NewWorld SA

Livre Blanc

Projet réalisé par SCAFFIDI FONTI Mathis et PERDIGON Théo

modification : 3 juin 2022

Sommaire

- Infrastructure réseau

1. Liste des besoins

Bâtiment 3.0

L'aile Sud :

- Pôle Logistique
- Pôle Direction
- Pôle DC
- Pôle Dev NT
- Pôle Coeur SI

Les DMZ :

- DMZ privée, accessible dans l'intranet.
- DMZ publique, accessible par internet.

1 sous réseau pour les points d'accès Wifi (22).
1 sous réseau pour la ToIP.

Bâtiment Logigot

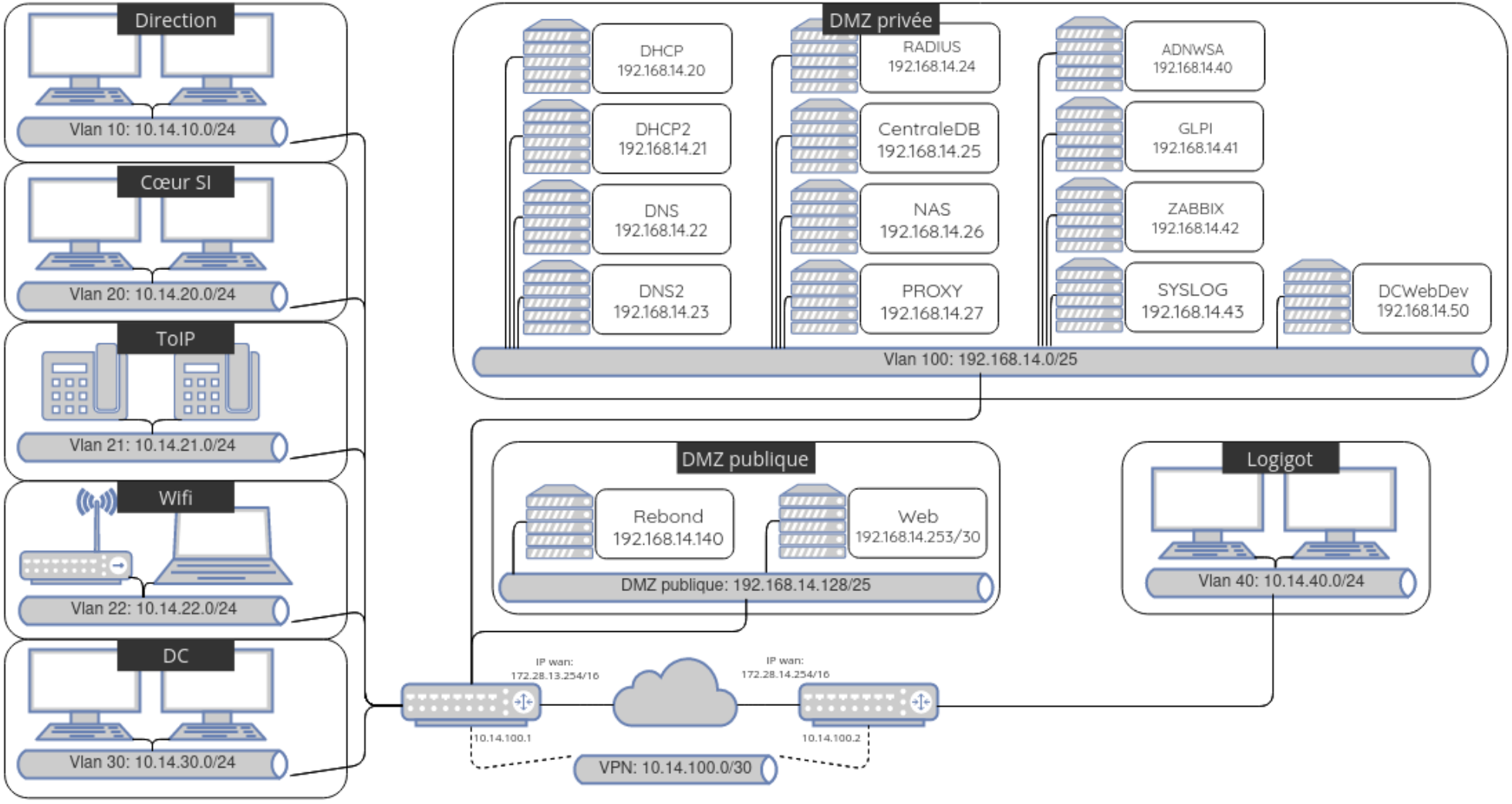
- Bureau Entrées/Sorties

1 VPN point à point pour l'interconnexion entre les 2 sites.

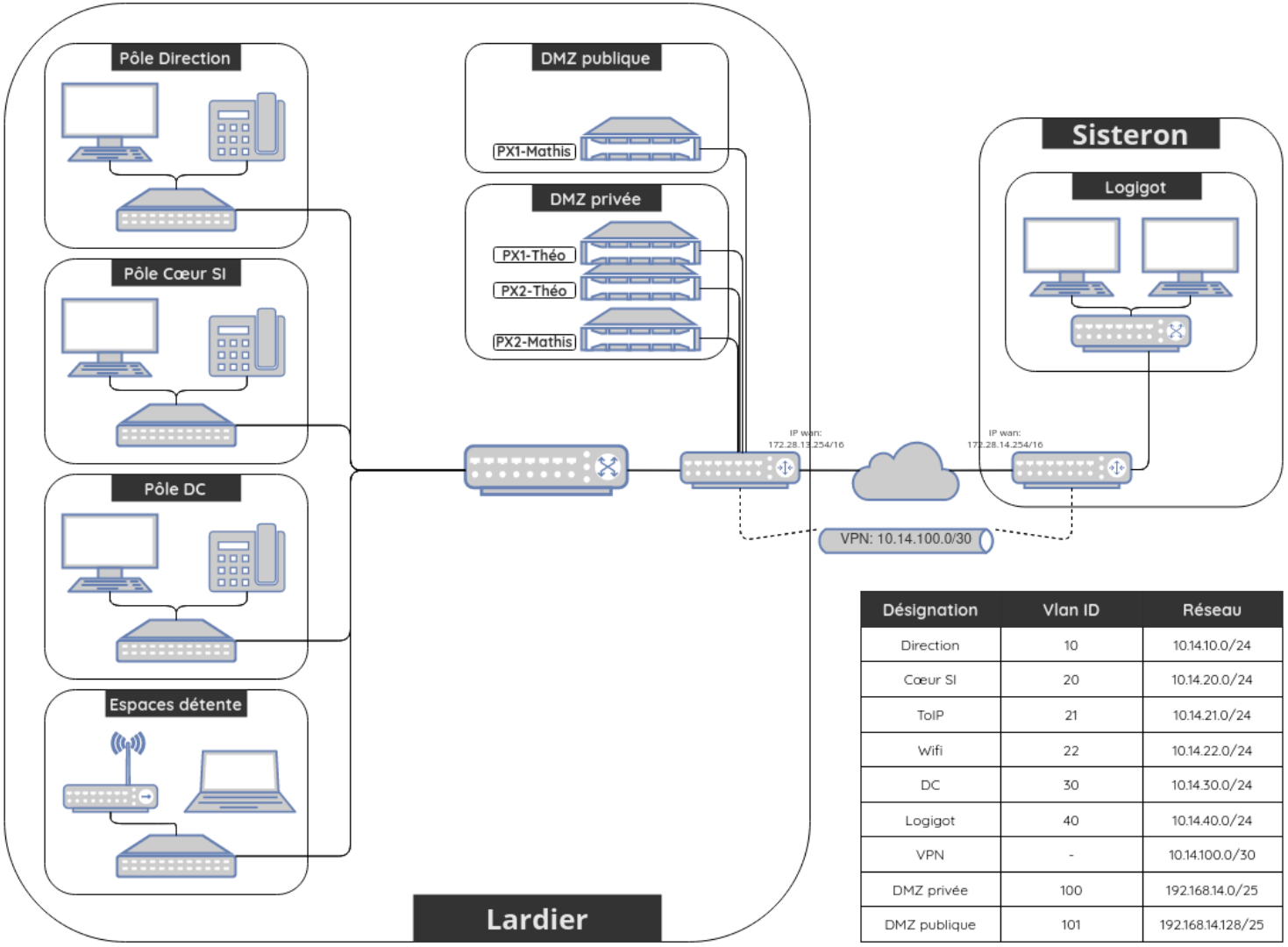
Tableau récapitulatif :

