

MARCHÉ DE FOURNITURES ET SERVICES

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES

Maître de l'ouvrage

DIRECTION INTERDÉPARTEMENTALE DES ROUTES ATLANTIQUE

Objet du marché

Fournitures de matériels, configuration, installation, intégration et maintenance des outils de sécurisation informatique nécessaires au bon fonctionnement du réseau du CIGT

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES

SOMMAIRE

	Pages
1 Présentation générale.....	4
1.1 Contexte.....	4
2 Objet.....	4
2.1 Objet du marché.....	4
3 Architecture.....	4
3.1 Principes généraux.....	4
3.2 Évolutivité.....	5
3.3 Sécurité.....	5
3.4 Remarque sur les pare-feux et hétérogénéité du matériel.....	5
3.5 Facilité d'exploitation.....	5
4 Consistance des prestations.....	6
5 Spécifications des équipements.....	6
5.1.1 Spécifications par type de pare-feu.....	6
5.1.2 Spécifications Bastion de sécurité.....	7
5.1.3 Spécifications d'un puits de LOGS.....	8
6 Mise en œuvre.....	8
6.1 Fournitures de l'administration.....	8
6.2 Fournitures du (des) titulaire (s).....	9
6.3 Transfert de compétence.....	9
6.4 Garantie.....	9
7 Description des unités d'œuvre.....	9
7.1 Fournitures.....	9
7.1.1 Fourniture d'un pare-feu filtrant type 1 – Cœur de réseau.....	9
7.1.2 Fourniture d'un pare-feu filtrant type 2 – Accès terrain.....	10
7.1.3 Fourniture d'un pare-feu filtrant type 3 – Accès distant.....	10
7.1.4 Fourniture d'un pare-feu filtrant type 4 – Terrain.....	10
7.1.5 Fourniture d'un bastion de sécurité.....	10
7.2 Prestations.....	10
7.2.1 Installation d'un pare-feu filtrant type 1 – Cœur de réseau.....	10
7.2.2 Installation d'un pare-feu filtrant type 2 – Accès terrain.....	10
7.2.3 Installation d'un pare-feu filtrant type 3 – Accès distant.....	11
7.2.4 Installation d'un pare-feu filtrant type 4 – Terrain.....	11
7.2.5 Installation d'un bastion de sécurité.....	12
7.2.6 Installation d'un puits de LOGS.....	12
7.2.7 Mise en place d'une solution RADIUS/LDAP.....	12
7.2.8 Formation.....	13
7.3 Maintenance.....	13
7.3.1 La maintenance téléphonique.....	13
7.3.2 Maintenance corrective.....	13
7.3.3 Maintenance préventive annuelle.....	13

7.3.4 Maintenance évolutive.....	14
7.4 Astreintes.....	14
7.5 Vérification de Service Régulier (VSR).....	14
8 GARANTIE.....	14
9 Propriétés.....	15
9.1.1 Propriétés des mots de passe.....	15
9.1.2 Responsabilité contre les intrusions.....	15
9.1.3 Discretion.....	15
10 Annexe.....	16
10.1 Schéma d'architecture déployé au CIGT et entre le CIGT et le terrain (à mettre à jour lorsque la nouvelle architecture sera déployée 1/09/2025).....	16
10.2 Note technique ANSSI – Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu v1.0.....	17

1 Présentation générale

1.1 Contexte

La Direction Interdépartementale des Routes Atlantique (DIRA) gère plus de 628 km de routes nationales non concédées dont l'emprise s'étend sur 6 départements (Gironde, Charente, Charente-Maritime, Deux-Sèvres, Pyrénées Atlantiques et la Vienne). L'exploitation de ces routes est assurée par un PC (Poste de Commandement) routier localisé à Lormont en Gironde (CIGT de Lormont).

Dans le cadre de sa mission, le PC utilise divers systèmes informatiques, notamment pour superviser et piloter des équipements dynamiques de signalisation (PMV), pour recueillir des données (stations de comptage, météo, caméras) mais également pour échanger des données avec des partenaires.

L'ensemble de ces outils sont interconnectés, entre eux, par des réseaux de transmissions dont la sécurité est assurée par un ensemble de pare-feux. L'objectif de ce marché est d'une part de remplacer une partie des matériels arrivant en fin de vie, de déployer de nouveaux équipements de sécurité mais aussi de fournir aux techniciens du CIGT (Centre d'Intervention et de Gestion du Trafic) chargés d'assurer la sécurité des réseaux, un ensemble complet et cohérent de prestations leur permettant de veiller, entre autres, au bon fonctionnement de l'ensemble des équipements compris dans le spectre de la sécurité. Dans le cadre de ce marché des prestations d'ingénierie pourront être formulées afin de répondre à de nouveaux besoins ou de nouvelles contraintes.

