



**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*

**Direction générale
des Finances publiques**

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES

N° DGFIP-DGS-2500013 du 26/06/2025

RELATIF À

LA FOURNITURE ET À LA MAINTENANCE DE SOLUTIONS DE SÉCURITÉ
ET À LA FOURNITURE DE PRESTATIONS ANNEXES

Le présent document comporte 95 feuillets, numérotés de 1 à 95.

SOMMAIRE

1 CONTEXTE DE L'APPEL D'OFFRES.....	5
1.1 Introduction.....	5
1.2 Présentation de la DGFIP.....	5
1.3 Présentation du bureau SI-3 et de la DMOCSS.....	7
2 DESCRIPTION DE L'APPEL D'OFFRES.....	8
2.1 Objet de l'appel d'offres.....	8
2.2 Catégories de prestations.....	8
2.3 Allotissement.....	8
2.4 Durée du marché.....	8
2.5 Présentation générale des lots.....	9
2.5.1 Lot 1 : PAS - Existant.....	9
2.5.2 Lot 2 : PAS - Acquisitions.....	9
2.6 Documents constitutifs du CCTP.....	10
2.6.1 Les documents communs aux lots 1 et 2.....	10
2.6.2 Les documents spécifiques au lot 1.....	10
2.6.3 Les documents spécifiques au lot 2.....	10
3 DISPOSITIONS GÉNÉRALES.....	11
3.1 Assurance qualité.....	11
3.2 Délais d'exécution.....	11
3.3 Périodes.....	11
3.4 Livrables.....	11
3.5 Connexions à distance.....	12
3.6 Continuité des intervenants.....	12
3.7 Moyens des intervenants.....	12
3.8 Conditions d'installation.....	12
3.9 Modalités des livraisons.....	13
3.10 Prix des prestations.....	13
3.11 Licences.....	13
4 LOT 1 : PAS - EXISTANT.....	14
4.1 Objet du lot.....	14
4.2 Présentation des PAS.....	14
4.3 Acquisitions de compléments de parc.....	14
4.3.1 L'acquisition "d'appliance" pour l'administration des consoles série.....	14
4.3.2 L'acquisition d'une solution d'authentification de type Wallix.....	14
4.3.3 L'acquisition "d'appliance" de type Skyhigh Secure Web Gateway.....	16
4.3.4 L'acquisition "d'appliance" de type Fortinet FortiAuthenticator.....	16
4.3.5 L'acquisition "d'appliance" Cisco de type sonde active.....	16
4.4 Acquisitions d'extensions.....	17
4.4.1 L'acquisition d'un module réseau de type carte 4 ports SFP+ pour équipement Skyhigh.....	17
4.4.2 L'acquisition d'un module de type GBIC SFP+ pour équipement Skyhigh.....	17
4.4.3 L'acquisition d'un module réseau de type carte 8 ports cuivre pour équipement CheckPoint.....	18
4.4.4 L'acquisition d'un module réseau de type carte 4 ports SFP+ pour équipement CheckPoint.....	18
4.4.5 L'acquisition d'un module réseau de type carte 8 ports SFP+ pour équipement CheckPoint.....	18
4.4.6 L'acquisition d'un module réseau de type carte 2 ports QSFP28 pour équipement CheckPoint.....	18
4.4.7 L'acquisition d'un module de type GBIC SFP+ / QSFP+ / QSFP28 pour équipement CheckPoint.....	18
4.4.8 L'acquisition de mémoire pour équipement CheckPoint.....	19
4.4.9 L'acquisition de licence de mise à niveau "virtual systems" pour équipement CheckPoint.....	19
4.4.10 L'acquisition de licence d'administration pour équipement CheckPoint.....	19
4.4.11 L'acquisition d'un module réseau de type carte 8 ports SFP+ pour équipement Cisco.....	20
4.4.12 L'acquisition d'un module réseau de type carte 4 ports QSFP+ pour équipement Cisco.....	20

