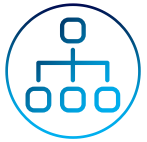
GS11 Technique de sécurisation

Sécurisation d'une infrastructure

A. NICOLAS, A. PINON - A20

PLAN



Partie I - Architecture du SI

> *Choix d'architecture*

> *Technologies utilisées*

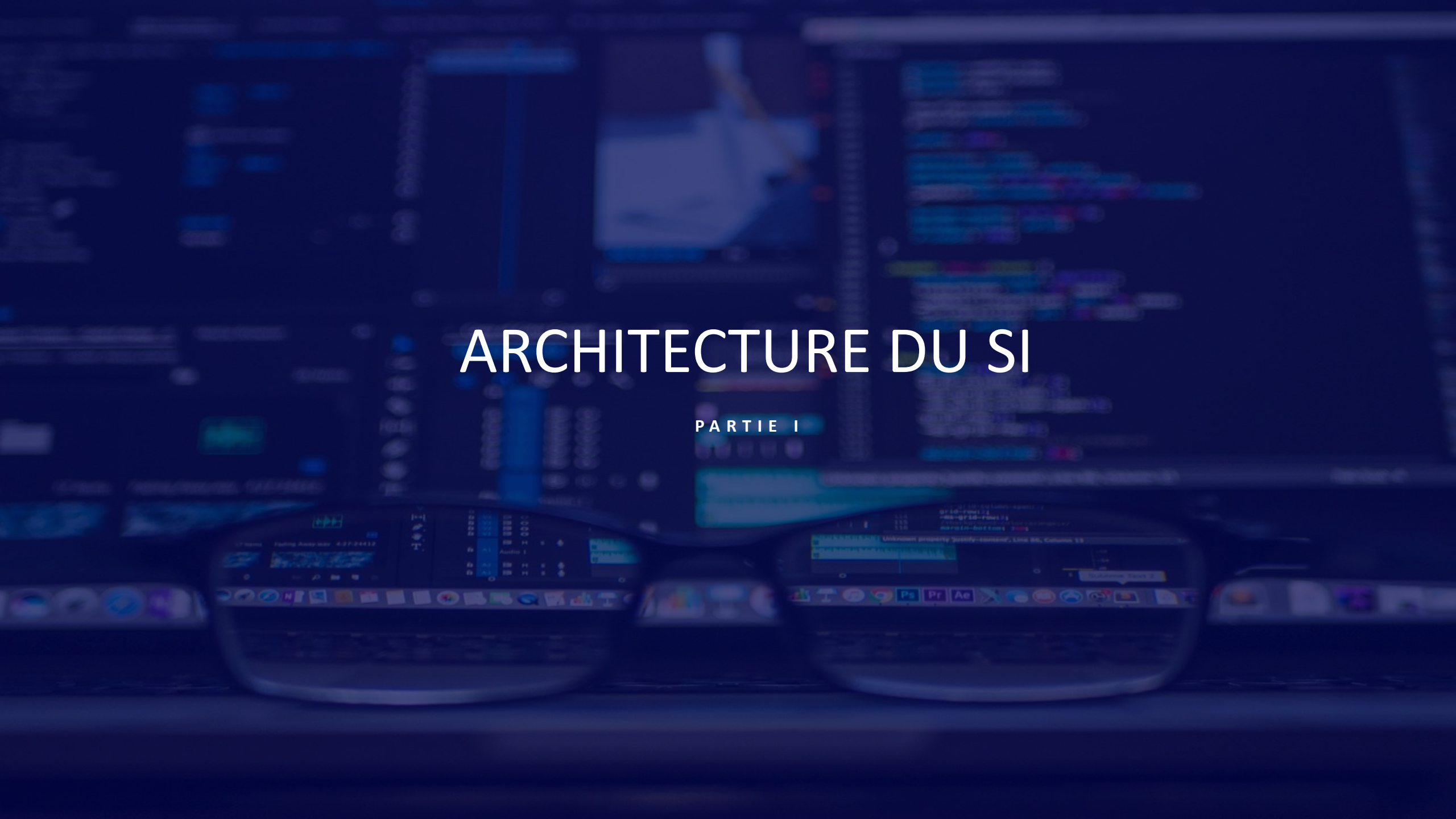
Partie II – Mise en œuvre

> ***Pare-feu** VYoS*

> ***Commutateur** Cisco*

> ***Serveur Web** Apache2*

> ***Active Directory** & Environnement **Windows***

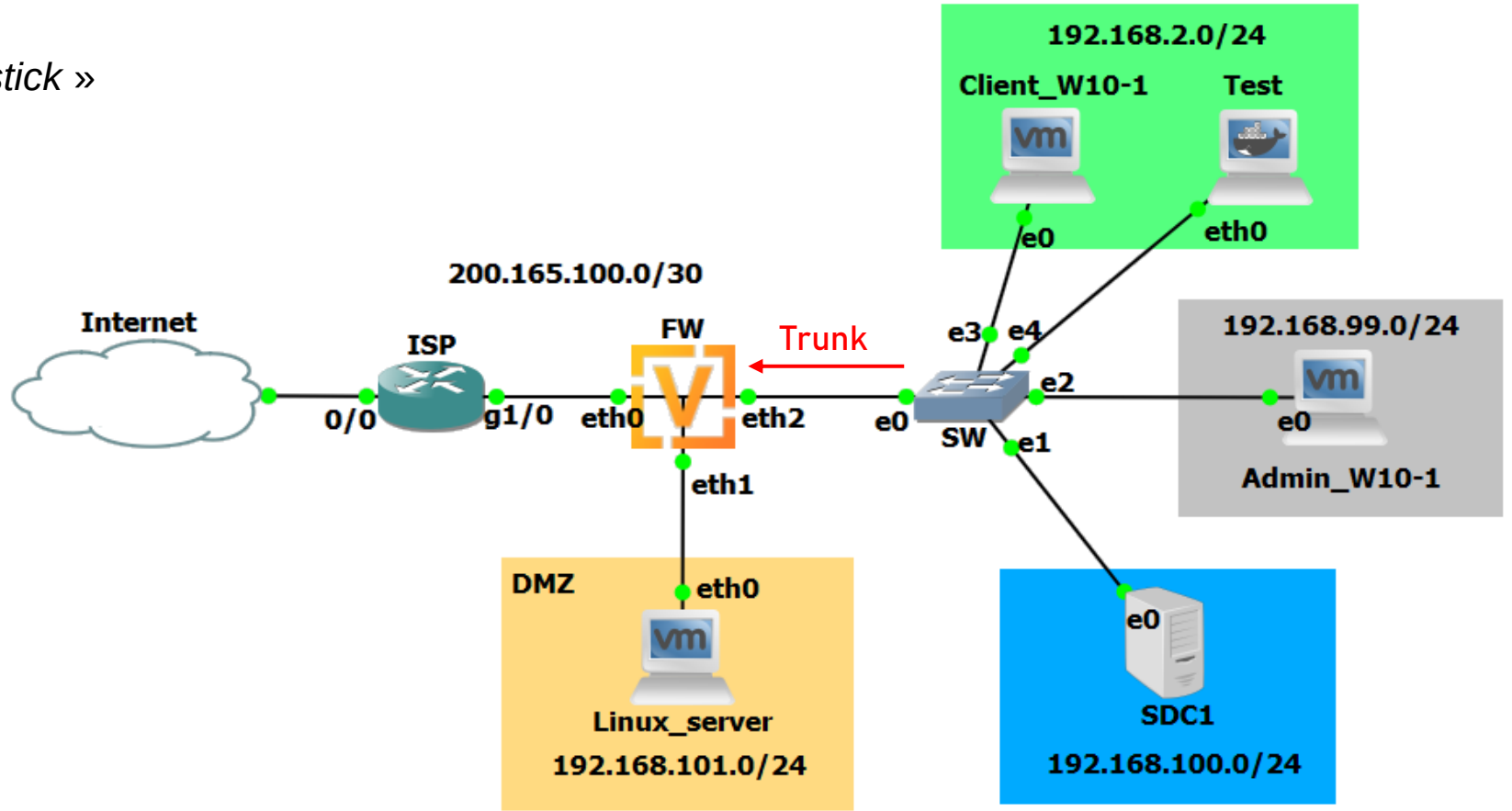


ARCHITECTURE DU SI

PARTIE I

Présentation de l'architecture

- Architecture « *Router-on-a-stick* »
- 4 VLAN:
  - Utilisateurs
  - Gestion
  - Serveurs
  - *Invité*
- DMZ pour le serveur Web



