



GS11 – TECHNIQUES DE SECURISATION

Projet SSI : Sécuriser l'infrastructure SI d'une entreprise



Axel NICOLAS

Antoine PINON

Automne

Table des Matières

2	Architecture logique du SI	2
2.1	Choix d'architecture	2
2.2	Configuration des VLANs	3
2.3	Plan d'adressage IP	3
3	Pare-feu VyOS	3
3.1	Accès Internet et NAT/PAT/Port-forwarding	4
3.2	Domaine Active Directory	4
3.3	DMZ	4
3.4	Accès Management	4
3.5	Invité	4
4	Switch CISCO	4
5	Serveur Web	5
5.1	Installation du service et création de l'utilisateur <i>webadmin</i>	5
5.2	Gestion des droits	5
5.3	Durcissement de la configuration	6
6	Active Directory	6
6.1	Stratégie d'annuaire	6
6.2	Installation des rôles AD et DNS	7
6.3	Configuration des UO, des groupes et des utilisateurs	7
6.4	Stratégies de groupe (GPO)	7

Table des Illustrations

Figure 1:	Schéma d'Architecture du SI	2
Figure 2:	Simulation du SI sous Packet Tracer	5
Figure 3:	Ogranisation de l'entreprise "MonBeauReseau"	6
Figure 4:	Configuration du service DNS - Zone de recherche inversée	7
Figure 5:	UOs et Groupes de sécurité	7
Figure 6:	Utilisateurs et Compte à privilège	7
Figure 7:	Stratégies de groupe configurées	8

Note de Synthèse

Pour ce projet, nous nous plaçons en tant qu'administrateur réseau d'une petite entreprise qui cherche à améliorer la sécurité de son Système d'Information afin de protéger ses informations et limiter sa surface d'attaque.

L'objectif est de simuler une architecture réseau simple et d'en sécuriser les différents éléments incluant :

- Un pare-feu, on utilise ici la distribution Linux spécialisée VYOS ;
- Un switch Cisco ;
- Un serveur web Apache httpd sous Linux (*Ubuntu Server*) ;
- Un contrôleur de domaine Active Directory sous *Windows Server 2016* ;
- Un poste de travail client et un poste d'administration, tous deux sous *Windows 10 Entreprise* ;

Pour ce faire, nous utiliserons les outils de virtualisation suivants :

- GNS3 2.2.16
- VMware Workstation 15.1.
- Packet Tracer 7.2.2

Ce document présentera tout d'abord l'architecture réseau qui a été choisie. Les sections qui suivent résumeront les diverses actions entreprises sur chaque composant du SI.

1 Architecture logique du SI

1.1 Choix d'architecture

Puisque nous n'avons pas de routeur en aval du pare-feu, celui-ci fonctionnera dans une architecture "Router-on-a-stick", on doit donc créer une sous-interface (ou interface virtuelle) pour chaque VLAN présent dans notre LAN. La connexion entre le switch de distribution et le Firewall se fait alors via un lien 802.1q (Trunk). Le routage du trafic inter-VLANs a lieu quant à lui au niveau du pare-feu.