4.4.13 L'acquisition d'un module de type Gbic SFP / SFP+ / QSFP+ pour équipement Cisco.....	20
4.4.14 L'acquisition de licence d'activation du VPN SSL pour les pare-feu Cisco.....	21
4.4.15 L'acquisition de licence d'activation de la fonctionnalité AMP pour les "appliances" Cisco de type sonde active.....	21
4.4.16 L'acquisition de solutions d'administration centralisée pour pare-feu et sondes Cisco.....	21
4.4.17 L'acquisition d'un module de type Gbic SFP / SFP+ pour pare-feu Fortinet.....	22
4.4.18 L'acquisition de jeton pour équipement Fortinet.....	22
4.4.19 L'acquisition de licence d'activation de VDOMs supplémentaires pour pare-feu Fortinet.....	23
4.4.20 L'acquisition d'alimentation électrique pour FortiManager FMG-400G.....	23
4.4.21 L'acquisition de solutions d'administration centralisée pour pare-feu Fortinet.....	23
4.4.22 L'acquisition de solutions de journalisation centralisée pour pare-feu Fortinet.....	23
4.4.23 L'acquisition d'un module de type Gbic SFP / SFP+ pour équipement Radware.....	24
4.4.24 L'acquisition d'extension mémoire pour équipement Radware.....	24
4.4.25 L'acquisition de licence d'activation des fonctionnalités WAF pour équipement Radware.....	24
4.4.26 L'acquisition de licence d'activation des fonctionnalités GSLB pour équipement Radware.....	25
4.4.27 L'acquisition de licence d'augmentation de bande passante pour équipement Radware.....	25
4.4.28 L'acquisition de licence d'activation de vADC supplémentaires pour équipement Radware.....	25
4.4.29 L'acquisition de licence "Cyber Controller" pour équipement Radware.....	25
4.4.30 L'acquisition de licence "Secure Path" pour équipement Radware.....	25
4.4.31 L'acquisition de licence "Bot Manager" pour équipement Radware.....	26
4.4.32 L'acquisition de licence pour module Secure Track+ pour équipement Tufin.....	26
4.4.33 L'acquisition de licence pour module Secure Change+ pour équipement Tufin.....	26
4.4.34 L'acquisition d'un abonnement pour la mise à jour des signatures SNORT.....	26
4.4.35 L'acquisition de licence de complément de parc pour la solution EDR HarfangLab.....	27
4.4.36 L'acquisition d'un abonnement pour la mise à jour de la solution ADACIS ARIMES Standalone.....	27
4.4.37 L'acquisition d'un abonnement pour la mise à jour de la solution ADACIS AGRIOS.....	27
4.4.38 L'acquisition d'un abonnement pour la mise à jour de la solution HACK THE BOX.....	27
4.5 Maintenance de l'existant et des nouvelles extensions.....	29
4.5.1 La maintenance standard (en période HO).....	29
4.5.2 L'extension de maintenance (en période HNO).....	32
4.5.3 Le support de la solution antivirusle DGFIP.....	34
4.6 Prestations d'assistance annexes.....	40
4.6.1 La veille et le conseil.....	40
4.6.2 Le transfert de compétences.....	41
4.6.3 Solution antivirus WithSecure : Prestation de transfert de connaissances.....	42
4.6.4 La désinstallation, le déplacement et la réinstallation de matériel.....	43
4.6.5 L'installation de matériel.....	45
5 LOT 2 : PAS - ACQUISITIONS.....	46
5.1 Objet du lot.....	46
5.2 Acquisitions de matériels, de logiciels.....	46
5.2.1 L'acquisition d'un pare-feu.....	47
5.2.2 L'acquisition d'un pare-feu Web applicatif.....	54
5.2.3 L'acquisition d'un équipement de type accélérateur de flux.....	56
5.2.4 L'acquisition d'un serveur mandataire.....	61
5.2.5 L'acquisition de TAP réseau.....	63
5.2.6 L'acquisition d'un agrégateur de liens réseaux.....	64
5.2.7 L'acquisition d'une solution d'effacement de données.....	66
5.2.8 L'acquisition d'un scanner de vulnérabilité.....	66
5.2.9 L'acquisition d'un serveur mandataire pour des tests de sécurité.....	67
5.2.10 L'acquisition d'un boîtier de cryptographie.....	68
5.2.11 L'acquisition d'une solution de chiffrement.....	70
5.2.12 L'acquisition de token USB PKI.....	71
5.2.13 L'acquisition d'une solution SIEM souveraine avec CTI intégrée.....	72
5.2.14 L'acquisition d'une solution de géolocalisation d'adresses IP avec détermination d'ASN.....	73
5.2.15 L'acquisition d'une solution de détection d'adresses IP utilisant des mécanismes de masquage (proxies, VPN, Tor, etc.).....	74
5.2.16 L'acquisition d'une solution anti-DDOS de niveau 3 à 7 sans déchiffrement SSL.....	75
5.2.17 L'acquisition d'une solution SaaS anti-DDOS souveraine de niveau 3 à 7.....	78
5.2.18 L'acquisition d'une solution de Bot Manager.....	79
5.2.19 L'acquisition d'une solution d'annuaire inversée.....	80
5.2.20 L'acquisition d'une solution de reconnaissance faciale et d'image.....	81
5.3 Maintenance des acquisitions.....	83

