PARE-FEUX

DiIR CENTRE EST

Service Exploitation et Sécurité

Pôle Équipements et Systèmes

2026

Cahier des Clauses Techniques particulières (CCTP)

Maintenance des pare-feux des PC de la DIR Centre-Est

Direction Interdépartementale des Routes
Centre Est

Table des matières

1 - PRÉSENTATION GÉNÉRALE....4
1.1 - Objet du document....4
1.2 - Contexte....4
1.3 - Objet de la prestation....5
1.4 - Périmètre....5
1.5 - Organisation du marché....8
1.6 - Propriété....9

2 - DESCRIPTION DES PRESTATIONS....10
2.1 - Initialisation du marché....10
2.2 - Prestations générales....11
2.3 - Prestations de fourniture....12
2.4 - Caractéristiques des pare-feux....12
2.5 - Contrats de maintenance....19
2.6 - Maintenance préventive....21
2.7 - Maintenance corrective....23
2.8 - Maintenance évolutive....28
2.9 - Forfaits d'intervention....38
2.10 - Formations et transferts de compétence....39

3 - SÉCURITÉ ET CONFIDENTIALITÉ....40
3.1 - Confidentialité des informations....40
3.2 - Disponibilité des données et des systèmes....41
3.3 - Exigences liées à la télémaintenance....41
3.4 - Destruction des données....42
3.5 - Respect des lois et réglementations....42
3.6 - Respect des référentiels de sécurité....43
3.7 - Mesures techniques et organisationnelles....43
3.8 - Processus de gestion des incidents....45
3.9 - Vie du contrat....46
3.10 - Transfert et réversibilité....48
3.11 - Obligations spécifiques aux interventions sur site....49

4 - CONDITIONS D'EXÉCUTION....50
4.1 - Généralités....50
4.2 - Prise en charge et remise des équipements en fin de marché....50

4.3 - Personnel d’intervention du titulaire.....50
4.4 - Sécurité et accès aux sites.....50
4.5 - Obligation du maître d’ouvrage.....51
4.6 - Opération de vérification.....51

1 - Présentation générale

1.1 - Objet du document

Le présent Cahier des Clauses Techniques Particulières (CCTP) a pour objet de définir les prestations techniques attendues du titulaire dans le cadre du marché de maintenance des pare-feux de la DIR Centre-Est.

Il précise le contexte du marché, le périmètre fonctionnel et technique de la solution, les prestations attendues, les modalités d'exécution ainsi que les exigences applicables en matière de maintenance, d'évolution, de sécurité, de documentation et de qualité de service.

1.2 - Contexte

La Direction Interdépartementale des Routes Centre-Est (désignée par DIR CE dans la suite du présent document) gère 1 233 km de routes nationales non concédées situés sur 3 régions (Rhône-Alpes, Auvergne, Bourgogne) et 11 départements (Allier, Ardèche, Aube, Drôme, Isère, Loire, Nièvre, Rhône, Saône-et-Loire, Savoie, Yonne). L'exploitation de ces routes nationales est réalisée par 5 PC routiers répartis sur son territoire :

L'exploitation de ces routes est assurée par 5 PC routiers répartis sur le territoire de la DIR CE :

- PC de Genas dans le Rhône ;
- PC Gentiane (à Grenoble) dans l'Isère ;
- PC Hyrondelle (à Saint-Étienne) dans la Loire ;
- PC Osiris (à Albertville) en Savoie ;
- PC de Moulins dans l'Allier.

Ces PC sont placés sous l'autorité de 3 services régionaux de la DIR CE couvrant chacun une zone géographique :

- SREX de Lyon pour les PC de Genas et Hyrondelle ;
- SREX de Moulins pour le PC de Moulins ;
- SREI de Chambéry pour les PC Gentiane et Osiris.

Dans le cadre de leurs missions, les PC utilisent divers systèmes informatiques, notamment pour superviser et piloter des équipements dynamiques de signalisation (PMV) et de recueil (stations de comptage, météo, caméras). 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.

La maintenance à distance des ses systèmes est assuré au travers d'un accès unique, composé d'un serveur d'authentification, de pare-feux et de bastions qui permettent de garantir une authentification sécurisée et la traçabilité des accès.

L'objectif de ce marché est de fournir aux techniciens des PC chargés d'assurer la sécurité

des réseaux un ensemble complet et cohérent de prestations leur permettant de veiller au bon fonctionnement de ces équipements de sécurité et de les faire évoluer en fonction des nouveaux besoins et nouvelles contraintes.

1.3 - Objet de la prestation

Le présent marché a pour objet la maintenance préventive, curative et évolutive des pare-feux de la DIR Centre-Est. Le marché comporte les prestations suivantes :

- la fourniture de pare-feux et de solutions de sécurité conformément aux besoins et exigences de sécurité de la DIR Centre-Est,
- la maintenance préventive, curative et évolutive des pare-feux, bastions et de l'accès de télémaintenance de la DIR Centre-Est,
- le conseil pour les évolutions de l'infrastructure sécurisée de la DIR Centre-Est,
- des audits ponctuels pour vérifier le niveau de sécurité de l'infrastructure de la DIR Centre-Est.

1.4 - Périmètre

1.4.1 - Sites d'intervention

Le Titulaire du marché sera amené à intervenir sur l'ensemble du territoire couvert par les PC routiers de la DIR CE (tunnels inclus).

1.4.2 - Systèmes maintenus

Les prestations du marché concernent des matériels et des systèmes permettant de garantir la sécurité des infrastructures de la DIR Centre-Est. Les marques et modèles des matériels ainsi que les noms des logiciels n'apparaissent pas dans ce document. Toutes les références de matériels et applications couvertes par le présent marché sont indiqués dans l'annexe 2 du CCTP, disponible uniquement sur demande.

Les systèmes concernés sont les suivants :

1.4.2.a - Pare-feux filtrants

Les pare-feux filtrant sont utilisés par la DIR CE pour

- assurer le routage et le filtrage entre réseaux dont les politiques de sécurité diffèrent.
- pour établir des liens sécurisés avec des sites distants raccordés au site principal par l'intermédiaire d'un VPN opéré.
- assurer du filtrage applicatif, du routage, de la translation d'adresses et le chiffrement des données (tunnel IPSec).
- cloisonner les réseaux et les applications pour garantir leur sécurité et contrôler les flux.

Généralement, sur un site ils sont déployés par paire avec un pare-feu principal/primaire et un pare-feu de secours/secondaire. Il existe ainsi deux types de redondance possible :

- un type de redondance en haute disponibilité (signalée par le sigle « HA » - « High Availability »). Dans cette configuration, le pare-feu de secours scrute une éventuelle panne du pare-feu principal et ce dernier fait de même avec le secours. Ainsi, lors d'une panne avérée, l'un prend la place de l'autre et inversement ;
- un type de redondance manuelle. Dans cette configuration, le pare-feu de secours est en veille. Lors d'une détection de panne, il est activé manuellement par les techniciens de maintenance.

Les pare-feux filtrants sont déclinés sous deux formes :

- une version basée sur des appliances et logiciels propriétaires et commerciaux ;
- une version basée sur un logiciel propriétaire ou libre de droits dans une appliance dédiée.

Ils sont installés :

- soit sur des serveurs (non pris en charge par le présent marché) mais dont la configuration matérielle fera l'objet d'une validation par le Titulaire dans le cas d'une nouvelle acquisition par la DIR Centre-Est ;
- soit en « appliance » c'est-à-dire une solution complète qui intègre à la fois le matériel, le système d'exploitation et le logiciel. Dans la suite du CCTP, le terme « appliance » sera utilisé afin de viser une solution de cette nature.

1.4.2.b - Accès de télémaintenance (ou accès distant sécurisé)

La DIR Centre-Est a mis en place un point d'accès unique pour les connexions à distance des titulaires et techniciens en situation de télémaintenance.

L'accès de télémaintenance a plusieurs objectifs :

- centraliser les connexions des titulaires externes et les techniciens en situation de télémaintenance,
- limiter les accès aux seules ressources autorisées,
- sécuriser les accès à privilèges,
- enregistrer les sessions et consigner les actions.

Le système est composé :

- D'un serveur d'authentification de type RADIUS sur lequel l'utilisateur s'identifie à l'aide d'un code à utilisation unique généré par un « authentificateur ». Il peut s'agir d'un logiciel propriétaire et commercial ou libre de droit ;
- De 2 bastions assurant la traçabilité et la légitimité des accès ;
- Un serveur VPN
- Et deux pare-feux de type applicatif en cascade pour valider le VPN et chiffrer les

données entre le client et les bastions.

- De clés « authentificateurs » détenues par les utilisateurs.

La DIR Centre-Est utilise deux types de bastions , des bastions libres de droits et un bastion sous licence.

1.4.2.c - Client pour l’accès à distance

La connexion au système d'accès distant sécurisé (authentification et échanges cryptés) se fait au travers d'une connexion Internet et du poste de l’utilisateur sur lequel est installé et paramétré le logiciel VPN de la DIR Centre-Est. Chaque utilisateur dispose d’une configuration unique.

1.4.2.d - Remarque sur les pare-feux et hétérogénéité du matériel

Afin de renforcer la sécurité, les 3 types de pare-feux susmentionnés sont de marques distinctes. L’hétérogénéité des constructeurs du parc de pare-feux de la DIR Centre-Est 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 (voire 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.

1.4.3 - Parc de pare-feux existant

Les licences détenues par la DIR Centre-Est et faisant l'objet de ce marché sont décrites dans l'ANNEXE 2 du présent CCTP.

1.4.4 - Parc de licences existant

Les licences détenues par la DIR Centre-Est et faisant l'objet de ce marché sont décrites dans l'ANNEXE 2 du présent CCTP.

1.4.5 - Consistance des prestations

Le marché comprend :

1. Des prestations de fourniture :
   - Appliance de pare-feu filtrant ;
   - Logiciel de pare-feu filtrant ;
   - Bastion sous licence commerciale ;
   - Bastion libre de droit ;
   - Contrats de maintenance éditeur pour l'ensemble des fournitures ci-dessus ;
   - Logiciel d'authentification de type RADIUS
   - Authentificateur ;
   - Système de gestion centralisée des journaux ;
   - Systèmes d'exploitation Microsoft Windows pour serveur et poste de travail ;
2. Des prestations de maintenance :
   - Maintenance préventive ;
   - Maintenance corrective : diagnostic et résolution de dysfonctionnement ;
   - Maintenance évolutive : conseil en architecture, installation, mise en redondance, mise à jour, audit de règles, mise à jour des politiques de sécurité, création de tunnels IPSec ;
3. Des prestations de transfert de compétence :
   - Formation « pare-feu filtrant commercial » ;
   - Formation « bastion » ;
   - Formation « gestion des logs » ;
   - Formation « accès distant sécurisé » ;

1.5 - Organisation du marché

Il s'agit d'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.

Au fur et à mesure de ses besoins, la DIR Centre-Est émettra des bons de commande

précisant les prestations souhaitées (unités d'œuvre du marché).

Ce mécanisme vaut pour toutes les prestations, qu'elles soient préventives, curatives ou évolutives sur le matériel et les logiciels.

Dans le cas d'évolutions fonctionnelles, une note d'expression des besoins rédigée par la DIR Centre-Est et constituant les spécifications fonctionnelles accompagne en plus le bon de commande.

1.6 - Propriété

La DIR Centre-Est est propriétaire de toutes les productions (développements, dossiers, documentations, etc.) réalisées dans le cadre des unités d'œuvre décrites dans le présent document.

