement par un cable console, nous devons donc permettre le paramétrage à distance par l'intermédiaire d'un VLAN dédié : le VLAN 100 Administration, lequel permettra les connexions en SSH

Concernant les règles d'accès entre services et avec l'extérieur, nous utiliserons un parefeu Zyxell.

A1.3.4 Déploiement d'un service

C1.3.4.3
Mettre en exploitation le service

+

A3.2.1 Installation et configuration d'éléments d'infrastructure

C3.2.1.1
Installer et configurer un élément d'interconnexion, un service, un serveur, un équipement terminal utilisateur
C3.2.1.3
Installer et configurer des éléments de sécurité permettant d'assurer la protection du système informatique

<u>Administration à distance SSH</u>

Création du VLAN100 Administration :

```
SWRDC(config)#vlan 100
SWRDC(config-vlan)#name Administration
```

On lui attribue une adresse étant celle de destination en cas de connexion SSH :

```
SWRDC(config)#int vlan 100
SWRDC(config-if)#
%LINK-5-CHANGED: Interface Vlan100, changed state to up

SWRDC(config-if)#ip add 172.16.100.249 255.255.255.0
SWRDC(config-if)#no sh
SWRDC(config-if)#exit
```

Pour nous 5 adresses (1 par switch) 172.16.100.249-253 attribuées chacune au port 24 :

```
SWRDC(config)#int fa 0/24
SWRDC(config-if)#switchport access vlan 100
SWRDC(config-if)#no sh
```

On crée le domaine puis on génère la clé rsa de 2048b pour passer en mode SSH sur l'équipement et enfin on active ssh :

```
SWRDC(config)#crypto key generate rsa
The name for the keys will be: SWRDC.GSBGR5.local
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
SWRDC(config)#ip domain-name GSBGR5.local
SWRDC(config)#crypto key generate rsa
% You already have RSA keys defined named SWRDC.GSBGR5.local .
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: SWRDC.GSBGR5.local
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

SWRDC(config)#ip ssh version 2
*mars 1 0:23:31.221:  %SSH-5-ENABLED: SSH 1.99 has been enabled
```

2 minutes d'inactivité maximum avant déconnexion + 5 essais de connexion infructueux max:

```
SWRDC(config)#ip ssh time-out 120
SWRDC(config)#ip ssh auth-retries ?
% Unrecognized command
SWRDC(config)#ip ssh authentication-retries ?
  <0-5>  Number of authentication retries
SWRDC(config)#ip ssh authentication-retries 5
```

Passage des 16 connexions possibles en mode ssh uniquement :

```
SWRDC(config)#line vty 0 15
SWRDC(config-line)#login local
SWRDC(config-line)#transport input ssh
```

Je dissimule ensuite de façon légère les mots de passe affichés dans la config :

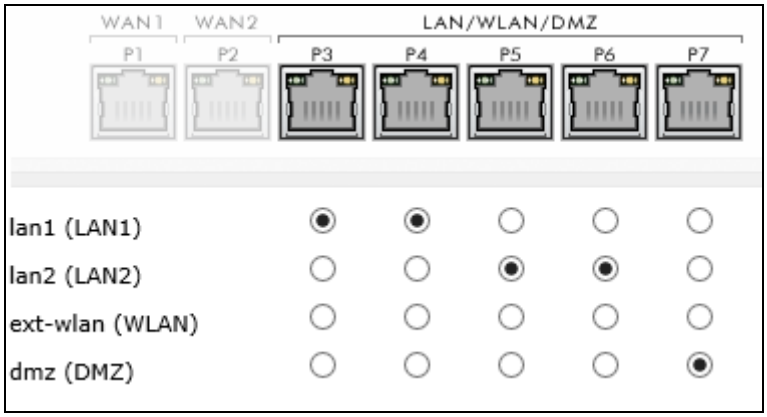
```
SWRDC(config)#service password-encryption
```

Essai de connexion en ssh par invite de commande, on constate par le dernier prompt que passe en administrateur (**#**) :

```
C:\>ssh -l admin 172.16.100.249
Open
Password:



SWRDC>en
Password:
SWRDC#exit
```

La procédure est à répéter sur les éléments du reste du réseau.
Les règles inter-service sont appliquées par le ZYXEL dont voici un extrait de la configuration:

Tout d'abord quelle zone est appliquée à quel port :



Création des interfaces virtuelles, passerelles des VLAN de la zone LAN :