Désignation	VLAN ID	Réseau	Passerelle	Interface
Direction	10	10.14.10.0 /24	10.14.10.254	0/1.10
Logistique	11	10.14.11.0 /24	10.14.11.254	
Coeur SI	20	10.14.20.0 /24	10.14.20.254	0/1.20
ToIP	21	10.14.21.0 /24	10.14.21.254	0/1.21
Wifi	22	10.14.22.0 /24	10.14.22.254	0/1.22
DC	30	10.14.30.0 /24	10.14.30.254	0/1.30
Dev NT	31	10.14.31.0 /24	10.14.31.254	
Bureau Logigot	40	10.14.40.0 /24	10.14.40.254	
VPN		10.14.100.0 /30		s0/0/1
DMZ privée	100	192.168.14.0 /25	192.168.14.126	0/1/0 & 0/1/1
DMZ publique	101	192.168.14.128 /25	192.168.14.254	0/1/2

2. Schéma logique

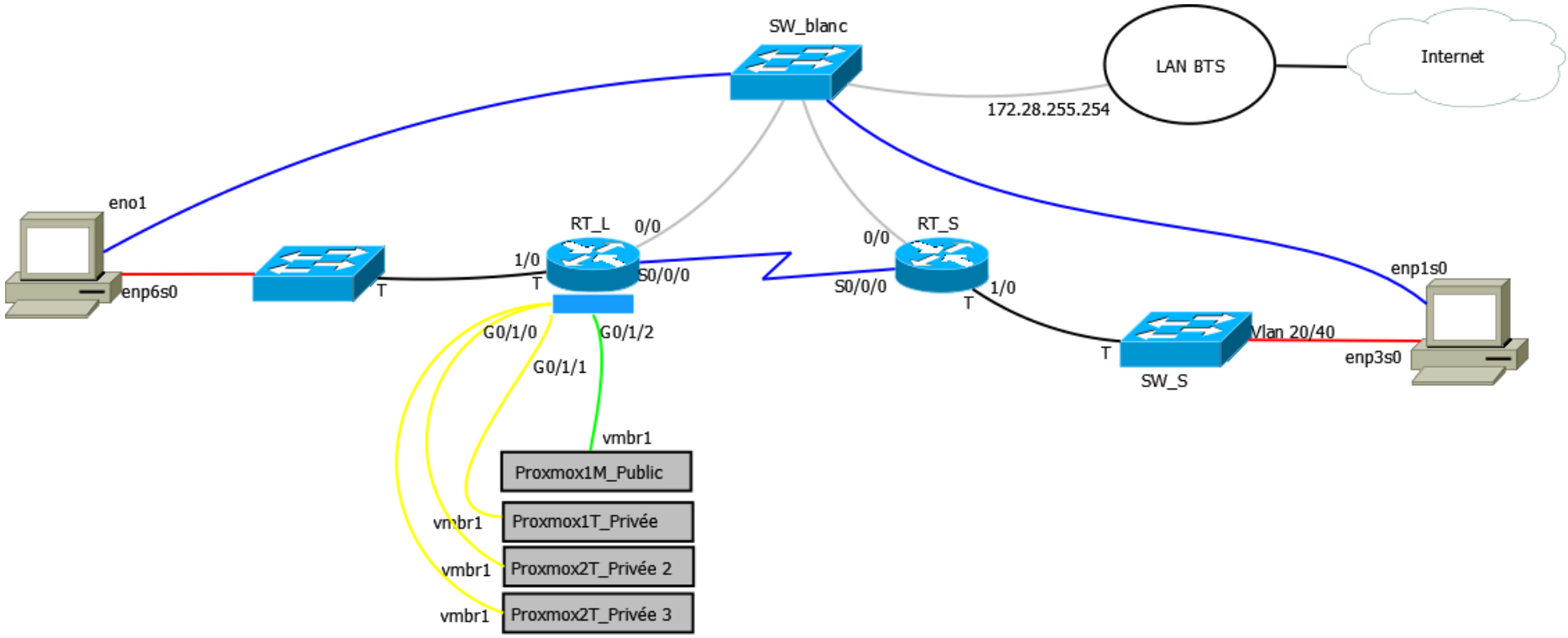


3. Schéma physique



Désignation	Vlan ID	Réseau
Direction	10	10.14.10.0/24
Cœur SI	20	10.14.20.0/24
ToIP	21	10.14.21.0/24
Wifi	22	10.14.22.0/24
DC	30	10.14.30.0/24
Logigot	40	10.14.40.0/24
VPN	-	10.14.100.0/30
DMZ privée	100	192.168.14.0/25
DMZ publique	101	192.168.14.128/25