5.3.1 La maintenance standard (en période HO).....	83
5.3.2 L'extension de maintenance (en période HNO).....	86
5.4 Prestations d'assistance annexes.....	88
5.4.1 La veille et le conseil.....	88
5.4.2 Le transfert de compétences.....	89
5.4.3 La désinstallation, le déplacement et la réinstallation de matériel.....	91
5.4.4 L'installation de matériel.....	93

1 CONTEXTE DE L'APPEL D'OFFRES

1.1 INTRODUCTION

Le présent appel d'offres a pour objet la fourniture et la maintenance de solutions de sécurité et la fourniture de prestations annexes à la Division Réseau - Poste de travail - Sécurité (DMOCSS) du Bureau des infrastructures et de la sécurité (SI-3) du service des systèmes d'information de la Direction Générale des Finances Publiques (DGFIP).

1.2 PRÉSENTATION DE LA DGFIP

La Direction Générale des Finances Publiques est une des directions du Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique.

Créée par décret du 3 avril 2008, la Direction générale des finances publiques (DGFIP) est le résultat de la fusion des anciennes Direction générale des Impôts et Direction générale de la Comptabilité publique.

La Direction générale des finances publiques a repris l'intégralité des attributions des directions auxquelles elle s'est substituée, et exerce ainsi une grande variété de missions relevant de la fiscalité et de la gestion publique.

En matière fiscale, la DGFIP :

- conçoit et élabore les textes législatifs et réglementaires relatifs à la fiscalité ainsi que les instructions générales interprétatives nécessaires à leur application ;
- conçoit et élabore les textes législatifs et réglementaires relatifs au recouvrement des recettes publiques, au cadastre et à la publicité foncière, veille à leur mise en œuvre et exerce les missions d'administration correspondantes ;
- veille à l'établissement de l'assiette, à la mise en œuvre du contrôle des impôts, droits, cotisations et taxes de toute nature ainsi qu'à leur recouvrement et à celui des autres recettes publiques ;
- représente le ministère dans les négociations internationales en matière fiscale ;
- instruit les demandes d'agréments fiscaux.

Dans le domaine de la gestion publique, la DGFIP :

- contrôle la production et la qualité des comptes de l'État et concourt à leur valorisation ;
- élabore les règles et les procédures relatives au contrôle et au paiement des dépenses publiques, à la gestion financière et comptable des établissements publics nationaux ainsi que des établissements publics locaux d'enseignement et veille à leur mise en œuvre ;
- élabore les règles et les procédures relatives à la gestion financière et comptable des collectivités territoriales et de leurs établissements et veille à leur mise en œuvre. Elle concourt à la valorisation des comptes de ces collectivités et établissements, elle anime l'expertise économique et financière des projets d'investissements publics et l'action économique de ses services déconcentrés ;
- élabore les règles et les procédures en matière d'acquisition, de gestion et de cession des biens domaniaux, d'établissement de l'assiette et de contrôle des redevances domaniales ainsi que de recouvrement des produits domaniaux de toute nature, et veille à leur mise en œuvre ;
- élabore, en liaison avec la Direction Générale du trésor et de la politique économique, les règles et les procédures relatives à la gestion de la dette publique, à l'exécution des opérations de trésorerie de l'État, ainsi qu'à la réalisation d'opérations de collecte de l'épargne au profit de l'État et des correspondants du trésor, et veille à leur mise en œuvre.

De manière transversale, la DGFIP pilote, anime et évalue ses services déconcentrés, définit la politique des ressources humaines pour ses services, alloue leurs moyens et assure la gestion de ses personnels.

Elle conçoit et met en œuvre les méthodes et instruments d'analyse, d'audit et de contrôle de gestion de leur activité permettant d'accroître leur performance ; elle élabore et veille à la mise en œuvre des règles et procédures relatives à la vérification de l'utilisation des fonds publics.

La DGFIP a, auprès des préfets et des acteurs économiques locaux, un rôle de soutien aux entreprises.

Elle intervient dans les dispositifs d'attribution d'aides aux entreprises en création et en développement.

Elle est également un acteur essentiel pour l'octroi de plans de règlement des dettes fiscales et sociales dans le cadre des Commissions des chefs de services financiers (CCSF) ainsi que dans les dispositifs de préventions et de soutien des entreprises en difficulté au sein des Comités départementaux d'examen des problèmes de financement des entreprises (CODEFI).

La DGFIP représente environ 95 000 agents.