#	Status	Name	Port/VID	IP Address	Mask
1		vlan10	lan2/10	static --172.16.10.254	255.255.255.0
2		vlan100	lan2/100	static --172.16.100.254	255.255.255.0
3		vlan150	lan2/150	static --172.16.150.254	255.255.255.0
4		vlan20	lan2/20	static --172.16.20.254	255.255.255.0
5		vlan200	lan2/200	static --200.200.5.254	255.255.255.0
6		vlan30	lan2/30	static --172.16.30.254	255.255.255.0
7		vlan40	lan2/40	static --172.16.40.254	255.255.255.0
8		vlan50	lan2/50	static --172.16.50.254	255.255.255.0
9		vlan60	lan2/60	static --172.16.60.254	255.255.255.0

Je crée ensuite trois objets de type adresse qui serviront lors de la configuration du Pare-feu :

- Le VLAN 100 (Administration) a accès au serveur DMZ
- La zone LAN a accès à la zone LAN uniquement pour le VLAN 200 (serveur AD)
- Le VLAN 40 (Développement) a accès au FTP sur la DMZ

#	Name	Type	Address
1	DMZ_SUBNET	INTERFACE SUBNET	dmz-10.5.0.0/16
2	EXT_WLAN_SUBNET	INTERFACE SUBNET	ext-wlan-0.0.0.0/32
3	LAN1_SUBNET	INTERFACE SUBNET	lan1-192.168.15.0/24
4	LAN2_SUBNET	INTERFACE SUBNET	lan2-100.100.5.0/24
5	WLAN-1-1_SUBNET	INTERFACE SUBNET	wlan-1-1-10.59.1.0/24
6	vlan100	SUBNET	172.16.100.0/24
7	vlan200	SUBNET	200.200.5.0/24
8	vlan40	SUBNET	172.16.40.0/24

Les ACL ou règles de filtrage :

Status	Priority	From	To	Schedule	User	Source	Destination	Service	Access
	1	LAN2	DMZ	none	any	vlan100	any	any	allow
	2	WAN	DMZ	none	any	any	any	DNS	allow
	3	LAN2	DMZ	none	any	vlan40	any	FTP	allow
	4	LAN2	LAN2	none	any	any	vlan200	any	allow
	5	LAN2	WAN	none	any	any	any	any	allow
	6	WAN	DMZ	none	any	any	any	SFTP	allow
	7	WAN	DMZ	none	any	any	any	HTTPS	allow
	8	DMZ	WAN	none	any	any	any	any	allow
	9	LAN2	DMZ	none	any	any	any	HTTPS	allow
	10	LAN2	DMZ	none	any	any	any	DNS	allow
	11	LAN1	DMZ	none	any	any	any	any	allow
	12	LAN1	LAN1	none	any	any	any	any	allow
	13	LAN1	ZyWALL	none	any	any	any	any	allow
	14	LAN1	any (Excluding ZyWALL)	none	any	any	any	any	allow
	Default	any	any	none	any	any	any	any	deny