2 Objet

2.1 Objet du marché

Le présent marché concerne plusieurs aspects au niveau de la sécurité informatique et des réseaux :

- Le renouvellement et la maintenance de l'ensemble des équipements de sécurité informatiques (pare-feux),
- Le déploiement de nouveaux pare-feux,
- La mise en place d'une solution de bastion de sécurité dans l'architecture actuelle,
- La mise en place d'un puits de LOGS,
- La mise en place d'une solution LDAP ou RADIUS,
- Différentes prestations de sécurité pour répondre à la directive de NIS2.

Le présent marché est un marché à bons de commande. L'exécution des prestations est commandée au « Titulaire » sous la forme d'unités d'œuvre telles qu'elles sont décrites dans le présent CCTP.

3 Architecture

3.1 Principes généraux

Le schéma d'architecture joint en annexe décrit la topologie de réseau telle qu'elle a été imaginée et qui a été déployé par la maîtrise d'ouvrage. Actuellement, les pare-feux sont administrés à l'aide d'équipements sur site, sans recours aux technologies cloud.

Les principes généraux sont :

- **Remplacement en haute-disponibilité** des pare-feux FORTINET 100-D permettant d'assurer la sécurité des éléments constituant le système informatique du CIGT, vis-à-vis des équipements de terrain et du réseau Intranet du Ministère, nommé RIE. Il s'agit de pare-feux filtrants de type 1 « cœur de réseau ».
- **Remplacement en haute-disponibilité** des pare-feux STORMSHIELD SN510 permettant d'assurer la sécurité des éléments constituant le système informatique du CIGT vis-à-vis des équipements s'appuyant sur un réseau opéré. Il s'agit de pare-feux filtrants de type 2 « accès terrain ».

- **Remplacement en haute-disponibilité** des pare-feux FORTINET 81-F permettant d'assurer un accès distant sécurisé par le biais. Il s'agit de pare-feu filtrant de type 3 dit « accès distant ».
- **Mise en place en haute-disponibilité** de pare-feux terrains permettant de sécuriser la remontée des données issues du terrain vers le réseau « accès terrain ».

3.2 Évolutivité

Dans le cadre du présent marché plusieurs équipements devront à terme être déployés :

- des pare-feux fonctionnant en haute-disponibilité, entre les réseaux de terrain qui arrivent au CIGT et le réseau « accès terrain » afin de cloisonner au maximum les accès extérieurs et notre réseau de production. Il s'agit de pare-feu filtrant de type 4 dit « terrain », ces pare-feux seront équipés de sonde IDS (Système de détection d'intrusion) afin de ne pas perturber le bon fonctionnement du système (latence, gigue...).
- des pare-feux fonctionnant en haute-disponibilité, pour les types 1 et 2 devront prendre en compte outre le filtrage un mécanisme d'IPS (Système de prévention d'intrusions) permettant un blocage après analyse des paquets entiers.
- des pare-feux fonctionnant en haute-disponibilité, pour le type 3 devront obligatoirement permettre la détection des intrusions (IDS) mais aussi la prévention des intrusions (IPS) en permettant le blocage en fonction du type d'attaques qu'ils détectent.
- une solution de type bastion de sécurité devra être mise en place afin de concourir à une optimisation de la sécurité vis-à-vis des liens ou accès extérieurs, avec notamment l'enregistrement des accès.
- la mise en place d'une solution de centralisation des logs,
- la mise en place d'une solution sécurisée de type RADIUS ou LDAD pour l'ensemble des acteurs (internes et externes) des SI.

3.3 Sécurité

Une attention toute particulière du prestataire sera attendue sur cet aspect dans les choix des équipements.

En effet, l'ANSSI a établi une note technique sur les recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu (**Annexe 8-2 du CCTP**) particulièrement précise et sévère pour ce qui concerne le réseau, et la DIRA doit impérativement la respecter. Des dérogations sont prévues, mais elles doivent rester exceptionnelles et bien cernées techniquement.

Le titulaire du marché devra en outre se conformer à l'arrêté du 18 septembre 2018 (<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037436658>) portant approbation du cahier des clauses simplifiées de cybersécurité.

En cas de dérogations, le titulaire devra les expliciter dans son offre.

3.4 Remarque sur les pare-feux et hétérogénéité du matériel

Afin de renforcer la sécurité, au niveau des 4 types de pare-feux susmentionnés, deux marques distinctes de matériels devront être obligatoirement proposées. L'hétérogénéité des constructeurs du parc de pare-feux de la DIRA est volontaire et émane d'un principe de sûreté de fonctionnement. En effet, elle permet d'avoir des MTBF différents et/ou d'éventuels défauts (voir failles) propres à chaque constructeur et donc disjoints. Cela permet d'augmenter la résilience globale de l'ensemble et par conséquent la combinaison de ces principes réduit la probabilité d'apparition d'une défaillance.