Architecture du SI

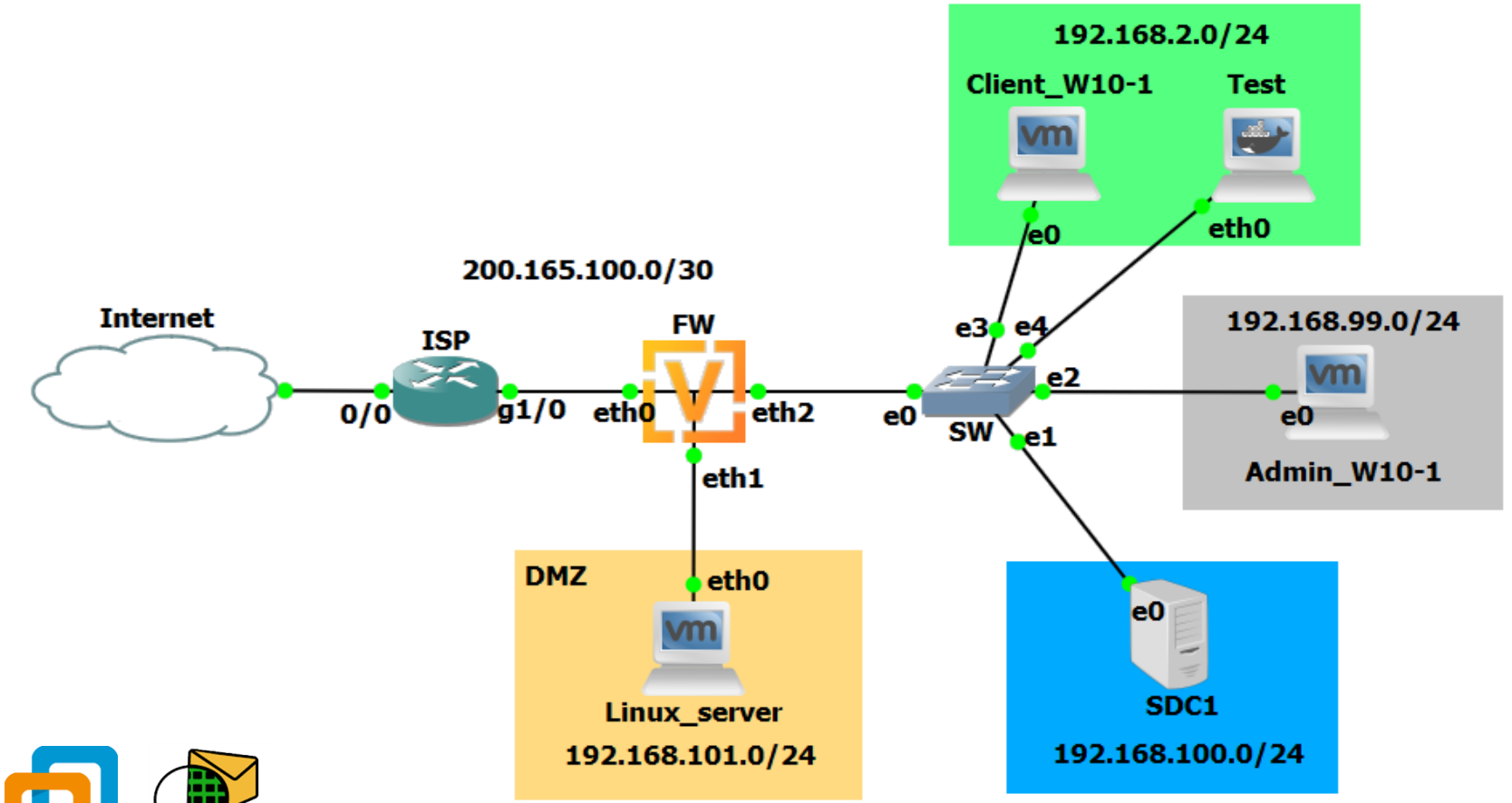
Technologies utilisées

Windows 10

ubuntu

docker

GNS3



MISE EN ŒUVRE

PARTIE II

Pare-feu VYoS - Présentation

- Gestion simplifié des interfaces et sous-interfaces
- Possibilité de gérer des objets (groupes d'adresses et de réseaux)
- Filtrage basé sur *netfilter*
  - Chaque stratégie de pare-feu est implémentée sous forme de ***chaîne*** dans *iptables*.
  - 3 chaînes locales: WAN-LOCAL, DMZ-LOCAL et LAN-LOCAL

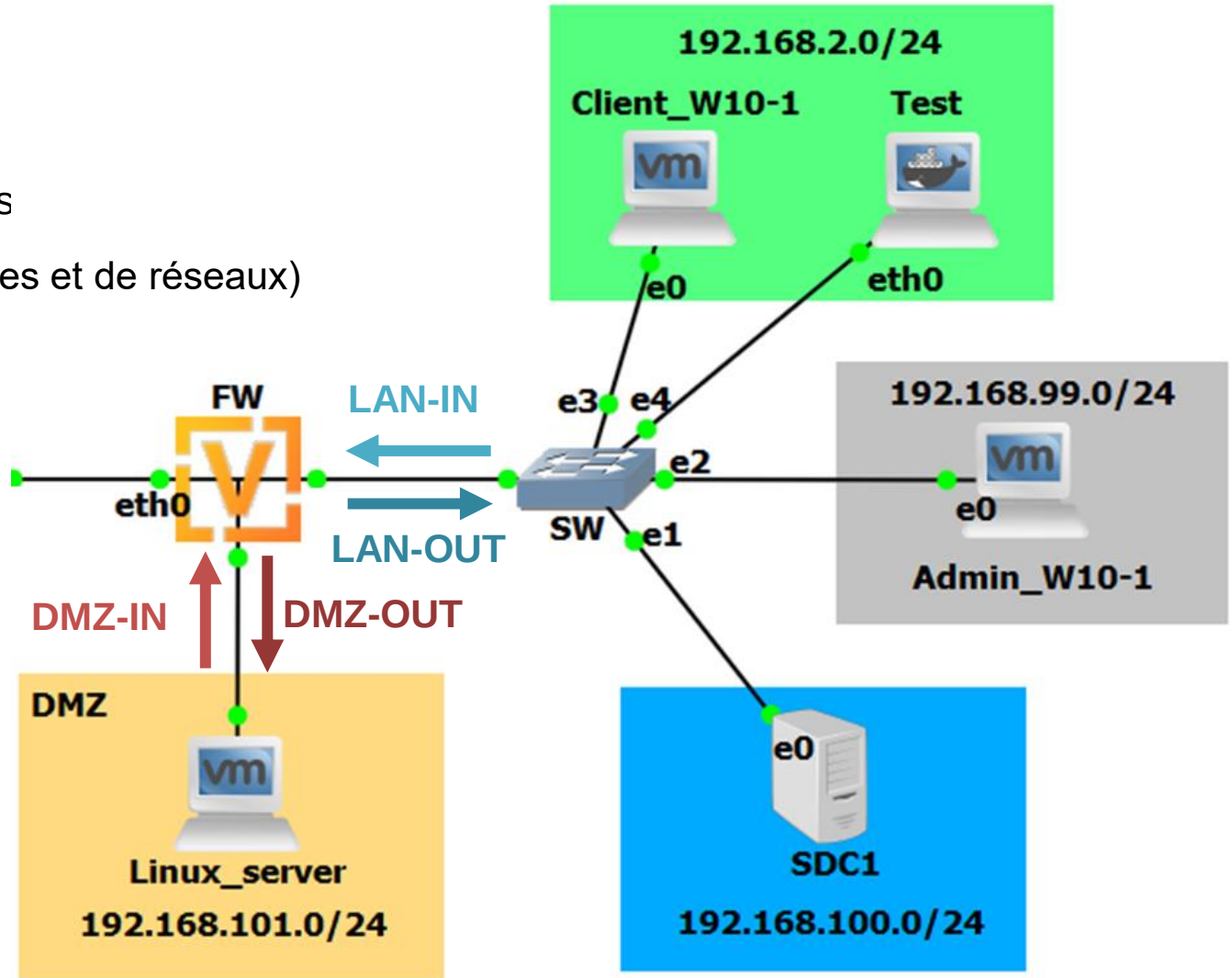
VYoS

```
set firewall name DMZ-LOCAL default-action 'drop'
```

iptables

```
-N DMZ-LOCAL
-A DMZ-LOCAL -m comment --comment
"DMZ-LOCAL-10000 default-action drop" -j DROP
```

IN / OUT = FORWARD ; LOCAL = IN



Mise en œuvre

Pare-feu VYoS - Configuration

- Accès Internet : NAT simple

```
set nat source rule 2 description "SNAT from USERS network"
set nat source rule 2 outbound-interface 'eth0'
set nat source rule 2 source address '192.168.2.0/24'
set nat source rule 2 translation address masquerade
```

- Accès au serveur web
  - ✓ ***Port forwarding***, accès depuis l'IP publique sur les ports 80/443
  - ✓ ***NAT-Reflection***, accès par le LAN également sur l'IP publique

```
set nat destination rule 10 description "Port Forward: HTTP WebServ"
set nat destination rule 10 destination port '80'
set nat destination rule 10 inbound-interface 'eth0'
set nat destination rule 10 protocol 'tcp'
set nat destination rule 10 translation address '192.168.101.1'
```

