RENOUVELLEMENT DES ÉQUIPEMENTS DE FILTRAGE RÉSEAU

Cahier des Clauses Techniques Particulières

N° 2026-05

EPELFI - Etablissement Public d'Exploitation du Livre Foncier Informatisé
2a, rue de l'Artisanat - 67700 SAVERNE - Siret 130 004 633 00017 - APE 8411Z
http://www.livrefoncier.fr - Tél. : +33 (0) 3 88 01 83 20 - Fax : +33 (0) 3 88 01 83 29

Table des matières

Marché de renouvellement des équipements de filtrage réseaux 4

1. Objet du marché 4

2. Périmètre du marché 5

2.1. Périmètre inclus 5
2.2. Périmètre exclu 6
2.3. Répartition des responsabilités d'exploitation des pare-feux 6

3. Contexte 6

3.1. Pouvoir adjudicateur 6
3.2. Interlocuteurs 7
3.3. Contexte du renouvellement 9

4. Existant 12

4.1. Architecture générale des plateformes 12
4.2. Inventaire des pare-feux (synthèse) 13
4.3. Charge constatée 13
4.4. Socle de supervision et de journalisation actuel 13
4.5. Applicatifs structurants traversant les frontières de filtrage 14

5. Cible 14

5.1. Architecture existante et cible 14
5.2. Périmètre matériel 15
5.3. Exigences fonctionnelles 17
5.4. Exigences de capacité et de flux 17
5.5. Exigences de sécurité 18
5.6. Maintien en conditions de sécurité (MCS) 18

6. Prestations attendues du titulaire 20

6.1. Phase ANALYSE 20
6.2. Phase CONCEPTION 20
6.3. Phase DÉPLOIEMENT 21
6.4. Phase DOCUMENTATION 21
6.5. Phase FORMATION ET TRANSFERT DE COMPÉTENCES 22
6.6. Réversibilité 22

7. Tranches et calendrier 23

7.1. Tranche ferme n°1 (TF1) — BUILD (renouvellement et déploiement) 23
7.2. Tranche ferme n°2 (TF2) — Formation et transfert vers l'exploitation 24
7.3. Tranche ferme n°3 (TF3) — Maintien en conditions de sécurité (MCS) 24
7.4. Calendrier de référence 24

8. Livrables 25

9. Conditions d'exécution 26

9.1. Localisation des prestations 26
9.2. Habilitations et confidentialité 26
9.3. Sous-traitance 26
9.4. Comitologie 26

9.5. Outils 27
Annexe A : Glossaire 27
Annexe B : sans objet 28
Annexe C : Liste des équipements existants 29
Annexe D : sans objet 29
Annexe E : Détail Quantitatif estimatif (DQE) 29
Annexe F : Charge mesurée des paresf-feux sur 12 mois 29
F.1. Charge CPU et mémoire 30
F.2. Sessions actives et débit 30
F.3. Volumes cumulés sur 12 mois 30
F.4. Synthèse pour le dimensionnement cible 30
Annexe G : Reprise du matériel pour le recyclage 31

Marché de renouvellement des équipements de filtrage réseaux

Documents de Référence

Référence	Libellé	Date	Révision
ANSSI PA-044	Recommandation ANSSI PA-044 (citée au §5.3.2)	26/01/2018	1.0
RFC 2119	RFC 2119 — termes de convention d'exigence (cf. conventions du document)	Mars 1997	1.0
RGS	Référentiel Général de Sécurité (cité au §3.3.3) -- Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives	02/02/2010	En vigueur au jour de la publication du marché

Note : Préambule de lecture

Le présent CCTP est **autoportant** : il ne renvoie à aucun document antérieur. Il décrit l'existant, exprime la cible attendue et précise les prestations exigées du titulaire.

Les clauses sont rédigées en **mode capacités ANSSI** (vocabulaire fonctionnel et de sécurité, sans prescription de marque ou de produit). Les seules désignations commerciales figurant dans le document concernent l'inventaire factuel de l'infrastructure existante (cf. Article 4 et Annexe C).

Conventions :

- **DOIT / DEVRA** — exigence ferme (équivalent RFC 2119 « MUST »).

- **DEVRAIT** — exigence forte recommandée, qui peut être amendée par le titulaire à condition d'apporter une justification motivée (équivalent « SHOULD »).

- **PEUT** — option laissée à l'appréciation du titulaire (équivalent « MAY »).

1. Objet du marché

L'Établissement Public d'Exploitation du Livre Foncier Informatisé (EPELFI), créé par la loi n° 2002-306 du 4 mars 2002, est chargé, depuis le 1er janvier 2008, d'assurer l'exploitation du Livre foncier informatisé d'Alsace-Moselle ainsi que, plus récemment, du Registre informatisé des Associations d'Alsace-Moselle.

L'EPELFI délivre et retire les habilitations et contrôle les accès des utilisateurs (personnels du Ministère de la Justice, professionnels habilités, autres utilisateurs professionnels, particuliers…) aux applications et données du Livre foncier d'Alsace-Moselle et du Registre des Associations d'Alsace-Moselle

L'EPELFI est également chargé de délivrer les copies non certifiées du Livre foncier d'Alsace-Moselle et des informations du Registre des Associations d'Alsace-Moselle.

Cet ensemble de solutions métier constitue le Système d'Information (SI) de l'EPELFI.

L'EPELFI est une structure permanente qui a notamment pour missions :

- D'assurer ou faire assurer le bon fonctionnement et l'évolution des solutions métier du SI.
- D'assurer ou faire assurer l'exploitation et la maintenance des systèmes techniques du SI.

Le site de production informatique se situe à Saverne et son PRA est assuré par un datacenter du ministère de la justice situé à Nantes.

Le présent marché a pour objet le **renouvellement complet des équipements de filtrage réseau (pare-feux)** des plateformes de l'EPELFI de Saverne (production) et de Nantes (préproduction / plan de reprise d'activité), incluant la fourniture, l'installation, la migration, la mise en exploitation, la documentation et le transfert de compétences associés.

Le marché couvre également, en tranche ferme n°2, la formation et le transfert vers l'exploitation (montée en compétence des équipes de l'EPELFI et passage de témoin) et, en tranche ferme n°3, le maintien en conditions de sécurité (MCS) de l'ensemble des pare-feux installés à compter de la mise en service de chaque site et pour la durée du marché (cf. Article 7). Le maintien en conditions opérationnelles (MCO) des pare-feux est assuré par l'EPELFI au moyen de ses ressources internes (cf. §2.3).

Les principales cibles techniques du marché sont :

- Une architecture de défense en profondeur appuyée sur au moins deux solutions distinctes de filtrage (préconisations ANSSI), dont au moins une solution qualifiée ANSSI sur les frontaux Internet (cf. §5.5.4) ;
- La généralisation de la **haute disponibilité** sur l'ensemble des couples de pare-feux ;
- La **traçabilité immuable des journaux de sécurité des pare-feux** ;
- L'authentification **multi-facteurs** pour l'administration des pare-feux.

2. Périmètre du marché

2.1. Périmètre inclus

Sont inclus dans le présent marché :

- La fourniture des matériels actifs de filtrage réseau et de leurs accessoires (alimentations, modules, émetteurs-récepteurs optiques -transceivers-, câblage spécifique) ;
- La fourniture des licences associées ;
- La conception détaillée de l'architecture cible ;
- La mise en exploitation, la recette et la bascule en production ;
- La documentation d'exploitation et le transfert de compétences vers les équipes de l'EPELFI ;
- En tranche ferme n°2, la formation et le transfert vers l'exploitation ;
- En tranche ferme n°3, le maintien en conditions de sécurité (MCS) des pare-feux (cf. Article 7).

2.2. Périmètre exclu

Sont explicitement **exclus** du présent marché :

- Les serveurs (physiques/virtuels), le réseau SAN, le stockage et l'infrastructure de sauvegarde ;
- Les commutateurs LAN ;
- la **capacité du lien WAN inter-sites Saverne ↔ Nantes** : le dimensionnement et le contrat de transport sont instruits séparément par l'EPELFI ;
- Le **service VPN d'accès distant** : Ce service est porté par une plateforme indépendante tout deux hors périmètre des pare-feux.
- Le maintien en conditions opérationnelles (MCO) des pare-feux : il n'entre pas dans le présent marché et est assuré par l'EPELFI au moyen de ses ressources internes (cf. §2.3) ;
- La gestion courante des règles de filtrage en exploitation (ouverture, fermeture ou modification des flux) : elle demeure sous la responsabilité interne de l'EPELFI ; le titulaire n'intervient qu'en appui, conseil, traitement des sujets complexes et escalade de niveau avancé, et non comme activité principale ;
- L'audit périodique de sécurité : il est confié à un acteur indépendant du titulaire, afin de garantir l'impartialité des constats, et fait l'objet d'une commande distincte hors du présent marché.

