Architecture Sécurisée pour Mutuelle Santé

Réponse à appel d'offres – Module : Infrastructures réseau et sécurité

HNAIEN Achraf

Formateur :
Mr. Kevin DE SOUSA

Sommaire

- Prérequis
- Architecture
- Housing
- Matériel
- Prestation
  - ORGANISATION
  - INGÉNIERIE & DÉPLOIEMENT
  - CHARGE
- Synthèse financière
  - Architecture Datacenter
  - Architecture Agences
  - Services et administration
  - Synthèse financière globale

Prérequis

Prérequis

Contexte du Projet

Mission

Réponse à l’appel d'offres stratégique pour votre mutuelle santé de dimension nationale et internationale

Enjeu majeur : protection des données de santé sensibles dans le respect du RGPD

Objectifs

- Architecture sécurisée et résiliente
- Infrastructure évolutive
- Conformité réglementaire stricte
- Continuité de service garantie

Sécurité
Protection des données de santé sensibles selon normes RGPD

Résilience
Haute disponibilité et continuité d'activité

Évolutivité
Architecture adaptable aux besoins futurs

Prérequis

Périmètre Technique et Contraintes

500
Sites en France

2 sièges principaux et 498 agences réparties sur le territoire

30
Agences internationales

Présence mondiale nécessitant une architecture unifiée

10K
Utilisateurs

Collaborateurs en France et à l'international

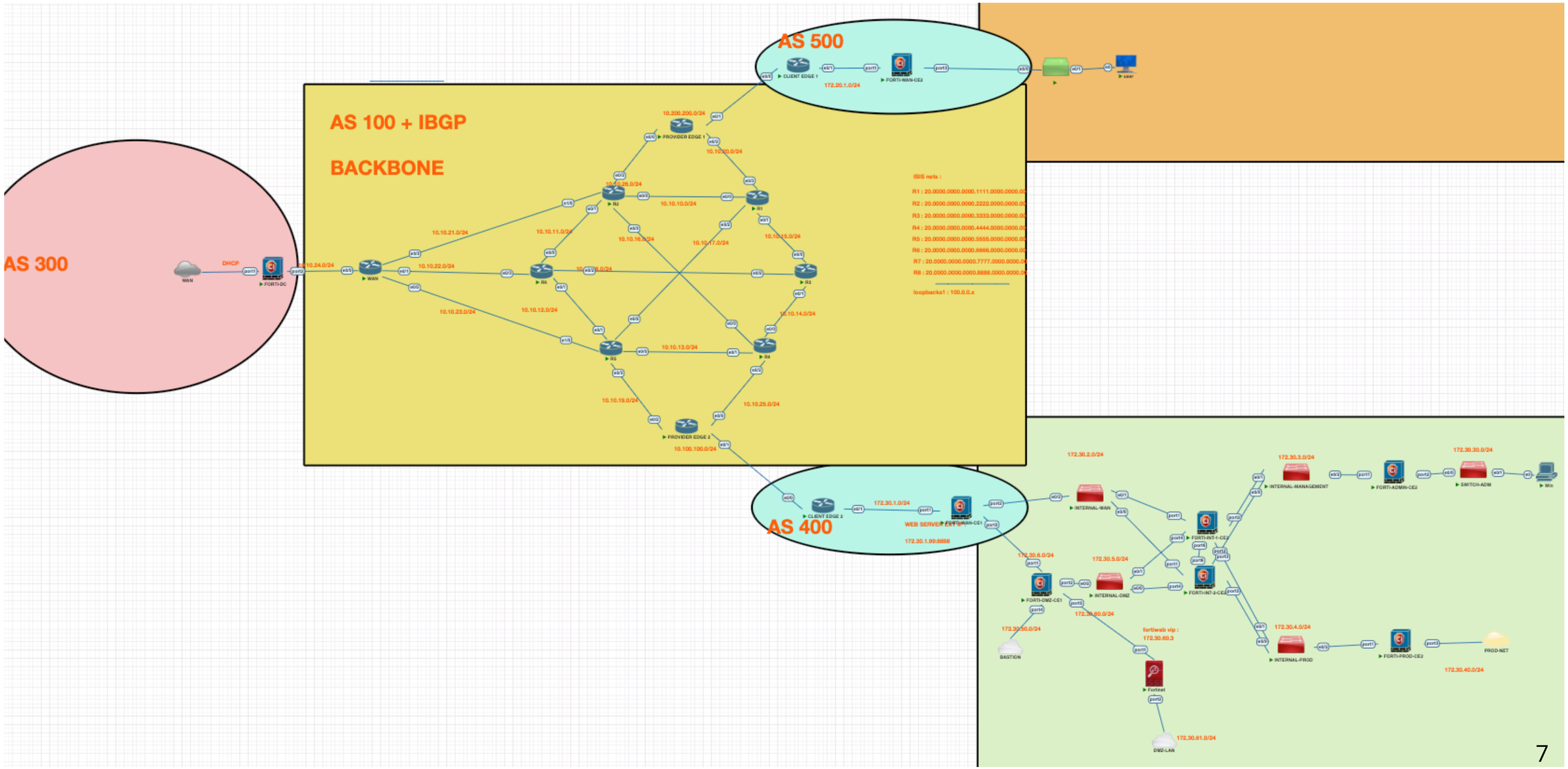
Haute Disponibilité
Exigences critiques pour garantir la continuité de service 24/7 sur l'ensemble des sites