- Accès de gestion: SSH, MMC et Terminal Server

```
# Accept SSH trafic from mgmt
set firewall name LAN-LOCAL rule 1100 action 'accept'
set firewall name LAN-LOCAL rule 1100 destination port '22'
set firewall name LAN-LOCAL rule 1100 protocol 'tcp'
set firewall name LAN-LOCAL rule 1100 source group network-group 'NET-MANAGEMENT'
set firewall name LAN-LOCAL rule 1100 state new 'enable'
```

✓ Autoriser les flux Active Directory

TCP	Description
53	DNS
88*	Kerberos Key Distribution Center
135*	RPC Endpoint Mapper
139*	NetBIOS Session Service
389*	LDAP
445*	SMB, Net Logon
464	Kerberos password change
636	LDAP over SSL
3268	LDAP GC (Catalog Global)
3269	LDAP GC SSL
49152-65535*	FRS RPC, DFSR RPC, RPC for LSA, SAM, NetLogon. (Application des GPOs.)

UDP	Description
53*	DNS
88	Kerberos Key Distribution Center
123	NTP (W32Time)
137	NetBIOS Name Resolution
138	NetBIOS Datagram Service
389*	LDAP, DC Locator, Net Logon
636	LDAP over SSL

Légende :

* - *Configuration minimale*

Optionnel

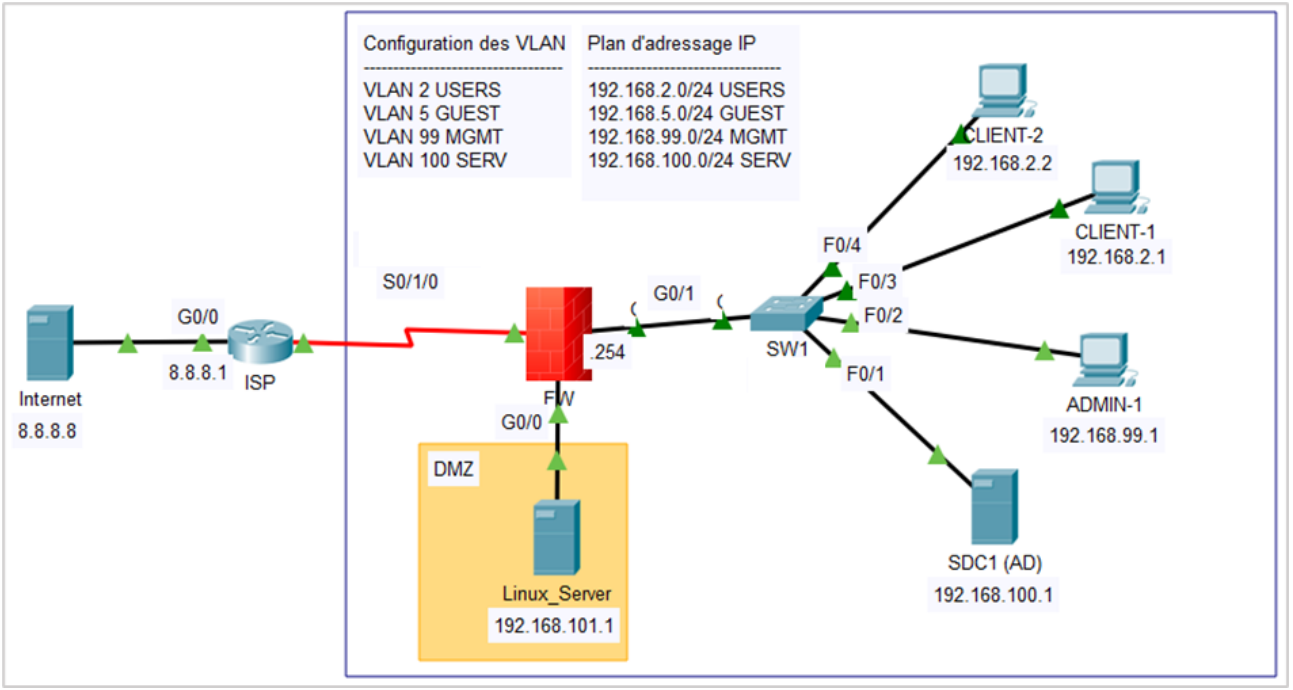
Switch Cisco

- Configuration de base

```
! * General *
hostname SW1
no ip domain-lookup
service password-encryption
banner motd # Unauthorized Access is Prohibited #
enable secret cisco
line vty 0 4
 login local
 logging synchronous
 exit
```

- Parade contre les attaques ARP: *port-security*

```
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation shutdown
! switchport port-security violation restrict
! switchport port-security violation protect
switchport port-security maximum 1
```



- Configuration SSH

```
! * SSH *
ip domain-name monbeaureseau.com
crypto key generate rsa general-keys modulus 1024
ip ssh version 2
ip ssh authentication-retries 3
ip ssh time-out 120
ip ssh logging events
!
username admin privilege 15 secret cisco
```

Mise en œuvre

Serveur Web - Durcissement de la configuration

- Création d'un VHOST

```
<VirtualHost *:80>
    # Hôte utilisé, 1 ServerName / VirtualHost
    ServerName www.monbeaureseau.com
    # Alias, plusieurs possibles
    ServerAlias monbeaureseau.com mbr.com
    ServerAdmin webmaster@example.com
    DocumentRoot /var/www/html/www.monbeaureseau.com

    # Enregistrer les logs au format `combined` dans un fichier séparé
    CustomLog ${APACHE_LOG_DIR}/www.monbeaureseau.com-access.log combined
    # Enregistrer les logs d'erreur dans un fichier séparé, même format
    ErrorLog ${APACHE_LOG_DIR}/www.monbeaureseau.com-error.log

    <Directory /var/www/html/www.monbeaureseau.com>
        # ExecCGI, FollowSymlinks, Includes, Indexes
        Options All
        # Pas de surcharge avec le fichier .htaccess
        AllowOverride None
    </Directory>
</VirtualHost>
```

