ARCHITECTURE TECHNIQUE

Stephane ANDRE - Elmouatassim HAGGAG

DAT

Historique du document

Date	Version	Auteur	Sections	Objets
25/10/2023	1.0	Elmouatassim / Stephane	ALL	Création du document
01/11/2023	1.1	Elmouatassim / Stephane	ALL	Création Schéma
08/11/2023	1.2	Elmouatassim / Stephane	ALL	Finalisation Document

1. CONTEXTE & OBJECTIFS

Le présent dossier technique a pour objectif de détailler les aspects clés de l'architecture réseau et de sécurité qui sont essentiels pour une PME œuvrant en tant que sous-traitant d'Airbus, une entreprise majeure de l'industrie aéronautique. L'aéronautique est un secteur fortement réglementé et sensible, où la sécurité des données et de l'infrastructure informatique est cruciale.

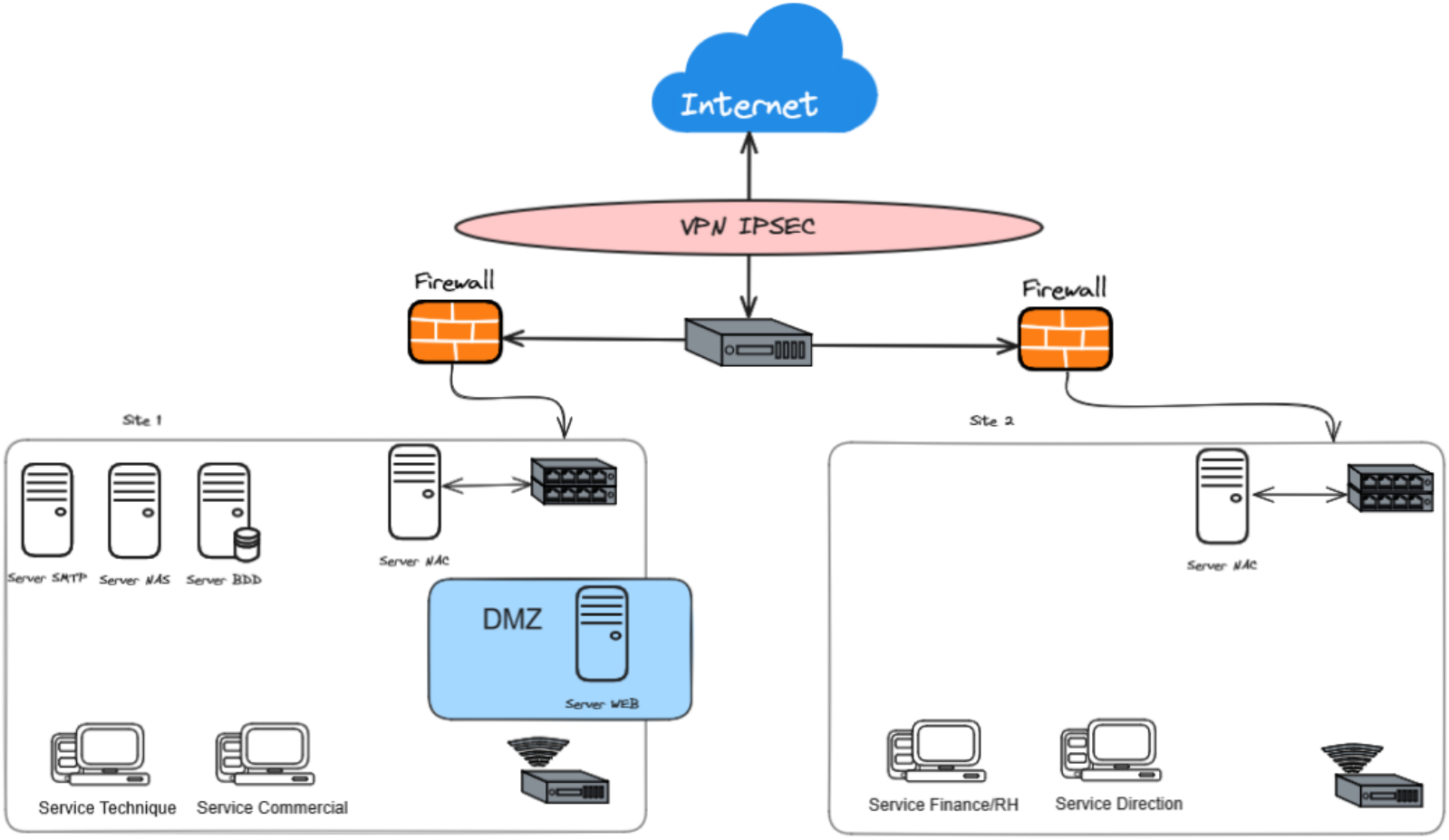
L'objectif de cette architecture technique est de définir les technologies, les produits et les techniques nécessaires pour développer et soutenir le système, et de garantir que les composants du système sont compatibles et conformes aux normes et aux orientations définies par les besoins énoncés par le client. De ce fait cela nous impose de mettre en œuvre des mécanismes capables d'assurer la haute disponibilité