L'organigramme complet, les textes et les activités de la Direction Générale des Finances Publiques sont disponibles à l'adresse URL suivante :

<https://www.economie.gouv.fr/dgfip/>

1.3 PRÉSENTATION DU BUREAU SI-3 ET DE LA DMOCSS

Le bureau SI-3 appartient au Service des Systèmes d'Information - Sous Direction de la Production. Au sein de ce bureau, la Division Réseau - Poste de travail - Sécurité (DMOCSS) exerce les activités de sécurité opérationnelle de la DGFIP, de pilotage des entités territoriales ayant un rôle en matière de sécurité.

2 DESCRIPTION DE L'APPEL D'OFFRES

2.1 OBJET DE L'APPEL D'OFFRES

Le présent appel d'offres a pour objet la fourniture et la maintenance de solutions de sécurité et la fourniture de prestations annexes. Il concerne l'acquisition de matériels et de logiciels, la maintenance et support du parc existant ainsi que des acquisitions et des prestations transverses relatives aux fournitures objet du marché.

2.2 CATÉGORIES DE PRESTATIONS

Les prestations demandées sur la durée du marché sont à bons de commande pour un délai d'exécution donné.

Le tableau ci-dessous résume les grandes catégories de prestations demandées.

Code	Prestation
ACQ	Acquisitions
MAINT/STD	Maintenance standard
MAINT/EXT	Extension de la maintenance
VEIL	Veille et conseil
TRANS	Transfert de compétences
DEPL	Désinstallation, déplacement, réinstallation de matériel
INST	Installation de matériel

2.3 ALLOTISSEMENT

L'appel d'offres est constitué de deux lots :

- **LOT 1 PAS - EXISTANT** : acquisitions de compléments de parc (matériels et logiciels) et d'extensions pour des Passerelles d'Accès Sécurisés (PAS) existantes, maintenance des matériels existant au jour de la notification du marché et des extensions acquises dans le présent marché (Lot 1), support des logiciels associés à ces matériels, support de la solution antivirus des postes de travail, veille et conseil, transfert de compétences, désinstallation / déplacement / réinstallation de matériel, installation de matériel ;
- **LOT 2 PAS - ACQUISITIONS** : acquisitions de matériels et de logiciels, maintenance de ces acquisitions (Lot 2), veille et conseil, transfert de compétences, désinstallation / déplacement / réinstallation de matériel, installation de matériel.

2.4 DURÉE DU MARCHÉ

La durée des marchés relatifs à chacun des lots est de 48 mois. Ils sont conclus pour une période de 24 mois fermes à compter de leur date de notification. Ils pourront ensuite être reconduits tacitement jusqu'à deux fois par période de 12 mois, pour une durée maximale totale de 48 mois.

2.5 PRÉSENTATION GÉNÉRALE DES LOTS

2.5.1 Lot 1 : PAS - Existant

Ce lot comprend les fournitures et prestations ci-dessous :

Type	Code	Prestation
Fourniture	LOT1/ACQ	Acquisitions
Maintenance	LOT1/UO/MAINT/STD/AVECG ¹	Maintenance standard (en période de garantie)
	LOT1/UO/MAINT/STD/HORSG ²	Maintenance standard (hors période de garantie)
	LOT1/UO/MAINT/EXT/AVECG	Extension de maintenance (en période de garantie)
	LOT1/UO/MAINT/EXT/HORSG	Extension de maintenance (hors période de garantie)
Prestations annexes	LOT1/UO/VEIL	Veille et conseil
	LOT1/UO/TRANS	Transfert de compétences
	LOT1/UO/DEPL	Désinstallation, déplacement, réinstallation de matériel
	LOT1/UO/CONF	Installation de matériel

La description des prestations du lot 1 est donnée au chapitre 4.

2.5.2 Lot 2 : PAS - Acquisitions

Ce lot comprend les fournitures et prestations ci-dessous :

Type	Code	Prestation
Fourniture	LOT2/ACQ	Acquisitions
Maintenance	LOT2/UO/MAINT/STD/AVECG	Maintenance standard (en période de garantie)
	LOT2/UO/MAINT/STD/HORSG	Maintenance standard (hors période de garantie)
	LOT2/UO/MAINT/EXT/AVECG	Extension de maintenance (en période de garantie)
	LOT2/UO/MAINT/EXT/HORSG	Extension de maintenance (hors période de garantie)
Prestations annexes	LOT2/UO/VEIL	Veille et conseil
	LOT2/UO/TRANS	Transfert de compétences
	LOT2/UO/DEPL	Désinstallation, déplacement, réinstallation de matériel
	LOT2/UO/CONF	Installation de matériel

La description des prestations du lot 2 est donnée au chapitre 5.