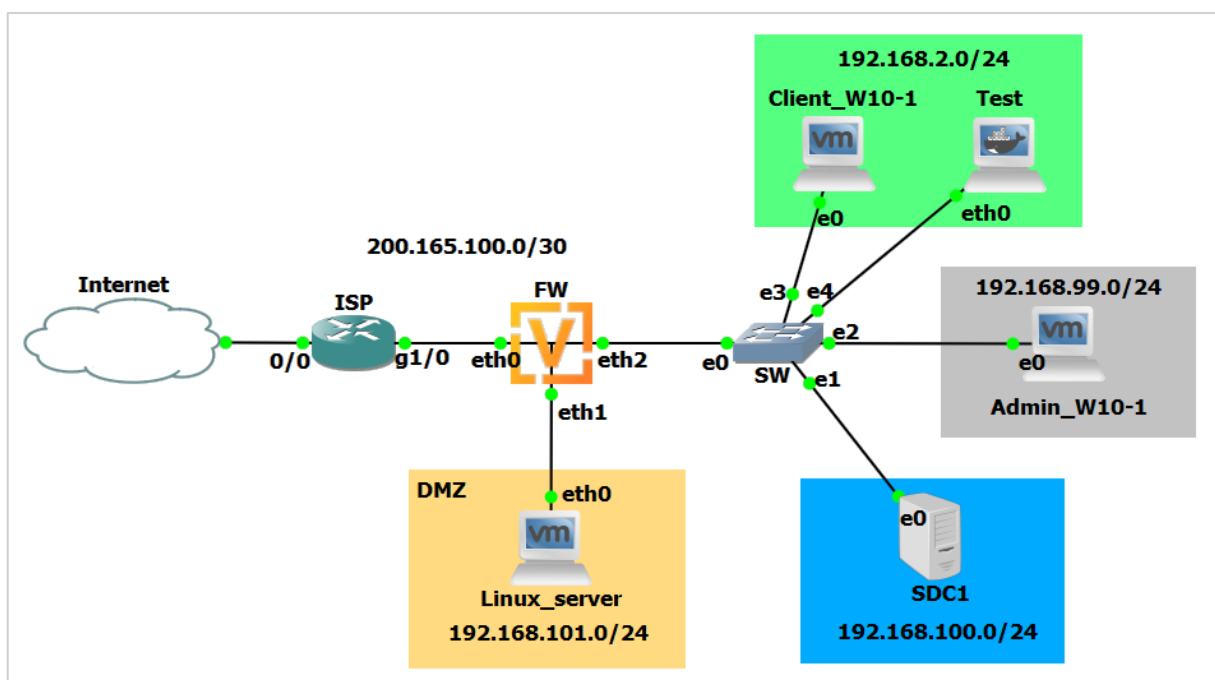


Figure 1: Schéma d'Architecture du SI

Trois VLANs dédiés ont été créés pour isoler les postes utilisateur, les postes administration et les serveurs. Un quatrième VLAN nommé "invité" a ensuite été ajouté comme *failover*.

Conformément aux bonnes pratiques de sécurité, on mettra en place une DMZ pour les serveurs accessibles depuis l'extérieur, dans notre cas, le serveur web de notre entreprise fictive.

Enfin, l'accès à Internet passe par un routeur Cisco qui joue le rôle du fournisseur d'accès. Le lien vers Internet à proprement parler est réalisé par l'objet GNS3 « Cloud », fonctionnant sur le serveur local et relié à une interface VMWare configurée en tant que NAT (par défaut *VMware Network Adapter VMnet8*). Symbolisé par un nuage sur le schéma ci-dessous, cet objet interconnecte le réseau virtuel et la machine physique qui elle, possède une connexion à Internet.

Notez qu'un conteneur *docker Ubuntu* a été rajouté à la simulation pour faciliter les tests de connectivité et d'accès aux ressources (pages web, connexion SSH, etc.) sur le réseau.

1.2 Configuration des VLANs

Nom du VLAN	Numéro du VLAN
UTILISATEURS	2
INVITE	5
MAINTENANCE	99
SERVEURS	100

1.3 Plan d'adressage IP

Equipement	Interface	Adresse Ipv4	Masque	Gateway
Routeur ISP	G0/0 (vers INTERNET)	DHCP (auto)	DHCP (auto)	DHCP (auto)
	G1/0 (vers FW)	200.165.100.1	255.255.255.252	-
FW	eth0 (vers ISP)	200.165.100.2	255.255.255.252	-
	eth1 (vers DMZ)	192.168.101.254	255.255.255.0	-
	eth2.2	192.168.2.254	255.255.255.0	-
	eth2.5	192.168.5.254	255.255.255.0	-
	eth2.99	192.168.99.254	255.255.255.0	-
	eth2.100	192.168.100.254	255.255.255.0	-
SW	VLAN99	192.168.99.128	255.255.255.0	-
Linux_server	eth0 (vers FW)	192.168.101.1	255.255.255.0	192.168.101.254
Client_W10-1	e0	192.168.2.1	255.255.255.0	192.168.2.254
Admin_W10-1	e0	192.168.99.1	255.255.255.0	192.168.99.254
SRVDC1	e0	192.168.100.1	255.255.255.0	192.168.100.254

