Projet d'Interconnexion

Rapport technique

Maxime Garlatti
Tristant Moreau
Haytham Zaabool
Arthur Sauvezie
Anas Sabir
Alexandre Mohib

23 janvier 2026

Table des matières

Chapitre 1

Introduction et objectifs

Ce projet vise à concevoir et valider une architecture réseau réaliste articulée autour :

— d'un réseau d'entreprise (services internes, politiques de sécurité, accès contrôlé) ;
— d'un accès distant via une zone privée de type « box » ;
— d'un tunnel VPN permettant l'accès sécurisé aux ressources internes ;
— du déploiement de services applicatifs (Web, FTP, VoIP.).

Chapitre 2

Architecture globale

2.1 Topologie

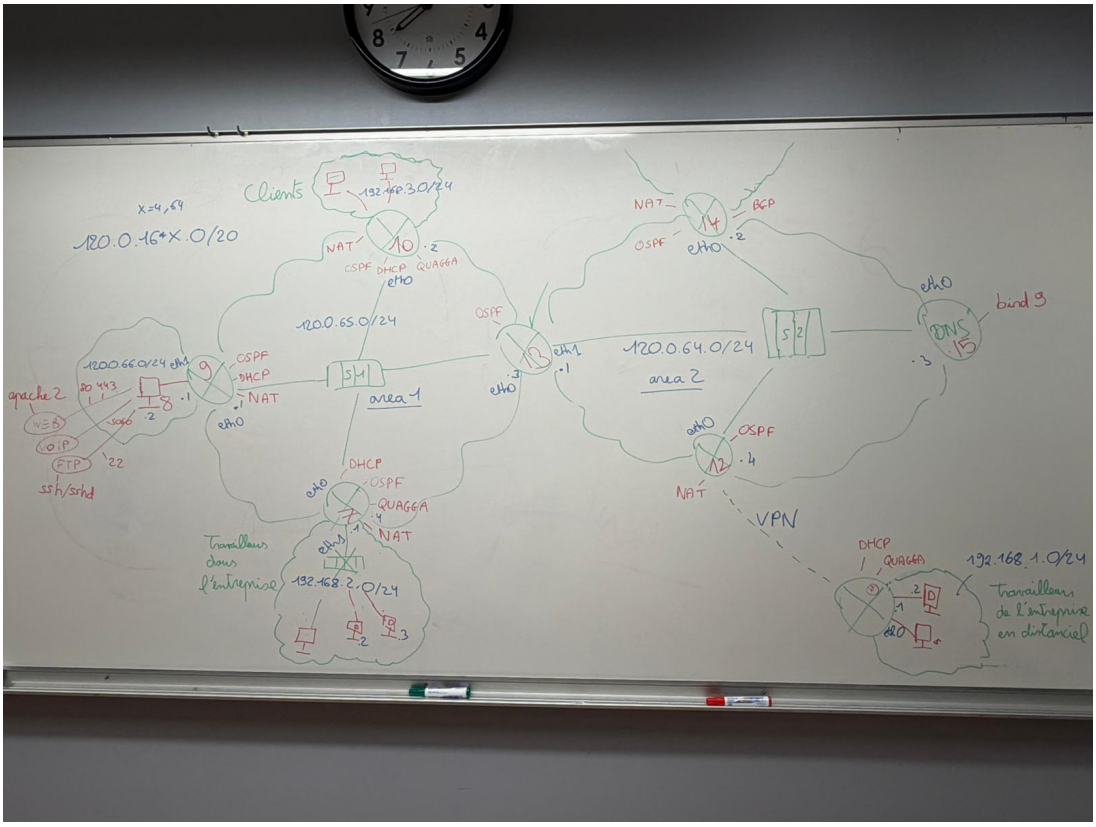

FIGURE 2.1 – Schéma de la topologie réseau

Chapitre 3

Stratégie de routage

3.1 Choix d'OSPF et justification

3.1.1 Justification du choix

OSPF (Open Shortest Path First) a été retenu car il :

— converge rapidement en cas de panne de lien ou de modification de topologie ;

— permet une structuration hiérarchique par *areas* ;

— simplifie la maintenance par rapport à un routage statique dès que la topologie devient non triviale.