Accès Sécurisés
Protection renforcée des accès aux Datacenters et contrôle des flux Internet

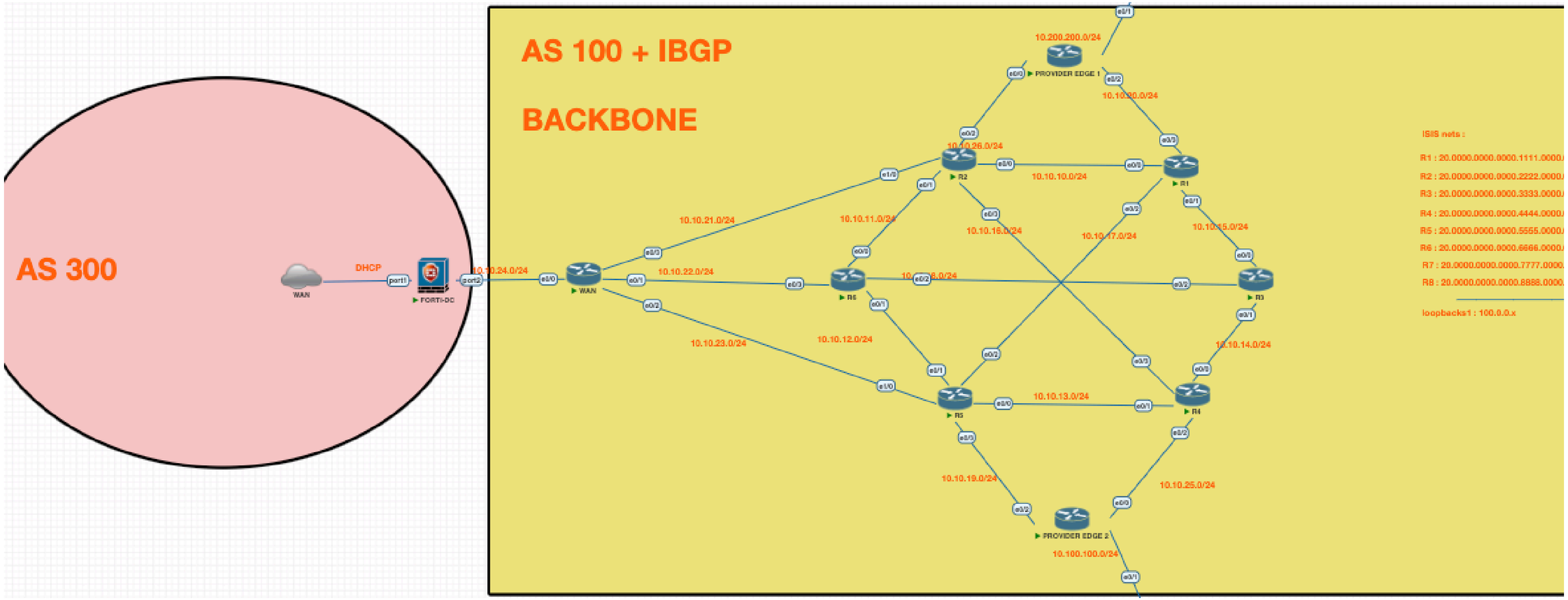
Architecture Distribuée
Gestion centralisée avec capacités locales pour optimiser performance et sécurité