¹Les UO avec garantie (AVECG) correspondent à une demande de maintenance pour une période où la garantie du constructeur ou de l'éditeur continue de courir sur le produit concerné.

²Les UO hors garantie (HORSG) correspondent à une demande de maintenance pour une période où la garantie du constructeur ou de l'éditeur a expiré sur le produit concerné.

Ces dernières pourraient aussi concerner une période "end of support" voire "end of sale".

Si des équipements venaient à ne plus bénéficier de support "hardware" de la part du constructeur, le soumissionnaire veillera à assurer lui-même ce support en réparant ou remplaçant les équipements concernés par du matériel équivalent ("broker").

Si des équipements venaient à ne plus bénéficier de support "software" de la part du constructeur, le soumissionnaire veillera à assurer lui-même ce support (configuration, solution de mitigation, base de connaissance). Il ne sera cependant pas tenu de corriger le code en cas de faille de sécurité.

2.6 DOCUMENTS CONSTITUTIFS DU CCTP

Le CCTP est composé du présent document et des documents répertoriés dans les tableaux ci-après.

2.6.1 Les documents communs aux lots 1 et 2

La présentation des PAS fait l'objet d'un document annexe intitulé :

- " DGFIP-DGS-2500013_pas5_cctp_annexe_presentation_des_PAS.odt "

La version des Antivirus utilisée par la DGFIP fait l'objet d'un document annexe intitulé :

- " DGFIP-DGS-2500013_pas5_cctp_annexe_version_Antivirus.odt "

Ces fichiers confidentiels seront joints dans une archive séparée dont le mot de passe devra être demandé par les candidats sur la PLACE.

2.6.2 Les documents spécifiques au lot 1

Le périmètre relatif aux matériels et logiciels à maintenir se trouve dans les fichiers du dossier de consultation :

- DGFIP-DGS-2500013_pas5_lot1_annexe_financiere_maintenance_parc_materiels.ods
- DGFIP-DGS-2500013_pas5_lot1_annexe_financiere_maintenance_parc_logiciels.ods

Les fichiers à compléter par les candidats permettant la comparaison des offres :

- DGFIP-DGS-2500013_pas5_cctp_lot1_annexe_caracteristiques.ods
- DGFIP-DGS-2500013_pas5_lot1_annexe_financiere.ods
- DGFIP-DGS-2500013_pas5_lot1_scenario_confidentiel_parc_existant.ods
- DGFIP-DGS-2500013_pas5_lot1_scenario_global.ods

Ces fichiers confidentiels seront joints dans une archive séparée dont le mot de passe devra être demandé par les candidats sur la PLACE.

2.6.3 Les documents spécifiques au lot 2

Les fichiers à compléter par les candidats permettant la comparaison des offres :

- DGFIP-DGS-2500013_pas5_cctp_lot2_annexe_caracteristiques.ods
- DGFIP-DGS-2500013_pas5_lot2_annexe_financiere.ods
- DGFIP-DGS-2500013_pas5_lot2_scenarios.ods

Ces fichiers confidentiels seront joints dans une archive séparée dont le mot de passe devra être demandé par les candidats sur la PLACE.

3 DISPOSITIONS GÉNÉRALES

3.1 ASSURANCE QUALITÉ

Le Plan d'Assurance Qualité (PAQ) et le Référentiel d'Assurance Qualité (RAQ) sont applicables aux prestations des différents lots.

Le Référentiel d'Assurance Qualité regroupe l'ensemble documentaire qui couvre le cycle de vie d'un projet et la démarche projet. Il a pour but de faciliter l'appropriation de la démarche qualité de la DGFIP. Le RAQ est organisé autour de quatre grands thèmes :

- le RAQ Gestion de projet ;
- le RAQ Modélisation ;
- le RAQ Bascule ;
- le RAQ Sécurité.

Les documents constitutifs du RAQ seront rédigés par le titulaire en partenariat avec la DGFIP au début du marché.

3.2 DÉLAIS D'EXÉCUTION

Les délais suivent les règles ci-dessous :

- les jours sont des jours ouvrés ;
- la semaine correspond à 7 jours calendaires, soit 7 jours consécutifs ;
- les mois sont décomptés de quantième à quantième.

3.3 PÉRIODES

Deux périodes sont définies :

- la période qualifiée de « normale » (**HO**), les jours ouvrés, de 8h à 19h ;
- la période **HNO** : 19h-8h les jours ouvrés et 24h/24 les jours non ouvrés (week-end et jours fériés).

