



**MINISTÈRE
DE LA TRANSFORMATION
ET DE LA FONCTION
PUBLIQUES**

*Liberté
Égalité
Fraternité*



CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES

LOT 1 du marché exprimé dans la DU
IRA_NANTES_02_IR_2022

Résumé

Remplacement d'équipements réseaux et communication

IRA de NANTES

Jean-luc.lagadec@ira-nantes.gouv.fr

TABLE DES MATIERES

Introduction.....	2
Planning du projet.....	2
Description de l'infrastructure existante.....	3
Moyens humains.....	4
Interconnexions	4
Description du besoin.....	6
Firewall.....	6
InTerconnexion	6
Prestation d'intergration, d'installation et de migration	7
Etude d'interconnexion	7
Etude des configurations existantes	7
Installation des équipements	7
Déploiement sur l'infrastructure.....	7
Migration des configurations	7
Sauvegardes	7
phase de recette	7
Retrait ancienne infrastructure	7
Recette et Documentation	8
Maintenance et support	8
Confidentialité	8

INTRODUCTION

Le projet consiste au remplacement d'équipements de sécurité réseau (firewall) et d'interconnexion (pile switch de niveau 2).

L'ambition de ce projet est de doter l'établissement d'une infrastructure sur site pouvant répondre aux nécessités de continuité de service et aux besoins d'évolution et d'extension des capacités.

Il doit permettre d'engager ainsi une évolution durable pour une période minimale de 5 ans.

Les objectifs recherchés sont :

- Garantir la continuité des services critiques,
- Assurer un temps de reprise d'activité conforme aux exigences.
- Moderniser l'environnement technique lié à l'infrastructure réseaux,
- Garantir la sécurité des données critiques,

Le présent document recense les besoins attendus et exigences pour les prestations

Il comporte trois parties :

- La description de l'infrastructure existante.
- La description des besoins et évolutions matérielles attendue.
- Les exigences des prestations d'intégration, d'installation et de migration.

PLANNING DU PROJET

La totalité des prestations attendues doit être réalisée à compter de la date d'acceptation du marché jusqu'au **28 octobre 2022**, y compris période de recette.

Le fonctionnement de l'infrastructure existante doit être maintenue et garantie pendant toute la durée des prestations. Dans le cas où des indisponibilités sont nécessaires celles-ci devront être planifiées dans un mode dégradé ou pendant des horaires ne perturbant pas le fonctionnement des services (entre 12h30 et 14h00, après 17h30)

DESCRIPTION DE L'INFRASTRUCTURE EXISTANTE

L'infrastructure réseau actuelle est constituée de 2 nœuds firewall FORTIGATE 200D , fortiOS 6.0.14 en cluster actif/passif.

- La distribution de niveau 2 est constitué de 3 switchs FORTISWITCH 248 FPOE.
- La couverture wifi est assurée par des bornes FORTI FP221 et FP223 intégrées au FORTIGATE

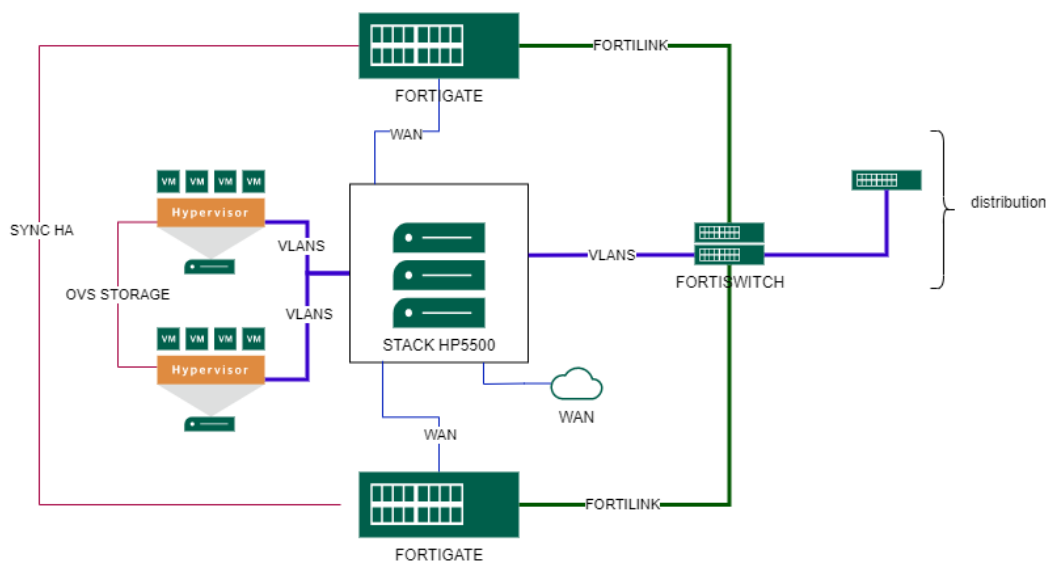
L'ensemble des équipements réseau est managé à partir du FORTIGATE et lien FORTILINK