Architecture

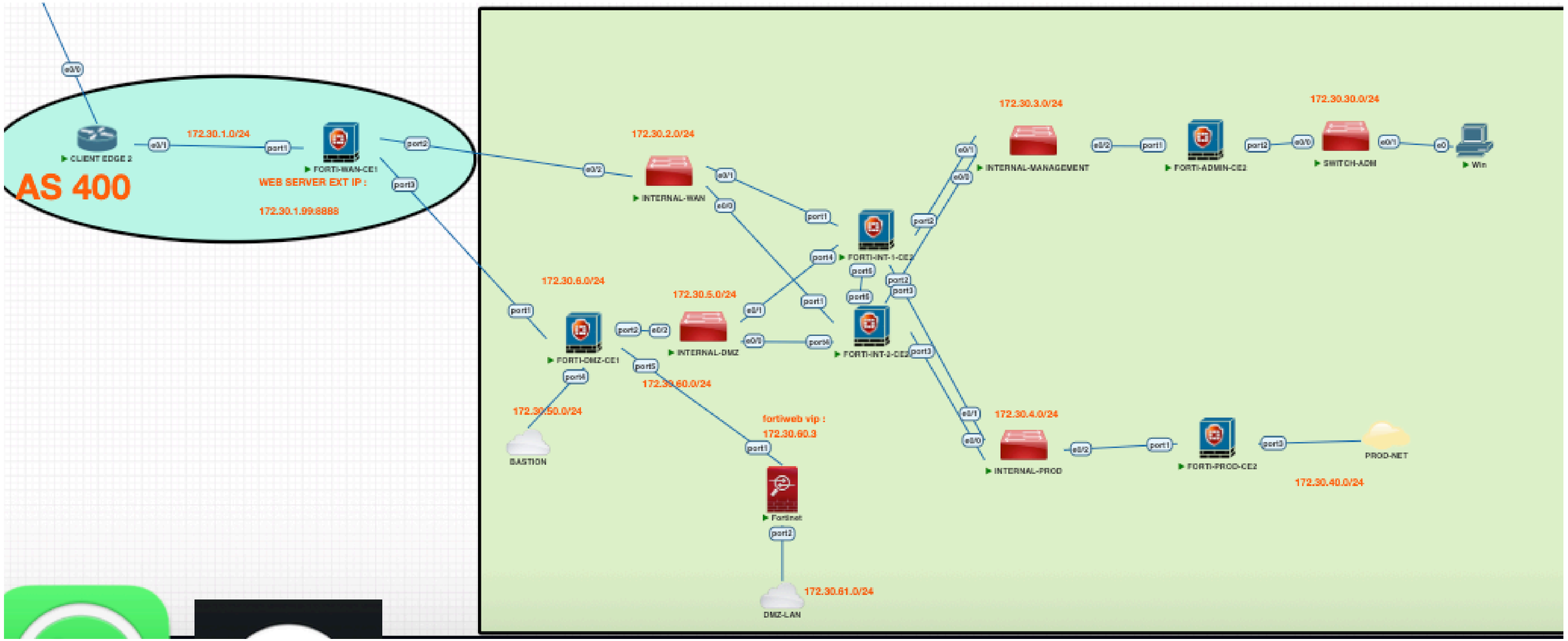
Objectif de l’infrastructure



Backbone


AS 300
WAN
DHCP
port1
FORTI-DC
port2
10.10.24.0/24
AS 100 + IBGP
BACKBONE
WAN
10.10.21.0/24
10.10.22.0/24
10.10.23.0/24
R6
10.10.11.0/24
10.10.12.0/24
R5
10.10.13.0/24
10.10.19.0/24
PROVIDER EDGE 2
10.100.100.0/24
R2
10.10.26.0/24
10.10.10.0/24
10.10.16.0/24
R1
10.10.17.0/24
10.10.15.0/24
R3
10.10.14.0/24
R4
10.10.25.0/24
PROVIDER EDGE 1
10.200.200.0/24
ISIS nets :
R1 : 20.0000.0000.0000.1111.0000
R2 : 20.0000.0000.0000.2222.0000
R3 : 20.0000.0000.0000.3333.0000
R4 : 20.0000.0000.0000.4444.0000
R5 : 20.0000.0000.0000.5555.0000
R6 : 20.0000.0000.0000.6666.0000
R7 : 20.0000.0000.0000.7777.0000
R8 : 20.0000.0000.0000.8888.0000
loopbacks1 : 100.0.0.x

Site principal



Site principal

Zone Production

- Protégée par le firewall Prod.

Héberge :

- Active Directory
- DNS sécurisé Pi-hole
- Zabbix (supervision)
- Syslog (journalisation)
- Autres services internes