2 Pare-feu VyOS

Comme indiqué précédemment, nous avons utilisé la distribution Linux VYOS, conçue spécialement pour le routage, pour simuler notre pare-feu. L'avantage étant la simplicité de configuration des fonctionnalités réseau et l'accès à tous les outils Linux, la fonction de pare-feu est d'ailleurs assurée par *netfilter (iptables)*. Toutefois, il n'est pas recommandé de faire trop de modifications directement sur le système, puisque si la configuration réelle et la configuration enregistrée diffèrent trop, des bogues peuvent apparaître. Pour cette raison, nous sommes passés par l'interface dédiée pour configurer le Firewall et non par un fichier *iptables.sh* classique.

Ainsi, nous avons configuré les interfaces et sous-interfaces du pare-feu, le mode Trunk sur le lien vers le switch ainsi que le routage.

2.1 Accès Internet et NAT/Port-forwarding

Nous avons ensuite mis en place du NAT pour que les machines du LAN puissent accéder à Internet. Un port-forwarding a été configuré pour que les utilisateurs externes aient accès au site web de l'entreprise sur l'adresse IP publique du pare-feu en passant par les ports 80 (HTTP) et 443 (HTTPS). Puisque nous ne sommes pas dans une configuration de type « Split-DNS », on met également en place du « NAT Reflection » pour que les utilisateurs du LAN accèdent au site web de la même manière, sans passer par l'adresse privée.

2.2 Domaine Active Directory

Pour que les machines du LAN accèdent au domaine AD, on autorise les ports suivants vers le contrôleur de domaine :

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

2.3 DMZ

Le trafic émanant de la DMZ est bloqué s'il ne fait pas partie d'une connexion déjà établie.

2.4 Accès Management

Grâce à trois *LOCAL POLICY* (WAN, DMZ et LAN), tous les accès locaux (sur le Firewall) sont bloqués sauf pour le management par SSH. Le poste administrateur peut également se connecter au routeur, au switch et au serveur Linux en SSH et à l'AD par Terminal Server (3389) et MMC.

2.5 Invité

Les postes utilisateur du VLAN invité ne peuvent qu'aller sur Internet. Ils n'ont aucun accès au reste du LAN puisque l'on bloque toutes les connexions vers les adresses *rfc1918* (Adresses IPv4 privées).

3 Switch CISCO

Le Switch de niveau 2 a été simulé avec une version simplifiée du SI sur *Packet Tracer*.

Une configuration minimale a été implémentée conformément aux instructions de Cisco (cf. Cours du CCNA). Elle pose des bases de sécurité comme l'accès à la console restreint par mot de passe et le chiffrement des identifiants enregistrés.