3.1.2 Périmètre OSPF

OSPF est activé sur l'ensemble des liens internes au système autonome ainsi que pour l'interconnexion :

— liens routeur-routeur au sein de l'AS ;

— interfaces vers les LAN internes (entreprise/services) ;

— lien entre les autres AS.

Chapitre 4

Services applicatifs

4.1 Serveur FTP

4.1.1 Objectif

L'objectif est de fournir un service FTP accessible dans le périmètre défini (réseau interne et/ou via VPN), avec une politique d'accès compatible avec les contraintes de comptes utilisateurs sur les machines.

4.1.2 Déploiement sous contraintes

Dès les premières étapes, une contrainte technique majeure a été identifiée : l'exécution de la commande *vsftpd –version* indiquait que le démon vsftpd n'était pas installé sur le système.

Par ailleurs, l'absence d'accès à Internet sur les machines constituait une limitation supplémentaire, rendant impossible toute installation classique via un gestionnaire de paquets en ligne. Cette double contrainte a représenté le premier défi dans la mise en œuvre du serveur FTP.

4.1.3 Choix de mode d'accès : authentification vs accès anonyme

Le fonctionnement standard d'un serveur FTP repose sur des comptes locaux. Or, dans le contexte des postes disponibles, l'utilisation de comptes exploitables n'était pas réaliste. Une configuration alternative a donc été retenue : un accès anonyme, permettant une connexion sans identifiants, tout en conservant un contrôle strict sur les droits d'écriture.

4.1.4 Solution trouvée

Afin de contourner cette limitation, une solution d'installation hors ligne a été étudiée et mise en œuvre.

Dans un premier temps, la version exacte du système et du noyau a été identifiée à l'aide de la commande *uname -a*, permettant de déterminer la version d'Ubuntu utilisée ainsi que les dépendances associées. Sur une machine disposant d'un accès Internet, le paquet vsftpd correspondant a ensuite été téléchargé, puis transféré sur la machine cible à l'aide d'une clé USB.

L'installation locale du service a été réalisée via l'outil *dpkg*, suivie du redémarrage du démon à l'aide de la commande *sudo systemctl restart vsftpd*, ce qui a permis de lancer correctement le serveur FTP.

4.1.5 Configuration et adaptation du serveur FTP

Une fois le service opérationnel, une tentative de connexion au serveur a été effectuée en utilisant la commande `ftp`, suivie de l'adresse IP de la machine hébergeant le service. À ce stade, le serveur exigeait une authentification par nom d'utilisateur et mot de passe. Or, dans le contexte des machines de l'établissement, aucun compte utilisateur avec des identifiants exploitables n'était disponible. Cette contrainte rendait impossible l'utilisation du serveur FTP dans son mode d'authentification standard.

Pour résoudre ce problème, une analyse approfondie de la documentation officielle de `vsftpd` a été menée. Celle-ci a mis en évidence la possibilité de configurer un serveur FTP anonyme, permettant un accès sans authentification. Cette configuration a nécessité la modification du fichier de configuration du service, notamment l'activation explicite des connexions anonymes. Après application des changements et redémarrage du démon, l'accès au serveur FTP anonyme a pu être validé avec succès.

Cependant, bien que la connexion au serveur fût désormais possible, les opérations de dépôt de fichiers n'étaient pas autorisées. Cette limitation s'expliquait par l'absence d'une arborescence adaptée et par des droits d'accès insuffisants sur le système de fichiers. Une structure spécifique a donc été mise en place, comprenant un répertoire racine dédié au service FTP, contenant un sous-répertoire `uploads`. Ce dernier a été configuré avec des permissions appropriées afin d'autoriser l'écriture et la lecture des fichiers par les utilisateurs anonymes, tout en conservant un contrôle minimal sur la sécurité du système. La gestion rigoureuse des droits d'accès s'est ainsi révélée déterminante pour assurer le bon fonctionnement du serveur FTP dans ce contexte contraint.

4.2 VOIP

4.2.1 Introduction

Cette partie décrit la mise en place d'un service de téléphonie d'entreprise dans un contexte contraint.