- Suppression du VHOST par défaut
- Suppression des modules inutiles (CGI, etc.)
- Limiter les fuites d'informations

sudo nano /etc/apache2/conf-available/security.conf

```
ServerTokens Prod
ServerSignature Off
```

- Limiter les accès

sudo nano /etc/apache2/apache2.conf

```
<Directory />
  Order Deny,Allow
  Deny from all
  Options None
  AllowOverride None
</Directory>
```

Mise en œuvre

Serveur Web

- Création de l'utilisateur « *webadmin* »

```
#Création de l'utilisateur webadmin et ajout au groupe www-data.
sudo useradd webadmin -g www-data -d /var/www
sudo passwd webadmin
```

- Gestion des permissions des répertoires

```
# Passer webadmin en propriétaire du root directory /var/www.
sudo chown -R webadmin:www-data /var/www


# www-data que lire et exécuter dans /var/www
sudo su
find /var/www -type d | xargs chmod 750 # drwx r-x ---
find /var/www -type f | xargs chmod 650 # -rw- r-x ---
exit
```

```
sudo apt-get install acl

# www-data pourra lire et modifier les fichiers dans /var/log, mais pas exécuter.
sudo setfacl -m "u:www-data:rw-" /var/log/apache2/*

# www-data pourra lire et exécuter les fichiers dans le répertoire /etc/apache2
sudo setfacl -Rm "u:www-data:r-x" /etc/apache2
```

- Validation des ACL

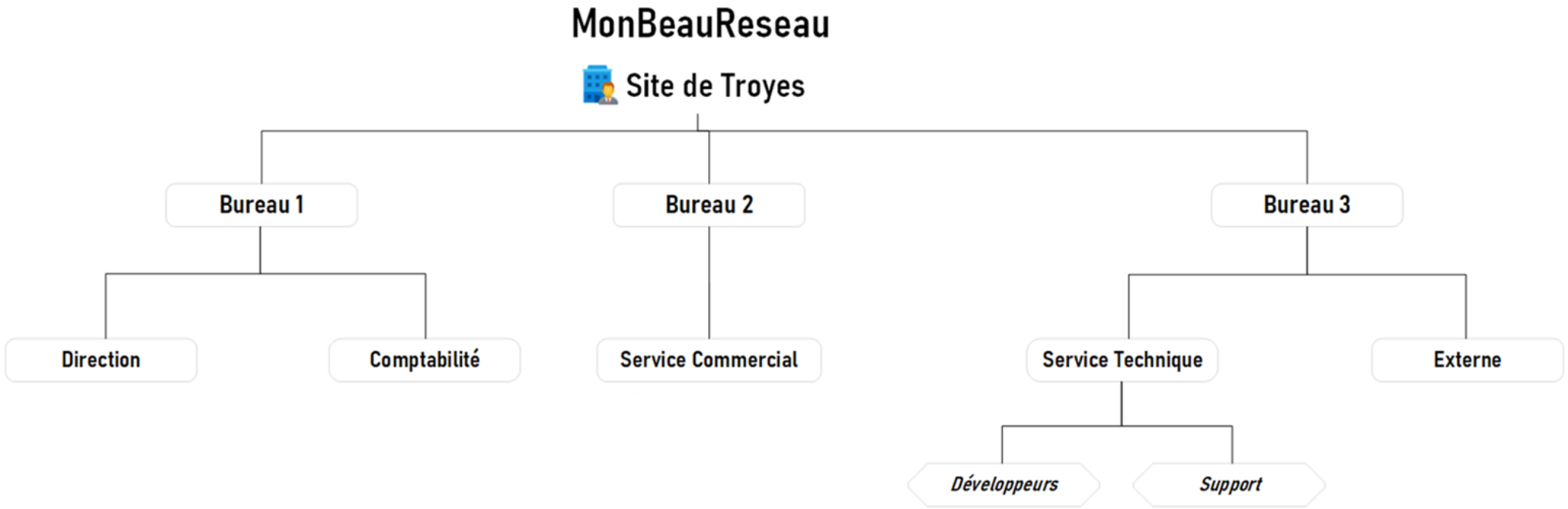
```
stduser@linux-server-1:~$ getfacl /etc/apache2
getfacl: Removing leading '/' from absolute path names
# file: etc/apache2
# owner: root
# group: root
user::rwx
user:www-data:r-x
group::r-x
mask::r-x
other::r-x
```