2.3. Répartition des responsabilités d'exploitation des pare-feux

- L'exploitation courante et l'administration système des pare-feux objets du présent marché — ci-après désignées maintien en conditions opérationnelles (MCO) — sont assurées par l'EPELFI au moyen de ses ressources internes, à compter de la mise en service de chaque site. Le MCO recouvre notamment l'administration du système d'exploitation des équipements, la gestion du cycle de vie des règles de filtrage (création, modification, suppression), la gestion des comptes d'accès et des habilitations et l'exploitation quotidienne des pare-feux.
- Le titulaire assure, au titre de la tranche ferme n°3, le maintien en conditions de sécurité (MCS) de ces mêmes équipements : veille sur les vulnérabilités publiées et qualification de leur applicabilité au parc, application des correctifs et des mises à jour de micrologiciel, montées de version, surveillance et analyse des journaux, paramétrage et recommandations de sécurité.
- Aucun autre prestataire n'intervient sur les pare-feux objets du présent marché. Le titulaire est, pendant toute la durée du marché, l'unique intervenant externe sur ce périmètre.
- Cette répartition résulte d'un choix de l'EPELFI de conserver la maîtrise interne de l'exploitation de ses équipements de filtrage et de limiter strictement les accès externes à ceux-ci. L'EPELFI conduit par ailleurs une réflexion sur les modalités d'exercice global du maintien en conditions opérationnelles de son infrastructure ; le périmètre en sera, le cas échéant, précisé dans un marché ultérieur, sans que le présent marché n'emporte d'engagement quant à son contenu ou à son calendrier.
- Les candidats sont invités à dimensionner leur offre sur la base de cette répartition, dont les modalités opérationnelles sont précisées au §5.6, au §7.3 et au §9.1 du présent CCTP.

3. Contexte

3.1. Pouvoir adjudicateur

L'EPELFI est un établissement public administratif placé sous la tutelle du Ministère de la Justice (Direction des Services Judiciaires). Il assure l'exploitation du Livre Foncier informatisé d'Alsace-Moselle (application **AMALFI** — publicité foncière) et du registre des associations (application **AMALIA** — environ 92 000 associations gérées).

L'établissement est implanté sur deux sites :

Saverne (siège) — plateforme de production (PROD) ;
Nantes (SNMJ — Site Nantais du Ministère de la Justice) — plateforme de préproduction et de reprise d'activité (PPRA) avec la volonté d'aller vers un PCA.

3.2. Interlocuteurs

Conformément à la réglementation, l'EPELFI désigne une Personne responsable du marché (PRM). Pour la présente consultation, le point de contact unique des candidats est le responsable des moyens généraux et des achats : les questions d'ordre procédural lui sont adressées et les questions d'ordre technique sont traitées sous son couvert. Les interlocuteurs de l'EPELFI sont identifiés par leur fonction, à l'exclusion de toute donnée nominative.

La répartition des responsabilités entre l'EPELFI et le titulaire est portée par la matrice RACI ci-après, établie en cohérence avec le §2.3 ; elle figure également dans la foire aux questions issue du sourçage, pièce du marché.

Thématique	Activité	R	A	C	I
BUILD	Adaptations réseau physiques : - Installation des nouveaux équipements (rackage / brassage / mise en service) - Modifications existants (déplacements / rebrassage…)	**Titulaire**	EPELFI (DSI)	EPELFI (DSI)	EPELFI (DG) EPELFI (RSSI)
BUILD	Adaptations réseau logiques potentielles **(1)** : - Modifications du plan IP (adressage / VLANs…) - Modifications de la matrice de flux	EPELFI (DSI)	EPELFI (DSI)	**Titulaire**	EPELFI (DG) EPELFI (RSSI)
BUILD	Pilotage et reporting : - Pilotage et suivi des intervenants - Reporting - Animation projet	**Titulaire**	EPELFI (DSI)	EPELFI (RSSI)	EPELFI (DG)
BUILD	Ingénierie : - Cadrage initial - Définition de l'architecture cible (physique / logique) - Définition de la stratégie de bascule (procédures / planning)	**Titulaire**	EPELFI (DSI) EPELFI (RSSI)	EPELFI (DSI)	EPELFI (DG)
MIGRATION	Préparation bascule : - Reprise des configurations (comptes, objets, règles)	**Titulaire**	EPELFI (DSI)	EPELFI (DSI)	EPELFI (DG) EPELFI (RSSI)
MIGRATION	Bascule selon la stratégie établie	**Titulaire**	EPELFI (DSI)	EPELFI (DSI)	EPELFI (DG) EPELFI (RSSI)
RECETTE	- Phase de VABF - Phase de VSR	**Titulaire**	EPELFI (DSI)	EPELFI (DSI)	EPELFI (DG) EPELFI (RSSI)
TRANSFERT	Formation pour montée en compétences des équipes DSI sur activités de MCO relatives aux pare-feux	**Titulaire**	EPELFI (DSI)	EPELFI (RSSI)	EPELFI (DG)
TRANSFERT	MCO sur les pare-feux : - Formation continue des équipes DSI : coaching / sensibilisation sur le terrain	**Titulaire (2)**	EPELFI (RSSI)	EPELFI (DSI)	EPELFI (DG)

RUN	MCO sur les pare-feux : - Maintien en conditions opérationnelles - Gestion des accès et habilitations - Gestion des changements (paramétrage système et objets systèmes, VLANs, ADOM, VDOM...) - Montées de versions système et micrologiciels	EPELFI (DSI)	EPELFI (RSSI)	**Titulaire (3)**	EPELFI (DG)
RUN	MCO - Gestion des flux : - Ouverture / Fermeture / Modifications de règles - Déclaration d'objets de type adresses / protocoles / ports / plages	EPELFI (DSI)	EPELFI (RSSI)	**Titulaire**	
RUN	MCS - Supervision des pare-feux : - Collecte et analyse des journaux de sécurité - Reporting et préconisations	**Titulaire**	EPELFI (RSSI)	EPELFI (DSI)	EPELFI (DG)
RUN	MCS - Veille sécuritaire et correctifs : - Veille CVE sur périmètre des équipements de sécurité - Application des correctifs de sécurité - Veille micrologiciels éditeurs des équipements de sécurité - Montées de version selon stratégie Titulaire	**Titulaire**	EPELFI (RSSI)	EPELFI (DSI)	EPELFI (DG)
RUN	MCS - Gestion des pannes et défaillances : - Restauration des configurations - Remplacement des équipements défectueux	**Titulaire**	EPELFI (DSI)	EPELFI (DSI)	EPELFI (DG)
RUN	MCS - Gestion des incidents - HO sur la journée de présentiel	**Titulaire**	EPELFI (RSSI)	EPELFI (DSI)	EPELFI (DG)
RUN	MCS - Gestion des incidents - Hors journée de présentiel	EPELFI (DSI)	EPELFI (RSSI)	**Titulaire (4)**	EPELFI (DG)
RUN	Activités de support N1 (et N2/N3 hors pare-feux)	EPELFI (DSI)	EPELFI (DSI)	EPELFI (DSI)	**Titulaire**
RUN	Activités de support N2 / N3 sur pare-feux : - En HO sur la journée de présentiel	**Titulaire (5)**	EPELFI (DSI)	EPELFI (DSI)	
RUN	Activités de support N2 / N3 sur pare-feux : - En HO / HNO hors journée de présentiel	EPELFI (DSI)	EPELFI (DSI)		**Titulaire**
GOUVERNANCE	- Préparation des COSUI - Animation des COSUI	**Titulaire**	EPELFI (DSI)	EPELFI (RSSI)	EPELFI (DG)
GOUVERNANCE	- Préparation des COPIL - Animation des COPIL	**Titulaire**	EPELFI (DSI)	EPELFI (RSSI)	EPELFI (DG)
GOUVERNANCE	- Préparation des COSTRA - Animation des COSTRA	EPELFI (DSI)	EPELFI (DG)	EPELFI (RSSI) **Titulaire**	

(1) En fonction de l'architecture préconisée par le Titulaire, notamment afin d'intégrer les impacts liés aux factorisations de clusters de pare-feux. Dans une logique de réduction de ces impacts au minimum.

(2) Afin de permettre aux équipes DSI d'être capables de réaliser progressivement l'exhaustivité des activités de MCO relatives aux pare-feux.

(3) Sur périmètre croissant jusqu'à exhaustivité des thématiques récurrentes de MCO via accompagnement Titulaire opéré via la formation continue évoquée au **(2)**.

(4) Aucune réactivité n'est attendue du Titulaire, au mieux, si cela est possible. Régularisations sur imputations en conséquence.

(5) Après qualification de la demande par le niveau 1 de support (équipes DSI) et affectation au niveau 2 pour prise en compte et traitement.

3.3. Contexte du renouvellement

Fin de support des matériels actuels

Les pare-feux actuellement en service arrivent en fin de support constructeur :

MARQUE A : fin de support **17 juin 2026** ;
MARQUE B : fin de support **31 août 2026**.

Les schémas ci-après situent les pare-feux dans l'architecture réseau de chacun des deux sites. Ils décrivent l'existant à la date de publication du présent dossier de consultation et n'emportent aucune exigence d'architecture cible.