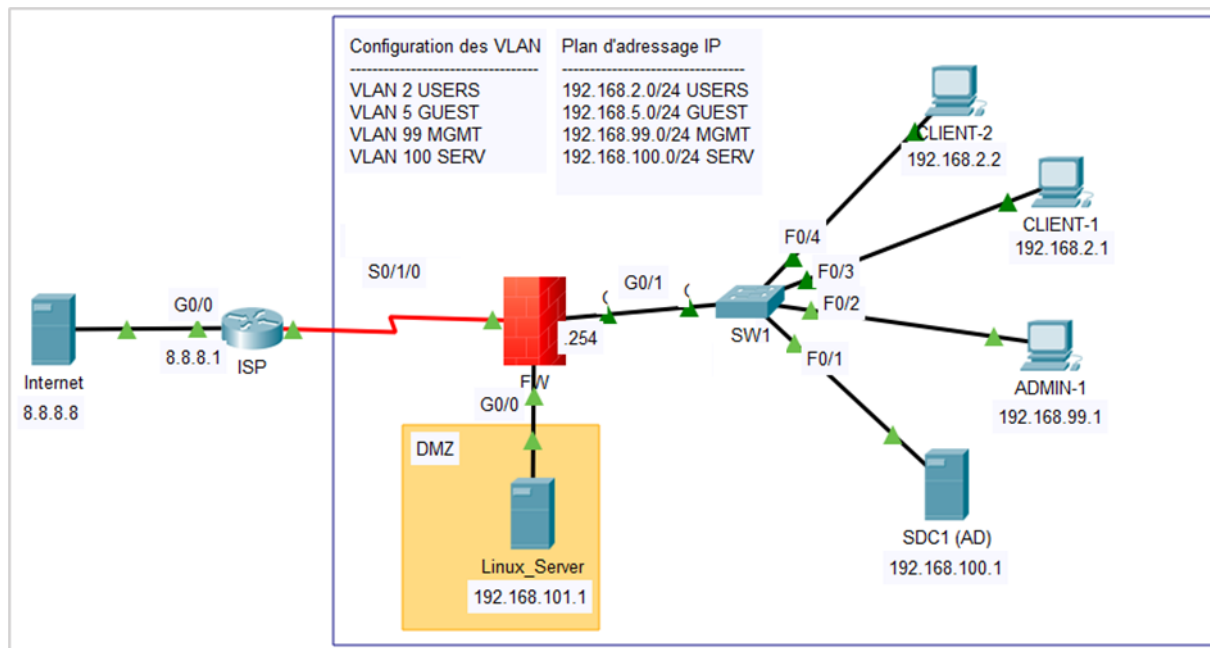


Figure 2: Simulation du SI sous Packet Tracer

Les 4 VLANs, le mode accès sur les interfaces, le lien Trunk vers le pare-feu ainsi que l'interface de gestion ont ensuite été configurés.

Concernant la remédiation aux attaques ARP, nous utilisons la fonction *port-security* pour limiter le nombre d'équipements associés à un port physique. La restriction est appliquée sur chaque interface selon l'adresse MAC de l'équipement connecté.

4 Serveur Web

4.1 Installation du service et création de l'utilisateur *webadmin*

Nous avons installé le service Apache2 sur la dernière distribution d'Ubuntu Server disponible. La première étape a ensuite été de créer la racine dans `/var/www/html/www.monbeaureseau.com/` et de configurer et d'activer un « Hôte virtuel » pour notre site Web.

Une fois le site en place, nous avons créé l'utilisateur « *webadmin* » avec la commande *useradd*. Nous l'avons ajouté au groupe *www-data* et doté d'un mot de passe par la même occasion.

4.2 Gestion des droits

À l'aide de la commande *chown*, on passe l'utilisateur *webadmin* en propriétaire du répertoire racine `/var/www`.

On utilisera une variante pour que *www-data* ne puisse que lire et exécuter dans `/var/www`. Puisque les droits de lecture, d'écriture et d'exécution n'ont pas la même signification pour un répertoire ou pour un fichier, on utilise la commande *find* en complément de la commande *chown* :

```
find /var/www -type d | xargs chmod 750 # drwx r-x ---
find /var/www -type f | xargs chmod 650 # -rw- r-x ---
```

Pour la suite, nous devons attacher des droits pour l'utilisateur www-data à des dossiers et fichiers gérés par l'utilisateur root. Cette fois-ci, il n'est pas prudent de changer le propriétaire des dits fichiers, ni d'ajouter des droits excessifs aux autres utilisateurs, c'est pourquoi nous avons utilisé des ACLs.