3.5 Facilité d'exploitation

Afin d'intervenir le plus efficacement possible lors de problèmes détectés, il est souhaité que l'architecture déployée soit la plus simple possible à analyser. Le réalisateur s'attachera pour ce faire à trouver le meilleur compromis possible entre fiabilité et simplicité.

La mise en place de configurations complexes, destinées à améliorer de façon mineure le fonctionnement habituel est à proscrire. Cela génère souvent des difficultés d'administration, qui entraînent en cascade et indirectement des problèmes de fonctionnement au quotidien.

4 Consistance des prestations

De façon générale, les prestations consistent à fournir, configurer, installer et intégrer des pare-feux ainsi qu'une solution de bastion de sécurité dans un environnement en exploitation 24h/24h. De fournir des prestations de transfert de compétence par une formation sur les différents matériels installés et une documentation complète afin de pouvoir les exploiter (constructeur, de mise en œuvre et exploitation). De mettre en place une maintenance téléphonique, corrective ou préventive suivant les besoins.

On considère que les locaux techniques ou armoires sont installés, les fibres optiques prêtes à être brassées, l'énergie disponible, 240 Vac/50 Hz, les baies et les rails DIN en place prêts à accueillir les équipements et leurs connectiques.

Le titulaire devra prévoir lors du basculement une reprise de l'ancien système dans un laps de temps restreint en cas de défaillance de la nouvelle architecture.

Les différentes unités d'œuvre sont définies et décrites dans la suite du document.

5 Spécifications des équipements

5.1.1 Spécifications par type de pare-feu

Commun à tous les pare-feux :

La documentation fournie par le titulaire du marché comprendra au minimum :

- La documentation du constructeur,
- La documentation d'installation,
- La documentation d'exploitation du produit,
- La documentation de configuration,
- Les cahiers de tests et de non régression.

Les matériels déployés seront de type industriel et devront s'insérer dans des baies 19 pouces.

5.1.1.1 Pare-feux filtrant de type 1 – Cœur de réseau

Les caractéristiques minimales sont :

- Filtrage de paquets
- Mode Statefull Inspection
- VPN IPSec et SSL
- Administration via SSH, HTTPS.
- Support de SNMP v3
- Support du Multicast
- HA actif/actif natif
- Certification EAL4+

Au niveau des interfaces, elles doivent supporter à minima :

- 8 x GE RJ45
- 2 x GE SFP

Pare-feu filtrant type 2 – Accès terrain

Les caractéristiques minimales sont :

- Mode statefull inspection.
- Support du multicast
- VPN en multipoint
- Filtrage MAC.
- Filtrage couple @IP – port TCP ou UDP
- Support de VLAN.
- Administration via SSH, HTTPS.

- Support de SNMP v3.
- Support de VRRP.
- IPSEC avec DES, 3DES, AES et certificats X509, SH2 et pre-shared secret.
- HA actif/actif natif
- Certification EAL4+

Au niveau des interfaces, elles doivent supporter :

- 8 x GE RJ45

5.1.1.2 Pare-feu filtrant type 3 – Accès distant

Les caractéristiques sont :

- Mode statefull inspection.
- Filtrage de paquets
- VPN en multipoint
- Filtrage MAC.
- Filtrage couple @IP – port TCP ou UDP
- Administration via SSH, HTTPS.
- HA actif/actif natif
- Support de SNMP v3
- Double authentification par Token
- TLS (SSL)
- IDS, IPS
- Certification EAL4+

Au niveau des interfaces, elles doivent supporter :

- 8 x GE RJ45

5.1.1.3 Pare-feu filtrant type 4 - Terrain

Les caractéristiques sont :

- Mode statefull inspection.
- Filtrage de paquets
- VPN en multipoint
- Filtrage MAC.
- Filtrage couple @IP – port TCP ou UDP
- Administration via SSH, HTTPS.
- HA actif/actif natif
- Support de SNMP v3
- TLS (SSL)
- Certification EAL4+

Au niveau des interfaces, elles doivent supporter :

- 8 x GE RJ45

5.1.2 Spécifications Bastion de sécurité

Le serveur devra être suffisamment dimensionné afin de permettre une journalisation des activités sur une période d'un mois au maximum.

Le titulaire devra prendre en compte :

- le type et la fréquence des connexions aux réseaux internes de production de la DIRA, (le nombre de connexions simultanées est fixé à 20),
- la nature des données à sécuriser, qui exigent un niveau de chiffrement et de confidentialité adapté,
- la disponibilité et la fiabilité du bastion informatique, qui devra garantir une continuité de service et une résistance aux pannes,

- la facilité d'utilisation et de gestion de ce dernier.