Zone DMZ

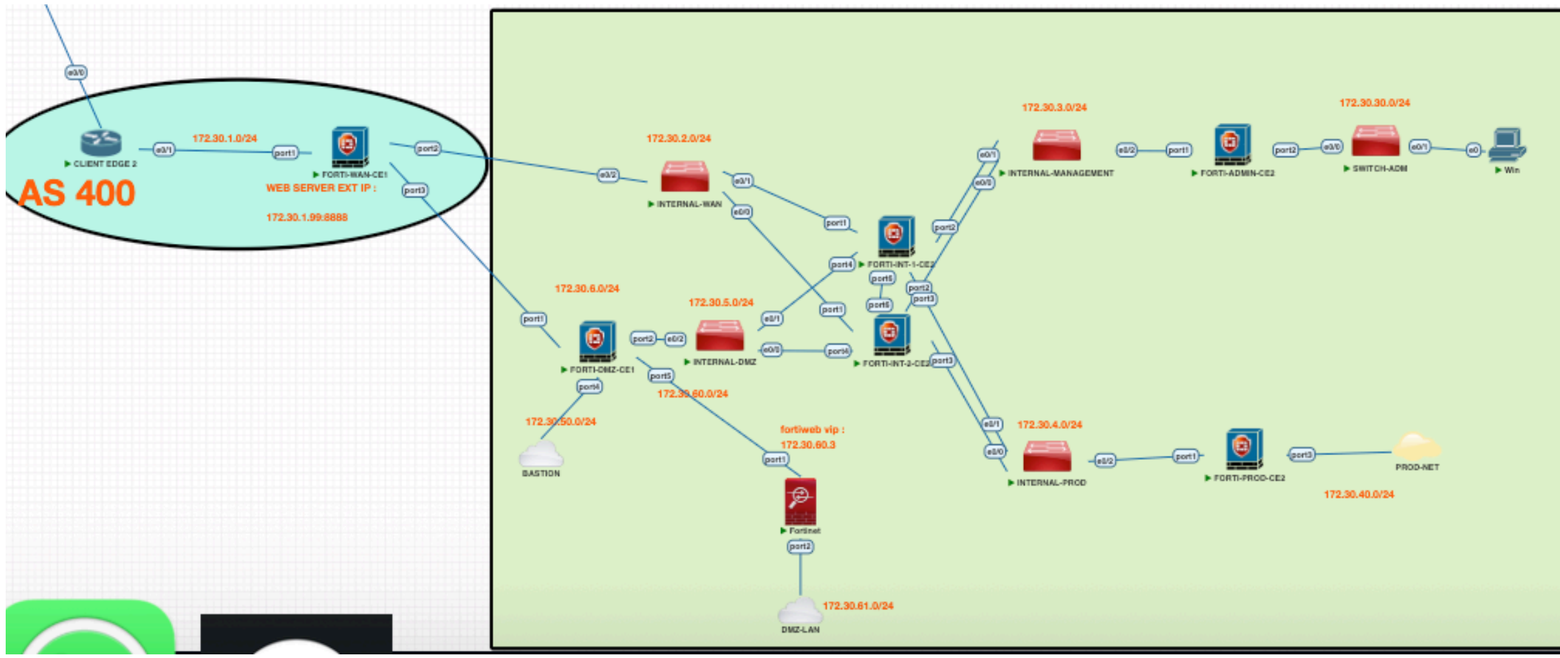
- Protégée par le firewall DMZ.

Contient :

- Un VLAN pour Guacamole (accès externe contrôlé)

Derrière le WAF :

- Deux serveurs web
- Répartition de charge (load balancing)



Zone Admin

- Protégée par le firewall Admin.
- Contient le bastion Guacamole, utilisé pour l'administration sécurisée de l'infrastructure.

Interconnexion sécurisée entre sites

VPN site à site

Un tunnel VPN IPsec est établi entre : le firewall WAN CE2 (Site 2) et le firewall DMZ du Site 1

- **Protocole IPsec**

  Chiffrement AES-256, authentification mutuelle par certificats

- **Tunnel permanent**

  Connexion persistante avec mécanisme de reconnexion automatique

- **Bande passante garantie**

  QoS priorisée sur le backbone opérateur

Objectif du VPN

Permettre à un utilisateur du Site 2 ::

- D'accéder au bastion Guacamole dans la zone Admin du Site 1.
- D'administrer l'infrastructure de manière sécurisée, tracée et contrôlée.