4.2.2 Choix de la solution technique

Dans le cadre du projet, on devait mettre en place un service de téléphonie (VoIP) pour permettre la communication vocale au sein de l'entreprise. Normalement, la solution standard sur Linux repose sur le serveur Asterisk. Toutefois, on a rencontré le même blocage technique que pour le FTP : les machines de l'école ne permettaient pas d'installer de nouveaux services complexes ou n'avaient pas les accès nécessaires pour configurer Asterisk correctement.

Pour contourner cette limitation, on a décidé de changer d'approche et d'héberger le service sur une machine personnelle sous Windows. On a choisi d'utiliser 3CX.

4.2.3 Mise en œuvre et validation

Une fois le serveur 3CX installé sur l'ordinateur personnel, il fallait des téléphones pour tester les appels. Comme on ne disposait pas de téléphones IP physiques (hardphones) ou d'un routeur téléphonique spécifique, on a utilisé la machine elle-même comme un "softphone". Un softphone est un logiciel qui simule un téléphone physique directement sur l'ordinateur.

Concrètement, on a configuré le serveur 3CX pour gérer les extensions (les numéros internes) et on a installé l'application cliente 3CX sur le même ordinateur. Cela nous a permis de valider que le serveur fonctionnait bien : on a pu s'enregistrer sur le standard et simuler le fonctionnement d'un poste téléphonique d'entreprise, malgré les contraintes matérielles.

Chapitre 5

Sécurité et Services Réseau

5.1 Pare-feu

Introduction

La sécurisation des services exposés constitue un élément central de l'architecture mise en place. Le filtrage réseau repose sur une politique stricte appliquée au niveau du routeur d'accès aux services.

5.1.1 Politique de filtrage

La mise en production d'un serveur FTP dans un réseau d'entreprise impose l'utilisation d'une politique de filtrage stricte, afin de limiter la surface d'attaque et de garantir que seuls les flux légitimes atteignent les services internes (FTP, serveur Web, VoIP). Dans notre architecture, cette fonction de filtrage est assurée principalement par le routeur N9, qui joue le rôle de passerelle vers le réseau des services. Le principe retenu est un modèle *"deny by default"* : tout trafic est bloqué par défaut, puis des exceptions explicites sont ajoutées uniquement pour les flux autorisés.pl

Ainsi, au niveau du routeur N9, seules les requêtes provenant d'adresses IP considérées comme trusted (réseaux internes des AS de l'entreprise) sont autorisées à transiter vers le réseau des services. Toute source externe ou non reconnue est systématiquement bloquée. Dans le cas des employés se connectant à distance via un VPN, une stratégie de NAT (masquerade) est mise en œuvre : les clients VPN reçoivent une adresse "trusted" lors de la sortie vers les services internes, ce qui leur permet d'accéder aux services de l'entreprise (FTP, Web, VoIP) sans ouvrir le réseau à des sources non maîtrisées.

5.1.2 Restriction côté clients

Par ailleurs, une restriction supplémentaire a été appliquée côté clients selon la logique de l'architecte réseau : les postes clients sont supposés transiter via le routeur N10, identifié par l'adresse IP *120.0.65.2*. Dans ce modèle, le pare-feu autorise uniquement les flux provenant de cette adresse IP vers les ports nécessaires au serveur Web, ce qui permet de cloisonner l'accès et d'empêcher des postes non autorisés de contacter directement certains services. Cette approche renforce la sécurité globale en appliquant un contrôle d'accès par origine, en plus du filtrage par port et protocole.

5.2 VPN

5.2.1 Introduction

Cette section présente la mise en place du tunnel sécurisé reliant le réseau privé distant à l'infrastructure de l'AS.

5.2.2 Architecture du VPN

Le VPN relie deux extrémités :

— Le routeur d'entrée de l'AS, dont l'adresse IP dans le réseau de l'entreprise est 120.0.64.4

— La box représentant les utilisateurs distants, dont l'adresse dans le réseau privé est 192.168.1.1

Ce VPN permet à des clients situés dans le réseau privé d'accéder aux ressources internes de l'AS de manière sécurisée. Les machines mises à disposition par l'école disposent déjà d'OpenVPN, j'ai donc choisi cette solution.