La mise en place d'un bastion de sécurité comprend la mise en place ou l'utilisation, si celui-ci est déjà déployé, d'un proxy qui fait l'intermédiaire entre le/les réseau(x) interne et le réseau externe, en masquant les adresses IP des serveurs internes. Il comprend également la mise en place ou l'utilisation d'un serveur d'authentification, qui vérifie les identifiants des différents utilisateurs qui souhaitent accéder au réseau interne.

Il est à noter que le serveur d'authentification à déployer ne sera pas virtualisé.

5.1.3 Spécifications d'un puits de LOGS

Les logs sont des informations particulières créées par les différentes composantes d'une infrastructure informatique (machines, applications, systèmes, réseaux, etc.).

Ils permettent de suivre le fonctionnement de l'infrastructure en dressant un historique complet et détaillé de toute l'activité de celle-ci. Démarrage, exécution d'instructions, échecs d'opération, accès ou tentatives d'accès, tout est enregistré.

Des informations cruciales qui assurent la performance et la protection de l'infrastructure et aident à mettre en place les bonnes actions de correction ou maintenance, en cas de besoin.

Pour permettre leur exploitation, les logs sont stockés dans des fichiers spécifiques qui sont généralement facilement accessibles. Le problème se pose cependant quand nous avons affaire avec une architecture complexe, composée de dizaines ou centaines d'entités (serveurs, applications, systèmes, etc.). Chaque élément disposant de ses propres logs, leur gestion devient rapidement fastidieuse, voire impossible. La solution consiste alors à mettre en place un puits de logs.

Il s'agit de collecter, selon des règles précises et avec des outils spécialisés et automatisés, les logs d'une infrastructure et de les stocker dans un espace commun, en vue de les exploiter plus tard.

Les puits de logs ont plusieurs avantages :

- Ils permettent de stocker tous les logs dans un seul endroit, économisant ainsi temps, efforts et ressources informatiques.
- Ils filtrent les logs pour ne retenir que les plus pertinents.

Ayant subi un traitement particulier dans la collecte, les données dans le puits sont converties en informations structurées et utiles, au lieu de fichiers bruts inexploitable.

Réunir les logs dans un seul endroit simplifie le suivi et monitoring en temps réel de l'activité.

La gestion des droits d'accès : il est crucial de garder les données des logs exactes et transparentes pour comprendre les origines des problèmes qui surviennent et savoir quel utilisateur a réalisé quelle action. Les utilisateurs de puits ne doivent en aucun cas pouvoir altérer les informations, compte tenu de leur caractère sensible.

Le positionnement du puits de log devra également être sécurisé, il s'agira de le positionner dans un réseau étanche, afin de ne pas être une cible dans le cas d'une attaque externe.

6 Mise en œuvre

6.1 Fournitures de l'administration

- Le plan d'affectation de fibres optiques si elles existent,
- Les schémas ou clichés photographiques des baies,
- Le plan d'architecture réseau,
- Le plan d'adressage IP complet,
- Le plan de nommage des équipements,
- Les règles de pare-feu mises en place,
- Les conditions d'accès aux sites en cas de besoin,
- Les machines qui doivent être fournies tel que décrit dans le reste du document.

6.2 Fournitures du (des) titulaire (s)

- Les documents d'origine éventuellement modifiés et à jour,
- Les schémas d'architecture modifiés et à jour (DAT),
- Les fichiers de configuration des équipements,
- Les documentations complètes des matériels fournis (en français),
- Les documentations complètes des logiciels fournis (en français),
- Les cahiers de recette et de test,
- Les documents demandés dans chacune des unités d'œuvre décrite dans la suite du document.

Les documentations seront fournies :

- Au format PDF pour ce qui concerne les documentations fournisseurs.
- Au format LibreOffice pour les documents rédigés.

Un cahier de recette site sera utilisé pour chaque recette site/type, suivant le rythme des déploiements commandés par l'administration.

Le document sera fourni par le titulaire avant chaque déploiement, il sera validé par l'administration qui pourra y ajouter un complément de tests si celle-ci le juge nécessaire.

6.3 Transfert de compétence

Chaque prestation d'installation de matériel donnera lieu à un transfert de compétence.

Le public concerné est composé de techniciens de maintenance et de l'administrateur du CIGT ; soit 6 personnes au maximum.

La formation est prévue dans les locaux du CIGT à Lormont.

Exemple de projet de programme pour le déploiement d'un pare-feu (à valider entre le titulaire du marché et l'administration) avant le début de la formation :

- Généralités sur la théorie de la sécurité.
- Principes généraux du pare-feu,
- Installation du pare-feu,
- Configuration du pare-feu en place,
- Procédure de secours s'il y a lieu,
- Exemples de modifications de la configuration,
- Configuration, procédure de secours,
- Vérification des logs.

Le titulaire devra prévoir un support pour chaque formation (pare-feu, bastion de sécurité, ...) qu'il fournira préalablement à la formation.