Confidentialité

Chiffrement de bout en bout

Intégrité

Protection contre altération

Authentification

Vérification des identités

Site principal : Services transverses

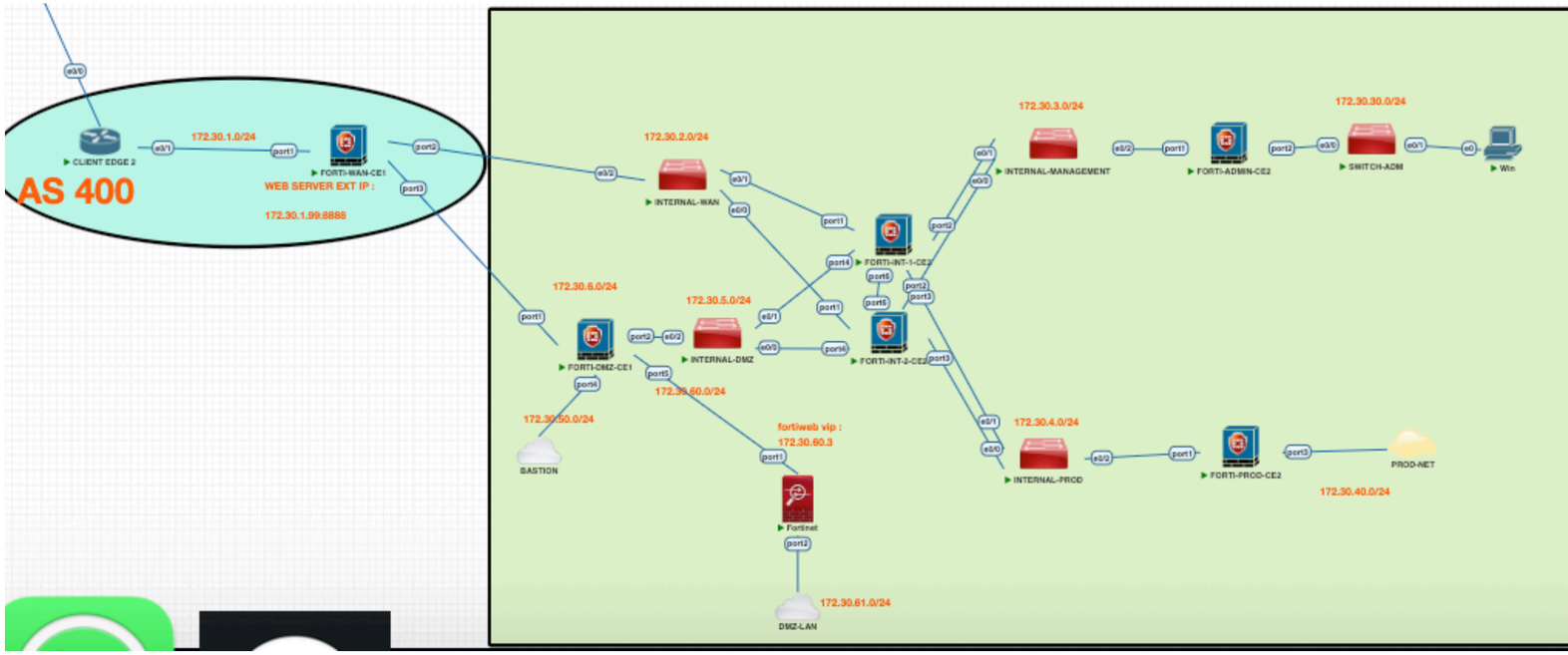
DNS sécurisé

Tous les équipements (firewalls, serveurs, postes) utilisent :

- Pi-hole comme DNS sécurisé.

Bénéfices :

- Filtrage des domaines malveillants
- Protection contre le phishing
- Contrôle des requêtes DNS



Supervision

Zabbix est utilisé pour :

- Surveiller les équipements réseau
- Superviser les serveurs et services
- Générer des alertes en cas d'incident

Journalisation

Serveur Syslog centralisé :

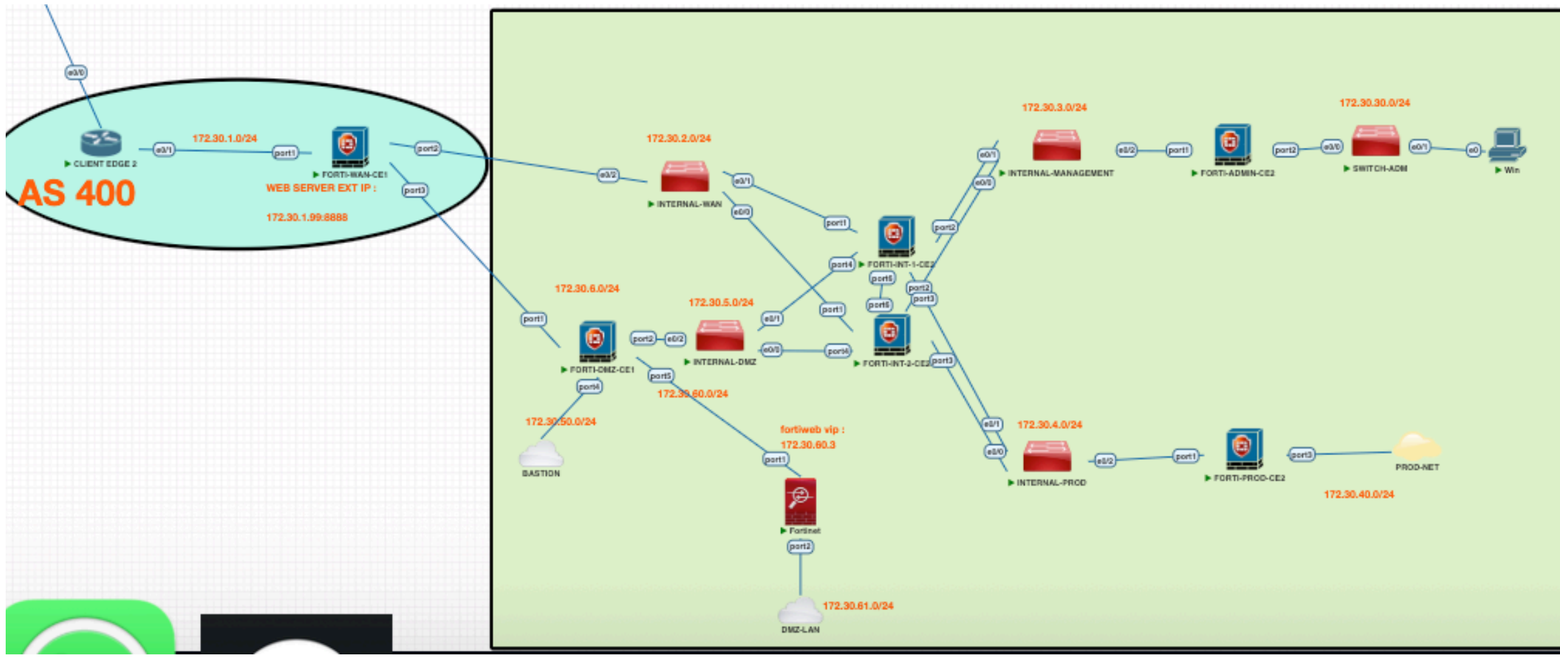
- Collecte les logs de tous les firewalls et équipements.
- Permet l'analyse de sécurité, l'audit et la traçabilité.