4. Schéma câblage



5. Routeurs

Lardier:
ip wan : 172.28.13.254 (int: g0/0)
ssh : theo/a***n
secret : tp******n

Sisteron:
ip wan : 172.28.14.254 (int: g0/0)
ssh : admin/r**t
secret : m**h

Configuration NWSA:
Des sauvegardes des configurations sont réalisées à partir de chacun des routeurs, en local et sur un serveur ftp.

Lardier:

```
flash:NWSA_Lardier
```

Sisteron:

```
flash:NWSA_Sisteron
```

Serveur FTP:
ip : 172.28.200.100
id : p07
mdp : e****01

Fichiers de sauvegarde:

```
~/NWSA_R_Lardier
~/NWSA_S_Lardier
~/NWSA_R_Sisteron
~/NWSA_S_Sisteron
```

6. Switch

Lardier:
ip gestion vlan 20 : 10.14.20.253 (int: fe2)
ssh : theo/tp*****on

Configuration des interfaces:

Direction	CoeurSI	ToIP	ToIP	Wifi	DC	Trunk	HS
10	20	21	21	Tagged	30	Tagged	HS
fe1	fe2	fe3	fe4	fe5	fe6	fe7	fe8

Sisteron:
ip gestion vlan 20 : 10.14.40.253 (int: fe2)
ssh : cisco/m**h

Configuration des interfaces:

CoeurSI	Logigot						Trunk
20	40						Tagged
fe1	fe2	fe3	fe4	fe5	fe6	fe7	fe8

- Services DHCP

1. Lardier

En cas de panne sur un serveur DHCP, les clients ne sont plus en mesure, une fois le bail expiré, de reçevoir une adresse IP, ce qui pose un problème majeur de communication et de disponibilité. Il faut donc avoir un serveur DHCP de secours.

Deux serveurs DHCP sont donc en placent en **failover**, un maître et un esclave. Ils sont tous les deux placés dans la **DMZ privée** - VLAN 100.

- Serveur maître : **192.168.14.106/25**
- Serveur esclave : **192.168.14.107/25**

Identifiant : mntnnc
Mot de passe : a***n

Peer : DHCP-NWSA
Plage d'adresse pour chaque VLAN : 10.14.**<n°VLAN>**.1 - 10.14.**<n°VLAN>.**100
Bail : 6 heures

2. Sisteron

Le serveur DHCP est directement placé sur le routeur Sisteron pour desservir le VLAN Logigot.
Plage d'adresse : 10.14.40.**1** - 10.14.40**.100**

- Service d'annuaire centralisé

1. Organisation

L'annuaire est constitué de 4 Unités organisationnelles. Dans chaque unité, des groupes correspondant aux postes des utilisateurs sont configuré :

- Direction :
    - PDG
    - Direction Logigot
    - Secrétaire
    - ChefComptable
    - AgentComptable
- CoeurSI :
    - ResponsableSI
    - TechnicienSI
- Développement :
    - ResponsableDev
    - TechnicienDev
- Logigot :
    - Stockage
    - Routage
    - RespLivraisons
    - Livraisons

2. Espaces de stockage et accès

Chaque utilisateur dispose d'un lecteur réseau personnel limité à 200Mo d'espace disque ainsi que deux lecteurs réseau commun, un concernant son unité organisationnelle et un dernier lecteur réseau commun à toute l'entreprise nommée "BoiteATout".

Chaque utilisateur dispose d'un mot de passe de base a*****F*** et à l'obligation de le changer à la première connexion.

3. Informations d'administration

Ce serveur est situé dans la **DMZ privée**
IP du serveur : **192.168.14.40/25**
Domaine : **nw07-btsinfogap.org**
Mot de passe administrateur : A*******19

- Service DNS

En cas de panne sur un serveur DNS en **failover**, un deuxième serveur prend automatiquement le relais. Le serveur maître est placé dans le premier serveur de la DMZ privée et le serveur esclave est placé dans le second serveur de la **DMZ privée** pour assurer une redondance adéquate.