6.4 Garantie

L'entreprise fournira dans son mémoire technique un descriptif précis concernant les conditions de garantie de tous les éléments fournis, qu'ils soient matériels ou logiciels ; ce document décrira :

- Durée de la garantie.
- Niveau de garantie.
- Mode d'exécution.

7 Description des unités d'œuvre

7.1 Fournitures

7.1.1 Fourniture d'un pare-feu filtrant type 1 – Cœur de réseau

Telle que décrit au chapitre 5.1.1.1

7.1.2 Fourniture d'un pare-feu filtrant type 2 – Accès terrain

Telle que décrit au chapitre 5.1.1.2

7.1.3 Fourniture d'un pare-feu filtrant type 3 – Accès distant

Telle que décrit au chapitre 5.1.1.3

7.1.4 Fourniture d'un pare-feu filtrant type 4 – Terrain

Telle que décrit au chapitre 5.1.1.4

7.1.5 Fourniture d'un bastion de sécurité

Telle que décrit au chapitre 5.1.1.5

7.2 Prestations

7.2.1 Installation d'un pare-feu filtrant type 1 – Cœur de réseau

L'installation d'un pare-feu filtrant de type 1 comprend au minimum :

- Rédaction de la procédure de migration d'architecture, du planning associé et du plan de test,
- Validation par le maître d'ouvrage de la procédure,
- Mise en place du matériel,
- Paramétrage des commutateurs concernés par la connexion du pare-feu,
- Paramétrage du pare-feu avec les données de la politique de sécurité du site,
- Paramétrage du pare-feu avec les éléments de haute disponibilité,
- Connexion et mise en œuvre du pare-feu en haute disponibilité,
- Connexion et mise en œuvre du pare-feu,
- Test du pare-feu,
- Test de bascule des pare-feux,
- Rédaction du journal des actions effectuées, du document d'installation et d'exploitation.

Le prestataire devra proposer une intervention n'entraînant qu'un minimum d'interruption de service.

Le prestataire fournira pour chaque installation :

- Une procédure de migration,
- Un planning de la migration,
- Un plan de tests,
- Un journal des actions effectuées,
- Une documentation d'installation,
- Une documentation d'exploitation.

7.2.2 Installation d'un pare-feu filtrant type 2 – Accès terrain

L'installation d'un pare-feu filtrant de type 2 comprend au minimum :

- Rédaction de la procédure de migration d'architecture, du planning associé et du plan de test,
- Validation par le maître d'ouvrage de la procédure,
- Mise en place du matériel,
- Paramétrage des commutateurs concernés par la connexion du pare-feu,
- Paramétrage du pare-feu avec les données de la politique de sécurité du site,
- Paramétrage du pare-feu avec les éléments de haute disponibilité,
- Connexion et mise en œuvre du pare-feu en haute disponibilité,
- Connexion et mise en œuvre du pare-feu.
- Test du pare-feu.

- Test de bascule des pare-feux.
- Rédaction du journal des actions effectuées, du document d'installation et d'exploitation.

Le prestataire devra proposer une intervention n'entraînant qu'un minimum d'interruption de service.

Le prestataire fournira pour chaque installation:

- Une procédure de migration,
- Un planning de la migration,
- Un plan de tests,
- Un journal des actions effectuées,
- Une documentation d'installation,
- Une documentation d'exploitation.

7.2.3 Installation d'un pare-feu filtrant type 3 – Accès distant

L'installation d'un pare-feu filtrant de type 3 comprend au minimum :

- Rédaction de la procédure de migration d'architecture, du planning associé et du plan de test.
- Validation par le maître d'ouvrage de la procédure
- Mise en place du matériel.
- Paramétrage des commutateurs concernés par la connexion du pare-feu.
- Paramétrage du pare-feu avec les données de la politique de sécurité du site,
- Connexion et mise en œuvre du pare-feu en haute-disponibilité.
- Test du pare-feu.
- Rédaction du journal des actions effectuées, du document d'installation et d'exploitation.

Le prestataire devra proposer une intervention n'entraînant qu'un minimum d'interruption de service.

Le prestataire fournira pour chaque installation :

- Une procédure de migration,
- Un planning de la migration,
- Un plan de tests,
- Un journal des actions effectuées,
- Une documentation d'installation,
- Une documentation d'exploitation.

7.2.4 Installation d'un pare-feu filtrant type 4 – Terrain

L'installation d'un pare-feu filtrant de type 4 comprend au minimum :

- Rédaction de la procédure de migration d'architecture, du planning associé et du plan de test.
- Validation par le maître d'ouvrage de la procédure
- Mise en place du matériel.
- Paramétrage des commutateurs concernés par la connexion du pare-feu.
- Paramétrage du pare-feu avec les données de la politique de sécurité du site,
- Connexion et mise en œuvre du pare-feu.
- Test du pare-feu.
- Rédaction du journal des actions effectuées, du document d'installation et d'exploitation.