Site principal : Publication des Services

Sur le firewall WAN CE1, une VIP (Virtual IP / DNAT) est configurée :

Elle pointe vers la VIP du WAF FortiWeb.

Permet la publication sécurisée du site web via inspection applicative.



Housing

Un Hébergement Souverain et Certifié HDS

Validation du Socle Technique

- POC validé sur infrastructure Proxmox (64 Go RAM, CPU AMD 3800X).
- Validation de la scalabilité et des politiques de sécurité pour les flux futurs.

Redondance & Souveraineté

- Extension vers un Cloud certifié HDS et idéalement SecNumCloud.
- Hébergement et traitements sur un périmètre souverain (France/UE).

Mise en Production HDS

- Migration vers des baies privatives en datacenter certifié HDS.
- Conformité réglementaire totale pour les données de santé de la mutuelle.

KPI de Résilience

- Disponibilité cible : 99,9% (SLA haute performance).
- Objectifs de reprise : RTO : 4h | RPO : 15 min.
- Périmètre de sécurité : Datacenter HDS + Cloud souverain.

Matériel

Architecture Sécurisée & Haute Disponibilité

Sécurité Périmétrique & Web

- Fortinet FortiGate 600F : Gestion des flux Internet et inspection profonde.
- WAF FortiWeb : Protection critique des API et serveurs applicatifs publiés.

Segmentation & Réseau Local

- Switches Cisco Catalyst 9200 : Segmentation interne (Est/Ouest) du datacenter.
- Isolation physique et logique des serveurs Linux et Windows.

Administration & Accès

- Accès sécurisés pour l'infogérance et l'administration distante (bastion d’administration).
- Journalisation centralisée pour répondre aux audits de conformité HDS (syslog).

Interconnexion des Sites

Cœur de Réseau

- Routeurs Cisco ISR 4331 pour la redondance des liens entre sièges et agences.
- Support pour agences France et agences internationales.

Sécurité des Agences

- Déploiement de FortiGate 80F sur les sites.
- Filtrage local et tunnels VPN sécurisés vers le datacenter central.

Performance Utilisateurs

- Connectivité fluide pour les utilisateurs répartis en agences distantes.
- Optimisation des flux pour l'accès aux ressources hébergées en datacenter.

Modèle Économique

Agilité Financière via le Partenariat Constellation

Optimisation Budgétaire

- Transformation du projet en charges opérationnelles (OpEx).
- Réponse à la contrainte DSI : aucun déblocage de capital massif initial.

Offre par Abonnement (Constellation)

- Achat du matériel (Cisco et Fortinet) inclus dans le forfait.
- Mise à jour automatique des licences de sécurité et support technique 24/7.