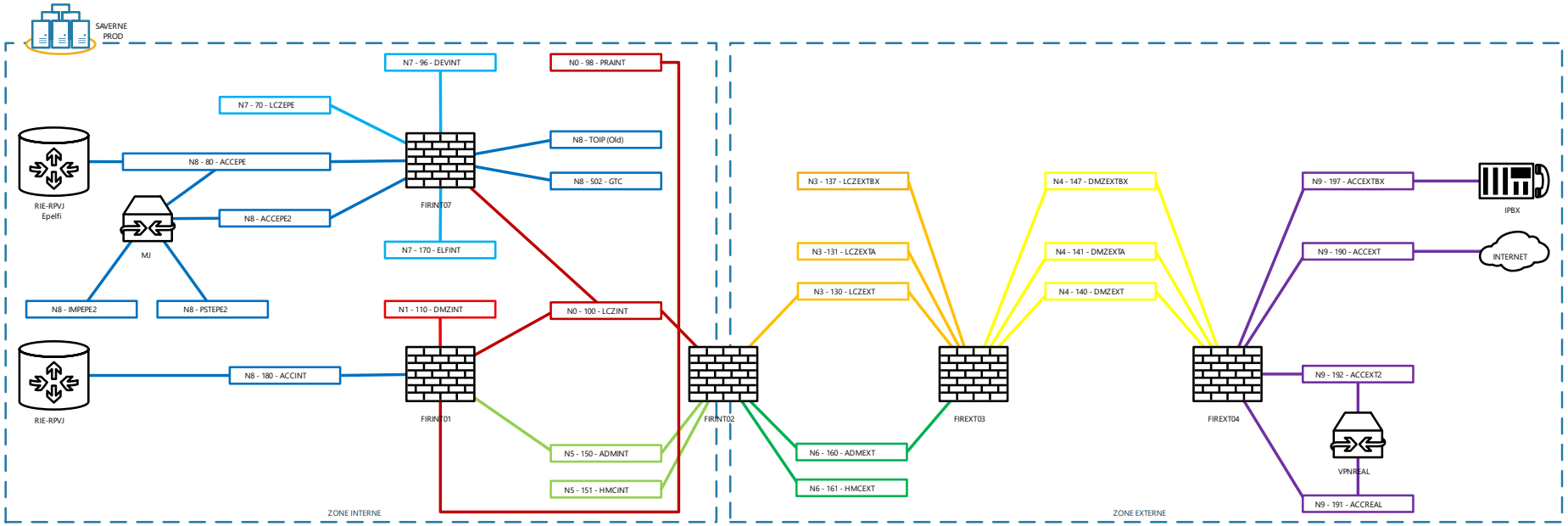


Figure 1 — Architecture de filtrage du site de Saverne (PROD)

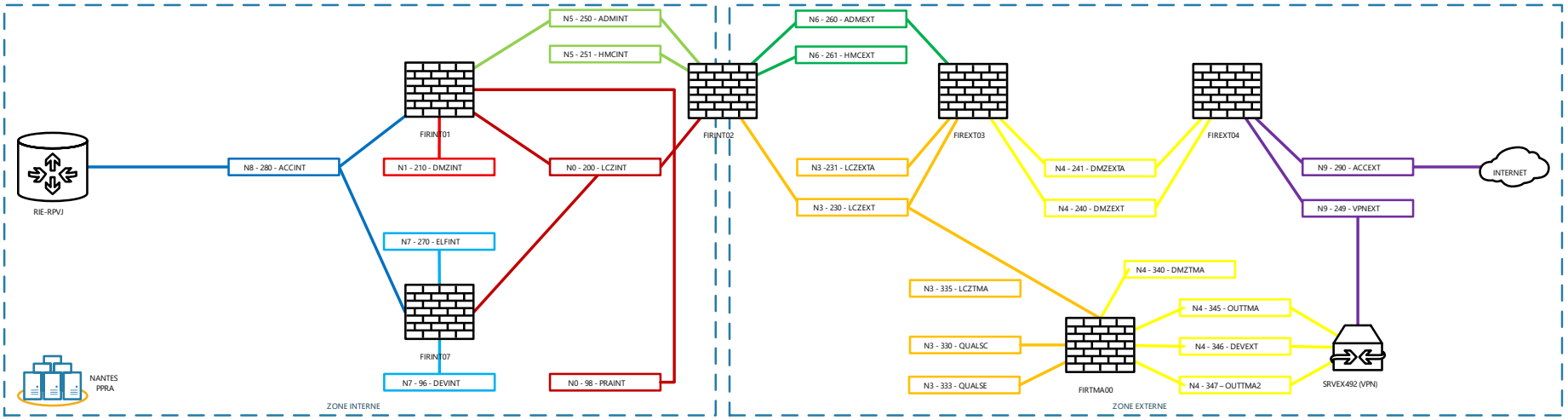


Figure 2 — Architecture de filtrage du site de Nantes (PPRA)

Croissance d'usage constatée

Sur une **année glissante** (mars 2025 – février 2026), les indicateurs de charge mesurés par les plateformes de supervision et de métrologie existantes sur l'ensemble des paires de pare-feux portent sur :

- **La charge CPU** moyenne et pic par cluster (cf. Annexe F) ;
- **La consommation mémoire** moyenne et pic par cluster ;
- **La bande passante réseau** (débit moyen et pic, en réception et en émission).

Les analyses (cf. Annexe F) montrent que **la capacité de traitement n'est pas un facteur dimensionnant** sur l'horizon du présent marché : **la marge retenue est de +5 %** de croissance organique annuelle.

Note — les pare-feux fournis seront amortis sur 7 ans. Leur dimensionnement doit donc rester pertinent au-delà de la durée contractuelle du présent marché.

Renforcement de la posture de sécurité

L'EPELFI exploite des services publics critiques (publicité foncière, registre associatif) soumis à un référentiel exigeant (RGS, recommandations ANSSI, contraintes Ministère de la Justice, RPVJ). Le renouvellement vise à changer les pare-feux en :

- Maintenant le niveau de sécurité actuel ;
- Optimisant les ressources matérielles et logicielles ;
- Assurant la présence d'au moins **deux solutions distinctes** afin de respecter les préconisations ANSSI ;
- Intégrant au moins une solution de filtrage qualifiée ANSSI sur les frontaux Internet (cf. §5.5.4), la souveraineté des solutions demeurant un élément d'appréciation de la valeur technique.

La description de l'infrastructure actuelle à reproduire est présentée à l'Article 4 (existant). Les principes d'architecture cible et les pistes de consolidation soumises au titulaire sont détaillés à l'Article 5.

4. Existant

4.1. Architecture générale des plateformes

Chaque site (Saverne PROD et Nantes PPRA) implémente une **séparation physique** des deux zones de sécurité majeures (zone interne / zone externe) ainsi qu'une **séparation des réseaux d'administration** des réseaux fonctionnels.

L'infrastructure compte **11 paires de pare-feux** (22 boîtiers) configurées en haute disponibilité actif/passif, organisées en clusters intra-site. Cinq identifiants logiques (FIRINT01, FIRINT02, FIRINT07, FIREXT03, FIREXT04) sont déployés en double instance : un cluster HA en production à Saverne et un cluster HA en préproduction / reprise d'activité à Nantes — soit 10 paires HA au total. Une onzième paire dédiée (FIRTMA00) porte le périmètre TMA AMALFI exclusivement à Nantes.

Les zones réseau gérées par les pare-feux comprennent :

Zones internes : production AMALFI, production AMALIA, administration, exploitation, infrastructure;
Zones externes : frontal Internet, frontal RPVJ (Réseau Privé Virtuel Justice), frontal partenaires ;

L'architecture comporte au total **49 zones VLAN**, **458 flux** documentés et **51 équipements** rattachés au plan de filtrage.

4.2. Inventaire des pare-feux (synthèse)

Le tableau ci-dessous présente une vue d'orientation des paires de pare-feux en service. **L'inventaire complet et détaillé** (identifiants physiques, modèles, dates de fin de support, topologie de chaque paire) est consolidé en **Annexe C**.

Identifiant logique	Site	Rôle
FIRINT01	Saverne (PROD) et Nantes (PPRA)	Accès internes via DMZ
FIRINT02	Saverne (PROD) et Nantes (PPRA)	Frontière zone interne ↔ zone externe
FIRINT07	Saverne (PROD) et Nantes (PPRA)	Accès internes ELFI (RPVJ et métiers)
FIREXT03	Saverne (PROD) et Nantes (PPRA)	Accès externes depuis DMZ
FIREXT04	Saverne (PROD) et Nantes (PPRA)	Accès externes vers DMZ (frontal Internet)
FIRTMA00	Nantes (PPRA)	Accès externes depuis VPN TMA AMALFI

4.3. Charge constatée

L'EPELFI a procédé à une analyse de la charge des pare-feux sur **12 mois pleins** (du 1er mars 2025 au 28 février 2026), à partir des exports issus des plateformes de supervision et de métrologie existantes. Les indicateurs collectés portent sur la charge CPU, la consommation mémoire, le nombre de sessions actives et le débit (en réception et en émission) sur l'ensemble des interfaces actives de chacune des paires de pare-feu du parc.