3.4 LIVRABLES

Tous les livrables doivent être fournis sous format papier et dématérialisé, exclusivement en français. Dans le cas de la fourniture sous format dématérialisé, le format retenu devra, être compatible OpenDocument³⁴, permettre à l'administration d'exploiter et de retravailler facilement le document. Le titulaire a la responsabilité de mettre à disposition les livrables attendus par l'administration sur le site concerné de l'administration.

³<https://fr.wikipedia.org/wiki/OpenDocument>

⁴conformément au RGI (Référentiel Général d'Interopérabilité) :

http://references.modernisation.gouv.fr/sites/default/files/Referentiel_General_Interoperabilite_V2.pdf

Pour certaines prestations, des jalons intermédiaires ont été identifiés. Ces jalons devront faire l'objet d'une présentation à l'administration de l'avancement précis des livrables et activités en cours.

Pour les livrables documentaires (et en fonction des livrables, de leur contenu et volume), le titulaire devra, en accord avec l'administration, proposer une planification détaillée et étalée dans le temps pour la remise de ces dits livrables (par exemple : remise de versions intermédiaires, description détaillée du contenu, table des matières du livrable). Des points de visibilité intermédiaires de ces livrables devront être également proposés par le titulaire (plan de production).

Le titulaire fournira à la livraison du matériel au plus tard et sans supplément de prix, une documentation technique complète en langue française sous forme papier et fichier électronique mentionnant la composition, les caractéristiques du matériel et la synthèse des fonctionnalités ainsi que leurs procédures courantes d'utilisation et de maintenance. La mise à jour de la documentation sera fournie à la personne publique à chaque évolution.

3.5 CONNEXIONS À DISTANCE

Il n'est pas autorisé de connexions à distance entre les plates-formes du titulaire et celle de l'administration (par exemple, pas de télémaintenance, pas d'accès à distance sur des ressources physiques).

3.6 CONTINUITÉ DES INTERVENANTS

Le titulaire privilégiera la continuité des prestations commandées par la pérennité de ses intervenants, sur la durée du marché.

3.7 MOYENS DES INTERVENANTS

Les personnels devront être équipés par le titulaire d'un ordinateur (de préférence un portable à jours des correctifs de sécurité) et des logiciels associés aux prestations qu'ils réaliseront (LibreOffice, un antivirus mis à jour régulièrement). Cet ordinateur devra être protégé par des moyens d'authentification forts et complètement chiffrés ainsi que par une suite de sécurité intégrant notamment des fonctions de protection contre les virus et les intrusions.

Cet équipement ne devra pas être raccordé au SI⁵ de la DGFIP.

Lorsque cela sera nécessaire, la DGFIP fournira au titulaire les moyens de se connecter au SI de la DGFIP.

3.8 CONDITIONS D'INSTALLATION

Le candidat devra fournir les spécifications du matériel concernant les aspects suivants :

- dimensions de l'équipement : volume nécessaire à l'installation, au nombre de U requis dans une armoire ;

⁵Système d'Information

- l'alimentation électrique, la mise à la terre des matériels sachant que les équipements fonctionnent 24 heures sur 24 ;
- les contraintes de climatisation (consommation électrique (W) et dissipation thermique (BTU)) sachant que les matériels seront installés dans des salles disposant de la climatisation ;
- les contraintes de rayonnement électromagnétique.

3.9 MODALITÉS DES LIVRAISONS

Sauf autorisation expresse de la DGFIP, délivrée au cas par cas, les livraisons partielles ne sont pas acceptées. Le stockage temporaire des matériels devra s'effectuer sur le site du titulaire avant d'être livrés en totalité à la DGFIP.

L'enlèvement des emballages (matériels et logiciels le cas échéant) est à la charge du titulaire lorsque leur déploiement est réalisé par ce dernier.

Les candidats s'engagent sur des délais de livraison qu'ils devront préciser (lesquels ne pourront toutefois être supérieurs à 4 semaines). Le titulaire assurera sous sa responsabilité la livraison des équipements qui feront l'objet d'une validation par la DGFIP engendrant le transfert de propriété. L'expiration du délai constitue le point de départ pour l'application des pénalités prévues au marché.

3.10 PRIX DES PRESTATIONS

Les soumissionnaires fourniront des prix pour chaque prestation. Ces prix seront renseignés dans l'annexe financière.

Le prix des UO présenté par les soumissionnaires devra tenir compte de tous les coûts liés à cette UO (par exemple : hébergement, frais de déplacement, frais de livraison). Aucun frais de mission ne pourra être exigible par le titulaire sur la durée du marché.