À l'aide de la commande *setfacl*, on peut facilement définir des restrictions d'accès pour que www-data puisse lire et modifier les fichiers dans */var/log*, mais pas les exécuter et qu'il puisse lire et exécuter les fichiers dans le répertoire */etc/apache2*.

On peut également utiliser les ACL pour s'assurer que tout fichier créé correspond à la politique de permissions en permettant aux fichiers et répertoires d'hériter les ACLs.

4.3 Durcissement de la configuration

Pour réduire la surface d'attaque, nous avons appliqué certaines des recommandations présentées dans le cours GS11 sur la sécurisation des serveurs web telles que :

- La limitation des accès au strict nécessaire dans *apache2.conf*
- Les bonnes pratiques pour limiter les fuites d'information dans *security.conf*
- La suppression des fichiers inutiles (*htdocs*, *cgi-bin*)
- Le verrouillage des comptes inutilisés
- Etc.

5 Active Directory

5.1 Stratégie d'annuaire

Avant de déployer un contrôleur de domaine, il convient de penser une stratégie d'annuaire. Pour ce faire, la méthodologie la plus simple est de :

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

Pour l'entreprise « MonBeauReseau », on présumera de l'organisation suivante :

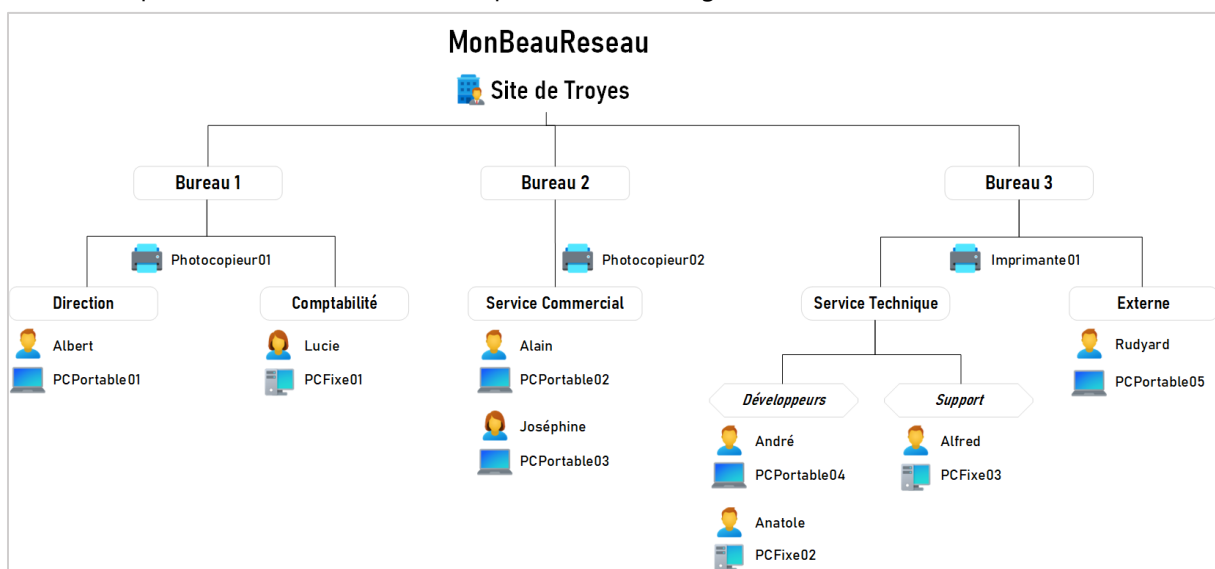
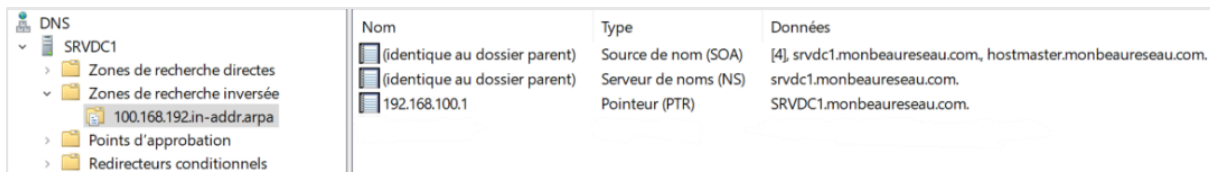