Les principaux constats sont les suivants :

- **Aucun pare-feu n'est contraint en CPU sur la période** : la charge moyenne reste inférieure à 3 % sur l'ensemble du parc, et le pic maximum constaté ne dépasse pas 12 % (FIRINT01) ;
- **Le profil de charge est dominé par deux paires** : FIRINT01 (cœur de production) et FIRINT07 (frontal arrière RPVJ + métiers) portent l'essentiel des volumes ;
- **Le boîtier dédié à la TMA AMALFI** présente une croissance des sessions actives de l'ordre de **+22 % sur 12 mois**, cohérente avec la dynamique d'usage observée au §3.3.2 ;
- **La capacité de traitement n'est pas un facteur dimensionnant** sur l'horizon du présent marché : les marges sont très significatives sur l'ensemble du parc.

Les **valeurs détaillées par boîtier** (charge CPU moyenne et pic, sessions actives moyennes et pic, débit moyen et pic, volume cumulé) sont consolidées en **Annexe F — Charge mesurée des pare-feux sur 12 mois**.

Les flux dimensionnants identifiés sont à traduire en exigences de capacité pour la cible (cf. §5.4).

4.4. Socle de supervision et de journalisation actuel

Le socle de supervision actuel s'appuie sur les plateformes de supervision et de métrologie existantes (cf. §3.3.2).

Le socle de supervision de l'EPELFI est appelé à évoluer, dans une logique d'harmonisation et d'unification des journaux de sécurité. La DSI prévoit l'adjonction d'une plateforme de centralisation des évènements de sécurité, dont la solution n'est pas arrêtée à ce jour. Les architectures proposées DOIVENT en conséquence présenter le plus haut degré d'interopérabilité possible avec ce type de solutions, afin de ne pas créer de contrainte d'intégration future.

4.5. Applicatifs structurants traversant les frontières de filtrage

Plusieurs composants applicatifs structurants franchissent les frontières de zones de sécurité et conditionnent la configuration cible :

Message Queuing — mécanisme de messaging / queuing assurant une rupture de protocole entre les zones internes et externes AMALFI. Ce flux critique inter-zones devra être explicitement traité dans les règles de filtrage cibles (cf. la matrice des flux établie en phase ANALYSE).

Reverse Proxy — reverse proxy de sécurité et SSO en frontal de la zone externe AMALFI. Il filtre les accès entrants des utilisateurs habilités et du grand public avant relais vers les serveurs applicatifs ; ses flux sortants vers Internet (validation OCSP, mise à jour de listes de révocation, etc.) sont à recenser lors de la migration.

5. Cible

5.1. Architecture existante et cible

L'architecture décrite ci-après est, pour l'essentiel, celle qui existe aujourd'hui : le présent marché n'en demande pas la refonte. Les exigences énoncées décrivent l'état à atteindre après renouvellement du matériel ; les seuls écarts recherchés par rapport à l'existant sont les pistes de consolidation soumises au titulaire au §5.1.3.

Principes d'architecture

L'architecture cible repose sur les principes suivants :

- **Défense en profondeur : l'architecture comporte au moins deux solutions distinctes de filtrage, conformément aux préconisations ANSSI. Au moins une des solutions de filtrage sur frontaux Internet DOIT être qualifiée ANSSI (cf. §5.5.4) ; la souveraineté des solutions est appréciée au titre de la valeur technique.**
- **Haute disponibilité généralisée** : tous les couples de pare-feux DOIVENT fonctionner en mode actif/passif, avec bascule automatique transparente.
- **Séparation stricte des plans** : plan de données, plan de contrôle et plan d'administration sont logiquement séparés, avec des réseaux d'administration dédiés et isolés.

Déchiffrement TLS et inspection profonde de paquets

Le **déchiffrement TLS et l'inspection profonde de paquets ne sont pas attendus** dans le cadre du présent marché. Cette position s'applique aussi bien aux flux entrants qu'aux flux sortants administrés et constitue un **élément structurant pour le dimensionnement** des pare-feux cibles.

> *Note d'orientation (hors exigence)* — l'activation ponctuelle de capacités de déchiffrement à des fins d'investigation ciblée demeure techniquement possible avec les solutions cibles. Cette possibilité ne constitue pas une exigence du présent marché.

Pistes de consolidation soumises au titulaire

L'EPELFI a identifié **trois pistes de consolidation non exclusives** qu'il soumet au titulaire pour étude et arbitrage technique. Le titulaire est invité à les analyser, à les retenir, à les amender ou à proposer une architecture alternative motivée techniquement (impact sécurité, capacité, résilience, coût, exploitabilité). **Toute alternative argumentée est recevable**.

Règle de panachage : tout flux en provenance d'Internet DOIT traverser au moins deux marques de pare-feux différentes. Au-delà de cette exigence, le cheminement peut s'effectuer sur une seule marque ; aucun panachage systématique n'est imposé.

Piste 1 — mutualisation soit de FIREXT03 et FIREXT04 (frontaux Internet), soit de FIRINT02 et FIREXT03, sur un cluster unique. Panachage de deux technologies et intégration d'au moins une solution souveraine qualifiée ANSSI. Le titulaire propose, dans son mémoire technique, le positionnement (première ou seconde ligne) de la solution souveraine qu'il estime le plus pertinent au regard du besoin, de son expertise de déploiement similaires et des recommandations ANSSI.

Piste 2 — fusion des fonctions portées par FIRINT01 (frontal interne production) et FIRINT07 (frontal arrière RPVJ et métiers) sur un couple unique avec montée en gamme prudente.

Piste 3 — intégration des fonctions de FIRTMA00 sous forme de **domaine virtuel TMA** au sein du cluster portant les fonctions FIREXT04 du site de Nantes, en préservant l'isolation logique requise pour la TMA AMALFI. Le service VPN d'accès distant demeure sur plateforme indépendante hors pare-feux.

Le titulaire DOIT prendre position formellement sur chacune de ces pistes dans son mémoire technique, en indiquant pour chaque piste : la décision retenue, la justification technique, l'impact estimé sur la sécurité, la capacité, la disponibilité et l'exploitation.

5.2. Périmètre matériel

Pare-feux à renouveler

L'ensemble des pare-feux listés au §4.2 **sera remplacé** dans le cadre du présent marché. Le titulaire propose le découpage fonctionnel et physique des équipements cibles ; cette proposition peut consister en :

- Un remplacement à l'identique de chaque paire ;
- Une mise en œuvre de tout ou partie des pistes de consolidation décrites au §5.1.3 ;
- Toute combinaison alternative motivée techniquement.

L'achat du matériel s'entent accompagné d'une garantie (support et maintenance) sur la durée du marché (3 ans).

Périphériques à intégrer (matériels existants conservés)

Matériel	Justification
Plateforme du service VPN d'accès distant	Conservée hors périmètre des pare-feux ; non touchée par le présent marché.

Périphériques de sécurité associés

Matériel	Statut
Solution de corrélation des journaux de sécurité — le titulaire DEVRA garantir la compatibilité avec le dispositif de journalisation immuable de l'EPELFI ou proposer une solution ad hoc équivalente ; dans tous les cas, les journaux DOIVENT être exportables vers le système de journalisation centralisé de l'EPELFI (cf. §5.3.3 et §5.3.4)	A intégrer par le titulaire

Outils de migration des règles de filtrage	À fournir / mobiliser par le titulaire ; le titulaire définit les règles cibles, les intègre sur les équipements de destination et prépare la migration avant déploiement sur site ; les équipes de l'EPELFI participent aux opérations de recette afin d'acquérir une compréhension opérationnelle de l'architecture cible.

Note d'orientation — l'EPELFI ne souhaite pas de console centralisée d'administration des pare-feux : l'administration s'effectue directement sur les équipements, depuis le site de Saverne. Les offres ne DOIVENT pas reposer sur un tel dispositif.

5.3. Exigences fonctionnelles

Filtrage

Les règles de filtrage cibles dépendent de l'architecture de sécurité retenue par le titulaire. Le titulaire DOIT procéder à la transposition complète des règles de filtrage actives vers la nouvelle architecture. Le jeu de règles livré DOIT permettre le bon fonctionnement de l'ensemble des applications et des flux communiqués par l'EPELFI ; aucun flux non validé par l'EPELFI ne DOIT être ouvert. La compatibilité avec les applications et les flux de l'EPELFI est appréciée pendant la période de vérification de service régulier proposée par le candidat. Cette migration DOIT faire l'objet d'une recette conjointe titulaire / l'EPELFI, sur la base d'un cahier de recettes fourni par le titulaire et coconstruit avec l'EPELFI, et d'une phase de probation en conditions réelles, dont les modalités sont définies au §6.3.

Authentification multi-facteurs

- L'**authentification multi-facteurs DOIT être activée** pour l'ensemble des accès administrateurs (CLI, GUI, API) sur tous les pare-feux. Cette exigence reflète la recommandation ANSSI PA-044.
- Le mécanisme d'authentification multi-facteurs s'appuie sur des comptes locaux définis sur les équipements et sur un dispositif d'authentification multi-facteurs de type AIR GAP. Les pare-feux n'étant pas rattachés à l'annuaire Active Directory (AD) de l'EPELFI à ce jour, l'authentification multi-facteurs ne suppose pas leur intégration à un annuaire d'identité externe.
- L'administration des pare-feux s'effectue exclusivement sur le site de Saverne. Aucun accès distant n'est ouvert au titulaire ; l'authentification multi-facteurs sécurise les seuls accès d'administration internes et ne constitue pas une ouverture d'accès externe.