A3.2.3 Mise à jour de la documentation technique d'une solution d'infrastructure

C3.2.3.2

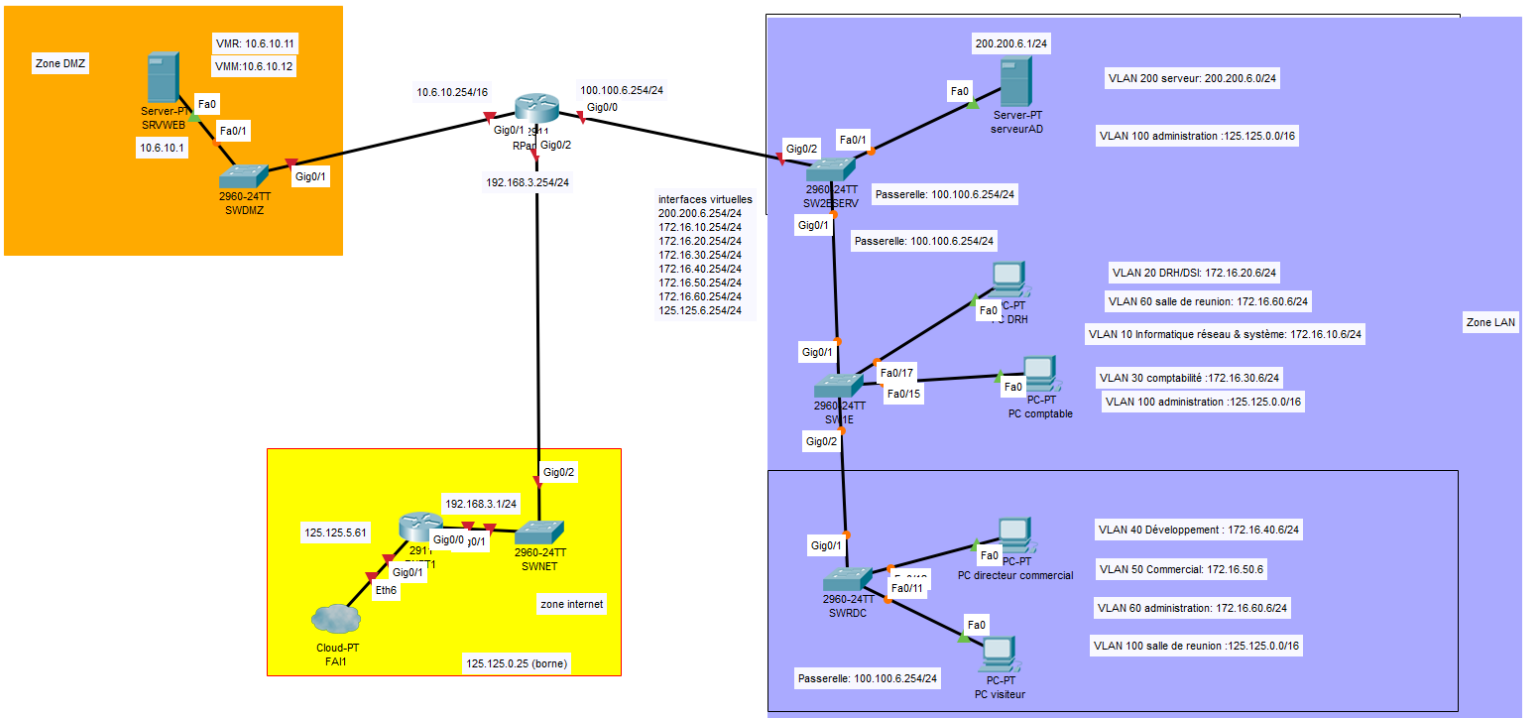
Mettre à jour la documentation

A4.2.4 Mise à jour d'une documentation technique

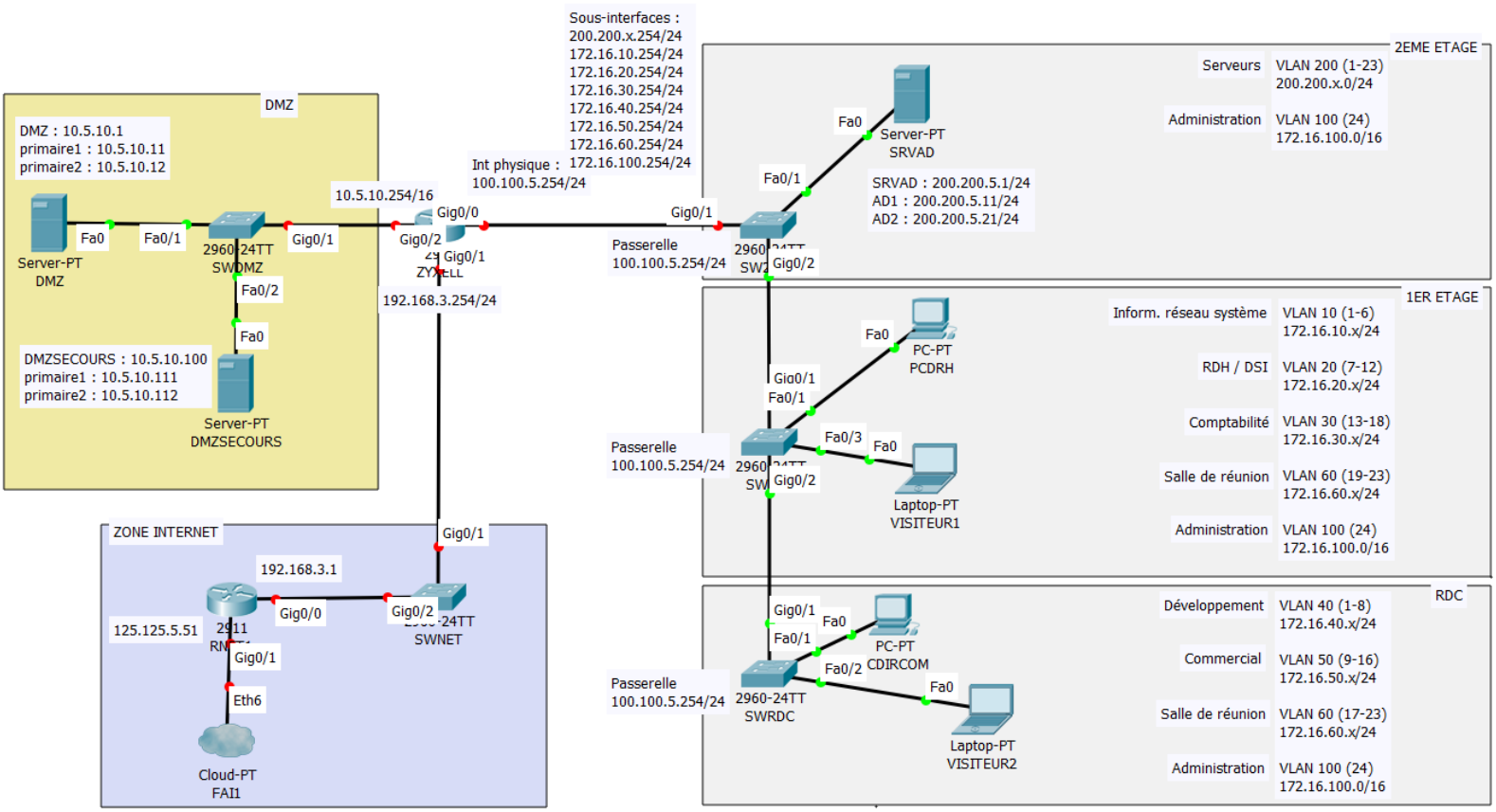
C4.2.4.2

Mettre à jour une documentation

Ancienne documentation :



Nouvelle documentation :



VLANs :	SWITCHES (VTP : GSBGR5) :	SERVEURS :
10 - Informatique_Reseau_Systeme 172.16.10.0/24 20 - RDH_DSI 172.16.20.0/24 30 - Comptabilité 172.16.30.0/24 40 - Developpement 172.16.40.0/24 50 - Commercial 172.16.50.0/24 60 - Salle de réunion 172.16.60.0/24 100 - Administration 172.16.100.0/24 200 - Serveurs 200.200.5.0/24	**SWNET** VLAN1 : 0-23 VLAN100 : 24 (172.16.100.253) **SWDMZ** VLAN1 : 0-23 VLAN100 : 24 (172.16.100.252) **SW2ESERVEURS** (Serveur VTP) VLAN200 : 0-23 VLAN100 : 24 (172.16.100.251) **SW1ER** VLAN10 : 1-6 VLAN20 : 7-12 VLAN30 : 13-18 VLAN60 : 19-23 VLAN100 : 24 (172.16.100.250) **SWRDC** VLAN40 : 1-8 VLAN50 : 9-16 VLAN60 : 17-23 VLAN100 : 24 (172.16.100.249)	**AD** 200.200.5.1/24 AD1 200.200.5.11/24 AD2 200.200.5.12/24 **DMZ** 10.5.10.1/24 primaire1 10.5.10.11/24 primaire2 10.5.10.12/24 **DMZ SECOURS** 10.5.10.100/24 primaire1 10.5.10.111/24 primaire2 10.5.10.112/24 mdp windows : mdp primaires :

A3.3.2 Planification des sauvegardes et gestion des restaurations

C3.3.2.3