Les nœuds sont hébergés dans 2 locaux dimensionnés (onduleur, climatisation). 1 local au rez de chaussé du bâtiment, 1 autre local au 2^{ème} étage du bâtiment. Les locaux sont équipés d'une baie 19 pouces (emplacements libres)

L'ensemble est connecté par agrégats LCAP cuivre à une pile IRF fibre de 3 HP A5500 assurant la distribution des différents VLAN (7 VLAN) vers les serveurs (HPE symplivity), routeurs internet et réseau ministériel et la redondance des liens. Le 3^{ème} commutateur est situé au 1^{er} étage. La pile assure également quelques distributions de niveau 2.

Les services portés par les équipements firewall, outre les règles IPV4 inter VLAN/DMZ:

- Interfaces VLAN et DHCP
- IP virtuelles publiques (12 IP) vers 'DMZ'
- Management switchs et bornes wifi
- VPN acces portail web SSL IpSec authentication par service LDAP
- Malware protection Web
- Antispam, web et dns filtrage.

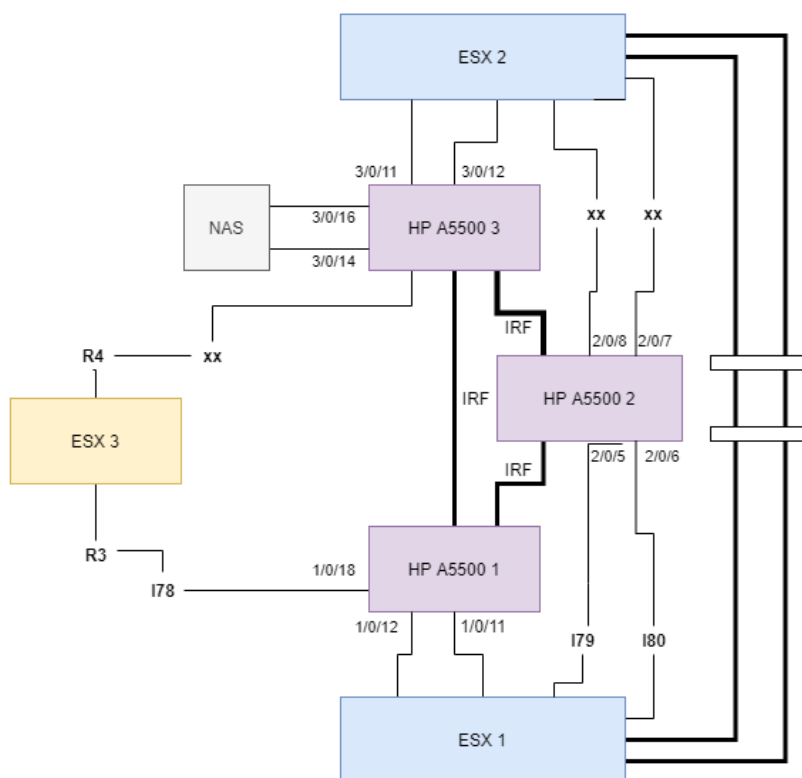


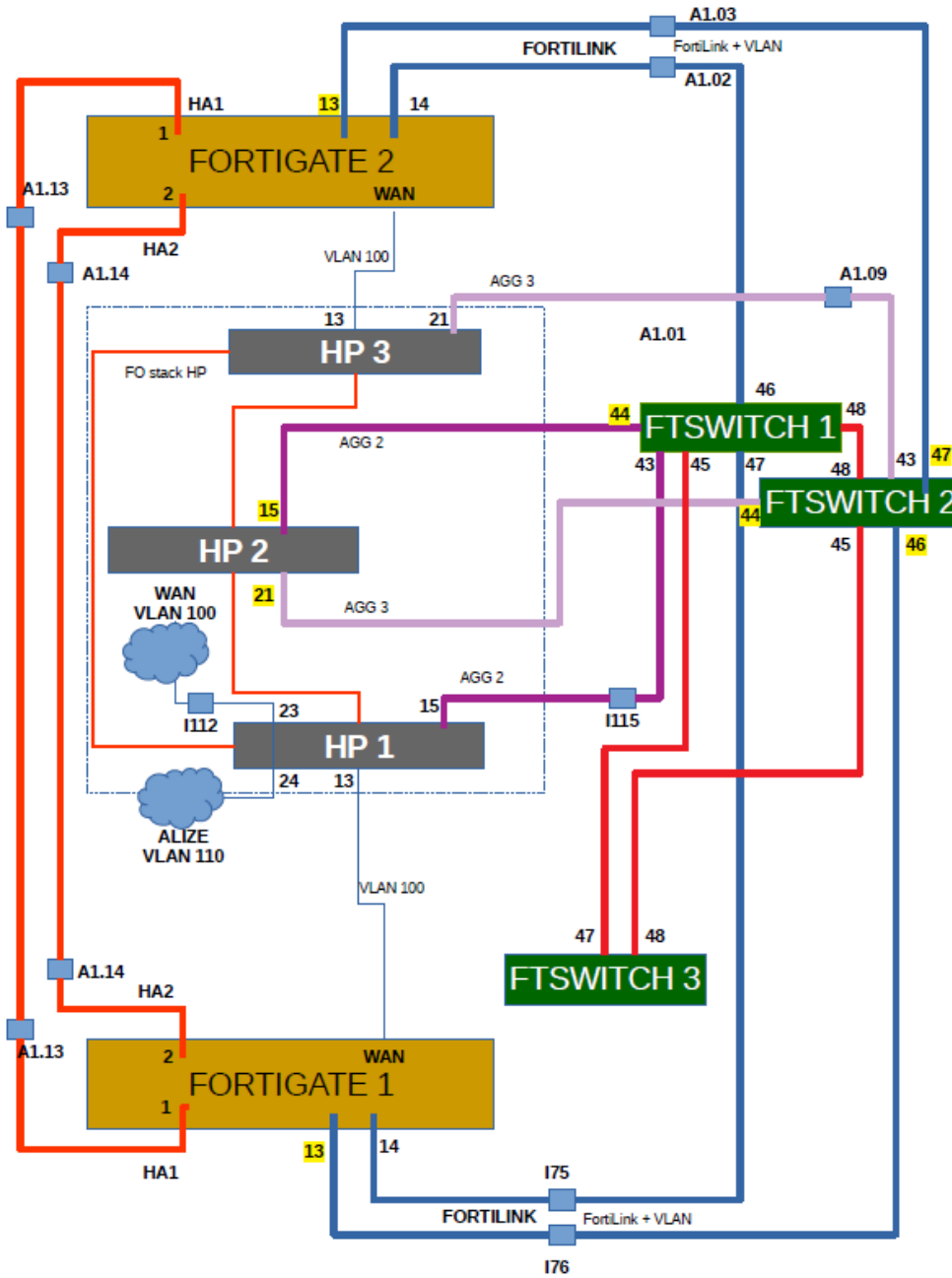
MOYENS HUMAINS

Le SI de l'établissement est administré et exploité par une seule personne (le Responsable des Systèmes d'Information) avec l'appui d'un prestataire de maintenance privé auquel sera transférée la maintenance à l'issue de la prestation.

L'Institut souhaite pas multiplier les prestations de maintenance pour des raisons de disponibilité de compétences locales sur l'ensemble de l'infrastructure SI.

INTERCONNEXIONS





DESCRIPTION DU BESOIN

FIREWALL

Compte tenu du niveau d'intégration des équipements FORTINET existants et conservés, la prestation exige le remplacement des firewalls par du matériel FORTIGATE à capacité équivalente.