Mise en œuvre

AD - Stratégie d’annuaire

- **Méthodologie**

  1. Distinguer la hiérarchie de l’entreprise

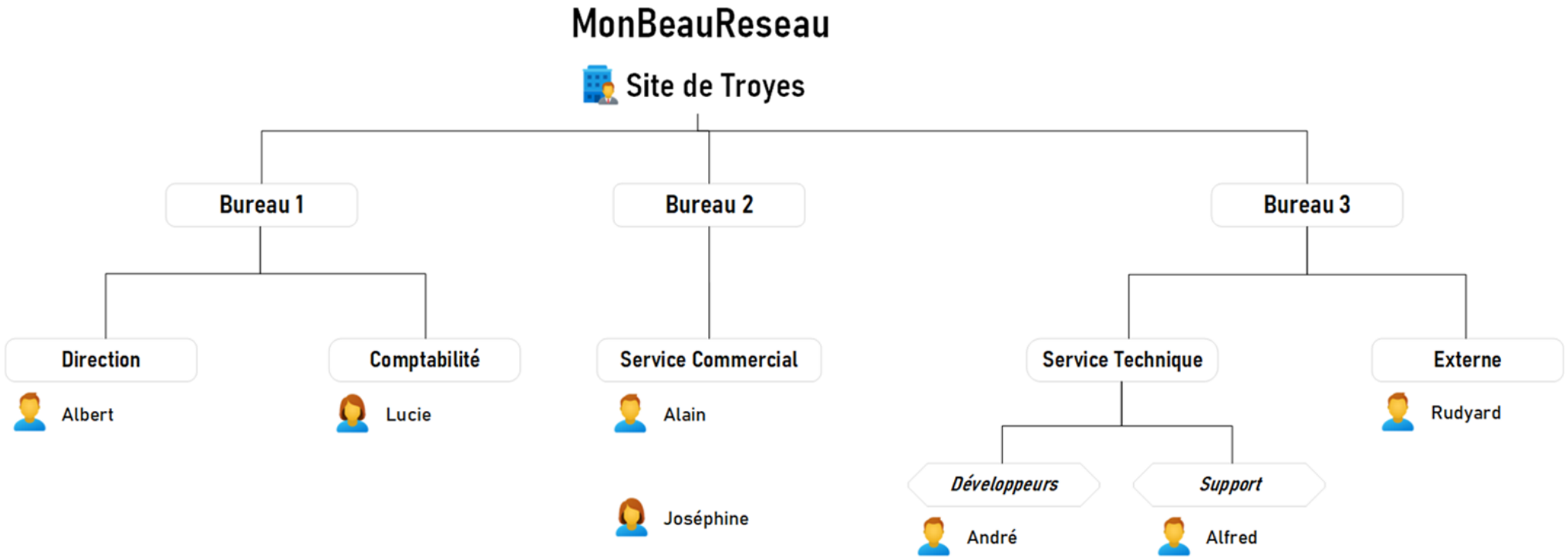


Mise en œuvre

AD - Stratégie d'annuaire

- **Méthodologie**

  1. Distinguer la hiérarchie de l'entreprise
  2. Identifier les utilisateurs



Mise en œuvre

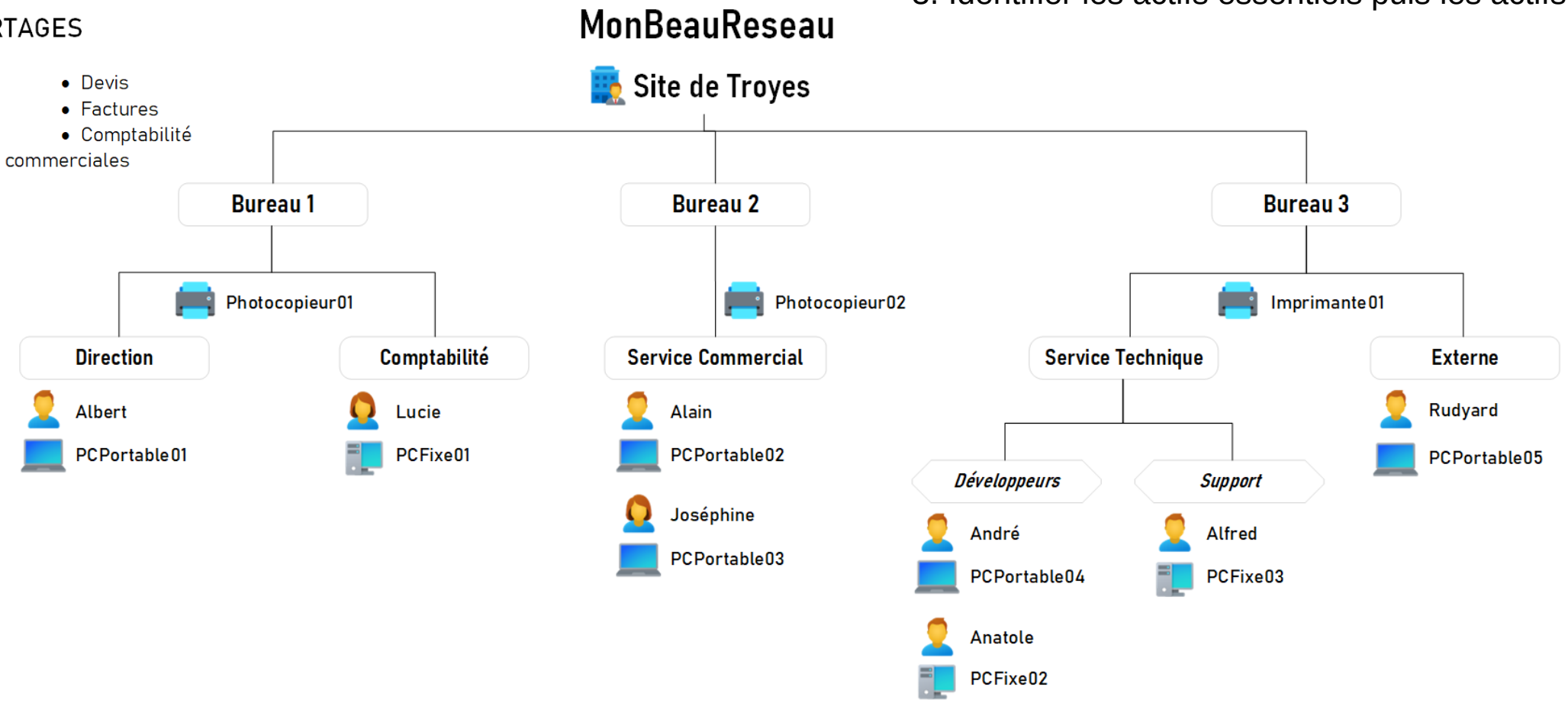
AD - Stratégie d'annuaire

- **Méthodologie**

1. Distinguer la hiérarchie de l'entreprise
2. Identifier les utilisateurs
3. Identifier les actifs essentiels puis les actifs supports.