Prévisibilité Financière

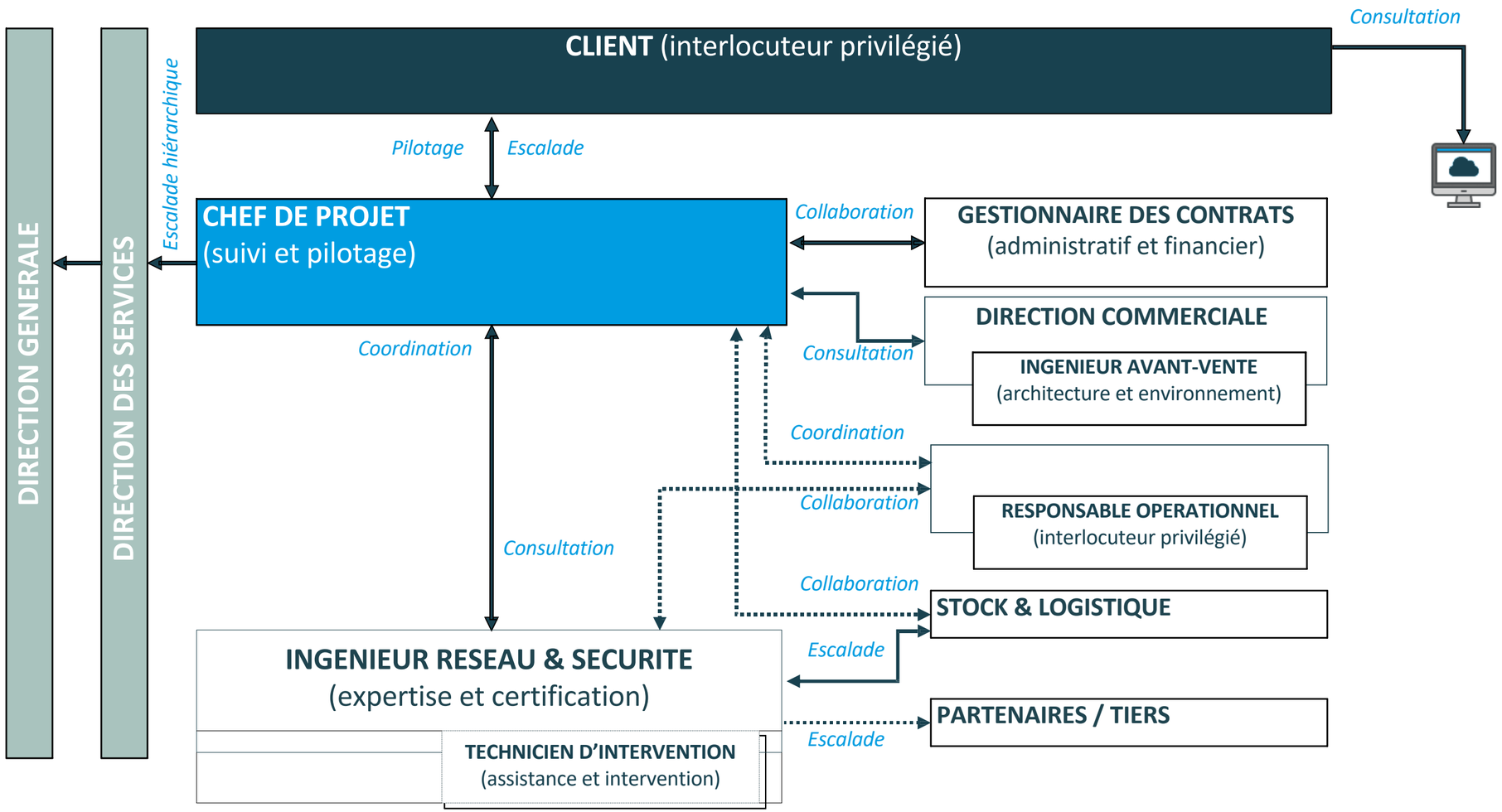
- Coûts globaux lissés sur une durée de 36 ou 60 mois.
- Visibilité totale sur le coût de possession (TCO) de l'infrastructure complète.

Évolutivité du Modèle

- Possibilité d'ajouter de nouvelles agences ou ressources Cloud selon la croissance.
- Mise à jour technologique simplifiée en fin de contrat.

Prestation

Prestation | ORGANISATION



Prestation | INGÉNIERIE & DÉPLOIEMENT

COLLECTE ET ATELIERS

- **"Master de configuration" renseigné par le Client**
- **Appréhension de l'environnement local**
- **Anticipation des contraintes de migration Ateliers techniques** (Client et tiers)

PRÉPARATION & LIVRAISON

- **Vérification du bon fonctionnement**
- **Pré-assemblage des éléments**
- **Pré-configurations de la solution**
- **Expédition sur site Client**
- **Réception et vérification par le Client**

CONCEPTION

- **Implantation physique et fonctionnalités activées**
- **Cohabitation avec l'environnement existant**
- **Stratégie d'ordonnancement et contraintes migration**
- **Template de configuration**
- **Analyse des risques et modalités de retour-arrière**

DOCUMENTATION TECHNIQUE

- **Dossier de spécifications techniques** (DST/DAT)
- **Cahier de recette** (CdR)
- **Plan de migration** (PM)
- **Dossier d'exploitation** (DEX)

CHEF DE PROJET

- **Interlocuteur privilégié**
- **Pilotage des opérations et adaptabilité**
- **Respect des engagements**
- **Communication et synchronisation régulière**
- **Suivi financier interne**