Journalisation et stockage immuable

Les pare-feux journalisent en interne ; les journaux sont consultables depuis les pare-feux. La rétention, d'au moins douze (12) mois, et l'immuabilité des journaux de sécurité sont portées par la solution retenue.

L'EPELFI dispose d'une capacité de stockage immuable, non activée à ce jour. Le titulaire DOIT, au choix, s'appuyer sur cette capacité ou proposer une solution embarquée assurant l'immuabilité. Dans tous les cas, la solution DOIT garantir une interopérabilité démontrée avec les solutions de centralisation du marché et une capacité d'export des journaux dans des formats et protocoles standard, que le candidat précise dans son mémoire technique (cf. §5.3.4). L'analyse avancée des journaux ne relève pas du présent marché.

Supervision

Le titulaire DOIT garantir que la métrologie des pare-feux peut être remontée vers un système tiers, dans des formats et protocoles standard. L'attendu porte sur la capacité d'export des indicateurs de bon fonctionnement : charge du processeur, mémoire, bande passante et état de santé des équipements. Le travail d'interconnexion avec le système de supervision est réalisé par la DSI de l'EPELFI.

5.4. Exigences de capacité et de flux

Dimensionnement

Le dimensionnement de la cible DOIT prendre en compte :

- La charge constatée sur 12 mois (cf. §4.3 et Annexe F) ;
- Une **marge de croissance organique de +5 % par an** sur la durée du marché ;

- La capacité de scalabilité décrite au §5.1.1.

Le titulaire fournit dans son mémoire technique les calculs de dimensionnement détaillés (sessions, débit, CPS) par équipement cible.

Flux critiques

Les flux critiques interzones documentés dans la matrice des flux établie en phase ANALYSE DOIVENT être explicitement traités dans la configuration cible. Ils incluent notamment les flux Message Queuing et Reverse Proxy mentionnés au §4.5.

5.5. Exigences de sécurité

Les exigences ci-dessous traduisent le cadre de sécurité retenu pour le présent marché. Elles constituent les bonnes pratiques de sécurité attendues du titulaire.

Authentification et contrôle d'accès

- Authentification multi-facteurs obligatoire sur tous les accès administrateurs (cf. §5.3.2) ;
- Séparation des rôles administrateurs (administrateur fonctionnel, administrateur sécurité, auditeur) ;
- Journalisation exhaustive des actes d'administration.
- Comptes d'administration strictement nominatifs et rotation périodique des secrets d'authentification ;
- Les opérations d'administration et d'exploitation des pare-feux s'effectuent exclusivement depuis les locaux de l'EPELFI ;
- Les équipements du site de Nantes sont administrés depuis le site de Saverne, au travers du plan d'administration inter-sites (cf. §9.1).

Cloisonnement et défense en profondeur

- Présence d'au moins deux solutions distinctes de filtrage (préconisations ANSSI), dont au moins une qualifiée ANSSI sur les frontaux Internet (cf. §5.5.4) ;
- Séparation stricte des plans de données, de contrôle et d'administration.

Traçabilité

- Stockage immuable des journaux (cf. §5.3.3) ;
- Horodatage sur référence de temps unique ;
- Capacité d'export des journaux vers un système de corrélation externe.

Conformité et qualification

Au moins une des solutions de filtrage sur frontaux Internet DOIT être **qualifiée ANSSI** au moment de la mise en exploitation ; son positionnement (première ou seconde ligne) est laissé à l'appréciation du titulaire, motivé dans le mémoire technique ;

Le titulaire DOIT préciser le niveau de qualification (Élémentaire, Standard ou Renforcée) et la date de validité de la qualification ;

La qualification ANSSI exigée DOIT être maintenue pendant toute la durée du marché. À défaut de renouvellement par l'ANSSI, le titulaire DOIT en informer l'EPELFI sans délai et proposer un plan de mise en conformité.

La conformité aux référentiels applicables (RGS, recommandations ANSSI, contraintes Justice) DOIT être documentée.

5.6. Maintien en conditions de sécurité (MCS)

Le titulaire assure le maintien en conditions de sécurité de l'ensemble des solutions retenues dans le cadre du marché, indépendamment de la marque ou du constructeur. Ce maintien en conditions de sécurité comprend :

- La supervision des pare-feux et l'exploitation des journaux ;
- Le reporting ;
- La veille sur les vulnérabilités (CVE) et la mesure de leurs impacts ;
- L'application des correctifs et les montées de version quand elles sont nécessaires.

Toute autre activité hors de ce périmètre est hors marché et sera traitée de gré à gré, en mode projet.

Les changements pris en charge au titre du maintien en conditions de sécurité s'entendent des gestes techniques courants sur les configurations (création ou modification d'un compte, modification des paramètres d'un réseau local virtuel, et opérations de même nature). Tout changement majeur est traité en mode projet, de gré à gré, hors du présent marché.

Les opérations de maintien en conditions de sécurité portant sur les équipements du site de Nantes — application des correctifs, supervision, exploitation des journaux — sont réalisées par le titulaire depuis le site de Saverne, au travers du plan d'administration inter-sites.

Le titulaire **PEUT solliciter les éditeurs** des solutions retenues en tant que de besoin pour conduire cet accompagnement. La responsabilité du pilotage de l'accompagnement reste celle du titulaire.

Les modalités précises (volume de jours, délais de réaction, périodicité des revues) sont précisées dans le mémoire technique.

La MCS n'inclut ni la maintenance ni la gestion des flux — ouverture, fermeture et modification des règles de filtrage, déclaration des objets — qui demeurent sous la responsabilité de l'EPELFI (cf. §2.2), le titulaire étant consulté. La répartition des responsabilités entre l'EPELFI et le titulaire (cf. §2.3) est portée par la matrice RACI figurant au §3.2 du présent CCTP et dans la foire aux questions issue du sourçage, pièce du marché ; les urgences de sécurité (par exemple la publication d'une CVE critique) font l'objet d'une escalade vers l'EPELFI et d'une coordination en comité de pilotage (cf. §9.4).

6. Prestations attendues du titulaire

Le titulaire produit, dès le démarrage du marché, un plan d'assurance qualité (PAQ) qui cadre l'ensemble des opérations et formalise la gouvernance du marché. Le PAQ figure parmi les premiers livrables et est validé par l'EPELFI.

Le titulaire conduit la prestation en cinq phases successives, complétées par une obligation de réversibilité.

6.1. Phase ANALYSE

Objectif : produire la connaissance partagée nécessaire à la conception. Cette phase comprend :

- La prise en main du contexte technique et fonctionnel auprès des équipes de l'EPELFI ;
- La consolidation de l'inventaire détaillé des règles de filtrage existantes par paire de pare-feux;
- La cartographie détaillée des flux et l'identification des flux critiques (cf. la matrice des flux) ;
- L'identification des contraintes spécifiques (RPVJ, TMA AMALFI, journalisation, plages CGNAT) ;
- La production d'une **note d'analyse** validée par l'EPELFI avant passage en phase CONCEPTION.

Les candidats proposent un rétroplanning détaillé de cette phase dans leur offre ; aucune durée n'est imposée par l'EPELFI.

6.2. Phase CONCEPTION

Objectif : produire l'architecture cible détaillée et la valider avec l'EPELFI.

- la production de l'**architecture cible** intégrant la prise de position du titulaire sur les pistes de consolidation (cf. §5.1.3) ;
- la définition de la matrice des flux cible et du plan de migration des règles validé conjointement avec l'EPELFI avant passage en phase DÉPLOIEMENT ;
- la définition du plan de bascule détaillé dont l'ordre de bascule des sites relève de la stratégie proposée par le candidat ; pour le site de Nantes, le plan précise les gestes physiques exécutés par les équipes internes de l'EPELFI, sous la responsabilité du titulaire, et les procédures écrites que celui-ci leur fournit ;
- la définition des procédures de retour arrière ;
- la production du **Dossier d'Architecture Technique (DAT)** validé par l'EPELFI avant passage en phase DÉPLOIEMENT.

> Note d'orientation — le plan d'adressage IP existant n'est pas un axe de transformation du présent marché : il n'est pas demandé de le refaire. Les adaptations à la marge qu'imposerait la factorisation de clusters (cf. §5.1.3) sont en revanche attendues et documentées par le titulaire.

Le calendrier de cette phase relève du rétroplanning proposé par les candidats (cf. §6.1).

6.3. Phase DÉPLOIEMENT

Objectif : déployer, migrer, recetter et basculer en production.