2 - Description des prestations

2.1 - Initialisation du marché

La phase d'initialisation du marché consiste à :

- Organiser et animer la réunion de lancement du marché ;
- Constituer l'équipe projet ;
- Prendre connaissance de l'environnement de la DIRCE ;
- Produire le plan d'assurance sécurité

2.1.1 - Réunion de lancement

Le titulaire participe à une réunion de lancement du marché organisé par la DIRCE.

- Objet : procéder au lancement officiel de la prestation
- Contenu : à proposer par le titulaire, et à valider par le commanditaire.
- Participants : pilote DIRCE de la prestation, équipe du titulaire, et tout autre acteur pertinent
- Lieu : PC de Genas ou à distance
- Fréquence : ponctuel, dans les 2 semaines suivant la notification, date à définir conjointement
- Support et compte-rendu : préparé et transmis par le titulaire, validé par la DIRCE.

2.1.2 - Constituer l'équipe projet

Le titulaire a pour objectif de constituer et présenter l'équipe d'intervention répondant aux besoins du projet et de la DIRCE, et conformément à celle proposée dans son offre.

Le titulaire fournira au commanditaire la structuration de l'équipe, l'organigramme associé, la répartition des rôles et responsabilités, les coordonnées de chaque membre ainsi que le taux d'affectation.

Le maître d'ouvrage aura en charge de nommer les contributeurs constituant l'équipe projet côté DIRCE.

2.1.3 - Prendre connaissance de l'environnement de la DIRCE

Le titulaire a pour objectif de prendre connaissance de l'infrastructure et des équipements déployés à la DIRCE. Pour cela, il est notamment demandé :

La DIRCE fournira :

- La documentation disponible, notamment les rapports des dernières visites préventives ;

- Les accès requis ;
- La disponibilité nécessaire pour répondre aux questions complémentaires.

2.1.4 - Finalisation du plan d'assurance sécurité

Le titulaire produit dans le mois suivant le démarrage du marché un plan d'assurance sécurité décrivant les mesures mises en œuvre pour répondre aux exigences du paragraphe 3 Sécurité et confidentialité. Le document précisera notamment :

- la gouvernance et l'organisation de la sécurité du titulaire avec des rôles nominatifs
- la sécurité technique, physique et logique mise en œuvre
- la gestion des vulnérabilités
- la gestion des incidents de sécurité
- la gestion de la réversibilité

2.2 - Prestations générales

SÉRIE 300 – MAINTENANCE GÉNÉRALITÉS	
301	Gestion annuelle des prestations
302	Service annuel de télé-assistance

2.2.1 - Gestion des prestations

Le Titulaire est tenu de mettre en place l'organisation nécessaire pour prendre en compte et gérer :

- La planification et le suivi des prestations ;
- La participation à des réunions périodiques (trimestrielles) ;
- Le suivi de la qualité des prestations ;
- La prise de connaissance des pare-feux déployés.

2.2.2 - Service d'assistance

Le Titulaire mettra à disposition des techniciens des PC de la DIR CE :

- Un standard unique pour prendre en compte les demandes de télé-assistance et les commandes d'intervention de maintenance corrective. A ce titre, le Titulaire communiquera un numéro de téléphone et une adresse de messagerie électronique tous deux joignables pendant les plages de travail c'est-à-dire du lundi au vendredi, hors jours fériés, entre 8h00 et 18h00 ;

- Un service de télé-assistance capable de répondre aux questions techniques ou fonctionnelles sur les matériels et logiciels disponibles dans le cadre du présent marché. Le temps cumulé consacré au traitement des demandes de la DIR CE ne pourra excéder l'équivalent de 150 heures (15 jours x 10 heures) par an. Le Titulaire tiendra un compte précis des demandes d'assistance avec au minimum les informations suivantes : PC à l'origine de la demande, contenu de la demande, description de la réponse et temps consacré au traitement de la demande.
- Une application de suivi des incidents de type web de suivi des incidents hébergée par le titulaire et accessible aux personnes autorisées en fonction de profils prédéfinis.

2.3 - Prestations de fourniture

Le titulaire devra assurer la fourniture d'équipements de sécurité de type pare-feu applicatif, des licences associées, des modules d'extension, des solutions d'authentification et des outils de gestion des journaux, conformément aux exigences du présent CCTP.

Les équipements fournis devront être neufs, complets et livrés avec :

- les alimentations et accessoires nécessaires à leur fonctionnement ;

- les supports d'installation ;

- la documentation technique en langue française ou anglaise ;

- les licences d'exploitation et d'administration ;

- les mises à jour logicielles nécessaires à la mise en service.

En cas de fourniture de matériel reconditionné, le titulaire devra demandé l'accord préalable de la DIR Centre-Est et s'assurer qu'aucune données pré existante ne soient présente sur l'équipement.

Les références citées dans le présent document sont données à titre indicatif. Tout équipement équivalent devra présenter des caractéristiques techniques, des performances et des niveaux de qualification au moins équivalents.

La liste des matériels et logiciels utilisés par la DIR Centre-Est est fournie en ANNEXE 2 au présent CCTP. Cette liste n'est transmise que sur demande conformément aux dispositions de l'article 3-1.1 du Règlement de la Consultation.

Le titulaire devra proposer des produits et solutions compatibles avec les équipements et solutions déjà en place à la DIR Centre-Est.

Tous les délais de livraison seront précisés sur chaque bon de commande.

2.4 - Caractéristiques des pare-feux

SÉRIE 100 – FOURNITURE	
	Fourniture Appliance pare-feux
101	Fourniture d'une appliance pare-feu qualifiée par l'ANSSI 4x100/1000/2500 MbE interfaces (configuration XS)
102	Fourniture d'une appliance pare-feu qualifiée par l'ANSSI 8x100/1000/2500 MbE interfaces+1 cage SFP (configuration S)
103	Fourniture d'une appliance pare-feu qualifiée par l'ANSSI 8x100/1000/2500 MbE interfaces + 2 interfaces SFP + 1 slot réseau vide (configuration M)
104	Fourniture d'une appliance pare-feu qualifiée par l'ANSSI 8x100/1000/2500 MbE interfaces + 2 SFP x10gbE + 1 slot réseau vide (configuration M+)
105	Fourniture d'une appliance pare-feu filtrant 6 interfaces RJ 45 10/100/1000 MbE + 1 slot d'extension (Check Point 5200 ou équivalent)
106	Fourniture d'une appliance pare-feu filtrant 10 interfaces + 1 slot d'extension (Check Point 6200 ou équivalent)
107	Fourniture d'un logiciel pare-feu dans une appliance intégrée standard – configuration miminum 6x2,5 GbE, 64Go SSD, 8 Go RAM – Netgate 6100 ou équivalent
108	Fourniture d'un logiciel pare-feu dans une appliance intégrée performante - 6x2,5 GbE, 2x SFP+ 10 Gbps, 2x128 Go SSD, 16 Go RAM – Negate 8200 ou équivalent
	Extention de matériel
120	Modules d'extension 8 ports Gigabit SFP pour appliance pare-feu filtrant Stormshield de la gamme SN500
121	Modules d'extension 8 ports Gigabit SFP pour appliance pare-feu filtrant Stormshield de la gamme SN700
122	Modules d'extension 4 ports 10 Gigabit SFP+ pour appliance pare-feu filtrant Stormshield de la gamme SN500
123	Modules d'extension 4 ports 10 Gigabit SFP+ pour appliance pare-feu filtrant Stormshield de la gamme SN700
124	Modules d'extension 8 ports cuivre 10/100/1000 pour appliance pare-feu filtrant Stormshield de la gamme SN
125	Modules d'extension 8 ports cuivre 100/1000/2500 pour appliance pare-feu filtrant Stormshield de la gamme SN
126	Modules d'extension 8 ports cuivre 10/100/1000 pour appliance pare-feu filtrant CheckPoint 5200 ou 6200
127	Modules d'extension 4 ports ports fibre 1 Gigabit SFP pour appliance pare-feu filtrant CheckPoint 5200 ou 6200
128	Transceiver SFP+ SR/SX pour appliance pare-feu filtrant
	Fourniture Licence pare-feux
130	Fourniture d'une licence de logiciel Antivirus pour un pare-feu filtrant modèle M
131	Fourniture d'une licence de logiciel Antivirus pour un pare-feu filtrant modèle M+
132	Fourniture d'une licence de logiciel Web control pour un pare-feu filtrant
133	Fourniture d'une licence de logiciel de détection de malware pour un pare-feu filtrant
134	Fourniture d'une licence de logiciel Industriel pour un pare-feu filtrant modèle M ou M+
135	Upgrade licence pare-feux qualifié par l'ANSSI 10 Gbps à 12 Gbps – clé d'activation pour upgrade SN220 vers SN320 sur boîtier existant
136	Upgrade licence pare-feux qualifié par l'ANSSI 38 Gbps à 46 Gbps - clé d'activation pour upgrade SN720 vers SN920 sur boîtier existant
	Accès distant sécurisé
140	Fourniture d'un logiciel serveur d'authentification de type RADIUS
141	Fourniture d'un lot de 5 authentificateurs compatibles
142	Fourniture d'un lot de 10 authentificateurs compatible
143	Fourniture d'une licence OEM du système d'exploitation Microsoft Windows Server 2025 ou équivalent
144	Fourniture d'une licence du système d'exploitation Microsoft Windows 11 ou équivalent
	Solution de gestion centralisée des journaux
150	Fourniture d'une application de gestion centralisée des journaux
	Bastion
160	Fourniture d'une licence perpétuelle pour un bastion d'administration – 10 sessions simultanées
	Machine virtuelle durcie
170	Fourniture d'une machine virtuelle durcie avec OS Microsoft Windows11 ou supérieure
171	Fourniture d'une machine virtuelle durcie avec OS Microsoft Windows Server 2025 (ou équivalent)
172	Fourniture d'une machine virtuelle durcie avec OS Debian 13 ou équivalent

Le matériel répond à minima aux spécifications suivantes :

- Qualification de l'ANSSI lorsque la DIR Centre-Est le demande
- Rackable en baie 19 pouces, taille 1U ;
- Alimentation unique ;
- Deux versions :
  - 4 interfaces Gigabit-Ethernet (connecteurs RJ45) ;
  - 8 interfaces Gigabit-Ethernet (connecteurs RJ45) ;
- Pas de RAID ;
- Optionnel : alimentations redondantes
- Garantie : 3 ans sur site.

Le logiciel répond à minima aux spécifications suivantes :

- Filtrage de paquets ;
- Stateful Inspection ;
- Détection et prévention des intrusions (IDS/IPS)
- Journalisation ;
- Administration sécurisée ;
- Proxies applicatifs ;
- VPN IPSec et SSL ;
- Résolution DNS ;
- Cluster en option ;
- Certification EAL4+ et IEC-62443-4-1;
- VLAN 802.1q ;
- Modes de déploiement :
  - Standalone ;
  - Redondance active/passive ;
  - Cluster.

Les options disponibles peuvent être :

- protection antivirus
- détection et protection anti-malwares
- extension web control : contrôle de la navigation web

Les équipements sont fournis avec les licences nécessaires à leur exploitation standard.