- Serveur maître (DNS) : **192.168.14.22/25**
- Serveur esclave (DNS2) : **192.168.14.23/25**

Identifiant : mntnnc
Mot de passe : a***n

Un script est présent sur le serveur esclave afin de garantir le transfert des fichiers de configuration. Une résolution d'adresse est faite pour chaque serveurs, VLANs et équipements réseaux.

Nom DNS	Adresse IP
DHCP	192.168.14.20
DHCP2	192.168.14.21
DNS	192.168.14.22
DNS2	192.168.14.23
RADIUS	192.168.14.24
CentraleDB	192.168.14.25
NAS	192.168.14.26
PROXY	192.168.14.27
ADNWSA	192.168.14.40
GLPI	192.168.14.41
ZABBIX	192.168.14.42
SYSLOG	192.168.14.43
DCWebDev	192.168.14.50
WAP	10.14.22.253

- Centrale de données

Une serveur de centralisation de base de données est installé dans la **DMZ privée**. Il permet à tous les services nécessitant une base de données d'en avoir une avec un accès externe sécurisé.

CentraleDB - **192.168.14.25/25**

Identifiants compte administrateur de la machine :

- Identifiant : mntnnc
- Mot de passe : a***n

Identifiants compte super administrateur de gestion des bases de données :

- Identifiant : gestion
- Mot de passe : a***n

Bases de données :

Nom serveur	Nom utilisateur	Base de données	Mot de passe
DCWebDev	'dcwebdev'@'dcwebdev.nw07-btsinfogap.org'	dcwebdev	a***n
GLPI	'glpi@'glpi.nw07-btsinfogap.org'	glpi	a***n
ZABBIX	'zabbix'@'zabbix.nw07-btsinfogap.org'	zabbix	a***n

- Point d'accès Wifi (PAW)

Un point d'accès Wifi CISCO TAP121 est installé dans l'espace détente. Il est connecté au port numéro 5 du switch Lardier. (port Tagged).

Adresse IP : **10.14.22.253/24**.

Identifiant : cisco
Mot de passe : a***n

SSIDs :

- NW07 → Connecté au VLAN 22 avec authentification via le serveur RADIUS
- NW07_CoeurSI → Connecté au VLAN 20 (Clé : N***A***n)

- Serveur RADIUS

Un serveur radius est installé, il permet aux clients du wifi NW07 de s'authentifier avec les identifiants identiques à ceux de l'AD grâce au protocole **NTLM** qui permet au RADIUS de demander les identifiants de ses utilisateurs directement au contrôleur de domaine.

Le serveur est situé dans la **DMZ privée** et a pour adresse **192.168.14.24/25**.

Identifiant : mntnnc
Mot de passe : a***n

- Serveur GLPI

Les utilisateurs pouvant générer des tickets sont importés depuis le dictionnaire LDAP du serveur contrôleur de domaine.
Tous les clients ainsi que tous les serveurs sont inventoriés via le plugin Fusioninventory. Il gère le déploiement du logiciel Putty pour tous les employés de la société.

Les utilisateurs appartenant au groupe ResponsableSI et TechnicienSI sont automatiquement habilités avec les droits de "Technician".

Le serveur est situé dans la **DMZ privée** et a pour adresse **192.168.14.41/25**.

Identifiant : mntnnc
Mot de passe : a***n

- Serveur NAS

Le serveur est situé dans la **DMZ privée** et a pour adresse **192.168.14.26/25**.
Il permet le stockage de toutes les configurations des serveurs ainsi que de paquets pour l'installation de ceux-ci.
Un script exécuté chaque jour via cron automatise la récupération des configurations. En cas d'erreur, les informations sont stockées dans un fichier de log et envoyées par mail au chef de service.

Identifiant : mntnnc
Mot de passe : a***n

- Service PROXY

Le serveur est situé dans la **DMZ privée** et a pour adresse **192.168.14.27/25**.
Les utilisateurs doivent obligatoirement s'authentifier afin d'utiliser internet. Les identifiants du serveur AD sont récupérés par le serveur proxy par le protocole **NTLM**.

Le proxy filtre aussi les contenus illicites et inappropriés à l'utilisation d'un poste professionnel grâce à une blacklist nationale mise à jour chaque semaine via un script.