Appliquer des procédures de sauvegarde et de restauration

Procédure de sauvegarde appliquée aux 5 commutateurs de la maquette ainsi qu'au routeur dont j'ai juste la photo du fichier mais démarche identique :

```
SW1E#copy runn tftp
Address or name of remote host []? 172.16.100.3
Destination filename [SW1E-confg]? SW1E_CONFIG_05-11-2019

Writing running-config...!!
[OK - 1090 bytes]

1090 bytes copied in 0 secs
```

```
SW2ESERVEURS#copy runn tftp
Address or name of remote host []? 172.16.100.3
Destination filename [SW2ESERVEURS-confg]?
SW2ESRV_CONFIG_05-11-2019

Writing running-config...!!
[OK - 1098 bytes]

1098 bytes copied in 0.002 secs (549000 bytes/sec)
```

```
SWDMZ#copy runn tftp
Address or name of remote host []? 10.5.10.28
Destination filename [SWDMZ-confg]? SWDMZ_CONFIG_12-11-2019

Writing running-config....!!
[OK - 1086 bytes]

1086 bytes copied in 3.002 secs (361 bytes/sec)
```

```
SWNET#copy run tftp
Address or name of remote host []? 192.168.3.3
Destination filename [SWNET-confg]? SWNET_CONFIG_12-05-2019

Writing running-config....!!
[OK - 1090 bytes]

1090 bytes copied in 3.011 secs (362 bytes/sec)
```

```
SWRDC#copy runn tftp
Address or name of remote host []? 172.16.100.3
Destination filename [SWRDC-confg]? SWRDC_CONFIG_05-11-2019

Writing running-config....!!
[OK - 1091 bytes]

1091 bytes copied in 3.005 secs (363 bytes/sec)
```