Les soumissionnaires indiqueront dans l'annexe financière, pour chaque acquisition, la durée de garantie constructeur ou éditeur incluse dans le prix d'acquisition, et devront tenir compte de cette période de couverture pour déterminer leurs propres tarifs de maintenance⁶.

3.11 LICENCES

Sauf précision contraire, les licences nécessaires pour l'activation des différentes fonctionnalités auront une durée correspondant à celle de la protection des droits d'auteur.

Elles seront donc toujours valides même à l'expiration du présent marché et/ou à la fin de vie de l'équipement qui peut aller au-delà de la fin de support du constructeur.

⁶ Les soumissionnaires compléteront ainsi deux types d'unités d'œuvre : la première incluant la période avec garantie constructeur (/AVECG), la seconde correspondant à la période hors garantie constructeur (/HORSG).

4 LOT 1 : PAS - EXISTANT

4.1 OBJET DU LOT

L'objet du lot 1 consiste en l'acquisition de compléments de parc (matériels et logiciels) et d'extensions pour les Passerelles d'Accès Sécurisés (PAS) existantes, maintenance des matériels et logiciels existant au jour de la notification du marché et des extensions acquises dans le présent marché, le support des logiciels associés à ces matériels, le support de la solution antivirus des postes de travail, des prestations de veille et conseil, transfert de compétences, désinstallation/déplacement/réinstallation de matériel, installation de matériel.

4.2 PRÉSENTATION DES PAS

La présentation des PAS fait l'objet d'un document annexe intitulé "DGFIP-DGS-2500013_pas5_cctp_annexe_presentation_des_PAS.odt".

Ce fichier confidentiel sera joint dans une archive séparée dont le mot de passe devra être demandé par les candidats sur la PLACE.

4.3 ACQUISITIONS DE COMPLÉMENTS DE PARC

Il s'agit de l'acquisition de matériels de sécurité, obligatoirement interopérables avec l'existant afin d'assurer une continuité technologique. Les prix comprendront la livraison.

4.3.1 L'acquisition "d'appliance" pour l'administration des consoles série

Il s'agit d'acquérir des "appliances" supplémentaires de la gamme Vertiv Avocent ACS 8000 ou équivalent afin d'étendre le parc actuel de la DGFIP.

Les équipements posséderont obligatoirement une double alimentation électrique et seront fournis avec tous les modules Gbics nécessaires.

Ils ne devront pas avoir de modem ou de connectique 4G/LTE.

Il est souhaité des équipements permettant le contrôle à distance de 16 ou 48 serveurs.

Référence du matériel	LOT1/ACQ/AVOCENT/ACS8016DAC-404
Référence du matériel	LOT1/ACQ/AVOCENT/ACS8048DAC-404

4.3.2 L'acquisition d'une solution d'authentification de type Wallix

Il s'agit d'acquérir une solution d'authentification et de traçabilité des accès privilégiés aux composants du système d'information de la DGFIP (de type accès exploitant) afin de compléter l'infrastructure existante.

Les fonctionnalités attendues sont les suivantes :

- authentification des exploitants à base du couple utilisateur/mot de passe, de certificats d'une IGC externe, de bi-clés ssh ;
- attribution des droits d'accès aux équipements en fonction de profils d'appartenance ;
- ouverture des sessions vers les équipements avec des comptes génériques pour le compte des exploitants, sans que ces derniers n'aient à connaître les crédenances ;
- possibilité de fixer une politique de mots de passe – renouvellement – complexité pour les utilisateurs ;
- support à minima des protocoles SSH, SFTP, RDP, VNC, X11, TELNET ;
- journalisation des connexions et des tentatives de connexion ;
- enregistrement des sessions ;
- possibilité de paramétrer des alertes sur l'accès à des comptes sensibles ;
- suivi des connexions actives en temps réel ;
- consultation et génération des statistiques et de rapports d'activité.

La solution fournie doit pouvoir fonctionner en relation avec un annuaire de type LDAP, LDAPS ou Active Directory en autonome avec sa propre solution de gestion des utilisateurs et des droits.

4.3.2.1 acquisition "d'appliance"

Le soumissionnaire proposera 6 configurations (sans licence) distinctes et de dimensionnements différents dont les caractéristiques sont détaillées ci-dessous.