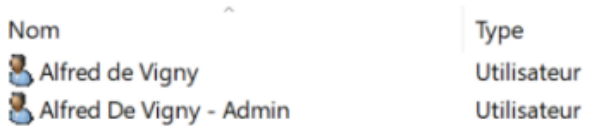
PARTAGES

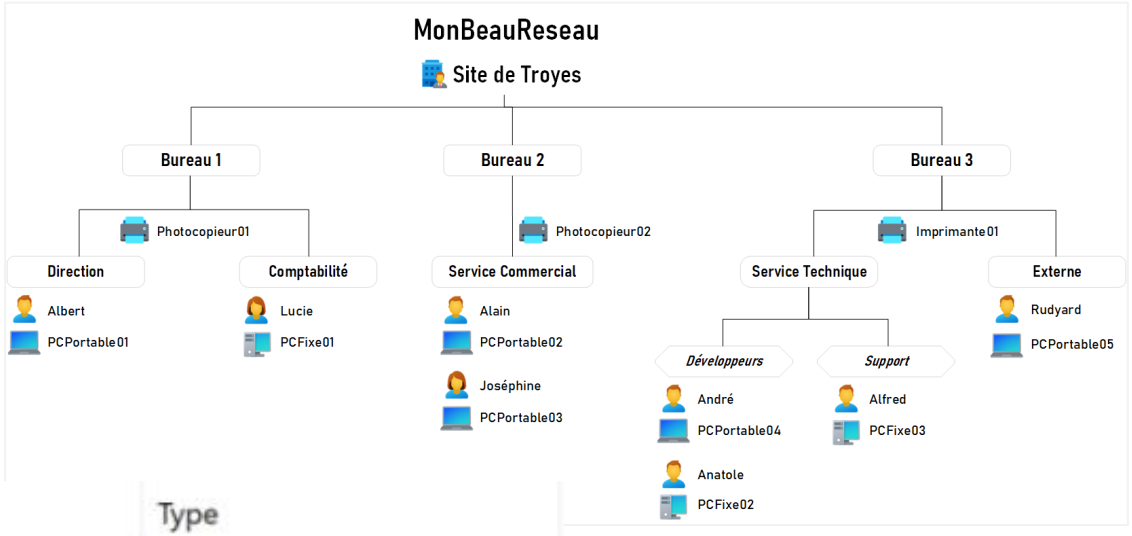
- Prospects
- Clients
- Partenaires
- Propositions commerciales
- Devis
- Factures
- Comptabilité



Mise en œuvre

AD – UO, groupes et utilisateurs





Mise en œuvre

AD – GPOs

- **Politique de mot de passe**: taille minimum de 10 caractères, au moins 1 majuscule, 1 minuscule et 1 chiffre.

Stratégies de comptes/ Stratégie de mot de passe

Stratégie	Paramètre
Antériorité maximale du mot de passe	181 jours
Antériorité minimale du mot de passe	30 jours
Appliquer l'historique des mots de passe	5 mots de passe mémorisés
Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivé
Le mot de passe doit respecter des exigences de complexité	Activé
Longueur minimale du mot de passe	10 caractères

AD – GPOs

- **Mise en veille** : L'écran de veille s'active après 10 min d'inactivité et verrouille la session. Un mot de passe est alors nécessaire pour accéder à la session.

Modèles d'administration masquer

Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.

Système/ Gestion de l'alimentation/ Paramètres de l'affichage et de la vidéo masquer

Stratégie	Paramètre	Commentaire
Activer le diaporama de l'arrière-plan du Bureau (sur batterie)	Désactivé	
Activer le diaporama de l'arrière-plan du Bureau (sur secteur)	Désactivé	

Système/ Gestion de l'alimentation/ Paramètres de la veille masquer

Stratégie	Paramètre	Commentaire
Demander un mot de passe lorsqu'un ordinateur sort de la veille (sur batterie)	Activé	Activé par Admin, A. DeVigny, 14/ 12/ 2020
Demander un mot de passe lorsqu'un ordinateur sort de la veille (sur secteur)	Activé	

AD – GPOs

- **Terminal Server** : Le port 3389 est ouvert, mais l'administrateur local des postes n'est pas accessible à distance.

✓ Autorisation pour l'utilisation du service

Modèles d'administration

Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.

Composants Windows/ Services Bureau à distance/ Hôte de la session Bureau à distance/ Connexions

Stratégie	Paramètre	Commentaire
Autoriser les utilisateurs à se connecter à distance à l'aide des services Bureau à distance	Activé	
Reconnexion automatique	Activé	

✓ Interdire l'accès à l'administrateur local

Configuration ordinateur (activée)

Stratégies

Paramètres Windows

Paramètres de sécurité

Stratégies locales/ Attribution des droits utilisateur

Stratégie	Paramètre
Interdire l'ouverture de session par les services Terminal Server	SRVDC1\ Administrateur, AUTORITE NT\ SERVICE LOCAL

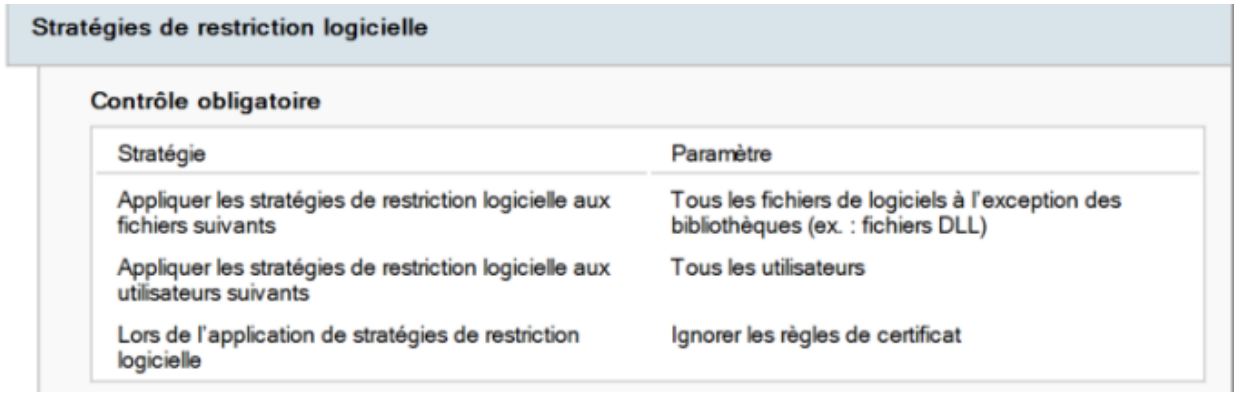
✓ Sur le Pare-feu

Nom	G..	Profil	Activée	Action	Remplacer	Programme	Adresse locale	Adresse distante	Protocole	Port local	Port distant
Terminal Server		Domaine	Oui	Autoriser	Non	Tout	Tout	Tout	TCP	3389	Tout