Le service VPN devra être proposé en option pour un nombre de licence de 25 utilisateurs en mode portail web, SSL, IpSec

Tous les matériels sont fournis avec maintenance et support constructeur Garantie J+1 24x7 5 ans

INTERCONNEXION

L'interconnexion actuelle est assurée par une pile IRF fibre de 3 switchs HP5500

Cette interconnexion assure la redondance des liens cuivres vers les hyperviseurs HPE Symplivity et les connexions externes internet et routeur réseau Ministériel ALIZE.

Elle interconnecte également les équipements fortiswitch de distribution niv2 par agrégat LACP cuivre.

Cette interconnexion ayant été mise en place dans un contexte différent de celui de l'architecture actuelle, le prestataire proposera un nouveau schéma d'interconnexion mieux adapté et redondant sur de nouveaux équipements fournis et intégrés par extension de l'infrastructure existante et permettant d'étendre aisément le réseau de distribution dans le futur.

PRESTATION D'INTERGRATION, D'INSTALLATION ET DE MIGRATION

Elles doivent pouvoir s'effectuer sans interruption de service.

ETUDE D'INTERCONNEXION

- Etude et proposition de remplacement du stack HP par une nouvelle topologie d'interconnexion.

ETUDE DES CONFIGURATIONS EXISTANTES

- Audit et contrôle de l'infra existante
- Mise à jour des firmware si nécessaire, y compris équipements conservés (Fortiswitch)
- Optimisation des configurations sur le matériel en place avant migration.

INSTALLATION DES EQUIPEMENTS

- Mise en rack des nœuds, brassage.
- Configuration réseau

DEPLOIEMENT SUR L'INFRASTRUCTURE

- Déploiement des nœuds
- Interconnexions
- Règles de déploiement

MIGRATION DES CONFIGURATIONS

- Customisation
- Validation du déploiement

SAUVEGARDES

- Préparation d'un plan de sauvegarde des configurations.

PHASE DE RECETTE

- Recette en production sur une période de 1 mois

RETRAIT ANCIENNE INFRASTRUCTURE

- A l'issue de la phase de recette.

RECETTE ET DOCUMENTATION

- Procédure de recette : validation du bon fonctionnement, validation des procédures.
- Dossier technique d'architecture.

MAINTENANCE ET SUPPORT

Les matériels seront sous garantie et support constructeur 5 ans

L'établissement souhaite avoir un contrat de support unique pour l'ensemble des éléments du projet étendu aux équipements réseaux et serveurs existant, le transfert de la maintenance vers le prestataire de maintenance de l'établissement est une exigence.

CONFIDENTIALITE

Les candidats doivent considérer comme strictement confidentielles toutes les informations, méthodes et documentations qu'ils peuvent être amenés à connaître dans le cadre des présentes, et qu'elles soient ou non identifiées comme étant confidentielles. Les candidats s'engagent à ne pas utiliser ces informations à des fins personnelles et à ne pas les dévoiler à des tiers.

Les candidats s'engagent formellement à tenir confidentielles ces informations de l'établissement et à ne les utiliser qu'aux seules fins de réalisation des présentes. En outre, les candidats s'engagent à ce que les informations confidentielles :

- soient protégées, conservées dans un lieu sûr et traitées avec les plus extrêmes protections, notamment par toutes mesures permettant d'empêcher l'accès de personnes non autorisées
- ne soient divulguées qu'aux seuls membres de leurs personnel et/ou partenaires ayant à les connaître pour les besoins de la formulation de l'offre commerciale et technique, et à la condition expresse, dans chaque cas, que ces employés et/ou partenaires s'engagent individuellement, à respecter les mêmes obligations de confidentialité que celles contenues aux présentes et que les candidats se portent forts du respect de cette obligation par leurs employés et/ou partenaires
- ne soient divulguées ni susceptibles d'être divulguées, directement ou indirectement, à tout tiers ou à toutes personnes autres que celles mentionnées ci-dessus.

Ces obligations de confidentialité resteront en vigueur pendant toute la durée des relations commerciales et contractuelles entre les candidats et votre entreprise et pour une période de DIX (10) ans courant à compter de la date de la diffusion du présent cahier des charges aux candidats.