- La **fourniture, la livraison, la mise en baie, l'installation et le câblage des équipements** : ces gestes physiques sont exécutés par le titulaire ou, en accord avec l'EPELFI, par ses équipes internes — cette délégation, que l'EPELFI souhaite, est systématique sur le site de Nantes, où le titulaire n'intervient pas en présentiel. Quel qu'en soit l'exécutant, ils s'accomplissent **sous la responsabilité du titulaire et sur ses procédures écrites**. La mise en configuration initiale est réalisée par le titulaire la production d'un plan de recette couvrant la bascule PPRA Nantes vers PROD Saverne ;
- La définition par le titulaire des règles cibles, leur intégration sur les équipements de destination et leur préparation avant déploiement sur site ; les équipes de l'EPELFI participent aux opérations de recette afin d'acquérir une compréhension opérationnelle de l'architecture cible ;
- L'intégration de la solution de journalisation immuable (solution de l'EPELFI ou solution ad hoc du titulaire, cf. §5.3.3);
- La recette unitaire et la recette d'intégration ;
- La **bascule en production** selon le plan validé en phase CONCEPTION ;
- Une période de vérification de service régulier (VSR), à inclure dans la démarche proposée par le candidat, sans durée ni modalité imposée ; elle est clôturée par un procès-verbal de VSR.
- Une phase de recette conjointe titulaire / EPELFI permettant de valider l'architecture cible et la configuration déployée ; la recette est prononcée site par site (site de Nantes puis site de Saverne, conformément au plan de bascule du §6.2) et formalisée par un procès-verbal contradictoire. Sur le site de Nantes, la recette logique est exécutée par le titulaire depuis le site de Saverne ; les contrôles physiques sont réalisés par les équipes internes de l'EPELFI, sur liste de contrôle fournie par le titulaire.

Le titulaire DOIT assurer la disponibilité de moyens de retour arrière pendant toute la durée de la bascule.

Les couvertures post-bascule sont distinctes : (i) la garantie matérielle du constructeur, dont le titulaire DOIT préciser la durée, au moins égale à la durée du marché ; (ii) la vérification de service régulier (VSR) définie ci-dessus ; (iii) le maintien en conditions de sécurité (MCS, cf. §5.6 et tranche ferme n°3). Aucune phase de garantie « prestation » distincte n'est exigée après la VSR, la couverture des évolutions et des incidents relevant ensuite de la MCS.

6.4. Phase DOCUMENTATION

Objectif : doter l'EPELFI d'un corpus documentaire complet permettant l'exploitation, la maintenance et la sécurisation autonomes de l'environnement cible.

- La livraison du **Dossier d'Exploitation (DEX)** : procédures d'exploitation, procédures d'incident, procédures de mise à jour ;
- La livraison du **Dossier d'Installation (DIN)** : procédures d'installation et de remise en état ;
- La livraison du dossier d'installation et de câblage par site (Saverne et Nantes) : plans de baie, plan de câblage et procédures pas-à-pas. Destiné à la réalisation de l'installation, ce dossier est distinct du dossier d'installation (DIN), qui porte les procédures de réinstallation et de remise en état en exploitation ;
- La livraison du **Dossier de Sécurité (DSE)** : durcissement, configuration de référence, procédures de gestion des correctifs ;
- La livraison de la **matrice des flux** cible documentée ;

- La livraison du **DAT finalisé** après bascule (mise à jour du DAT initial produit en phase CONCEPTION pour refléter la configuration effectivement déployée).

Les livrables documentaires DOIVENT être fournis en français, en formats éditables (Word, Excel, Visio ou équivalents libres) **et** PDF.

6.5. Phase FORMATION ET TRANSFERT DE COMPÉTENCES

Objectif : doter l'EPELFI de la capacité humaine à exploiter et maintenir l'environnement cible en autonomie.

Cette phase comprend deux composantes complémentaires :

Formation des équipes de l'EPELFI

- Le titulaire DOIT organiser des **sessions de formation** dédiées aux équipes de l'EPELFI sur les solutions mises en œuvre, couvrant a minima les volets administration, exploitation, sécurité et journalisation. Les formations DOIVENT être adaptées au contexte opérationnel de l'EPELFI et réalisées sur l'architecture réellement déployée, sur les sites de l'EPELFI.
- Le format peut combiner présentiel sur les sites de l'EPELFI et distanciel synchrone, à l'appréciation du titulaire et sur accord de l'EPELFI.
- Les supports de formation (slides, manipulations, fiches réflexes) sont livrés à l'EPELFI en version pérenne et réutilisable.
- Les modalités précises (volume de jours par profil, public cible, dispositif d'évaluation) sont précisées dans le mémoire technique.

Transfert de compétences opérationnel

Le titulaire DOIT organiser un **transfert de compétences accompagné** sur les opérations courantes (gestion des règles, exploitation des journaux, gestion des incidents, gestion des correctifs). Le transfert porte sur les solutions et procédures pour l'EPELFI, en particulier celles que les équipes seront amenées à exploiter au titre du MCO.

Le transfert s'inscrit dès les opérations de migration et de recette, et se poursuit dans la continuité de la bascule et de la période de vérification de service régulier, en mode binôme avec les exploitants de l'EPELFI sur des cas réels.

À l'issue du transfert, le titulaire produit une **attestation de transfert de compétences** validée conjointement par l'EPELFI et le titulaire.

6.6. Réversibilité

Le titulaire DOIT prévoir et documenter les conditions de réversibilité de la prestation, à savoir :

- la documentation complète et exhaustive permettant à l'EPELFI ou à un tiers désigné de reprendre l'exploitation, la maintenance et l'évolution de l'environnement cible ;
- les modalités de transfert des configurations, des journaux historiques et des éléments de licence ;
- les délais et les modalités d'accompagnement à la réversibilité, sur sollicitation de l'EPELFI, dans la limite d'un délai maximal d'accompagnement de trois (3) mois à compter de la sollicitation.

Le fonds documentaire de réversibilité (état de situation, documents socle et d'architecture à jour, procédures d'exploitation, extraction des tickets) est défini dans le plan d'assurance qualité (PAQ) produit par le titulaire. Les conditions contractuelles de réversibilité relèvent du CCAP.

7. Tranches et calendrier

Le marché, mono-attributaire, est structuré en trois tranches fermes. Le repère T0 correspond au premier jour de démarrage de la phase de BUILD (notification de la commande au titulaire).

Structure retenue : trois tranches fermes —

- TF1 « BUILD »,
- TF2 « Formation et transfert vers l'exploitation »,
- TF3 « Maintien en conditions de sécurité ».

Le maintien en conditions opérationnelles (MCO) des pare-feux est assuré par l'EPELFI (cf. §2.3).

La décomposition financière du marché figure à l'annexe E.

7.1. Tranche ferme n°1 (TF1) — BUILD (renouvellement et déploiement)

Périmètre

La tranche ferme couvre l'intégralité du renouvellement matériel et son accompagnement post-bascule, à savoir :

- Sur le site de Saverne (PROD) : la fourniture, l'installation et la mise en baie des pares-feux ainsi que la production du dossier d'installation et de câblage du site ; les gestes physiques peuvent, en accord avec l'EPELFI, être exécutés par ses équipes internes, sous la responsabilité du titulaire et sur ses procédures écrites ; sur le site de Nantes (PPRA), y compris le périmètre de la TMA AMALFI : la fourniture, la livraison, la préparation et la configuration des équipements ainsi que la production du dossier d'installation et de câblage, l'installation physique et la mise en baie étant exécutées par les équipes internes de l'EPELFI sous la responsabilité du titulaire, sur ses procédures écrites ; le titulaire n'intervient jamais en présentiel sur le site de Nantes ;
- La conception détaillée de l'architecture cible et la production des dossiers associés (DAT, plan de migration, plan de bascule) ;
- La définition des règles cibles de l'architecture de sécurité par le titulaire, leur intégration sur les équipements et leur préparation avant déploiement sur site, les équipes de l'EPELFI participant aux opérations de recette ;
- La mise en exploitation, la recette et la bascule en production ;
- La documentation d'exploitation et le transfert de compétences vers les équipes de l'EPELFI ;
- La garantie constructeur sur dysfonctionnement matériel (remplacement sur défaut) couvrant l'ensemble du matériel fourni pour toute la durée du marché.

Durées

Phase de déploiement (Build) — sites Saverne et Nantes : la date de bascule en production constitue un critère technique de l'offre ; la vérification de service régulier est conduite selon la démarche proposée par le candidat (cf. §6.3), aucune durée ni date fixe n'étant imposée ; seul le moratoire de mise en production constitue un jalon ferme.

L'EPELFI souhaite que la phase de BUILD soit close avant la fin de l'année 2026. Ce souhait ne constitue pas un jalon ferme : le moratoire de mise en production du 18 décembre 2026 au 4 janvier 2027 demeure la seule contrainte de calendrier opposable. Les plannings proposés sont appréciés au titre de la valeur technique de l'offre.

Garantie constructeur sur le matériel : couvre l'ensemble de la durée du marché.

Livrables associés

Note d'analyse (cf. §6.1), DAT (cf. §6.2), DEX / DIN / DSE (cf. §6.4), procès-verbal de VSR par site.

7.2. Tranche ferme n°2 (TF2) — Formation et transfert vers l'exploitation

Périmètre

Pour la solution retenue, le titulaire DOIT proposer un dispositif de formation et de transfert vers l'exploitation à deux niveaux :

- Formations sur la nouvelle technologie (administration, exploitation, sécurité) ;
- Volume de jours d'experts pour les gestes techniques en accompagnement des équipes de l'EPELFI.

Découpage et durée

La tranche ferme n°2 est un forfait unique, engagé dès la notification du marché.