Identifiant : mntnnc
Mot de passe : a***n

- Serveur rebond

Le serveur est situé dans la **DMZ publique** et a pour adresse **192.168.14.140/25**.
Un redirection DNAT est en place sur le routeur Lardier pour permettre l'accès au service ssh via le port 2207 en pointant le nom DNS **p7.btsinfogap.org**, ainsi qu'à l'interface web du service guacamole sur le port 8080.
L'application Fail2ban est également installée sur le serveur afin de se prémunir face aux attaques en force brute.

Identifiant : mntnnc
Mot de passe : a***n

- Serveur Web

Le serveur est situé dans la **DMZ publique** et a pour adresse **192.168.14.253/30** ceci permet de s'assurer que le serveur ne puisse pas communiquer avec le reste du réseau.
Il héberge le CMS Wordpress par lequel le site vitrine de NewWordlSA est maintenu.
Un redirection DNAT est en place sur le routeur Lardier pour permettre l'accès au site via le nom DNS : p7.btsinfogap.org .

Identifiant : mntnnc
Mot de passe : a***n

- Serveur SNMP

Un serveur SNMP est installé dans la **DMZ privée** à l'adresse **192.168.14.42/25**. Installé sous Debian avec la solution Zabbix 6.0, il sert à la supervision de tous les matériels du SI (Routeurs, switchs, serveurs...). La gestion du serveur se fait par une interface web disponible à l'adresse : **http://zabbix.nw07-btsinfogap.org.**
Ce service permet la remontée d'information de tous les matériels du réseau, ainsi que l'envoie de mail aux chefs de service en cas d'incident majeur.

Identifiant : mntnnc
Mot de passe : z****x

- Serveur Syslog

Un serveur Syslog est installé dans la **DMZ privée** à l'adresse **192.168.14.43/25**. Installé sous Debian 11 avec la solution Graylog, le serveur récupère les logs de tous les serveurs. Afin de générer par la suite différentes alertes en cas d'attaques ou d'arrêt d'un service.
Le serveur est géré par une interface web à l'adresse :
http://syslog.nw07-btsinfogap.org:9000.

Identifiant : admin
Mot de passe : U****W**1*A***W***9

- Accès à distance

Une solution de prise en main à distance des postes clients du réseau NewWorld est mise en place grâce à AnyDesk.

Mot de passe d'administration : A***w***9

- Filtrage

Afin de sécuriser les accès du réseau, des ACL (Access Control List) ont été mises en place sur les routeurs Cisco. Ci-dessous, le détail des accès configurés :

Les réseaux **LAN** n'ont pas accès directement à Internet, il doit passer obligatoirement par le serveur PROXY.

CoeurSi :

- Accès aux services fournis par la DMZ privée (DHCP, DNS, Proxy, AD).
- Peut accéder à toutes les machines du réseau en ssh.
- Peut accéder au serveur AD via le protocole RDP.
- Peut ping toutes les machines du réseau.
- Accès à l'interface web d'Apache Guacamole.

Wifi :

- Accès aux services fournis par la DMZ privée (DHCP, DNS, Proxy, AD).
- Le point d'accès peut accéder aux services du serveur RADIUS.

Direction, DC, Logigot :

- Accès aux services fournis par la DMZ privée (DHCP, DNS, Proxy, AD).

WAN :

- Autorisation des accès aux applications bénéficient du NAT/PAT .

DMZ privée :

- Le serveur ZABBIX peut contacter les agents du réseau (switchs, routeurs, WAP) via SNMP.
- Les 2 serveurs DHCP peuvent communiquer avec le relais DHCP (Routeur Lardier)
- Tous les serveurs ont accès à internet en TCP, UDP et ICMP.
- Le serveur PROXY peut accéder à l'interface web du WAP.

DMZ publique :

- Le serveur REBOND peut accéder aux serveurs de la DMZ privée en SSH.
- Le serveur REBOND peut accéder au Routeur Sisteron en SSH.
- Le serveur REBOND a accès au serveur AD via RDP.
- Le serveur REBOND peut contacter le serveur SYSLOG sur le port 5140 en TCP.
- Le serveur WEB n'a accès qu'à sa passerelle.

Pour plus de détails consulter le tableur → ACLs