Le prestataire devra proposer une intervention n'entraînant qu'un minimum d'interruption de service.

Le prestataire fournira pour chaque installation :

- Une procédure de migration,
- Un planning de la migration,
- Un plan de tests,
- Un journal des actions effectuées,
- Une documentation d'installation,
- Une documentation d'exploitation.

7.2.5 Installation d'un bastion de sécurité

L'installation d'un bastion de sécurité comprend au minimum :

- Rédaction de la procédure de migration d'architecture, du planning associé et du plan de test.
- Validation par le maître d'ouvrage de la procédure
- Mise en place du matériel.
- Paramétrage des commutateurs concernés par la connexion du bastion de sécurité.
- Paramétrage du bastion de sécurité les données de la politique de sécurité du site,
- Connexion et mise en œuvre du bastion de sécurité.
- Test du bastion de sécurité.
- Rédaction du journal des actions effectuées, du document d'installation et d'exploitation.

Le prestataire devra proposer une intervention n'entraînant qu'un minimum d'interruption de service.

Le prestataire fournira pour chaque installation :

- Une procédure de migration,
- Un planning de la migration,
- Un plan de tests,
- Un journal des actions effectuées,
- Une documentation d'installation,
- Une documentation d'exploitation.

7.2.6 Installation d'un puits de LOGS

L'installation d'un puits de LOGS comprend au minimum :

- Rédaction de la procédure de migration d'architecture, du planning associé et du plan de test.
- Validation par le maître d'ouvrage de la procédure
- Mise en place du matériel.
- Paramétrage des commutateurs concernés par la connexion du bastion de sécurité.
- Paramétrage du bastion de sécurité les données de la politique de sécurité du site,
- Connexion et mise en œuvre du bastion de sécurité.
- Test du bastion de sécurité.
- Rédaction du journal des actions effectuées, du document d'installation et d'exploitation.

Le prestataire devra proposer une intervention n'entraînant qu'un minimum d'interruption de service.

Le prestataire fournira pour chaque installation :

- Une procédure de migration,
- Un planning de la migration,
- Un plan de tests,
- Un journal des actions effectuées,
- Une documentation d'installation,
- Une documentation d'exploitation.

7.2.7 Mise en place d'une solution RADIUS/LDAP

L'installation d'une solution RADIUS ou LDAP dans le système actuel devra répondre à certaines règles de sécurité, ce système étant également très sensible, il ne devra pas être déployé sur un environnement virtuel ceci afin de prévenir une attaque sur le système de virtualisation.

- Rédaction de la procédure de mise en place du système
- Validation par le maître d'ouvrage de la procédure
- Mise en place du matériel.
- Paramétrage de la solution annuaire RADIUS/LDAP
- Test du système.
- Rédaction du journal des actions effectuées, du document d'installation et d'exploitation.

Le prestataire devra proposer une intervention n'entraînant qu'un minimum d'interruption de service.

7.2.8 Formation

Au titre du présent marché, le titulaire prendra en charge la formation des techniciens, et administrateurs ayant en charge la maintenance et l'exploitation du parc d'équipements. Cette formation aura lieu dans un délai de 15 jours après la recette sur site des équipements. Cette documentation sera physiquement indépendante des documents d'installation et d'exploitation afin d'être utilisable simplement et efficacement. Cependant, on peut admettre qu'elle fasse divers renvois aux documents d'installation et d'exploitation pour apporter des éclairages complémentaires mais non essentiels à la formation.

La formation sera réalisée au CIGT, à charge alors pour le titulaire d'assurer la mise à disposition des supports pédagogiques (ensembles et sous-ensembles...). Le support de cours en français sera adapté aux personnels de maintenance.

Cette formation sera organisée sur, à minima, une journée par type de matériel et/ou par type de solution déployée, elle devra comprendre une partie informatique et une partie matériels si besoin.

La formation devra notamment apporter toutes les connaissances utiles sur :

- Le fonctionnement général des pare-feux,
- Le fonctionnement général du bastion de sécurité,
- Techniques de diagnostic pour la maintenance préventive et curative,
- Techniques de configuration et de suivi d'un bastion de sécurité,
- Techniques de configuration et de fonctionnement d'un annuaire LDAP/RADIUS,
- Techniques de configuration et d'analyse d'un puits de LOGS

Le programme de chaque formation sera proposé par le titulaire à l'approbation de la maîtrise d'œuvre.

7.3 Maintenance

La maintenance concerne :

- Une assistance téléphonique,
- Une maintenance corrective,
- Une expertise après un incident, une attaque, un dysfonctionnement,
- Une maintenance préventive consistant à effectuer une visite annuelle des installations.

7.3.1 La maintenance téléphonique

Cela concerne une assistance téléphonique en jours ouvrés de 9h à 17h permettant de répondre aux problèmes techniques rencontrés et/ou signalés avec un volume forfaitaire annuel de 24h.