2.4.1 - Appliances qualifiées par l'ANSSI (prix 101 à 104)

Le titulaire fournit des appliances pare-feux qualifiées par l'ANSSI adaptées aux différents niveaux de capacité réseau attendus comprenant :

- Le matériel complet ;
- La licence d'utilisation ;
- Les supports d'installation ;
- La documentation
- le contrat du support pour la première année de fonctionnement (de la date d'achat jusqu'au 31/12 de l'année d'achat).

4 modèles se distinguant par leurs caractéristiques sont proposés :

- configuration XS : Appliance disposant de 4 interfaces Ethernet 100/1000/2500 MbE
- configuration S : Appliance disposant de 8 interfaces Ethernet 100/1000/2500 MbE, de 1 interfaces SFP 1 GbE
- configuration M : Appliance disposant de 8 interfaces Ethernet 100/1000/2500 MbE, de 2 interfaces SFP+ 1 GbE et d'un emplacement d'extension réseau libre
- configuration M+ : Appliance disposant de 8 interfaces Ethernet 100/1000/2500 MbE, de 2 interfaces SFP+ 10 GbE et d'un emplacement d'extension réseau libre

2.4.2 - Appliances de nouvelle génération

Le Titulaire fournira une appliance de pare-feu filtrant comprenant :

- Le matériel complet ;
- La licence d'utilisation ;
- Les supports d'installation ;
- La documentation
- le contrat du support pour la première année de fonctionnement (de la date d'achat jusqu'au 31/12 de l'année d'achat).

Les pare-feux de nouvelles génération intègrent l'inspection de paquets au niveau de l'application et de prévention des menaces.

2 modèles se distinguant par leurs caractéristiques sont proposés :

- une appliance comportant 6 interfaces Ethernet 10/100/1000 MbE et un slot d'extension, débit de prévention des menaces de 300 Mbps à 2 Gbps ;
- une appliance comportant 10 interfaces Ethernet 10/100/1000 MbE et deux slots d'extension débit de prévention des menaces de 1 Gbps à 3.7 Gbps .

2.4.3 - Pare-feux intégrés dans une appliance dédiée

Le titulaire fournit des solutions de pare-feux, propriétaires ou libres de droit, intégrées dans des appliances dédiées.

Les configurations minimales attendues sont de 2 types :

- appliance standard :
  - 6 interfaces 2,5 GbE,
  - un SSD de 64 Go minimum
  - 8 Go de mémoire vive ;
- appliance performante :
  - 6 interfaces 2,5 GbE,
  - 2 interfaces SFP+ 10 GbE,
  - deux SSD de 256 Go minimum
  - 16 Go de mémoire vive.

Les équipements permettent l'installation et l'exploitation de solutions logicielles de sécurité (propriétaire ou open source) compatibles avec les besoins du marché.

2.4.4 - Modules et extensions matériels

Le titulaire devra être en mesure de fournir les modules d'extension compatibles avec les appliances proposées.

Les extensions attendues comprennent notamment :

- des modules d'extension 4 ports fibre SFP+ 10 Gigabits ;

- des modules d'extension 8 ports cuivre 100/1000/2500 MbE ;

- des transceivers fibre SFP/SFP+ double débit 1G/10G de type SR/SX courte distance.

L'ensemble des modules devra être pleinement compatible avec les équipements proposés et supportés par le constructeur.

2.4.5 - Licences complémentaires de sécurité

Le titulaire devra fournir les licences logicielles complémentaires nécessaires à l'activation des fonctions avancées de sécurité.

Les licences susceptibles d'être demandées comprennent :

- antivirus ;

- filtrage et contrôle web ;
- détection de malwares ;
- fonctions de sécurité industrielle.

Le titulaire devra également proposer les licences d'évolution de capacité des équipements Stormshield existants, notamment :

- upgrade de licence pour pare-feu Stormshield SN220 vers SN320 ;
- upgrade de licence pour pare-feu Stormshield SN720 vers SN920.

Ces licences devront être compatibles avec les équipements déjà déployés et fournies sous forme de clés d'activation officielles du constructeur.

2.4.6 - Accès distant sécurisé et authentification forte

Le titulaire devra fournir une solution d'authentification centralisée de type RADIUS permettant la gestion sécurisée des accès distants et des authentifications multi-facteurs.

La prestation comprendra :

- les licences serveur (si solution éditeur);
- les supports d'installation ;
- la documentation ;
- les licences clients nécessaires.

Le Titulaire fournira, par lot de 5 ou 10, des tokens d'identification ou authentificateurs compatibles avec le logiciel serveur d'authentification de type Radius déployé à la DIR Centre-Est (système d'authentification ROAD).

Les solutions proposées devront être compatibles avec les pare-feux et systèmes d'exploitation retenus dans le cadre du marché.

2.4.7 - Système d'exploitation

Le titulaire devra pouvoir fournir :

- des licences OEM Microsoft Windows Server 2025 ou équivalent ;
- des licences Microsoft Windows 11 Professionnel ou équivalent.

Les licences devront être officielles, activables et accompagnées de leur documentation et supports associés.

Le titulaire peut proposer des licences reconditionnées à condition de demander l'accord préalable de l'acheteur.

2.4.8 - Solution de gestion centralisée des journaux

Le Titulaire fournira une solution pour la centralisation et l'analyse des logs comprenant :

- - un serveur de collecte de logs ;
- - un agrégateur de journaux ;
- - un outil de visualisation et d'analyse.

La solution devra permettre :

- la centralisation des événements de sécurité ;
- la recherche et la corrélation des événements ;
- l'export des journaux ;
- la conservation des traces conformément aux exigences réglementaires ;
- la génération d'alertes et de tableaux de bord.

L'ensemble devra être compatible avec les équipements de sécurité proposés dans le cadre du marché et la solution de gestion centralisées des journaux actuellement en production à la DIR Centre-Est décrits dans l'ANNEXE 2.

2.4.9 - Bastion

Le Titulaire fournira une solution de bastion permettant :

- le filtrage et le contrôle des accès distants ;
- le filtrage et le contrôle des accès à privilèges (flux d'administration) ;
- la traçabilité des accès.

Deux types de bastions sont proposés :

- 1 bastion libre de droit (open source) permettant le contrôle des accès basés sur les protocoles SSH et RDP
- 1 bastion sous licence commerciale de l'éditeur permettant le contrôle des accès basés sur les protocoles SSH, RDP et HTTP(S).

Les 2 types de bastions doivent répondre aux mêmes exigences, c'est à dire :

- sécurité : authentification forte, chiffrement et journalisation des connexions
- traçabilité : logs détaillées et enregistrement des sessions
- conformité : répondre aux exigences de l'ANSSI et au RGPD

Les solutions proposées devront être compatibles avec les solutions déjà déployées à la DIR Centre-Est et décrites dans l'ANNEXE 2.

2.4.10 - Machine durcie

Le Titulaire fournira une machine virtuelle type, prête à l'utilisation sur laquelle seront appliquées les règles de sécurisation listées dans les guides CIS.

3 types de machines durcies pourront être générées :

- 1 machine fonctionnant sous le système d'exploitation Windows 11 ou supérieur ;
- 1 machine fonctionnant sous le système d'exploitation Windows Server 2025corrgié ou supérieur ;
- 1 machine fonctionnant sous le système d'exploitation Debian 13 ou supérieur.

La licence Microsoft n'est pas fournie avec la machine virtuelle.

2.5 - Contrats de maintenance

SÉRIE 200 – CONTRATS DE MAINTENANCE	
	Contrat de maintenance pour pare-feu
201	Maintenance annuelle d'une appliance Stormshield SN170 ou équivalent
202	Maintenance annuelle d'une appliance Stormshield SN série 2xx ou équivalent
203	Maintenance annuelle d'une appliance Stormshield SN série 3xx ou équivalent
204	Maintenance annuelle d'une appliance Stormshield SN série 5xx ou équivalent
205	Maintenance annuelle d'une appliance Stormshield SN série 7xx ou équivalent
206	Maintenance annuelle d'une appliance Stormshield SN série 9xx ou équivalent
207	Maintenance annuelle d'une appliance Check Point 5200 ou équivalent
208	Maintenance annuelle d'une appliance Check Point 6200 ou équivalent
209	Maintenance annuelle d'une appliance Netgate 6100 ou équivalent
210	Maintenance annuelle d'une appliance Netgate 8200 ou équivalent
	Contrat de maintenance pour un bastion d'administration
220	Contrat de maintenance annuel pour un bastion d'administration sous licence Rubycat ou équivalent
	Contrat de maintenance pour un serveur d'authentification
230	Contrat de maintenance annuel pour un serveur d'authentification
	Contrat de maintenance pour un serveur d'authentification
240	Contrat de maintenance annuel pour Arimes Web - On Premise de 1 à 10 utilisateurs

2.5.1 - Objet des contrats

Le titulaire s'engage à souscrire annuellement, pour le compte de la DIR Centre-Est, aux contrats de support et de maintenance nécessaires auprès des éditeurs des logiciels, solutions ou composants techniques utilisés dans le cadre de la réalisation des prestations objet du marché. Ces contrats doivent garantir :

- La continuité du support technique (niveau 2 et 3) pour les matériels et logiciels déployés à la DIR Centre-Est ;
- L'accès aux mises à jour correctives et évolutives (patches, versions majeures/mineures) ;
- L'accès aux mises à jour de sécurité ;

- La conformité aux exigences légales et réglementaires (ex. : NIS2, RGPD, sécurité des systèmes d'information) ;
- La prise en compte et la correction des bogues.

2.5.2 - Périmètre des contrats de support

Les contrats de support doivent couvrir l'intégralité des logiciels, matériels ou outils tiers explicitement listés en annexe 2 du présent CCTP ou utilisés dans le cadre des prestations. À titre indicatif, cela inclut :

- Les matériels et logiciels des pare-feux fournis par des éditeurs ;
- Les bastions sous licence éditeur ;
- Le logiciel d'authentification RADIUS ;
- L'outil d'analyse des risques ;
- Exclusion : Les logiciels libres sans obligation de support commercial sont exclus de cette clause, sauf mention contraire dans le CCTP.

2.5.3 - Transmission des droits et obligations

Le titulaire s'engage à :

- Transférer au maître d'ouvrage les droits d'usage des licences et des contrats de support pour les logiciels intégrés dans les livrables du marché, sous réserve des restrictions légales ou contractuelles des éditeurs.
- Informer le maître d'ouvrage de toute modification substantielle des contrats de support (ex. : changement de SLA, augmentation des coûts, fin de support d'une version).
- Garantir la pérennité des contrats de support pour une durée indiquée sur le bon de commande.

2.5.4 - Documentation et reporting

Le titulaire doit fournir, à la demande du maître d'ouvrage :

- Un inventaire à jour des contrats de support souscrits (éditeur, référence, durée, SLA) ;
- Un rapport trimestriel sur les incidents remontés aux éditeurs, incluant :
  - La nature des incidents ;
  - Les temps de réponse et de résolution ;
  - Les actions correctives mises en œuvre.

2.6 - Maintenance préventive

SÉRIE 400 – MAINTENANCE PRÉVENTIVE	
401	Visite préventive sur 2 pare-feux filtrants en haute-disponibilité
402	Visite préventive sur 1 pare-feu standalone
403	Visite préventive sur un serveur d'authentification
404	Visite préventive sur un bastion sous licence
405	Visite préventive sur un bastion libre de droit
406	Visite préventive sur un système de centralisation et d'analyse des logs

2.6.1 - Objet des visites préventives

La maintenance préventive consiste à effectuer une inspection périodique des matériels et logiciels déployés.