5.2.3 Génération et échange de la clé

La première étape consiste à générer une clé de chiffrement partagée à l'aide de la commande suivante sur le routeur de l'AS :

```
openvpn --genkey --secret /etc/openvpn/secret.key
```

Cette clé doit être présente sur les deux extrémités du tunnel afin de permettre le chiffrement et l'authentification des échanges. Cependant, les postes de l'école ne permettent pas le transfert direct de fichiers. Il a donc été nécessaire de copier manuellement le contenu de la clé (via clé USB) sur la machine représentant la box.

Ce choix impose l'utilisation d'un VPN statique point-à-point, basé sur une clé prépartagée, et non d'un VPN de type client/serveur avec certificats.

5.2.4 Configuration du tunnel

Le tunnel VPN est configuré de type point-à-point, avec le sous-réseau virtuel : 10.255.255.0/30

— Routeur AS : 10.255.255.1

— Box : 10.255.255.2

L'interface virtuelle créée par OpenVPN est tun0. Tout le trafic destiné au réseau distant est routé à travers cette interface.

5.2.5 Routage et règles de transit

Pour autoriser le transit des paquets, l'IP forwarding est activé sur les deux routeurs, et des règles iptables sont ajoutées afin d'autoriser le trafic entre :

— le tunnel VPN (tun0)

— le réseau privé (192.168.1.0/24)

— le réseau de l'AS (120.0.64.0/24)

5.2.6 NAT et intégration dans l'AS

De plus, un mécanisme de NAT (MASQUERADE) est mis en place sur le routeur de l'AS. Ce NAT permet de masquer les adresses privées des clients distants.

Ainsi, les paquets provenant du client sont vus par le reste de l'AS comme provenant de l'adresse 120.0.64.4, ce qui est compatible avec les règles de sécurité internes du réseau de l'entreprise. Les réponses reçues par le routeur 120.0.64.4 sont ensuite redirigées à travers le tunnel vers le client distant. Ainsi, ce VPN permet à un client externe d'accéder aux ressources internes de l'AS de manière sécurisée, chiffrée, et contrôlée, tout en respectant les politiques de routage et de sécurité de l'entreprise

5.3 Zone Privée et Gestion des Accès Clients

5.3.1 Introduction

La zone privée vise à simuler un environnement domestique réaliste pour des utilisateurs en télétravail.

La configuration de la zone privée avait pour objectif de simuler de manière réaliste l'environnement domestique des utilisateurs finaux (télétravailleurs). Cette étape a nécessité la transformation de routeurs standards en passerelles résidentielles, fonctionnant sur le modèle des "Box" fournisseurs d'accès internet.

5.3.2 Mise en place du service DHCP

La première brique de cette infrastructure a été la mise en place du service DHCP (Dynamic Host Configuration Protocol) . Cette configuration était indispensable pour automatiser l'attribution des paramètres réseaux aux postes clients connectés au réseau local de la Box (LAN). Le service a été paramétré pour distribuer des adresses IP issues d'une plage privée (192.168.1.0/24), ainsi que l'adresse de la passerelle par défaut et les serveurs DNS, garantissant ainsi une connexion "plug-and-play" pour les machines clientes sans intervention manuelle.

5.3.3 Connectivité WAN et translation d'adresses

Dans un second temps, la question de la connectivité vers le reste du réseau (WAN) a été traitée. Les adresses IP attribuées aux clients étant des adresses privées non routables sur le réseau d'interconnexion, il était impératif de mettre en œuvre un mécanisme de translation d'adresses.

Initialement, avant le déploiement de la solution de tunnelisation, une règle de NAT de type Masquerade a été configurée directement sur l'interface de sortie du routeur "Box". Cette règle permettait de remplacer l'adresse source des paquets sortants (192.168.1.x) par l'adresse publique de la Box, rendant possible la communication transparente entre les clients de la zone privée et les services distants.

5.3.4 Évolution avec l'implémentation du VPN

Toutefois, l'architecture a évolué avec l'implémentation du VPN décrit précédemment. Dès l'activation du tunnel sécurisé, la stratégie de routage et de translation a été modifiée. La fonctionnalité de masquage, initialement portée par l'interface WAN de la Box pour

le trafic général, a été transférée et adaptée au contexte du VPN. Désormais, les flux à destination de l'entreprise sont encapsulés dans le tunnel, et c'est le mécanisme de NAT associé au VPN (sur le routeur de l'AS) qui assure la conformité des adresses, rendant le Masquerade local obsolète pour ces flux spécifiques tout en garantissant une sécurité accrue.