7.3.2 Maintenance corrective

La maintenance corrective, réalisée à n'importe quel moment par le titulaire, lorsqu'un dysfonctionnement est constaté par la DIRA sur les équipements en fonctionnement.

Le titulaire du marché se doit de prendre en compte sous 4h en heure ouvrée, chaque signalement. Il devra être mis en place une correction, même temporaire sous 72h au maximum ceci afin de permettre au CIGT de fonctionner.

Les prestations de maintenance corrective seront utilisées pour réaliser des diagnostics d'architecture suite à une demande de l'administration.

7.3.3 Maintenance préventive annuelle

La partie maintenance préventive annuelle sur site comprendra au minimum les éléments suivants :

- Audit annuel des règles mises en place,
- Mise à jour des produits,
- Mise à jour de la politique de sécurité,
- Mise à jour de la politique de sécurité, celle-ci pourra être demandée à la suite d'un audit ou à toutes autres modifications sur un ou plusieurs réseaux, l'ajout ou la suppression d'interface.

- La mise à jour consistera à installer la nouvelle politique, à réaliser les tests sur un des deux pare-feux puis à les installer sur le second.
- Vérification du bon fonctionnement de la haute disponibilité.

Le prestataire devra proposer une intervention n'entraînant qu'un minimum d'interruption de service.

Le prestataire fournira après chaque visite un rapport détaillé des actions réalisées.

Ce rapport devra être fourni sous 15 jours.

7.3.4 Maintenance évolutive

Dans le cadre des évolutions des missions du CIGT, de l'arrivée de nouveaux projets ou bien de la mise en place de nouvelles directives de sécurité, le prestataire du marché pourra être amené à proposer des solutions suivant l'importance de la demande.

7.4 Astreintes

Dans le cadre des missions du CIGT, l'ensemble des systèmes d'information se doit de fonctionner 24h/24. A cet effet, les personnels de maintenance de la DIRA sont mis à contribution tout au long de l'année. Dans le cadre d'une éventuelle cyberattaque, le CIGT de la DIRA souhaite qu'une assistance puisse être mise en place avec une prise en compte sous 4h afin de permettre au CIGT de continuer à fonctionner, en mode dégradé si besoin. L'astreinte devra être joignable 24h/24h par téléphone, l'appel déclenchant le délai d'intervention.

7.5 Vérification de Service Régulier (VSR)

À l'issue de la réception, les équipements et les logiciels concernés deviennent la propriété du maître d'ouvrage.

Les équipements et les logiciels passent alors en phase de vérification de service régulier. La durée de cette phase est fixée à 6 mois, elle se décompose en deux (2) périodes de trois mois chacune.

Cette phase a pour but de détecter des anomalies de fonctionnement de l'équipement dans le contexte de son utilisation par le CIGT mais aussi dans un contexte d'évolution envisagée. Elle vise également à révéler des anomalies à caractère répétitif relevant d'une mauvaise conception ou d'une mauvaise mise en œuvre.

Le système est considéré en exploitation et à ce titre tout dysfonctionnement constaté générera l'ouverture d'une procédure qui diffère suivant trois cas :

1. s'il s'agit d'un simple panne. Une procédure de maintenance corrective sera engagée durant la phase de garantie décrite au chapitre maintenance. La VSR se poursuivra normalement à condition que les délais des éventuelles interventions soient respectés.
2. s'il s'avère qu'une caractéristique spécifiée n'est plus atteinte. Une procédure de modification sera engagée, la VSR sera suspendue jusqu'à ce que les corrections nécessaires aient été effectuées.
3. s'il s'avère que le taux de pannes similaires devient symptomatique d'une mauvaise conception une procédure de modification sera engagée, la VSR sera arrêtée. Après correction, elle sera prolongée d'une durée de 3 mois.

Pendant la VSR, l'Entrepreneur assurera la maintenance des équipements et des logiciels installés dans les conditions décrites à l'article 18 du présent CCTP.

8 GARANTIE

Le titulaire fournira dans son mémoire technique un descriptif précis concernant les conditions de garantie de tous les éléments fournis, qu'ils soient matériels ou logiciels; ce document décrira :

- Durée de la garantie,
- Niveau de garantie,
- Mode d'exécution.

Par défaut il sera demandé :

- pour la partie « matériel » une garantie de 5 ans à minima après déploiement,
- pour la partie « logiciel » un support à minima sur 3 ans après installation.

9 Propriétés

Il convient, lors de l'installation des logiciels, de ménager de larges possibilités d'évolution et d'adaptation.

9.1.1 Propriétés des mots de passe

Les mots de passe sont la propriété exclusive du Maître d'ouvrage, Ils ne peuvent être modifiés sans autorisation.

Les mots de passe sont placés dans un dépôt de sécurité chez le titulaire et chez l'administrateur du système désigné par le Maître d'ouvrage.