Le titulaire est tenu d'assurer la maintenance préventive des matériels et logiciels (libres ou sous licence) utilisés dans le cadre du présent marché, afin de :

- Garantir la disponibilité, la performance et la sécurité des systèmes ;
- Prévenir les pannes et les vulnérabilités ;
- Prolonger la durée de vie des équipements et des logiciels ;
- Mettre à jour et/ou optimiser les paramétrages ;
- Respecter les obligations légales et réglementaires (ex. : RGPD, directives ANSSI et NIS2, normes ISO 27001).

Cette maintenance couvre :

- Les matériels (appliances) ;
- Les logiciels sous licence (commerciaux ou propriétaires) ;
- Les logiciels libres (open source) utilisés en production.

2.6.2 - Contenu de la prestation

Le Titulaire est tenu d'effectuer une visite préventive annuelle dans chacun des PC pour l'ensemble des pare-feux, bastion, serveur d'authentification et de gestion centralisée des journaux, le Titulaire effectuera :

- Le contrôle complet de l'état des systèmes d'exploitation et des logiciels installés, y compris les clients de connexion aux pare-feux installés sur des machines dédiées ;
- L'application des mises à jour de sécurité ;

- L’installation des mises à jour mineures ;
- L'évaluation de la nécessité de déployer des mises à jour éditeurs majeures disponibles ;
- L’identification des logiciels et matériels en fin de vie et la proposition d’un plan de migration ;
- Le cas échéant, une vérification du bon fonctionnement des tunnels IPSec ;
- L’évaluation des performances ;
- L’examen des logs des pare-feux ;
- La vérification de la validité du pare-feu secours ;
- La sauvegarde complète du système ;
- Une revue des règles des pare-feux ;
- La vérification de la cohérence de la documentation (ex schémas réseau) ;
- Si nécessaire, l'optimisation des règles.

2.6.3 - Livrable

A l'issue de son intervention, le Titulaire remettra à la DIR CE un rapport d'intervention complet précisant :

- le modèle et le numéro de série des équipements inspectés,
- la version de l’application ou du logiciel avant la visite préventive et la version à l’issue de la visite préventive,
- les actions de maintenance réalisées sur chaque pare-feu et les éventuelles préconisations d'évolution,
- les anomalies détectés et les actions correctives mises en œuvre ou proposées
- le compte-rendu d’analyse des logs,
- les règles de filtrages qu’il convient de revoir et l’éventuelle préconisation d’un audit approfondi des règles,
- la sauvegarde du système.

2.6.4 - Délais et temps d’indisponibilité

Le titulaire s’engage à intervenir à la date et dans le délai qui auront été convenus avec le maître d’ouvrage pour la réalisation des prestations. La date et le délai sont rappelés sur chaque bon de commande.

La procédure décrivant les modalités d’intervention de la visite indique notamment **à la fois le délai de la visite et le temps d’indisponibilité des équipements.** Le dépassement de ce délai engendrera l’application des pénalités prévues à l’article 4 du CCAP.

2.7 - Maintenance corrective

SÉRIE 500 – MAINTENANCE CORRECTIVE	
	Diagnostic
501	Expertise distante
502	Expertise sur site
503	Audit d'un dysfonctionnement réseau sur une architecture réseau simple (1 site)
504	Audit d'un dysfonctionnement réseau sur une architecture réseau complexe (multi sites)
	Actions correctives
510	Assistance pour la remise en service d'un pare-feu ou d'une application
511	Remise en état de fonctionnement d'un pare-feu
512	Remise en état de fonctionnement d'un serveur authentification RADIUS
513	Remise en état de fonctionnement d'un bastion libre de droits
514	Remise en état de fonctionnement d'un un bastion sous licence
515	Remise en état de fonctionnement et remise en service d'une application de gestion centralisée des journaux
516	Remise en service d'un pare-feu
517	Remise en service d'un serveur authentification RADIUS
518	Remise en service d'un bastion libre de droits ou sous licence
	Audits
530	Audit des règles d'un réseau d'un pare-feu

Les prestations de maintenance corrective consistent à diagnostiquer les dysfonctionnements constatés par la DIR Centre-Est et à rétablir le fonctionnement normal des matériels et logiciels en cas de défaillance, panne ou dysfonctionnement, dans les délais et conditions définis ci-dessous.

Il n'est pas demandé au titulaire d'assurer une astreinte 24/7 mais il doit disposer d'une équipe suffisamment dimensionnée pour prendre en compte les demandes d'intervention et réaliser les interventions dans les délais indiqués au § 2.7.6 du présent CCTP.

La maintenance corrective comprend les interventions suivantes :

1. Expertise et diagnostic : analyse technique pour identifier la cause de la défaillance, du dysfonctionnement ou une suspicion d'attaque.
2. Remise en état de fonctionnement : opérations techniques visant à réparer ou restaurer un composant défectueux.
3. Remise en service : opérations visant à rendre le système pleinement opérationnel dans son environnement initial.

Chaque intervention donne lieu à la rédaction d'un rapport par le Titulaire à destination de la DIR Centre-Est, consignant notamment la date, le lieu, les intervenants, la durée, la description de l'intervention, les mesures et tests effectués, les causes du problème, les solutions apportées, les préconisations à respecter, etc.

Le titulaire s’engage à réaliser les prestations suivantes, sans limitation.

2.7.1 - Expertise ou diagnostic

Cible : pare-feux, bastions, serveur d'authentification, serveur de centralisation des journaux

Contenu de la prestation

Suite à un problème constaté par la DIR Centre-Est, le Titulaire effectuera un diagnostic permettant d'identifier la cause du problème et proposera une solution pour le résoudre.

Avant toute intervention de remise en état de fonctionnement, le titulaire réalise une analyse approfondie de la défaillance. La DIR CE pourra avoir recours à cette prestation dans les cas suivants (la liste non exhaustive) :

- Incident ou attaque sur le réseau ;
- Dysfonctionnement d'un équipement ou d’une système faisant l’objet du marché ;
- Problème sur un flux réseau ;
- Problème sur un tunnel IPSec.

Les expertises ou diagnostics comportent plusieurs étapes :

1. la collecte des informations. La collecte des informations consiste à interroger les utilisateurs et/ou administrateurs de la DIR Centre-Est et à récupérer et analyser les logs.
2. l’analyse technique du problème ou du dysfonctionnement. On distingue deux types de prestations selon que l'expertise s'effectue à distance (depuis les locaux du Titulaire via l’accès de télémaintenance de la DIR Centre-Est) ou sur site (nécessitant donc un déplacement).
3. L’identification de la cause. Il s’agit de déterminer si le dysfonctionnement ou la défaillance est lié à un problème matériel, logiciel, humain ou externe et de classer la criticité de l’incident.
4. l’élaboration et la transmission d’un rapport de diagnostic. Le rapport peut être transmis oralement mais sa transposition écrite devra être transmise à la DIR Centre-Est dans les 24 heures ouvrées suivant l’incident ;
5. la validation du diagnostic par la DIR Centre-Est. Le titulaire doit obtenir l’accord de la DIR Centre-Est avec de procéder aux interventions.

2.7.2 - Assistance pour la remise en service d'un équipement

Cible : pare-feux, bastions, serveur d'authentification, serveur de centralisation des journaux

Contenu de la prestation

Dans le cas où les actions de dépannage peuvent être réalisées localement, le Titulaire procurera conseil et assistance téléphoniques aux techniciens de la DIR Centre-Est jusqu'à la remise en état de l'organe de sécurité en défaut.

Dans le cas contraire, le Titulaire se rendra sur site ou prendra la main à distance pour effectuer lui-même l'intervention de dépannage (cf. prestation suivante).

2.7.3 - Remise en état de fonctionnement d'un équipement

Cible : pare-feux, bastions, serveur d'authentification, serveur de centralisation des journaux

Contenu de la prestation

La remise en état de fonctionnement comporte l'ensemble des opérations techniques visant à réparer ou restaurer un composant défectueux. *Par exemple, remplacement d'une alimentation défectueuse sur une appliance, réparation d'un port défectueux, correction d'erreurs de configuration, ...*

L'intervention comprendra un diagnostic de la cause de la défaillance et en fonction du diagnostic les actions suivantes seront être réalisées :

- Remplacement ou réparation du composant défectueux ;
- Correction des erreurs logicielles ;
- Application des correctifs ;
- Ré-installation du logiciel, pare-feu ou serveur d'authentification : les versions les plus récentes ainsi que les derniers correctifs disponibles seront systématiquement installés ;
- Paramétrage du pare-feu avec les données de la politique de sécurité du site ou du serveur d'authentification ;
- Paramétrage des tunnels IPSec le cas échéant ;
- Test de l'équipement hors production ;

Le titulaire devra s'assurer que tous les correctifs de sécurité ont été appliqués avant de procéder à la remise en service de l'équipement ou de l'application.

2.7.4 - Remise en service d'un équipement

Cible : pare-feux, bastions, serveur d'authentification, serveur de centralisation des journaux

Contenu de la prestation

Après la remise en état de fonctionnement, le titulaire devra garantir que le système est opérationnel et conforme aux exigences du marché. Cette opération consiste à réintégrer le matériel réparé ou l'application dans l'environnement de production en réalisant les actions suivantes :

- Tests de validation du bon fonctionnement du matériel ou du logiciel ;
- Réintégration du matériel ou de l'application dans l'infrastructure en production ;

- Connexion et mise en œuvre de l'équipement ou de l'application ;
- Remise en service de la haute disponibilité (si existante) ;
- Test de l'équipement ou de l'application dans l'environnement de production.

2.7.5 - Audit de règles d'un pare-feux

Cible : pare-feux

Contenu de la prestation

A la demande de la DIR Centre-Est, le Titulaire vérifie la pertinence et la cohérence des règles sur un réseau de pare-feu.

Pour cela, il réalise les actions suivantes :

- Constitution de la matrice des flux du réseau audité grâce aux logs du pare-feu et à un renifleur si nécessaire ;
- Vérification de l'adéquation des règles avec la matrice des flux réalisée, de la cohérence des règles entre elles ;
- Formulation de préconisations afin optimiser les règles.