Ce document doit également :

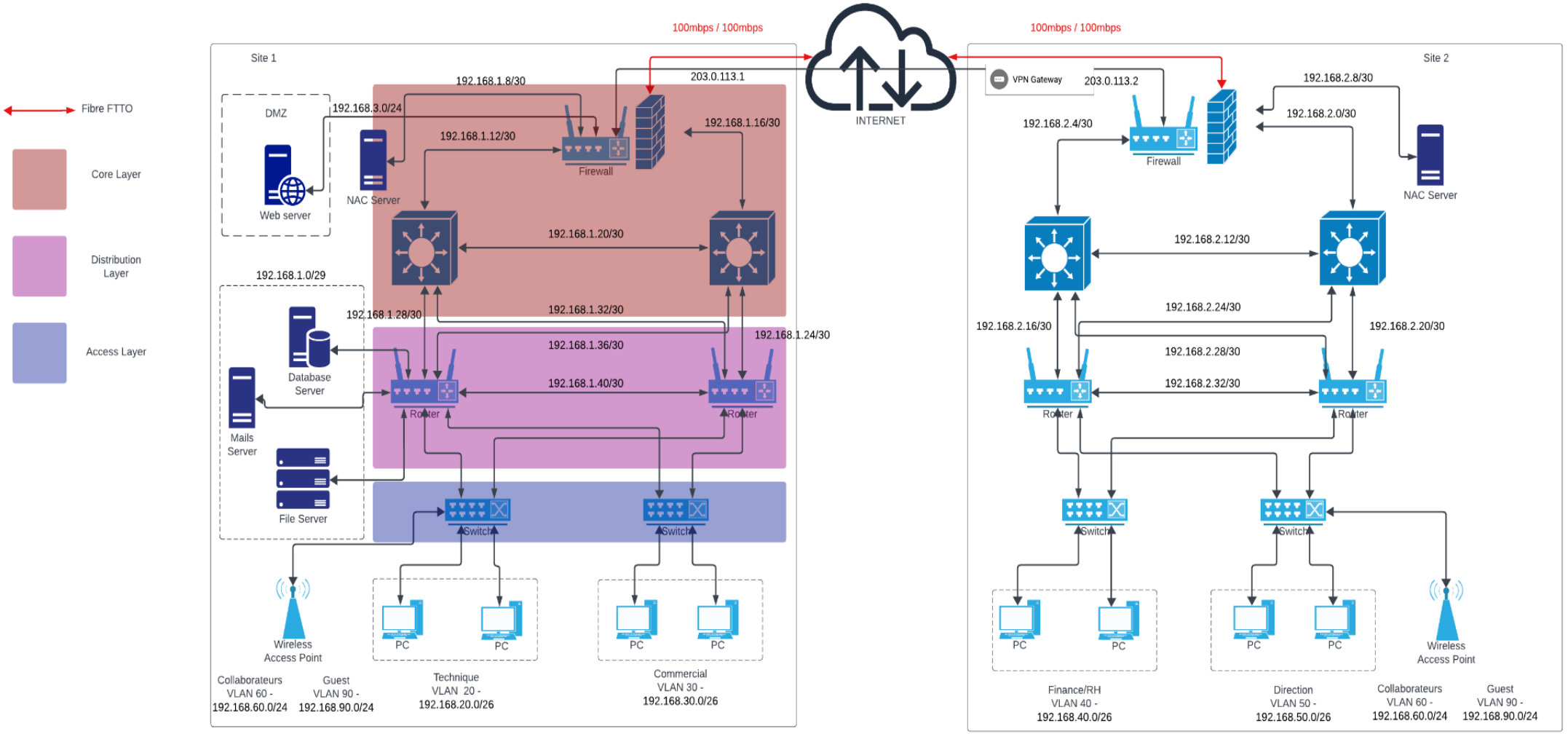
- Identifier et expliquer les risques inhérents à cette architecture technique
- Définir les exigences de base en matière de dimensionnement, d'archivage et de performance ;
- Identifier les spécifications matérielles et logicielles pour les différents types d'environnements ;
- définir des procédures pour la gérer une éventuelle évolution de l'architecture