7.3. Tranche ferme n°3 (TF3) — Maintien en conditions de sécurité (MCS)

Périmètre

La tranche ferme n°3 (TF3) couvre le maintien en conditions de sécurité (MCS) de l'ensemble des pares-feux installés, dont le périmètre est défini au §5.6.

La gestion des flux — ouverture, fermeture et modification des règles, déclaration des objets — demeure sous la responsabilité de l'EPELFI (cf. §2.2 et §5.6), le titulaire étant consulté. Le MCO des pares-feux étant assuré par l'EPELFI (cf. §2.3), en cas de divergence à la frontière entre exploitation et sécurité, l'arbitrage relève de l'EPELFI.

Découpage et durée

La tranche ferme n°3 (MCS) démarre à l'issue de la phase de Build et couvre la durée du marché, fixée à trois (3) ans fermes. Les modalités de renouvellement et d'extension éventuelle relèvent du CCAP/RC.

La continuité de la MCS et de la garantie matérielle au-delà de la durée du marché (trois ans) est hors périmètre du présent marché ; le risque résiduel correspondant — le parc étant amorti sur sept ans (cf. §3.3.2) — est accepté et formalisé au registre des risques (cf. CCAP).

Engagement

La tranche ferme n°3 (MCS) est engagée dès la notification du marché ; elle ne fait pas l'objet d'un affermissement. Son exécution démarre à l'issue de la phase de BUILD (mise en service).

7.4. Calendrier de référence

Les jalons principaux pressentis sont :

- T0 : notification de la commande au titulaire ;
- Bascule en production effective de chaque site (mise en service) : la date de livraison constitue un critère technique de l'offre, sans borne maximale imposée ;

- Mise en service : démarrage de l'engagement de la MCS (tranche ferme n°3) ;
  Moratoire de mise en production du 18 décembre 2026 au 4 janvier 2027 inclus : aucune bascule ni mise en production sur cette période ;
  Vérification de service régulier (VSR) : selon la démarche proposée par le candidat (cf. §6.3), aucune durée ni date fixe n'étant imposée ; seul le moratoire de mise en production constitue un jalon ferme.

Les durées indicatives ci-dessus pourront être ajustées d'un commun accord entre l'EPELFI et le titulaire en fonction du calendrier détaillé arrêté en phase CONCEPTION.

8. Livrables

Le titulaire produit, livre et fait valider les livrables suivants :

#	Livrable	Phase / jalon (réf. CCTP)	Tranche	Condition d'acceptation
1	Plan d'assurance qualité (PAQ) — cadrage des opérations et gouvernance du marché	Amont / gouvernance	TF1 — BUILD	Validé par l'EPELFI ; fourni parmi les premiers livrables
2	Note d'analyse	Phase ANALYSE (§6.1)	TF1 — BUILD	Validée par l'EPELFI avant passage en phase CONCEPTION
3	Architecture cible (prise de position sur les pistes de consolidation, §5.1.3)	Phase CONCEPTION (§6.2)	TF1 — BUILD	Validée par l'EPELFI
4	Dossier d'Architecture Technique (DAT)	Phase CONCEPTION (§6.2)	TF1 — BUILD	Validé par l'EPELFI avant passage en phase DÉPLOIEMENT
5	Matrice des flux cible et plan de migration des règles	Phase CONCEPTION (§6.2)	TF1 — BUILD	Validés conjointement avec l'EPELFI avant passage en phase DÉPLOIEMENT
6	Plan de recette (bascule PPRA Nantes → PROD Saverne)	Phase DÉPLOIEMENT (§6.3)	TF1 — BUILD	Validé par l'EPELFI
7	Procès-verbal de VSR	Phase DÉPLOIEMENT (§6.3)	TF1 — BUILD	VSR clôturée ; les réserves éventuelles font l'objet d'un plan d'action convenu avec l'EPELFI.
8	Dossier d'installation et de câblage par site — Saverne (PROD) et Nantes (PPRA) : plans de baie, plan de câblage et procédures pas-à-pas	Phase DOCUMENTATION (§6.4)	TF1 — BUILD	Un dossier par site. Pour le site de Nantes, installation exécutable par les équipes internes de l'EPELFI sans assistance en présentiel.
9	Dossier d'Exploitation (DEX)	Phase DOCUMENTATION (§6.4)	TF1 — BUILD	Livré : procédures d'exploitation, d'incident et de mise à jour
10	Dossier d'Installation (DIN)	Phase DOCUMENTATION (§6.4)	TF1 — BUILD	Livré : procédures d'installation et de remise en état
11	Dossier de Sécurité (DSE)	Phase DOCUMENTATION (§6.4)	TF1 — BUILD	Livré : durcissement, configuration de référence, gestion des correctifs
12	Matrice des flux cible documentée	Phase DOCUMENTATION (§6.4)	TF1 — BUILD	Livrée
13	DAT finalisé après bascule	Phase DOCUMENTATION (§6.4)	TF1 — BUILD	Mis à jour pour refléter la configuration effectivement déployée
14	Supports de formation (slides, manipulations, fiches réflexes)	Phase FORMATION ET TRANSFERT DE	TF2 — Formation et	Livrés en version pérenne et réutilisable

		COMPÉTENCES (§6.5.1)	transfert vers l'exploitation	
15	Attestation de transfert de compétences	Phase FORMATION (§6.5.2)	TF2 — Formation et transfert vers l'exploitation	Validée conjointement par l'EPELFI et le titulaire
16	Fonds documentaire de réversibilité	Réversibilité (§6.6)	—	Renvoyé au plan d'assurance qualité (PAQ) ; clause contractuelle au CCAP

Les livrables documentaires DOIVENT être fournis en français, en formats éditables (Word, Excel, Visio ou équivalents libres) **et** PDF.

9. Conditions d'exécution

9.1. Localisation des prestations

Les prestations s'exécutent principalement sur le site de **Saverne (siège de l'EPELFI)** et de **Nantes (SNMJ)**. Une part des prestations d'analyse, de conception et de documentation peut s'exécuter à distance, sur accord de l'EPELFI.

Les opérations d'administration et d'exploitation des pare-feux s'effectuent exclusivement depuis les locaux de l'EPELFI. Les équipements du site de Nantes (PPRA) sont administrés depuis le site de Saverne, au travers du plan d'administration inter-sites. Aucun accès d'administration depuis l'extérieur du système d'information de l'EPELFI n'est autorisé. Aucune intervention en présentiel du titulaire n'a lieu sur le site de Nantes, en phase de BUILD comme en RUN.

Aucun accès distant n'étant ouvert (cf. §5.5.1), le titulaire organise une présence sur site permettant de tenir les engagements de prise en charge. Les interventions se déroulent en heures ouvrées ; l'accès aux sites est assuré avec le concours des équipes de l'EPELFI. Les conditions d'accès aux sites sont précisées au CCAP (cf. §9.2).

9.2. Habilitations et confidentialité

Le titulaire et ses sous-traitants éventuels DOIVENT respecter les obligations de confidentialité et de protection des informations propres au contexte de l'EPELFI / Ministère de la Justice.

Le titulaire DOIT respecter les procédures d'accès aux locaux et aux systèmes de l'EPELFI.

9.3. Sous-traitance

La sous-traitance est admise dans les conditions du CCAP. Le titulaire reste pilote et responsable de l'ensemble de la prestation, y compris des parties sous-traitées.

9.4. Comitologie

La gouvernance du marché repose sur trois instances : le comité de suivi (COSUI), quinzomadaire, d'une durée de 30 minutes, tenu en visioconférence ; le comité de pilotage (COPIL), trimestriel, d'une durée de 2 heures, tenu sur le site de Saverne ; le comité stratégique (COSTRA), annuel, d'une durée de 2 heures, tenu sur le site de Saverne. Le responsable de la sécurité des systèmes d'information de l'EPELFI participe au comité de pilotage et au comité stratégique.

Le titulaire prépare et anime le comité de suivi et le comité de pilotage. Le comité stratégique est préparé et animé par l'EPELFI (direction des systèmes d'information), sous la responsabilité du directeur général ; le titulaire y est consulté.

L'interface entre le maintien en conditions de sécurité et le maintien en conditions opérationnelles, qui relève d'un marché distinct, est traitée au comité de pilotage ; les urgences de sécurité font l'objet d'une escalade vers l'EPELFI (cf. §5.6).

L'EPELFI installe une gouvernance documentée (plan de gouvernance intégré au PAQ), en accord avec le titulaire, et arbitre les situations d'urgence par voie d'escalade. Les candidats chiffrent dans leur offre la charge de pilotage correspondante.

9.5. Outils

Le titulaire fournit l'intégralité de l'outillage nécessaire à l'exécution des prestations, au premier rang duquel l'outil d'ouverture et de gestion des tickets. L'EPELFI n'utilise pas et ne met pas à disposition l'accès à ses propres outils. Le paramétrage de cet outillage, susceptible de nécessiter un délai, ainsi que son coût, sont intégrés par le candidat dans son offre.