2.7.6 - Délais

Toute intervention de correction doit se dérouler en respectant trois délais :

- **Délai d'intervention** : prise en compte de l'anomalie par le Titulaire, concrètement le diagnostic a commencé ;
- **Délai de remise en service** : mise en place d'un système provisoire apte à assurer le service minimum requis pour l'exploitation. Ce délai n'est applicable que dans le cas d'une intervention urgente ou critique ;
- **Délai de remise en marche nominale** : retour au fonctionnement nominal du système. Concernant ce délai, le titulaire devra effectuer son intervention et remettre en marche l'installation dans les 40 heures ouvrées. Ce délai ne comprend pas le délai d'approvisionnement du matériel de remplacement qui est indépendant du temps d'intervention.
- Les interventions urgentes concernent une panne ou une défaillance impactant un service essentiel (*par exemple un pare-feu cœur de réseau ou lié à la supervision des tunnels*)

	Délai d'intervention		Délai de remise en service	
	Normale	***Urgente***	***Normale***	***Urgente***
Expertise distante	8 heures ouvrables	4 heures ouvrables	Non applicable	Non applicable
Expertise sur site	16 heures ouvrables	8 heures ouvrables	Non applicable	Non applicable
Assistance pour la remise en service d'un pare-feu	8 heures ouvrables	4 heures ouvrables	Non applicable	Non applicable
Remise en état de fonctionnement d'un pare-feu	4 heures ouvrables	2 heures ouvrables	12 heures ouvrables	8 heures ouvrables
Remise en état de fonctionnement d'un bastion	8 heures ouvrables	4 heures ouvrables	24 heures ouvrables	12 heures ouvrables
Remise en état de fonctionnement d'un serveur d'authentification	8 heures ouvrables	4 heures ouvrables	24 heures ouvrables	12 heures ouvrables
Remise en état de fonctionnement d'une application de gestion centralisée des logs	48 heures ouvrables	24 heures ouvrables	5 jours ouvrables	3 jours ouvrables

Tableau récapitulatif des délais par type d'intervention

2.8 - Maintenance évolutive

SÉRIE 600 – MAINTENANCE ÉVOLUTIVE	
601	Conseil en architecture réseau sécurisé
	Déploiement de pare-feux
610	Déploiement d'un pare-feu filtrant standalone
611	Déploiement d'une paire de pare-feux filtrants en redondance à chaud
	Déploiement de pare-feux de secours
620	Mise en haute disponibilité d'un pare-feu
	Mise à jour de pare-feux
630	Mise à jour majeure d'un pare-feu
631	Mise à jour mineure d'un pare-feu
	Modification de la politique de sécurité d'un pare-feu
640	Audit des règles d'un réseau d'un pare-feu
641	Mise à jour de la politique de sécurité sur un pare-feu
	Création de tunnels IPSec
650	Création de tunnels IPSec sur un pare-feu
	Accès distant sécurisé
660	Installation d'un serveur d'authentification de type RADIUS
661	Mise à jour d'un serveur d'authentification
662	Installation d'un serveur d'un bastion sous licence
663	Installation d'un bastion libre de droits
664	Intégration d'un nouveau système dans le système de gestion des logs

La maintenance évolutive a pour objet d'assurer l'adaptation, l'optimisation et l'enrichissement des infrastructures réseau et des systèmes de sécurité, en réponse aux besoins fonctionnels ou techniques nouveaux, aux évolutions réglementaires, ou aux recommandations de sécurité. Elle couvre les prestations listées ci-dessous, organisées en quatre grandes familles :

- Conseil et architecture ;
- Déploiement et mise en œuvre de pare-feux ;
- Modification des politiques de sécurité ;
- Évolutions de l'accès de télémaintenance (accès distant sécurisé).

Le titulaire s'engage à réaliser ces prestations conformément aux bonnes pratiques du secteur (ex. : ISO 27001, ANSSI, ITIL) et aux exigences spécifiques du maître d'ouvrage.

Les prestations décrites dans ce paragraphe permettent de prendre en compte des besoins d'évolution ou d'optimisation de la sécurité des solutions de sécurité ou des infrastructures existantes.

Chaque intervention donnera lieu à la rédaction d'un rapport rédigé par le Titulaire à destination de la DIR CE, consignant notamment la date, le lieu, les intervenants, la durée et la description de l'intervention.

2.8.1 - Conseil en architecture

Cette prestation a pour objectif de faire réaliser par le Titulaire une étude fonctionnelle et technique d'architecture répondant à des besoins d'évolution ou d'optimisation de la sécurité du réseau de la DIR CE ou du réseau d'un des PC. Elle comprend :

- Le recueil et l'analyse du besoin en matière de sécurité et de performance ;
- La proposition d'une ou plusieurs architectures adaptées au besoin ;
- Une évaluation des risques ;
- Les recommandations techniques pour la mise en œuvre de la proposition retenue.

Un rapport d'analyse incluant l'état des lieux, les scénarios proposés, l'évaluation des risques et des coûts sera transmis à la DIR Centre-Est.

2.8.2 - Déploiement d'un pare-feu

Cible : pare-feux

Contenu de la prestation

Le Titulaire mènera les actions nécessaires au déploiement d'un pare-feu :

- Dans le cas d'un pare-feu installé sur un serveur, validation préalable du modèle de serveur que la DIR CE compte acquérir pour héberger le logiciel pare-feu ;
- Mise en place et raccordement du matériel (énergie et réseau) ;
- Aide au paramétrage des commutateurs concernés par la connexion du pare-feu ;
- Dans le cas d'un pare-feu installé sur un serveur : installation du système d'exploitation , y-compris installation des mises à jour de sécurité disponibles et sécurisation du système d'exploitation (application du guide de durcissement) ;
- Installation du logiciel pare-feu sur le serveur (les dernières versions de logiciel et de correctifs seront systématiquement installées) ;
- Installation du module management et configuration du GUI ;
- Paramétrage du pare-feu avec les données de la politique de sécurité du site ;
- Paramétrage d'une sauvegarde programmée et automatique ;
- Paramétrage des informations propres au site (DNS, synchronisation horaire, transfert des sauvegardes ...)
- Connexion et mise en œuvre du pare-feu ;

- Paramétrage de la mise en haute disponibilité si nécessaire et tests de bascule automatique;
- Paramétrage de l'envoi des logs vers une solution de gestion centralisée des logs ;
- Tests de filtrage et de performance du pare-feu ;
- Documentation technique.

Pour le déploiement d'une paire de pare-feux en redondance à chaud, le titulaire effectuera en plus des prestations listées ci-dessus, les prestations suivantes :

- Le paramétrage de la redondance ;
- Les tests de bascule automatique et de reprise de l'activité ;
- La documentation incluant les mécanismes de bascule.

Matériel, logiciel

La fourniture du matériel et de la licence du système d'exploitation ne fait pas partie de la présente prestation. Ils seront mis à disposition du Titulaire par la DIR CE qui les aura préalablement acquis, soit dans le cadre du présent marché (c'est le cas pour les appliances de pare-feu et les licences des applications), soit dans le cadre d'un autre marché (c'est le cas des serveurs).

Dans le cas d'un pare-feu filtrant libre de droits, la prestation comprend la fourniture du système d'exploitation et des différents logiciels composant la solution.

2.8.3 - Déploiement d'un pare-feu de secours en mode manuel

Cible : pare-feux

Contenu de la prestation

Le Titulaire mènera les actions nécessaires au déploiement d'un pare-feu de secours filtrant ou applicatif dont l'activation, en cas de panne du pare-feu principal, se fera par une intervention manuelle des techniciens de la DIR CE.

L'intervention comprendra les actions suivantes :

- Dans le cas d'un pare-feu filtrant, validation préalable du modèle de serveur que la DIR CE compte acquérir pour héberger le logiciel pare-feu ;
- Mise en place et raccordement du matériel (énergie et réseau) ;
- Dans le cas d'un pare-feu installé sur un serveur : installation du système d'exploitation , y-compris installation des mises à jour de sécurité disponibles et sécurisation du système d'exploitation (application du guide de durcissement) ;
- Installation du module management et configuration
- Installation du logiciel pare-feu sur le serveur de secours dans la même version que le pare-feu principal ;
- Paramétrage du pare-feu avec les données de la politique de sécurité du pare-feu principal ;

- Paramétrage d’une sauvegarde programmée et automatique ;
- Paramétrage des informations propres au site (DNS, synchronisation horaire, transfert des sauvegardes ...)
- Connexion et mise en œuvre du pare-feu ;
- Rédaction de la procédure de bascule manuelle ;
- Paramétrage de la gestion centralisée et de l’analyse des logs ;
- Test du pare-feu et de la procédure de bascule manuelle ;
- La documentation incluant les mécanismes de bascule manuelle.

Matériel, logiciel

Idem prestation précédente.

2.8.4 - Mise en haute disponibilité d'un pare-feu secours

Cible : pare-feu applicatif et filtrant.

Contenu de la prestation

Le Titulaire mènera les actions nécessaires au déploiement d'un pare-feu de secours filtrant ou applicatif en haute disponibilité :

- Dans le cas d'un pare-feu filtrant, validation préalable du modèle de serveur que la DIR CE compte acquérir pour héberger le logiciel pare-feu ;
- Mise en place et raccordement du matériel (énergie et réseau) ;
- Installation du logiciel pare-feu sur le serveur de secours dans la même version que le pare-feu principal ;
- Paramétrage du pare-feu avec les données de la politique de sécurité du pare-feu principal ;
- Connexion et mise en œuvre du pare-feu ;Test du pare-feu et de la procédure de bascule automatique ;
- La documentation incluant les mécanismes de bascule.

Matériel, logiciel

Idem prestation précédente.

2.8.5 - Mise à jour d'un pare-feu

Cible : pare-feux

Contenu de la prestations

Le Titulaire assure la mise à jour des pare-feux. Il installera sur le pare-feu principal, et le pare-feu de secours s'il existe, les mises à jour fournies par l'éditeur. Deux prestations sont prévues dans le marché suivant que la mise à jour à installer soit majeure ou

mineure.

Les mises à jour, majeures ou mineures, sont planifiées en collaboration avec la DIR Centre-Est.

Mise à jour majeure :

- Analyse d'impacts de la mise à jour ;
- Sauvegarde complète de la configuration ;
- Application de la mise à jour du ou des pare-feu. ;
- Mise à jour du GUI ;
- Test de non régression des pare-feux et GUI ;
- Validation par le maître d'ouvrage.

Mise à jour mineure (patch ou modification mineure) :

- Application de la mise à jour du ou des pare-feu. ;
- Mise à jour du GUI (si nécessaire) ;
- Vérification de l'intégrité des règles et des politiques ;
- Documentation des changements.

Livrable attendu :

Un rapport de mise à jour incluant :

- La version avant/après ;
- Les modifications apportées ;
- Les résultats des tests ;
- Les recommandations (ex. : ajustements de configuration).

2.8.6 - Mise à jour de la politique de sécurité sur un pare-feu

Cible : pare-feu

Contenu de la prestation

Le Titulaire mettra à jour les règles du pare-feu principal, et du pare-feu de secours s'il existe, conformément à la politique de sécurité de la DIR CE. La prestation comprend :

- La configuration de la nouvelle politique ;
- La mise en production de la nouvelle politique ;
- La réalisation des tests de validation ;
- La documentation des changements.

Cette prestation pourra être commandée à la suite d'un audit des règles, ou en cas d'ajout

ou de suppression d'une interface du pare-feu.

2.8.7 - Création de tunnels IPSec

Cible : pare-feu et routeur terrain

Contenu de la prestation

Le Titulaire mènera les actions nécessaires pour la création de tunnels IPSec entre deux pare-feux ou entre un pare-feu et un routeur distant suivants les recommandations de la DIR CE.

Les tunnels IPsec devront être compatibles avec les équipements existants (ex. : pare-feu, VPN déjà existants, ...).

La prestation comprend :

- La création du tunnel ;
- La création des règles de routage et de translation d'adresse ;
- Le paramétrage des associations de sécurité ;
- La réalisation des tests de connectivité et de sécurité ;
- La documentation (schémas, certificats, procédures de renouvellement et de maintenance, ...).

Livrable attendu :

Le titulaire rédige un rapport de configuration incluant les paramètres techniques des tunnels et le résultats des tests de connectivité.

2.8.8 - Déploiement d'un serveur d'authentification

Cible : serveur d'authentification.

Contenu de la prestation

Le Titulaire mènera les actions nécessaires au déploiement complet d'un serveur d'authentification RADIUS :

- Validation préalable du modèle de serveur que la DIR CE compte acquérir pour héberger le logiciel d'authentification ou validation des caractéristiques de la machine virtuelle ;
- Installation du système d'exploitation Windows Server ou Linux, y-compris installation des mises à jour de sécurité disponibles et sécurisation du système d'exploitation (application du guide de durcissement) ;
- Installation de l'antivirus mis à disposition par la DIR Centre-Est ;
- Installation du logiciel d'authentification ;
- Intégration éventuelle avec un annuaire existant ;
- Configuration et paramétrage du logiciel d'authentification ;
- Mise en production ;
- Tests de fonctionnement ;

- Documentation incluant l’installation, la maintenance et l’administration .