2. L'ARCHITECTURE TECHNIQUE

a. Schéma Global de l'architecture réseaux



b. Schéma logique de l'architecture réseaux



Services	IP/Masque	VLAN
Technique	192.168.20.0/26	20
Commerciale	192.168.30.0/26	30
Finance	192.168.40.0/26	40
Direction	192.168.50.0/26	50
Collaborateur	192.168.60.0/24	60
Guest	192.168.90.0/24	90

ETUDE DE CAS

En réponse aux besoins évoqués précédemment, nous avons élaboré un plan d'architecture basé sur un modèle de conception à trois niveaux. Ce choix n'est pas uniquement destiné à satisfaire les exigences actuelles, mais également à anticiper les besoins futurs. Ce modèle repose sur cinq principes fondamentaux :

- Hiérarchie : Le modèle propose une organisation en niveaux fonctionnels distincts, à savoir le Core, la Distribution et la couche Access.
- Modularité : Il offre une grande adaptabilité à la croissance et aux changements. L'évolution du réseau est simplifiée par l'ajout de nouveaux modules, évitant ainsi la nécessité de redessiner entièrement l'architecture du réseau.
- Résilience : Le modèle garantit une haute disponibilité (HA) proche des 100 %, assurant ainsi une continuité optimale des services.
- Flexibilité : Il permet une adaptation rapide du réseau aux changements au sein de l'entreprise, répondant ainsi efficacement aux besoins évolutifs.

- Sécurité : La sécurité est intégrée à chaque couche du modèle, assurant une protection globale du système.

Ainsi, notre architecture se concrétise à travers trois couches distinctes : le Core, la Distribution et la couche Access.
Le Core constitue le cœur du réseau. Il est responsable du traitement des données à haute vitesse et de la transmission des informations entre les différents éléments du réseau.
→ Caractéristiques : Haute capacité de bande passante, faible latence. Il agit comme une passerelle centrale, facilitant la communication entre les différents segments du réseau.

La couche de Distribution assure la connectivité entre les différentes parties du réseau, en gérant le flux de trafic entre le Core et la couche Access.
→ Caractéristiques : Contrôle du trafic, segmentation logique du réseau, mise en œuvre de politiques de sécurité. Elle garantit une distribution efficace des données vers les points appropriés du réseau.

La couche Access est la plus proche des utilisateurs finaux et des périphériques. Elle facilite l'accès des utilisateurs au réseau et gère la connectivité locale.
→ Caractéristiques : Gestion des périphériques d'accès (commutateurs, points d'accès), contrôle d'accès aux utilisateurs, segmentation des utilisateurs finaux. Elle offre un point d'entrée sécurisé pour les dispositifs connectés au réseau.

Chaque couche interagit de manière coordonnée pour optimiser les performances, la sécurité et la flexibilité du réseau. Le Core assure la rapidité et la fiabilité du traitement des données, la couche Distribution gère intelligemment le flux de trafic, tandis que la couche Access facilite l'accès sécurisé des utilisateurs finaux au réseau.

En combinant ces trois couches, notre modèle offre une infrastructure robuste et évolutive pour répondre aux besoins variés de l'entreprise.

Nous avons fait le choix de mettre en place une liaison internet fibrée à haute disponibilité avec un débit de 100 Mb/s sur chaque site, le choix de l'offre sera aussi dicté par la qualité de la GTR(Garantie du temps de rétablissement).Pour garantir une qualité maximale de notre connexion fibre, nous avons fait le choix d'une liaison FTTO (Fiber To The Office) qui a l'avantage d'être une fibre dédiée où l'accès internet est uniquement réservé à l'entreprise cliente. En complément, nous mettons en place une ligne ADSL de secours en cas de panne.