Annexe A : Glossaire

Acronyme / Terme	Définition
AD	annuaire d'utilisateurs et de droits.
AMALFI	Application de gestion de la publicité foncière d'Alsace-Moselle (Livre Foncier informatisé).
AMALIA	Application de gestion du registre des associations.
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information.
CCAP	Cahier des Clauses Administratives Particulières.
CCTP	Cahier des Clauses Techniques Particulières.
CGNAT	Carrier-Grade Network Address Translation — translation d'adresses à grande échelle (plages 100.64.0.0/10).
COPIL	Comité de pilotage du marché (cf. §9.4).
COSTRA	Comité stratégique du marché (cf. §9.4).
COSUI	Comité de suivi du marché (cf. §9.4).
CPS	*Connections Per Second* — connexions par seconde, métrique de capacité d'un pare-feu.
CVE	Common Vulnerabilities and Exposures — référentiel public des vulnérabilités logicielles.
DAT	Dossier d'Architecture Technique.
DCE	Dossier de Consultation des Entreprises.
DEX / DIN / DSE	Dossier d'Exploitation / Dossier d'Installation / Dossier de Sécurité.
DMZ	*Demilitarized Zone* — zone démilitarisée, segment réseau servant d'interface entre Internet et le SI interne.
Domaine virtuel	Instance de filtrage logiquement isolée au sein d'un même équipement physique de filtrage (terme générique, indépendant de la technologie cible).
DQE	Détail Quantitatif Estimatif.

DSI	Direction des Systèmes d'Information de l'EPELFI.
HA	Haute Disponibilité (en cluster ou en paire actif/passif).
MCO	Maintien en Conditions Opérationnelles.
MCS	Maintien en Conditions de Sécurité.
MFA	*Multi-Factor Authentication* — authentification multi-facteurs.
MQ	Abréviation de Message Queuing — mécanisme de messaging / queuing avec rupture de protocole (cf. §4.5).
NAT	*Network Address Translation* — translation d'adresses réseau.
NTP	*Network Time Protocol* — protocole de synchronisation horaire entre équipements.
OCSP	*Online Certificate Status Protocol* — protocole de vérification en ligne du statut des certificats.
PAQ	Plan d'Assurance Qualité.
PCA	Plan de Continuité d'Activité.
PPRA	Plate-forme de Pré-production et de Reprise d'Activité.
PRA	Plan de Reprise d'Activité.
PRM	Personne Responsable du Marché.
PROD	Plateforme de production.
Qualifié ANSSI	Solution ayant reçu une qualification de l'ANSSI à un niveau donné (Standard, Renforcé, Élémentaire), attestant son adéquation aux besoins de sécurité de l'État.
RACI	Matrice de répartition des responsabilités : réalise, approuve, consulté, informé.
RC	Règlement de la Consultation.
RGS	Référentiel Général de Sécurité.
RPVJ	Réseau Privé Virtuel Justice — réseau dédié du Ministère de la Justice.
SAN	*Storage Area Network* — réseau dédié de stockage par blocs.
SI	Système d'Information.
SNMJ	Site Nantais du Ministère de la Justice.
SNMP	Simple Network Management Protocol — protocole de supervision des équipements réseau.
SSO	*Single Sign-On* — authentification unique.
TF	Tranche ferme du présent marché. Le marché comporte trois tranches fermes : TF1 BUILD, TF2 formation et transfert vers l'exploitation, TF3 maintien en conditions de sécurité (MCS). Le maintien en conditions opérationnelles (MCO) des pare-feux est assuré par l'EPELFI (cf. §2.3).
TLS	*Transport Layer Security* — protocole de sécurisation des échanges.
TMA	Tierce Maintenance Applicative.
VLAN	Virtual Local Area Network — réseau local virtuel.
VPN	*Virtual Private Network* — réseau privé virtuel.
VSR	Vérification de Service Régulier.

Annexe B : sans objet

Sans objet.

Annexe C : Liste des équipements existants

Identifiant logique	Identifiant physique	Modèle	Site	Rôle	Topologie	Fin de support
FIRINT01 A/B	FIR001 A/B	MARQUE B	Saverne (PROD) et Nantes (PPRA)	Accès internes via DMZ	2 paires HA (1 par site)	31/08/2026
FIRINT02 A/B	FIR003 A/B	MARQUE A	Saverne (PROD) et Nantes (PPRA)	Frontière zone interne ↔ zone externe	2 paires HA (1 par site)	17/06/2026
FIRINT07 A/B	FIR701 A/B	MARQUE B	Saverne (PROD) et Nantes (PPRA)	Accès internes ELFI (RPVJ et métiers)	2 paires HA (1 par site)	31/08/2026
FIREXT03 A/B	FIR301 A/B	MARQUE B	Saverne (PROD) et Nantes (PPRA)	Accès externes depuis DMZ	2 paires HA (1 par site)	31/08/2026
FIREXT04 A/B	FIR401 A/B	MARQUE A	Saverne (PROD) et Nantes (PPRA)	Accès externes vers DMZ (frontal Internet)	2 paires HA (1 par site)	17/06/2026
FIRTMA00 A/B	FIRTMA	MARQUE A	Nantes (PPRA)	Accès externes depuis VPN TMA AMALFI	Paire HA	17/06/2026

Annexe D : sans objet

Sans objet.

Annexe E : Détail Quantitatif estimatif (DQE)

La pièce financière du marché est le détail quantitatif estimatif (DQE), fourni au format tableur avec le présent dossier de consultation.

Le candidat le complète et le remet dans son offre.

Aucun bordereau des prix unitaires n'est demandé.

Annexe F : Charge mesurée des paresf-feux sur 12 mois

Le tableau ci-dessous synthétise les indicateurs de charge mesurés sur la période **1er mars 2025 → 28 février 2026** (12 mois pleins) à partir des exports des plateformes de supervision et de métrologie existantes fournis par l'EPELFI. Les indicateurs sont exprimés par paire de pare-feux ; lorsque la mesure est disponible séparément sur les deux nœuds HA, c'est la valeur la plus élevée des deux nœuds qui est retenue pour la moyenne et pour le pic.

F.1. Charge CPU et mémoire

Pare-feu	CPU moyen	CPU pic (date)	Mémoire (régime)
FIRINT01	2,3 %	11,5 % (15/09/2025 14h)	n/a *(non remonté)*
FIRINT02	< 0,1 %	0,9 %	28–30 % stable
FIRINT07	1,3 %	7,7 % (16/07/2025 08h)	n/a *(non remonté)*
FIREXT03	1,0 %	1,3 % (01/03/2025 07h)	n/a *(non remonté)*
FIREXT04	< 0,1 %	0,6 % (17/07/2025 14h)	22–23 % puis 29–30 % (step-change 07/2025)
FIRTMA00	< 0,1 %	2,5 %	27–28 % stable

Lecture : aucun équipement ne dépasse 12 % de charge CPU sur la période. Le CPU n'est, à aucun moment et sur aucun équipement, en situation de saturation ou de pression notable.

F.2. Sessions actives et débit

Pare-feu	Sessions actives	Débit moyen	Débit pic
FIRINT01	n/a	n/a	> 3 Gbps (interfaces LCZINT et PRAINT)
FIRINT02	Stable	1 flux dominant ADMEXT ↔ ADMINT	251 Mb/s
FIRINT07	n/a	n/a	~ 2,3 Gbps (ACCEPE2 → DEVINT)
FIREXT03	n/a	n/a	13,9 MB/s (≈ 111 Mbps, batch hebdo)
FIREXT04	Stable	1,2 Mb/s (ouvré) / 50 kb/s (week-end)	3,7 Mb/s
FIRTMA00	228 → 279–291 (+22 % sur une année glissante)	n/a	345 Mb/s (mars-avr. 2025) → 197 Mb/s (été 2025+)

F.3. Volumes cumulés sur 12 mois

Pare-feu	Volume reçu	Volume émis
FIRINT01	≈ 1,2 Po	≈ 1,2 Po
FIRINT02	≈ 63 To	≈ 63 To
FIRINT07	≈ 306 To	≈ 282 To
FIREXT03	≈ 140 To	≈ 129 To
FIREXT04	≈ 9 To	≈ 9 To
FIRTMA00	≈ 127 To	≈ 212 To *(asymétrie marquée à investiguer)*

F.4. Synthèse pour le dimensionnement cible

Charge CPU non dimensionnante : la marge entre la moyenne et la capacité maximale du parc actuel est d'un à deux ordres de grandeur. Le renouvellement n'est pas justifié par un besoin de capacité de traitement.

Profil de charge concentré : deux paires (FIRINT01 et FIRINT07) portent l'essentiel des volumes du parc.

Croissance organique mesurable sur le périmètre TMA AMALFI (sessions +22 % sur une année glissante sur FIRTMA00), à intégrer aux exigences de dimensionnement (cf. §5.4.1, marge de croissance organique de +5 % par an).

Annexe G : Reprise du matériel pour le recyclage

Le titulaire met en œuvre la reprise et l'enlèvement des matériels existants dont les établissements souhaiteraient se séparer, suite à un remplacement effectué dans le cadre du présent marché.

A ce sujet, il est demandé au Candidat de développer dans son offre l'organisation des conditions de reprise et d'enlèvement ainsi que la potentielle valorisation de reprises d'équipements objet du présent marché.