Matériel

La fourniture du matériel ne fait pas partie de la présente prestation. Il sera mis à disposition du Titulaire par la DIR CE et sera conforme aux préconisations techniques émises par le Titulaire.

Logiciel et système d'exploitation commerciaux

La fourniture du logiciel et du système d'exploitation ne font pas partie de la présente prestation. Ils seront mis à disposition du Titulaire par la DIR CE qui les aura préalablement acquis dans le cadre du présent marché ou d’un autre marché.

Logiciel et système d'exploitation libres de droit

La fourniture du système d'exploitation font partie de la présente prestation.

2.8.9 - Mise à jour d'un serveur d'authentification

Cible : serveur d'authentification

Contenu de la prestation

Le Titulaire installera sur le serveur d'authentification les mises à jour fournies par l'éditeur ou les mises à jour de sécurité :

- Étude d’impact et vérification de la compatibilité avec les autres composants ;
- Application des mises à jour ;
- Vérification de la compatibilité avec les autres composants ;
- Test de non régression du service d'accès distant
- Fourniture d’un rapport d’intervention.

Deux prestations sont prévues dans le marché suivant que la mise à jour à installer soit majeure ou mineure.

2.8.10 - Déploiement d'un bastion

Cible : bastion

Contenu de la prestation

La DIR Centre-Est a mis en place des bastions servant de points d’accès unique et contrôlé à ses réseaux. Ces bastions ont pour objectifs de centraliser les accès, de mettre en place des règles authentification renforcées et de journaliser toutes les connexions (enregistrement des sessions).

Le Titulaire mènera les actions nécessaires au déploiement complet d’un bastion choisit en accord avec le maître d’ouvrage. Les prestations de déploiement comprennent :

- La validation du choix du bastion en fonction des besoins exprimés par la DIR Centre-Est ;
- La validation préalable du modèle de serveur que la DIR CE compte acquérir pour

héberger le bastion ;

- Installation du système d'exploitation, y-compris installation des mises à jour de sécurité disponibles et sécurisation du système d'exploitation (application du guide de durcissement) ;
- Installation de l'antivirus mis à disposition par la DIR Centre-Est ;
- Installation et configuration du bastion ;
- Configuration et paramétrage des comptes et des accès ;
- Mise en place de la journalisation centralisée des connexions ;
- Mise en production ;
- Tests de connexion, de performance et de fonctionnement
- Validation par le maître d'ouvrage ;
- Le transfert de compétences aux administrateurs de la DIR Centre-Est ;
- Fourniture de la documentation d'installation, de configuration, de maintenance et d'administration.

Matériel

La fourniture du matériel ne fait pas partie de la présente prestation. Il sera mis à disposition du Titulaire par la DIR CE et sera conforme aux préconisations techniques émises par le Titulaire.

Livrables attendus :

- Un rapport de déploiement incluant :
  - La configuration technique (OS, versions des logiciels, paramètres de sécurité) ;
  - Les règles d'accès (qui peut accéder à quoi, avec quelles restrictions) ;
  - Les résultats des tests (sécurité, performance, traçabilité) ;
- Un guide utilisateur pour les titulaires du maître d'ouvrage.
- Les licences et contrats de support pour les bastions sous licence commerciale.

2.8.11 - Déploiement d'un serveur de gestion centralisée des journaux (logs)

Cible : serveur de gestion des logs

Contenu de la prestation

Le Titulaire mènera les actions nécessaires au déploiement complet d'un serveur de gestion centralisée des logs. Il s'appuiera sur des solution libre de droits (open source).

La solution déployée devra être compatible avec les infrastructures existantes.

La solution choisit doit garantir la confidentialité et l'intégrité des données collectées, le titulaire s'assurera que ces exigences sont bien respectées au cours du déploiement.

Le déploiement comporte les étapes suivantes :

- Validation préalable de la DIR Centre-Est de la solution proposée par le titulaire ;

- Validation préalable du modèle de serveur que la DIR CE compte acquérir pour héberger le logiciel ;
- Proposition d'un calendrier de mise en œuvre et d'intervention ;
- Installation du système d'exploitation, y-compris installation des mises à jour de sécurité disponibles ;
- Installation de l'antivirus mis à disposition par la DIR Centre-Est;
- Installation et paramétrage du logiciel de centralisation des logs. L'application de centralisation des logs devra regrouper en un point unique les logs de tous les pare-feux de la DIR Centre-Est et du serveur d'authentification ou de tout autre système désigné par la DIR Centre-Est ;
- Configuration des sources de logs (pare-feux, équipements réseau ou applications)
- Configuration et paramétrage du logiciel d'analyse des logs. L'analyse des logs permettra la détection d'intrusions ou de comportements anormaux sur les échanges filtrés sur les pare-feux. Le titulaire assistera la DIR Centre-Est pour la mise en place des processus d'analyse des logs.
- Mise en place des alertes liées aux analyses des logs ;
- Mise en production ;
- Transfert de compétences aux administrateurs de la DIR Centre-Est ;
- Tests de fonctionnement ;
- Documentation incluant l'installation, la configuration, la maintenance et l'administration de la solution.

Matériel

La fourniture du matériel ne fait pas partie de la présente prestation. Il sera mis à disposition du Titulaire par la DIR CE et sera conforme aux préconisations techniques émises par le Titulaire.

Livrables attendus :

- Un rapport d'installation ou d'intégration incluant :
  - La configuration technique ;
  - un schéma fonctionnel et technique ;
  - Les tests réalisés ;
  - Les procédures d'exploitation et de maintenance ;
- Un guide utilisateur.

2.8.12 - Mise à jour d'un serveur de gestion centralisée et d'analyse des logs

Cible : serveur de gestion centralisée et d'analyse des logs

Contenu de la prestation

Le Titulaire installera sur le serveur de gestion des logs, les mises à jour fournies par

l'éditeur :

- Mise à jour de l’application et mises à jour de sécurité ;
- Analyse du fonctionnement de l’application
- Vérification de l’espace de stockage et de la qualité des données stockées
- Vérification des règles d’analyse.

2.8.13 - Garanties

Le titulaire devra **garantir le bon fonctionnement** des solutions déployées pendant une période de **3 mois** après la réception des travaux.

En cas de **défaillance avérée** liée à une prestation évolutive, le titulaire devra **intervenir sans frais supplémentaires** pour corriger le problème.

2.9 - Forfaits d'intervention

2.9.1 - Forfaits d'intervention géographique

Un forfait d'intervention est prévu selon un découpage géographique articulé autour de chaque service régional d'exploitation. Il comprend la prise en charge du déplacement (hors frais d'hébergement et de restauration) et du matériel nécessaires pour intervenir sur site et peut être commandé en complément de n'importe quel autre prix.

Trois zones géographiques sont identifiées :

- SREI de Chambéry : zone concernant le PC Gentiane (Grenoble), le PC Osiris (Albertville) et les tunnels rattachés au PC Osiris.
- SREX de Lyon : zone concernant le PC de Genas et le PC Hyrondelle (Saint-Etienne) et les tunnels rattachés au PC Hyrondelle.
- SREX de Moulins : zone concernant le PC de Moulins, le CEI de Dijon et le tunnel de Talant.

2.9.2 - Plus-value pour intervention de nuit

Cette plus-value s'applique aux prestations de maintenance corrective et évolutive dans un le cas où les contraintes d'exploitation de la DIR CE impose d'intervenir la nuit (de 22h à 6h).

2.9.3 - Plus-value intervention corrective urgente

Dans le cas où le dysfonctionnement est bloquant pour l'exploitation, typiquement indisponibilité simultanée d'un pare-feu principal et de son secours, la DIR CE a la possibilité de commander une intervention urgente pour l'exécution d'une prestation de maintenance corrective.

Dans ce cas, cela ne modifie en rien les modalités de passation de commande (procédure et plage horaire), en revanche **les délais d'intervention et de remise en service sont diminués de moitié (voir tableau défini au chapitre 2.7.6 - Délais)**. De plus, ces délais courent également en dehors des plages de travail. Ce qui signifie concrètement que

l’intervention pourra déborder la nuit, les week-ends ou les jours fériés.

2.10 - Formations et transferts de compétence

Les formations sont à destination des techniciens de la DIR CE chargés de l'administration et de la maintenance des pare-feux. Les sessions doivent pouvoir être organisées dans les locaux de la DIR CE et seront animées pour une assistance de 8 personnes maximum. Les supports de formation seront transmis 1 semaine avant le début de la formation.

Liste des formations requises :

- Formation « pare-feu filtrant propriétaire » ;
- Formation « pare-feu filtrant libre de droits » ;
- Formation « bastion » ;
- Formation « application de centralisation et d’analyse des logs »
- Formation « accès distant sécurisé ».

3 - Sécurité et confidentialité

Dans le cadre de la maintenance des pare-feu et solutions de sécurité de la DIR Centre-Est, le titulaire s'engage à respecter les exigences strictes de sécurité, de confidentialité et de traçabilité définies ci-dessous. Ces obligations s'appliquent à l'ensemble des intervenants du titulaire, y compris ses sous-traitants, et couvrent l'intégralité des données, configurations, logs, et équipements liés aux pare-feux et solutions de sécurité de la DIR Centre-Est faisant l'objet du marché.

3.1 - Confidentialité des informations

3.1.1 - Obligation de discrétion et de secret

Le titulaire et l'ensemble de ses intervenants sont tenus à une obligation stricte de confidentialité conformément à l'article 5 du CCAG FCS et aux règles internes de la DIR Centre-Est.

Les informations relatives à :

- L'architecture des réseaux de la DIR Centre-Est ;
- Les configurations des pare-feu et solutions de sécurité (règles, politiques, topologies) ;
- Les mécanismes de sécurisation (ex. : clés de chiffrement, certificats, mots de passe) ;
- Les logs et journaux d'activité ;
- Les vulnérabilités ou incidents détectés ; ne pourront être divulguées qu'aux seules personnes habilitées par la DIR Centre-Est, et uniquement dans le cadre strict de la prestation.

Le titulaire ne pourra utiliser les méthodologies, documentations, informations ou savoir-faire de la DIR Centre-Est, considérés comme confidentiel, à d'autres fins que l'exécution du marché.

La divulgation des informations ne devra se faire qu'aux seules personnes ayant le besoin d'en prendre connaissance.

3.1.2 - Engagement formel des intervenants

Le titulaire devra faire signer à tous ses intervenants (y compris les sous-traitants) un formulaire d'engagement de confidentialité et de sécurité, fourni par la DIR Centre-Est lors de la réunion de lancement.

Ces formulaires devront être transmis à la DIR Centre-Est sur demande, sans délai.

3.1.3 - Transmission et duplication des informations

Toute transmission ou duplication d'informations (configurations, logs, schémas réseau,

etc.) en dehors du périmètre de la DIR Centre-Est devra être autorisée par écrit par le responsable de la prestation de la DIR Centre-Est.

En cas de transmission d'informations sensibles (ex. : configurations critiques, clés de chiffrement), le titulaire devra :

- Utiliser des conteneurs sécurisés (outil Zed préconisé) ;
- Limiter l'accès aux seules personnes habilitées et identifiées ;
- Journaliser toute transmission (qui, quand, quoi, moyen utilisé).