Les mots de passe devront respecter les standards de préconisation de l'ANSSI (ANSSI-PG-078 08/10/2021).

9.1.2 Responsabilité contre les intrusions

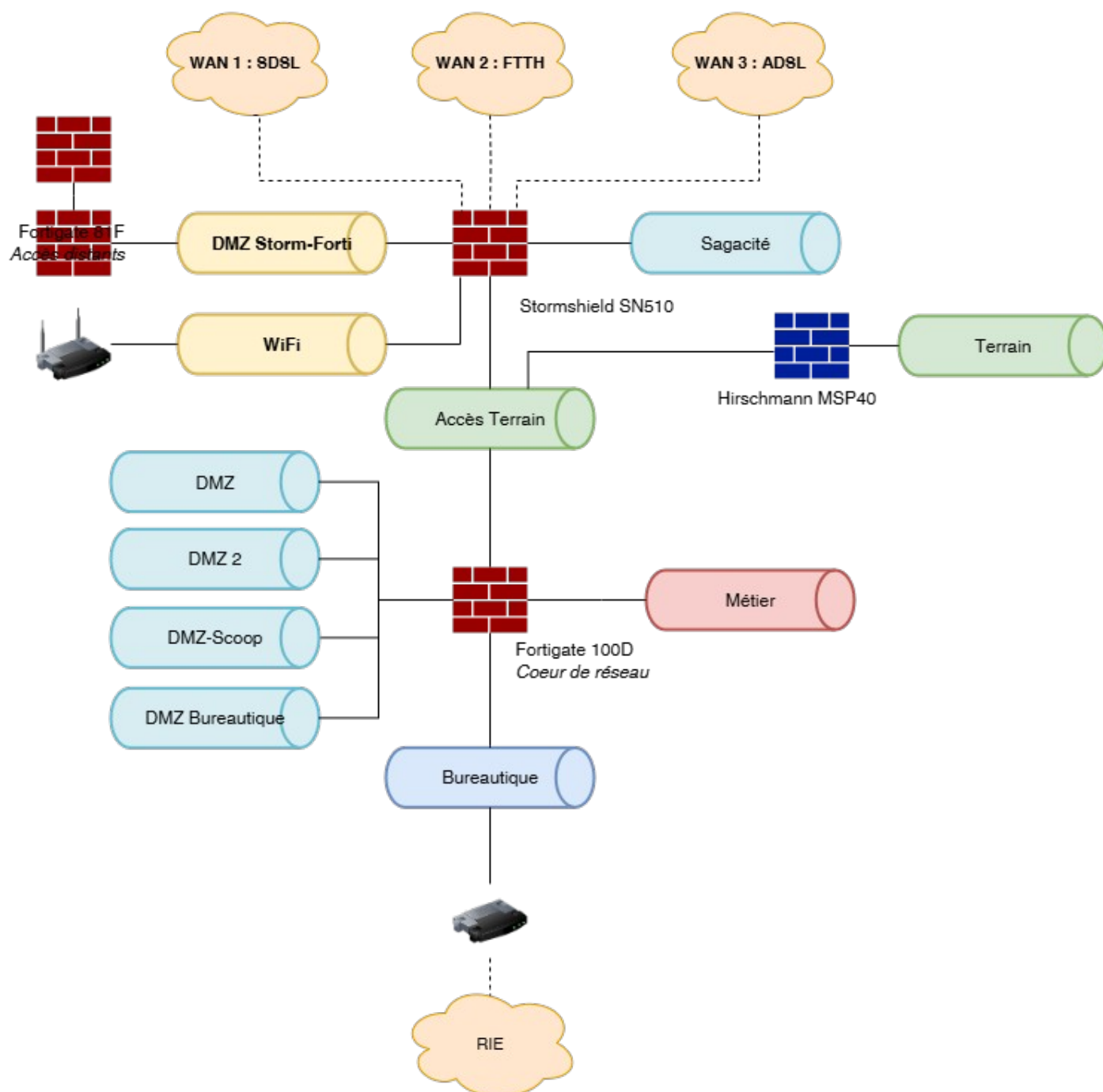
Le titulaire engage sa responsabilité vis-à-vis de l'utilisation abusive des mots de passe et des intrusions accidentelles. En particulier, toute nouvelle version d'un logiciel doit faire l'objet d'une garantie de non-infection par des virus de la part du distributeur.

9.1.3 Discretion

Le soumissionnaire a une obligation de discrétion pour les faits, informations, études ou décisions de niveau non public dont il pourra avoir connaissance dans le cadre de l'appel d'offres.

10 Annexe

10.1 Schéma d'architecture déployé au CIGT et entre le CIGT et le terrain (à mettre à jour lorsque la nouvelle architecture sera déployée 1/09/2025)



10.2 Note technique ANSSI – Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu v1.0