5.4 Authentification

5.4.1 Introduction

Cette partie décrit la mise en place d'un mécanisme d'authentification protégeant l'accès au site web de l'entreprise.

Une authentification est nécessaire pour se connecter de manière sécurisée au site de l'entreprise, son objectif est de sécuriser les données du site web qui pourraient être récupérées par un client depuis l'extérieur de l'entreprise.

5.4.2 Architecture et principe

L'intégralité de l'implantation du service d'authentification est située dans la machine de l'entreprise qui possède la page web (index.html). Ce choix est pertinent car c'est ainsi le serveur qui vérifie les identifiants de connexion du client et non l'inverse. Toutefois, avec un couple identifiant - mot de passe valide, n'importe quel client peut accéder au site de l'entreprise, sans vérification d'adresse IP (même avec un VPN). Cet aspect peut être amélioré avec des règles NAT.

5.4.3 Implémentation

Pour forcer le client à devoir entrer des identifiants de connexion, on modifie tout d'abord le fichier /etc/apache2/apache2.conf, on trouve la ligne correspon- dant à Directory /var/www/ et on remplace le paramètre None de AllowOverride par All. Ce changement permet de consulter le fichier .htaccess avant ouverture de la page web.

On crée d'ailleurs ce fichier .htaccess dans le dossier /etc/apache2/ et on y écrit les lignes suivantes :

```
AuthType Basic
AuthName "Zone Protge"
AuthUserFile /etc/apache2/.htpasswd
Require valid-user
```

Ces lignes correspondent aux paramètres de l'authentification (le type, le nom, le fichier de mots de passe et le critère de connexion). On va d'ailleurs créer le fichier .htpasswd dans le dossier /etc/apache2/.

5.4.4 Fonctionnement

Le fichier .htpasswd est un fichier texte qui contient un couple identifiant - mot de passe valide pour chaque ligne du fichier. Il s'agit donc du fichier qui va être consulté à chaque connexion depuis la machine d'un client avant de lui donner accès au site de l'entreprise.

Après avoir modifié ces fichiers, on n'oublie pas de redémarrer apache2 avec la commande : systemctl restart apache2

Ces étapes faites, le système d'authentification est fonctionnel et pour chaque connexion au site depuis une machine, le serveur demandera de s'identifier avant d'accéder au site.

5.5 DNS

5.5.1 Introduction

Un service DNS a été déployé afin de faciliter l'accès aux ressources internes par nom de domaine.

5.5.2 Objectif

La mise en place d'un service DNS permet de simplifier l'accès au site web de l'entreprise. L'objectif est de permettre aux utilisateurs d'entrer un nom facile à retenir dans leur navigateur (comme www.entreprise.fr) plutôt qu'une adresse IP . Pour réaliser cela, on a utilisé Bind9.

5.5.3 Automatisation de la configuration

Cependant, la configuration de ce service demande de modifier plusieurs fichiers, ce qui peut être long et source d'erreurs. Pour résoudre ce problème, nous avons mis en place un script d'automatisation. Au lieu de tout faire à la main, on peut simplement lancer ce script en lui indiquant le nom de domaine souhaité et l'adresse IP du serveur web.

5.5.4 Fonctionnement du script

Concrètement, lorsqu'on exécute le script, celui-ci vérifie si le domaine existe déjà. Si ce n'est pas le cas, on génère automatiquement le fichier de configuration nécessaire et on y associe le domain name à l'adresse IP du serveur. Enfin, on redémarre le service via le script pour valider les changements. Grâce à cette méthode, on peut rendre le site web accessible par son nom de manière rapide et fiable.

Chapitre 6

Conclusion

Ce projet met en évidence la nécessité d'articuler routage, sécurité (filtrage/NAT) et services applicatifs dans une architecture cohérente. Les principales difficultés provenaient des contraintes d'environnement (hors-ligne, transferts limités) et de l'exigence de cloisonnement, résolues par une démarche progressive et des validations systématiques.