3.1.4 - Intégrité et qualité des informations

Le titulaire se porte garant de :

- L'intégrité des configurations, logs et données traitées dans le cadre de la prestation ;
- L'absence de modification, destruction ou altération accidentelle des données ou des équipements ;
- La validation systématique des changements (ex. : mises à jour de règles de pare-feu) avant leur application en production.

3.2 - Disponibilité des données et des systèmes

Le titulaire devra :

- Maintenir la disponibilité des pare-feu et solutions de sécurité de la DIR Centre-Est conformément aux SLA définis dans le marché ;
- Assurer la conservation des configurations, logs et sauvegardes pendant toute la durée du contrat ;
- Restaurer les données en cas d'incident, dans les délais impartis.

3.3 - Exigences liées à la télémaintenance

Le titulaire ne pourra utiliser que la solution de télémaintenance mise à disposition par la DIR Centre-Est.

Aucun autre moyen de connexion (ex. : TeamViewer, AnyDesk, SSH direct) n'est autorisé sans accord écrit préalable de la DIR Centre-Est.

Toute session de télémaintenance devra :

- Être journalisée (logs de connexion, actions réalisées) ;
- Être supervisée par un représentant de la DIR Centre-Est (si demandé) ;
- Être interrompue immédiatement en cas de suspicion d'intrusion ou de comportement anormal.

3.4 - Destruction des données

3.4.1 - Fin de contrat ou rupture anticipée

À la fin du contrat ou en cas de rupture anticipée, le titulaire devra :

- Restituer à la DIR Centre-Est une copie intégrale et vérifiable de toutes les données confiées (configurations, logs, documentations, sauvegardes) ;
- Détruire toute copie résiduelle des données de la DIR Centre-Est dans ses systèmes d'information, dans un délai maximal de 30 jours après la restitution.

La restitution et la destruction devront être constatées par un procès-verbal (modèle fourni par la DIR Centre-Est), daté et signé par les deux parties.

3.4.2 - Mise au rebut de matériel

Pour tout matériel ou logiciel retiré du service (ex. : pare-feu obsolète, disque dur défectueux) :

Le titulaire devra effacer de manière sécurisée les données (ex. : méthode ANSSI N°3 : écrasement multiple ou destruction physique) ;

En cas d'impossibilité d'effacement sécurisé (ex. : panne matérielle), le support devra être :

- Détruit physiquement (broyage, incinération) sous la supervision de la DIR Centre-Est ;
- Ou stocké dans un local sécurisé en attente de destruction, sans possibilité de réutilisation.

Un procès-verbal de destruction devra être signé par les deux parties.

3.5 - Respect des lois et réglementations

3.5.1 - Loi Informatique et Libertés (LIL) et RGPD

Le titulaire s'engage à :

- Traiter les données personnelles (ex. : logs contenant des IP ou identifiants utilisateurs) conformément à la loi n°78-17 du 6 janvier 1978 et au RGPD ;
- Protéger les données contre toute fuite, altération ou accès non autorisé ;
    - Signaler sans délai (sous 72h maximum) au maître d'ouvrage toute violation de données (ex. : fuite de logs, accès non autorisé) ;
    - Respecter les délais légaux de conservation des données (ex. : logs conservés 12 mois maximum, sauf obligation légale contraire) ;
    - Ne pas utiliser les données à d'autres fins que celles prévues par le marché.

Remarque : La déclaration CNIL reste à la charge du maître d'ouvrage, mais le titulaire devra collaborer pour fournir les informations nécessaires.

3.5.2 - Obligations spécifiques RGPD

Le titulaire devra :

1. Traiter les données uniquement pour les finalités liées à la maintenance des pare-feu et solutions de sécurité ;
2. Garantir la confidentialité des données à caractère personnel (ex. : logs, configurations utilisateurs) ;
3. Veiller à ce que ses intervenants :
   - Soient soumis à une obligation de confidentialité (contrat ou loi) ;
   - Reçoivent une formation RGPD adaptée ;
4. Appliquer les principes :
   - Privacy by Design (sécurité dès la conception) ;
   - Privacy by Default (paramètres par défaut sécurisés) ;
5. Garantir que ses sous-traitants respectent les mêmes exigences RGPD. En cas de manquement d'un sous-traitant, le titulaire reste pleinement responsable devant X ;
6. Communiquer au maître d'ouvrage les coordonnées de son Délégué à la Protection des Données (DPO), s'il en a désigné un.

3.6 - Respect des référentiels de sécurité

3.6.1 - Référentiels interministériels (publiés par l'ANSSI)

Le titulaire s'engage à :

- Respecter les référentiels ANSSI applicables, notamment :
  - Guide de durcissement des pare-feu ;
  - Bonnes pratiques de gestion des logs ;
  - Recommandations pour la télémaintenance sécurisée ;
- Mettre à jour ses pratiques en cas de publication de nouveaux référentiels par l'ANSSI.

3.6.2 - La directive NIS2

Le titulaire devra respecter les exigences de la directive notamment les exigences de résilience et de sécurité de la chaîne d'approvisionnement.

3.7 - Mesures techniques et organisationnelles

3.7.1 - Protection des biens

Le titulaire s'engage à conserver et traiter les données de la DIR Centre-Est de manière séparée de ses propres données ou de données de ses autres clients. Il devra :

- décrire les mécanisme mise en œuvre pour cloisonner les environnements de la DIR Centre-Est des autres systèmes d'informations utilisés par le titulaire.
- décrire les mécanisme mise en œuvre pour séparer les données de la DIR Centre-Est des données de ses autres clients.
- Limiter l'accès sur le principe de restriction au besoin d'en connaître

3.7.2 - Protection des systèmes de la DIRCE

Le titulaire devra :

- Mettre en œuvre des mesures techniques et organisationnelles pour protéger les pare-feu et solutions de sécurité de la DIR Centre-Est ;
- Appliquer le principe du moindre privilège :
  - Les comptes d'administration devront avoir uniquement les droits strictement nécessaires ;
  - Les accès temporaires (ex. : pour une intervention) devront être révoqués immédiatement après usage ;

3.7.3 - Gestion des accès et des habilitations

Le titulaire devra :

- Limiter les accès aux pare-feu et solutions de sécurité aux seules personnes habilitées ;
- Utiliser des mécanismes d'authentification forte (ex. : MFA, certificats, clés SSH) ;
- Journaliser toutes les connexions (qui, quand, action réalisée) ;
- Révoquer immédiatement les accès en cas de départ d'un intervenant ou de suspicion de compromission.

3.7.4 - Gestion des mots de passe

Les mots de passe utilisés par le titulaire devront respecter la politique de mots de passe de la DIR Centre-Est. (longueur, complexité, renouvellement, ...)

Remarque : Le titulaire devra fournir à la DIR Centre-Est une copie de sa politique de gestion des mots de passe pour validation.

3.7.5 - Sauvegarde

Le titulaire doit mettre en place un système de sauvegarde des données liées aux prestations du marché. Des tests périodique de restauration doivent être formalisées.

Les données doivent être conservées pendant toute la durée du marché + 6 mois.

3.7.6 - Mises à jour et correctifs

Le titulaire s'engage à gérer les mises à jour et appliquer les correctifs de sécurité pour assurer le maintien en condition de sécurité des équipements et applications couverts par le marché. Pour cela, il devra :

- Appliquer les correctifs de sécurité (firmware, logiciels) dans un délai maximal de 15 jours après leur publication par l'éditeur ;
- Tester les mises à jour en environnement de pré-production avant déploiement en production ;
- Documenter les mises à jour (version, date, tests réalisés).

3.7.7 - Correspondant sécurité

Le titulaire doit désigner parmi son personnel un correspondant « sécurité » pour toute la durée de la prestation. Ce correspondant est notamment l'interlocuteur privilégié de la DIR Centre-Est pour toutes les questions relatives à la sécurité de la prestation, notamment dans le cadre d'investigations initiées par le ministère ou le prestataire suite à des incidents de sécurité opérationnels.

Ce correspondant doit être joignable aux horaires convenus dans le cadre contractuel. Tout remplacement de ce correspondant doit être notifié à la DIR Centre-Est préalablement à son entrée en vigueur. De plus, une suppléance de ce correspondant de sécurité doit être assurée pour pallier son indisponibilité.

3.7.8 - Gestion de crise sécurité

Sur son domaine de responsabilité SI, le prestataire doit disposer d'un processus formalisé et opérationnel de gestion de crise, apte à assurer le traitement d'événements remettant en cause de façon inacceptable pour la DIR Cente-Est le respect des engagements de service et de sécurité SI contractualisés.
Ce plan doit préciser au minimum :
Les principes d'escalade (critères de déclenchement, synoptique d'escalade) ;

- La composition de la cellule de crise : fonctions et responsabilités des membres (DIR Cente-Est et prestataire). La liste nominative des membres et de leurs suppléants est référencée dans un annuaire ;
- Les moyens dédiés à la gestion de crise (procédures opérationnelles, moyens de communication, salle(s) de crise).

3.8 - Processus de gestion des incidents

3.8.1 - Mise à disposition des politiques et procédures de sécurité du titulaire

Le titulaire s'engage à mettre à disposition de la DIR Centre-Est l'ensemble des documents (politiques, procédures, etc.) assurant l'exécution de la prestation dans le respect des exigences de la DIR Centre-Est.

3.8.2 - Signalement des incidents

Le titulaire doit alerter la DIR Centre-Est sans délai dès lors qu'il a détecté un incident par tout moyen à sa disposition, sur le périmètre lié aux prestations du marché :

- Toute défaillance de sécurité (ex. : intrusion, panne de pare-feu) ;
- Toute violation des règles de sécurité (ex. : accès non autorisé, configuration non conforme) ;
- Toute anomalie suspecte (ex. : trafic réseau inhabituel, tentative de brute-force).

Il fournira un rapport préliminaire sous 24 heures, incluant :

- La description de l'incident ;
- Les actions immédiates mises en œuvre ;
- Les impacts potentiels sur les services de la DIR Centre-Est.

3.8.3 - Traitement des incidents

Le titulaire doit contacter les interlocuteurs sécurité de la DIR Centre-Est désignés pour signaler tout incident de sécurité.

En cas d'incident sur le SI de la DIR Centre-Est, le titulaire participera activement à sa résolution, sous la direction de la DIR Centre-Est ;

En cas d'incident sur son propre SI, le titulaire autorisera la DIR Centre-Est à participer à l'enquête (si la DIR Centre-Est en fait la demande).

3.8.4 - Traçabilité

Le prestataire doit assurer la traçabilité des incidents de sécurité et doit disposer d'un processus formalisé et opérationnel de gestion des incidents de sécurité sur le périmètre du SI qui lui a été confié.

3.9 - Vie du contrat

3.9.1 - Continuité des services du prestataire

Le prestataire s'engage à assurer la continuité des services fournis au ministère dans le cadre de la prestation contractée. L'ensemble des services doit être disponible dans les délais maximums définis dans le contrat (définition du plan de continuité d'activité, organisation de crise, solutions de secours mises en œuvre, procédure de secours).

En cas de sinistre chez le prestataire, celui-ci s'engage à signaler l'événement au ministère selon la procédure d'alerte en vigueur (directive de gestion des alertes, incidents et situations de crise).Devoir d'information en cas de changement majeur

Le prestataire est tenu d'informer le ministère en cas de changement majeur de son actionnariat, d'une fusion ou d'une acquisition. Le cas échéant, l'apparition de conflits d'intérêts peut être une cause de rupture de contrat et de déclenchement des clauses de réversibilité.