Mise en œuvre

AD – GPOs

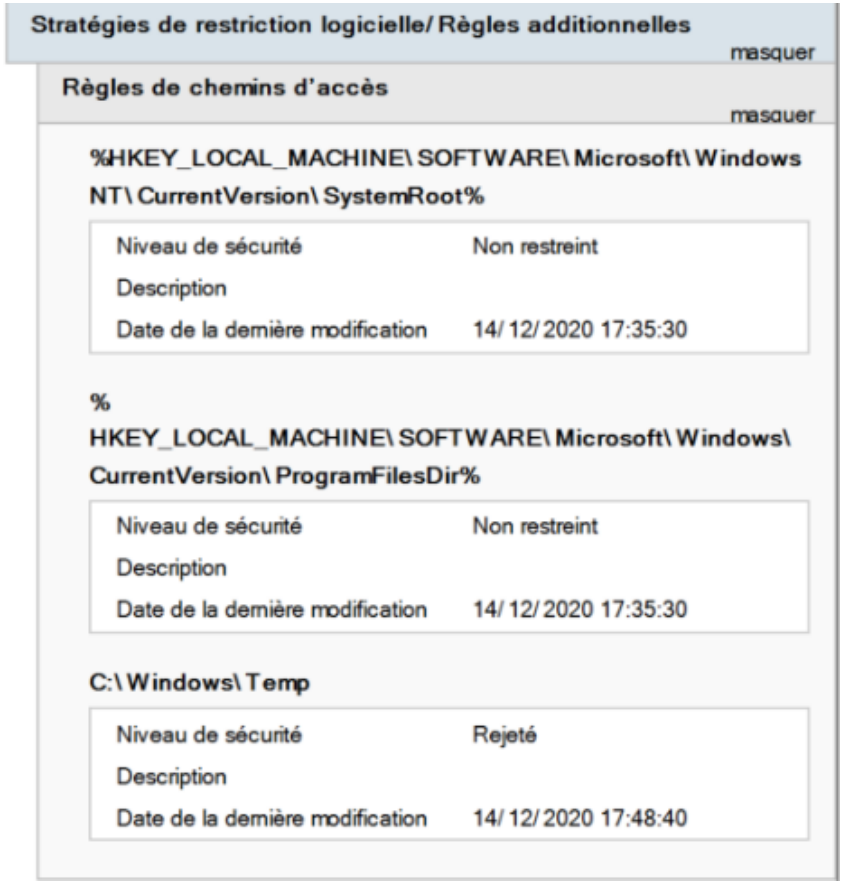
- **Stratégie de Restriction Logicielle** (SRP) : Une restriction est appliquée sur les postes pour n'autoriser que les programmes des répertoires Windows sauf *tmp*.



Stratégies de restriction logicielle

Contrôle obligatoire

Stratégie	Paramètre
Appliquer les stratégies de restriction logicielle aux fichiers suivants	Tous les fichiers de logiciels à l'exception des bibliothèques (ex. : fichiers DLL)
Appliquer les stratégies de restriction logicielle aux utilisateurs suivants	Tous les utilisateurs
Lors de l'application de stratégies de restriction logicielle	Ignorer les règles de certificat



Stratégies de restriction logicielle/ Règles additionnelles masquer

Règles de chemins d'accès masquer

%HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows NT\ CurrentVersion\ SystemRoot%

Niveau de sécurité	Non restreint
Description	
Date de la dernière modification	14/ 12/ 2020 17:35:30

% HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ ProgramFilesDir%

Niveau de sécurité	Non restreint
Description	
Date de la dernière modification	14/ 12/ 2020 17:35:30

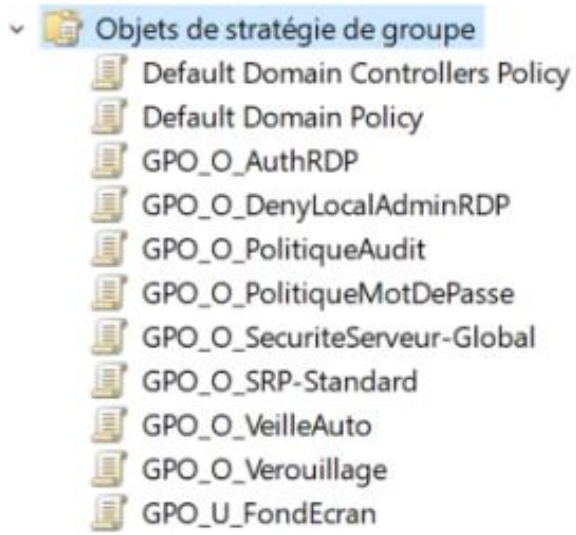
C:\ Windows\ Temp

Niveau de sécurité	Rejeté
Description	
Date de la dernière modification	14/ 12/ 2020 17:48:40

Mise en œuvre

AD – GPOs Optionnelles

- **Verrouillage**: Verrouillage des comptes après 5 tentatives de connexion échouées en moins de 10 minutes.
- **Politique d'audit**: Pour obtenir un niveau de sécurité satisfaisant, il convient d'avoir une politique d'Audit cohérente pour pouvoir investiguer les incidents pouvant se produire sur le domaine. (GS11)
- **Sécurité Globale des serveurs**: Bonne pratiques pour les attribution des droits utilisateurs, les options de sécurité local (Réseau, chiffrement, …). (GS11)
- **…**



Merci de votre attention