Chaque site dispose d'un firewalls pour assurer une sécurité optimale. Les firewalls sont configurés pour établir un VPN avec IPsec, afin de crypter les données entre les deux sites de bout en bout sans fuite possible ce qui permet une communication sécurisée entre les deux sites.
Les Firewall n'ont pas nécessairement besoin d'être du même constructeur, cependant par convenance et par soucis d'homogénéité, nous utilisons du matériels de même constructeur.

Nous avons ensuite fait le choix de mettre en place un Network Access Control (NAC) pour renforcer la sécurité de notre réseau. Le NAC nous permet de contrôler les accès, d'assurer la conformité des périphériques, de détecter les menaces internes, d'améliorer la visibilité, et de simplifier la gestion, tout en contribuant à respecter les réglementations en matière de sécurité.

Le site Web de l'entreprise, étant le principal point d'accès extérieur au réseau de l'entreprise, est placé dans une DMZ (zone démilitarisée) isolée du reste du réseau interne par le firewall.

Placer le site web d'une entreprise dans une DMZ (zone démilitarisée) est une stratégie de sécurité efficace qui isole le site web des réseaux internes, renforce la protection contre les menaces externes, et permet un contrôle d'accès précis pour assurer la sécurité des données et la surveillance du trafic.

Pour la connexion physique des différents serveurs, nous allons mettre en place deux commutateurs, 1 switch de 48 ports et 1 switch de 16 ports par site, pour assurer la redondance et la disponibilité. En ce qui concerne leur configurations de sécurité, nous allons mettre en place éléments suivant :

- La segmentation VLANs (Virtual Local Area Networks) : Divisez le réseau en segments virtuels pour isoler le trafic entre les différents services et serveurs et améliorer la sécurité.
- ACLs (Access Control Lists) : Configurez des listes de contrôle d'accès pour contrôler les flux de trafic entre les serveurs, en autorisant uniquement les connexions nécessaires et en bloquant les accès non autorisés.
- DHCP Snooping : Empêchez les attaques de type DHCP en surveillant et en filtrant le trafic DHCP non autorisé.
- Spanning Tree Protocol (STP) : Éviter les attaques type “tempêtes de broadcast” et améliorer la disponibilité.

Pour le réseau Wifi, nous allons mettre en place deux SSID par site, un premier réservé aux collaborateurs et régulé par toutes les technologies de contrôle d’accès listé précédemment. Ce réseau Wifi doit permettre aux collaborateurs d’avoir les mêmes accès que sur le réseau filaire. Et un second réservé aux visiteurs qui n’offre qu’un simple accès internet, protégeant ainsi les informations sensibles de l’entreprise et isolant le réseau d’une possible attaque externe.

Pour les utilisateurs nomades, nous prenons en charge la configuration du VPN. Tout d'abord, nous installons le client VPN sur les ordinateurs des employés nomades, choisissant un logiciel approprié tel que StrongSwan, Cisco VPN Client, ou en utilisant les clients intégrés dans certains systèmes d'exploitation.

Ensuite, nous nous chargeons de la configuration du logiciel en fournissant des détails tels que l'adresse IP du serveur VPN, les clés pré-partagées, et les paramètres de chiffrement pour les phases 1 et 2.

Il est essentiel que nous veillons à ce que les informations d'authentification, telles que le nom d'utilisateur et le mot de passe, soient correctement paramétrées. De plus, nous devons nous assurer que les paramètres avancés du client VPN correspondent à la configuration du serveur VPN.

En parallèle, le serveur NAC (Network Access Control) joue un rôle crucial dans l'authentification des appareils nomades. Il permet de vérifier et d'authentifier les dispositifs se connectant au réseau, renforçant ainsi la sécurité globale.

Une fois cette configuration effectuée, l'employé peut simplement tester la connexion VPN.

Ce DAT détaille une architecture réseau robuste répondant aux besoins de l'entreprise en termes de sécurité, de performance et de flexibilité. Chaque composant est choisi en fonction de ses avantages spécifiques pour répondre aux besoins de l'entreprise, tout en garantissant la continuité des services et la sécurité des données.