Prestation | CHARGE

TACHE	CHARGES
Phase d'initialisation	
Préparation de lancement (interne)	3
Réunion de lancement (CR inclus)	4,5
Phase d'audit	
Visites de site (audit physique)	6
Étude et analyse (audit logique)	15
Rapport d'audit (existant, recommandation, action)	9
Phase d'ingénierie	
Ateliers techniques Client	6
Conception de la solution	6
Préparation et livraison (vérification et pré configuration)	6
Phase de déploiement (Cœur et XMC)	
Installation des équipements	6
Brassage des interconnexions avec le réseau existant	6
Installation des outils centraux	9
Configuration et déclaration des équipements pilotes	9
Bascule et transition vers la nouvelle infrastructure	**9***
Assistance à la montée en charge (x2)	6
Signature du procès-verbal (PV MES Pilote)	3
Transfert de compétence sur XMC	3
Documentation technique (ne pas modifier l'intitulé)	
Dossier de spécifications techniques (DST ou DAT)	6
Cahier de recette (CdR)	7,5
Plan de migration (PM)	7,5
Dossier d'exploitation (DEX) - Extreme Management	9
Pilotage du projet	
Phase d'audit	5,5
Réunion de suivi hebdomadaire d'une heure sur 6 semaines	9
Documentation et livrables projet (relecture et suivi de la validation)	3,5

Synthèse Financière

Architecture Datacenter (Pour 2 Sites : Principal + Secours)

Chaque datacenter est certifié HDS. Le coût inclut la location des baies, l'énergie, et la réplication Cloud SecNumCloud.

Poste de dépense	Détail de l'équipement (x2 DC)	Coût Mensuel Estimé
Housing HDS	2 Baies privatives, Énergie (5kW/baie), Connectivité Inter-DC	4 500€
Sécurité WAF	2x FortiWeb (Hardware + Licence Gold 24/7)	480€
Réseau WAN	2x Cisco ISR 4331 (Lissage matériel + Support SmartNet)	220€
Commutation	10x Cisco Catalyst 9200 (Accès et Cœur DC)	650€
Pare-feu (Segmentation)	12x Fortinet FortiGate 80F (Cluster HA + Licences UTP)	1 100€
Compute & Backup	Serveurs loués + Réplication Cloud SecNumCloud (20 To)	3 800€
TOTAL DATACENTERS	**Sous-total mensuel pour les 2 DC**	**10 750 € / mois**

Architecture Agences (528 Sites)

C'est ici que le volume crée le poids financier principal. Nous utilisons un modèle de déploiement standardisé.

Logistique et Déploiement

- **Pré-configuration :** Avant d'envoyer les 528 FortiGate et Cisco en agence, ils doivent passer par un entrepôt pour être configurés (ZTP - Zero Touch Provisioning).
  - Coût estimé : ~50 € à 100 € par équipement.
- **Le Déploiement Terrain :** Faire intervenir un technicien pour brancher les box et tester les liens dans chaque agence.
  - Coût estimé : ~300 € à 500 € par site (selon la zone géographique).

Poste de dépense	Équipement par site (x528)	Coût Unit. Mensuel (Lissé 60 mois)	Coût Total Mensuel
Matériel Réseau	1x Cisco ISR 4331	85€	44 880€
Sécurité (SD-WAN)	1x FortiGate 80F + Licence UTP (Web filter, IPS)	75€	39 600€
Liaison Internet 1	Fibre Pro (FTTE/FTTO) débit garanti	180€	95 040€
Liaison Internet 2	Backup (Fibre Grand Public ou 4G/5G illimitée)	45€	23 760€
TOTAL AGENCES		**385 € / site**	**203 280 € / mois**

Services et Administration (Transverse)

- **Management Centralisé :** 2,26 € / site pour automatiser la sécurité des 530 agences et réduire les coûts de main-d'œuvre IT interne.
- **Sécurité Nomade (ZTNA) :** 0,85 € / utilisateur pour sécuriser 10 000 collaborateurs et prévenir les amendes RGPD massives.
- **Expertise NOC/SOC 24/7 :** Économie directe de 30 000 € / mois par rapport au coût de recrutement d'une équipe interne de nuit.
- **Bilan Économique :** Un investissement de 2,47 € / collaborateur pour garantir la continuité de service et la protection des données.

Service	Description	Coût Mensuel
Management Centralisé	FortiManager & FortiAnalyzer (Analyse de logs & Policy)	1 200€
Accès Nomades (MFA)	10 000 Licences ZTNA / FortiToken (Accès sécurisé)	8 500€
Infogérance	Monitoring 24/7, NOC/SOC par Constellation	15 000€
TOTAL SERVICES	**Sous-total mensuel services**	**24 700 € / mois**

Synthèse Financière Globale

- **Maîtrise Budgétaire :** Modèle majoritairement OpEx incluant matériel, licences et support.
- **Souveraineté Santé :** Hébergement certifié HDS et réplication SecNumCloud garantissant une protection totale des données.
- **Continuité Business :** SD-WAN intelligent avec double connectivité par site pour assurer 99,99 % de disponibilité.
- **Agilité & Croissance :** Coût marginal fixe de 385 € HT / mois facilitant l'intégration immédiate de nouveaux sites.

Indicateur Financier	Valeur
Coût Total Mensuel (OpEx)	**238 730 € HT / mois**
Coût par utilisateur et par mois	**23,87 € HT**
Investissement Initial (Projet/Set-up)	~ 250 000 € (Installation, configuration, déploiement)

Conclusion