3.9.2 - Maintien de la liste des intervenants

Le prestataire s'engage à fournir la liste des intervenants dès le lancement de la prestation

et à maintenir cette liste en fonction des départs et arrivées de nouveaux intervenants.

3.9.3 - Identification des suppléants

Le prestataire doit identifier un suppléant pour chaque personnel expert et/ou décideur afin d'assurer une polyvalence et de permettre la continuité de service.

3.9.4 - Sensibilisation du personnel

Le prestataire s'engage à assurer pour chaque intervenant une sensibilisation à la sécurité de l'information et aux règles de la DIR Centre-Est.

Le prestataire veille notamment à ce que son personnel intervenant dans le cadre de la Prestation respecte les dispositions concernant la sécurité telles que décrites dans les documents contractuels (CCAG, CCAP, CCTP).

3.9.5 - Sous-traitance d'une partie du contrat

En accord avec le CCAG FCS, le prestataire peut faire appel à une sous-traitance pour une partie de la prestation. Le prestataire devra préalablement déclarer à la DIR Centre-Est toute sous-traitance éventuelle.
Il est en charge d'obtenir les mêmes exigences de sécurité de la part de ses éventuels sous-traitants. Le prestataire devra décrire les procédures et règles de sécurité qu'il met en place lorsqu'il remet des informations sensibles à ses partenaires autorisés ou à la DIR Centre-Est. Lors de l'exécution du marché, la DIR Centre-Est pourra refuser la sous-traitance de parties essentielles du marché à des entreprises dont il n'a pas pu vérifier les capacités techniques et économiques, ainsi que les capacités en matière de sécurité, lors de la sélection du prestataire. L'ensemble des clauses et engagements de couverture de risques reste à la charge du prestataire, qui devra se réassurer auprès de son prestataire sous-traitant.
Dans le cas où aucune sous-traitance n'est prévue à date de signature du contrat, le prestataire doit malgré tout s'engager à respecter cette exigence dans le cas où un contrat de sous-traitance viendrait à être signé plus tard au cours de la Prestation.

3.9.6 - Audit et contrôle

La DIR Centre-Est se réserve le droit d'effectuer (ou de faire effectuer) des audits de sécurité sur le périmètre du marché (moyen, procédures, ..) afin de s'assurer de la prise en compte effective du niveau de sécurité requis. Les audits pourront porter sur:

Le titulaire en sera informé 2 semaines à l'avance (sauf urgence) ;

Les audits pourront inclure :

- Des tests d'intrusion (avec accord préalable) ;
- Des vérifications de conformité (ex. : respect des politiques de mots de passe, cloisonnement des environnements) ;
- Des contrôles documentaires (ex. : logs, rapports d'incidents).

À la fin du contrat, la DIR Centre-Est pourra effectuer un contrôle final pour vérifier la destruction effective des données.

3.9.7 - Devoir de conseil

Le prestataire doit communiquer au ministère toute remarque motivée permettant d'améliorer le niveau de sécurité de la DIR Centre-Est et signaler les difficultés et risques que certains choix peuvent entraîner.

3.9.8 - Conséquences en cas de mise en cause du prestataire dans un incident de sécurité

En cas de mise en cause dans un incident de sécurité au sein de la DIR Centre-Est ou de non-respect des règles de sécurité, le ministère peut mettre un terme au contrat et engager des poursuites judiciaires, selon la gravité des actes constatés.

3.10 - Transfert et réversibilité

3.10.1 - Sécurité de la phase de transfert

Le prestataire devra mettre en œuvre des mesures techniques et organisationnelles pour garantir la sécurité des données et des applications qui lui sont confiées, lors du transfert des prestations de la part du précédent prestataire.

Durant la phase de transfert, l'assurance de la sécurité résidera principalement dans :

- La gestion des accès, habilitations ;
- Le transfert de responsabilités ;
- La fourniture d'informations confidentielles ;
- La gestion de la continuité de l'activité.

NB : le précédent prestataire reste responsable de la sécurité jusqu'à la fin de la prestation. Si nécessaire, un protocole pourra être formalisé cadrant les responsabilités des prestataires entrant et sortant durant la phase de transfert.

3.10.2 - Réversibilité

En cas d'expiration ou de résiliation de tout ou partie des services fournis au ministère dans le cadre de la prestation contractualisée, le prestataire s'engage à éviter toute interruption ou baisse de la qualité des services avant la fin du contrat. Le prestataire s'engage également à assurer l'ensemble des opérations pour que la DIR Centre-Est puisse reprendre les services dans de bonnes conditions (transfert de compétences, documentations, etc.).

Pendant la phase de réversibilité, le titulaire devra transférer à la DIR Centre-Est ou au nouveau titulaire :

- Les configurations des pare-feu et solutions de sécurité ;
- Les documentations techniques (schémas, procédures, logs) ;
- Les contrats de support en cours (si applicable) ;

- Former le nouveau titulaire ou les équipes de la DIR Centre-Est pour assurer la prise en main ;
- Garantir une transition sans impact sur la sécurité des systèmes.

3.11 - Obligations spécifiques aux interventions sur site

Si le titulaire est amené à intervenir au sein des locaux de la DIR Centre-Est, il doit, au même titre que les agents de la DIR Centre-Est respecter un ensemble de règles. Les clauses suivantes devront être respectées :

- Respecter les exigences de sécurité internes de la DIR Centre-Est (ex. : badgeage, accompagnement, interdiction des équipements personnels) ;
- Utiliser uniquement le matériel fourni par la DIR Centre-Est (sauf accord écrit) ;
- Ne pas accéder à des ressources hors périmètre du marché ;
- Restituer tout matériel prêté par la DIR Centre-Est à la fin de la prestation ;
- Signaler immédiatement tout incident de sécurité survenant sur site.

D'une manière générale, il est recommandé l'appropriation des recommandations et bonnes pratiques de l'ANSSI (http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/), plus particulièrement sur les sujets : « Sécurité du poste de travail et des serveurs », « Sécurité de la messagerie », « Sécurité des médias amovibles » et « Sécurité des réseaux ».

Sanctions en cas de manquement

En cas de non-respect des obligations de sécurité ou de confidentialité, la DIR Centre-Est pourra :

- Appliquer des pénalités prévues à l'article 4 du CCAG.
- Suspendre temporairement la prestation ;
- Résilier le contrat pour faute, sans préavis ni indemnité ;
- Engager des poursuites judiciaires pour violation de la confidentialité, négligence ou faute grave.

A.17. Gestion des licences et des sources logicielles

- Le titulaire devra :
  - **Garantir la validité des licences** des logiciels utilisés pour la maintenance (ex. : outils de supervision, solutions de sauvegarde) ;
  - **Fournir les preuves de licence** à **X** sur demande ;
  - **Utiliser des sources d'installation officielles** (ex. : dépôts éditeurs, sites vérifiés) ;
  - **Ne pas utiliser de logiciels non autorisés** ou dont les licences ne couvrent pas l'usage prévu.

4 - Conditions d'exécution

4.1 - Généralités

L'entretien et la maintenance des installations définies à l'article 1 du présent C.C.T.P. devront être exécutées conformément aux conditions techniques, normes et règlements actuellement en vigueur.

Le personnel intervenant au titre du présent marché devra obligatoirement être titulaire d'un titre de certification lorsque l'intervention le nécessite.

4.2 - Prise en charge et remise des équipements en fin de marché

Le titulaire déclare être parfaitement informé de la consistance des matériels ou équipements dont il assure la maintenance.

Un procès verbal contradictoire de l'état des matériels ou équipements sera établi au début et à la fin de l'exécution du présent marché.

Le titulaire s'engage à laisser en fin d'exécution du marché les matériels ou équipements en état normal d'entretien et de fonctionnement.

4.3 - Personnel d'intervention du titulaire

Dans les 10 jours suivant la notification du marché, le titulaire devra, par écrit, désigner nommément les personnes habilitées pour la maintenance des matériels ou équipements qui font l'objet du présent marché (noms, qualifications, domaine d'intervention, habilitations).

Le titulaire aura nommé un responsable et devra donner un numéro de téléphone et un émail fixe pour que le maître d'ouvrage puisse effectuer à tout moment une demande d'intervention.

Le titulaire s'engage à ce que les personnes désignées pour intervenir aient une bonne connaissance des installations.

4.4 - Sécurité et accès aux sites.

Lors de ses interventions le titulaire doit prendre toutes les mesures nécessaires tendant à assurer la sécurité des usagers et du personnel intervenant.

Toutes infractions aux règles de sécurité constatées par le représentant du Maître d'Ouvrage engendrera le départ immédiat des personnels de l'entreprise du lieu d'intervention sans que le titulaire ne puisse prétendre au règlement de l'intervention débutée ou à l'interruption des délais d'intervention.

Sur certains sites et notamment ceux sur lesquels la DIR CE n'est pas propriétaire, cet accord peut prendre la forme d'une procédure d'intervention qui sera définie entre le propriétaire du site et le titulaire. Elle définira les conditions d'accès aux équipements.

Lorsque le maître d'ouvrage dispose d'une clé d'accès ou d'un badge aux locaux

techniques, ceux-ci pourront être retirés contre établissement d'un récépissé signé contradictoirement par les deux parties indiquant la date de prise en compte. Cette clé ou ce badge, non reproductibles sans l'autorisation expresse du Maître d'Ouvrage, devront impérativement lui être rendus.

Dans tous les cas, toute intervention sur un équipement nécessite l'information et l'accord préalable du maître d'ouvrage.

Aucune opération ne sera admise en dehors des horaires impartis par le maître d'ouvrage ou le propriétaire du site.

L'attention du titulaire est attirée sur le fait que des travaux ou opérations peuvent être réalisés par des entreprises extérieures dans la même période ; le titulaire s'organisera en conséquence et ne pourra prétendre à indemnité.

4.5 - Obligation du maître d'ouvrage

Le Maître d'Ouvrage s'engage à faire connaître au titulaire les anomalies qu'il est amené à constater, et ce, dans les meilleurs délais.

Il assure que toutes les interventions de maintenance n'étant pas du ressort du titulaire seront effectuées dans les règles de l'art, de telle façon que cela ne provoque pas de pannes intempestives sur les matériels ou équipements faisant l'objet du présent marché.

Il permet au personnel du titulaire d'avoir accès aux installations, aux schémas, aux paramétrages… et lui communiquera toutes modifications quant à l'installation/suppression des matériels et équipements.

4.6 - Opération de vérification

Le Maître d'Ouvrage se réserve le droit de contrôler, à tout moment, la quantité et la qualité des prestations effectuées en effectuant tous les tests nécessaires.

Pour ce faire, il pourra, le cas échéant faire appel à un organisme extérieur spécialisé .

Direction interdépartementale des routes Centre-Est

Immeuble la Villardière
228, rue Garibaldi
694 46 Lyon cedex 03
DIR Centre-Est@developpement-durable.gouv.fr

Tél : 04 69 16 62 00
Fax : 04 69 16 63 80

Direction interdépartementale des routes Centre-Est

Immeuble la Villardière
228, rue Garibaldi
694 46 Lyon cedex 03
DIR Centre-Est@developpement-durable.gouv.fr

Tél : 04 69 16 62 00
Fax : 04 69 16 63 80