Figure 3: Ogranisation de l'entreprise "MonBeauReseau"

5.2 Installation des rôles AD et DNS

Dans notre cas, nous ferons le choix d'installer une nouvelle forêt avec un seul domaine pour représenter la société « *Mon beau réseau* ». Ce choix est le plus courant et possède divers avantages, entre autres, il permet d'avoir un domaine unique appelé *domaine racine*.

Pour que les utilisateurs puissent rejoindre le domaine AD, il faut ensuite créer une zone de recherche inversée ainsi qu'un pointeur PTR associé au contrôleur de domaine dans le service DNS.



Nom	Type	Données
(identique au dossier parent)	Source de nom (SOA)	[4], srvdc1.monbeaureseau.com, hostmaster.monbeaureseau.com.
(identique au dossier parent)	Serveur de noms (NS)	srvdc1.monbeaureseau.com.
192.168.100.1	Pointeur (PTR)	SRVDC1.monbeaureseau.com.

Figure 4: Configuration du service DNS - Zone de recherche inversée

5.3 Configuration des UO, des groupes et des utilisateurs


Pour la création des UO, on reprendra l'organigramme ci-dessus en rajoutant un dossier pour les groupes de sécurité et un autre pour les partages éventuels. On crée également un groupe par service en suivant une nomenclature : GG pour Groupe Global, U pour Utilisateur et R pour Ressource.



Nom	Type
Troyes_GG_R_Imprimante_B1	Groupe de sécurité - Global
Troyes_GG_R_Imprimante_B2	Groupe de sécurité - Global
Troyes_GG_R_Imprimante_B3	Groupe de sécurité - Global
Troyes_GG_R_Serveurs	Groupe de sécurité - Global
Troyes_GG_U_Comptabilite	Groupe de sécurité - Global
Troyes_GG_U_Developpement	Groupe de sécurité - Global
Troyes_GG_U_Direction	Groupe de sécurité - Global
Troyes_GG_U_Management	Groupe de sécurité - Global
Troyes_GG_U_Manager Commercial	Groupe de sécurité - Global
Troyes_GG_U_Manager Developpement	Groupe de sécurité - Global
Troyes_GG_U_Service Commercial	Groupe de sécurité - Global
Troyes_GG_U_Support	Groupe de sécurité - Global
Troyes_GG_U_SysAdmin	Groupe de sécurité - Global

Figure 5: UOs et Groupes de sécurité

On ajoute ensuite les utilisateurs et l'on joint nos machines au domaine. Les administrateurs doivent avoir des comptes nommés et puisqu'il n'est nul besoin d'être systématiquement connecté en tant qu'utilisateur à privilège, on crée deux comptes pour l'administrateur système de l'entreprise.



Nom	Type
Alfred de Vigny	Utilisateur
Alfred De Vigny - Admin	Utilisateur

Figure 6: Utilisateurs et Compte à privilège

5.4 Stratégies de groupe (GPO)

Pour cette partie, nous avons configuré les GPO suivantes :

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

- **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.
- **Stratégie de Restriction Logicielle (SRP)** : Une restriction est appliquée sur les postes pour n'autoriser que les programmes des répertoires Windows sauf *tmp*.
- **Terminal Server** : Le port 3389 est ouvert, mais l'administrateur local des postes n'est pas accessible à distance.



D'autres GPO ont été ajoutés comme *PolitiqueAudit* et *SecuriteServeur-Global*. Elles implémentent les éléments de sécurité décrits dans le cours GS11 sur la sécurité des OS Windows et son annexe.

Figure 7: Stratégies de groupe configurées