Caractéristiques minimales							
CONFIGURATIONS	C0VM	C1VM	C1	C2	C3	C4	Remarques
Matériel "rackable" dans une armoire standard	format VM		Impératif				Préciser le nombre de U
Double alimentation électrique	N/A		obligatoire				Préciser la consommation électrique maximale (W) et le dégagement calorifique (BTU/h)
Nombre de serveurs gérés (adresse IP différente)	50	100	100	500	1 000	3 000	Minimum
Codification d'UO	LOT1/ ACQ/ WALLIX/ C0VM	LOT1/ ACQ/ WALLIX/ C1VM	LOT1/ ACQ/ WALLIX/ C1	LOT1/ ACQ/ WALLIX/ C2	LOT1/ ACQ/ WALLIX/ C3	LOT1/ ACQ/ WALLIX/ C4	

L'offre du candidat devra préciser le MTBF.

4.3.2.2 acquisition de licence supplémentaires

Le soumissionnaire proposera les licences permettant la gestion du nombre de serveurs souhaités pour les équipements ci-dessus (VM et "appliance") ou ceux existants déjà dans le parc DGFIP.

Référence du logiciel	LOT1/ACQ/WALLIX/LIC/50
-----------------------	------------------------

Référence du logiciel	LOT1/ACQ/WALLIX/LIC/100
Référence du logiciel	LOT1/ACQ/WALLIX/LIC/500
Référence du logiciel	LOT1/ACQ/WALLIX/LIC/1000
Référence du logiciel	LOT1/ACQ/WALLIX/LIC/3000

4.3.3 L'acquisition "d'appliance" de type Skyhigh Secure Web Gateway

Il s'agit d'acquérir des "appliances" supplémentaires de la gamme WBG-5500-F afin d'étendre les plateformes actuelles de la DGFIP.

Les équipements posséderont obligatoirement une double alimentation électrique.

Référence du matériel	LOT1/ACQ/SKYHIGH/WBG-5500-F
-----------------------	-----------------------------

L'offre du candidat devra préciser le MTBF.

4.3.4 L'acquisition "d'appliance" de type Fortinet FortiAuthenticator

Il s'agit d'acquérir des "appliances" supplémentaires de la gamme FortiAuthenticator afin d'étendre la plateforme actuelle pour l'authentification à double facteur de la DGFIP.

Les équipements posséderont obligatoirement une double alimentation électrique.

Les soumissionnaires proposeront une solution complète (matériel / logiciels associés / licences) pour la gestion d'un nombre de 2000 / 10000 utilisateurs.

Référence du matériel	LOT1/ACQ/FORTINET/FAC-2000
Référence du matériel	LOT1/ACQ/FORTINET/FAC-10000

L'offre du candidat devra préciser le MTBF.

4.3.5 L'acquisition "d'appliance" Cisco de type sonde active

Il s'agit d'acquérir des "appliances" supplémentaires de la gamme Secure Firewall afin d'étendre le parc de sondes actives de la DGFIP.

Les équipements posséderont obligatoirement une double alimentation électrique.

La sonde sera équipée d'interfaces réseau 1Gbps cuivre RJ45 et/ou 1Gbps/10Gbps/40Gbps fibre optique (connecteurs SC ou ST / LC duplex ou MTP/MPO 12 fibres) et des accessoires nécessaires à son fonctionnement (logiciels, cartes, câbles, fibre, extension).

Les équipements attendus auront à minima le nombre d'interfaces suivantes et seront fournis avec tous les modules Gbics nécessaires :

- Cisco FPR-3120
 - 1 interface CU dédiée au management de l'équipement ;

- 12 interfaces CU 1 Gbps ;
- 10 interfaces SFP+ 10Gbps.
- Cisco FPR-3140
 - 1 interface CU dédiée au management de l'équipement ;
 - 8 interfaces SFP+ 10Gbps ;
 - 2 interfaces QSFP+ 40Gbps.
- Cisco FPR-4225
 - 1 interface CU dédiée au management de l'équipement ;
 - 8 interfaces SFP+ 10Gbps ;
 - 4 interfaces QSFP+ 40Gbps.

Référence du matériel	LOT1/ACQ/CISCO/FPR-3120
Référence du matériel	LOT1/ACQ/CISCO/FPR-3140
Référence du matériel	LOT1/ACQ/CISCO/FPR-4225

L'offre du candidat devra préciser le MTBF.

4.4 ACQUISITIONS D'EXTENSIONS

Il s'agit de l'acquisition de matériels d'extension de sécurité, obligatoirement interopérables avec l'existant. Les prix comprendront la livraison.

Pour tout élément matériel, l'offre du candidat devra préciser le temps moyen entre deux pannes (MTBF).

Les normes exigées pour les grandes fonctionnalités demandées ci-dessous sont synthétisées dans l'annexe " DGFIP-DGS-2500013_pas5_cctp_lot1_annexe_caracteristiques ".

Ce fichier confidentiel sera joint dans une archive séparée dont le mot de passe devra être demandé par les candidats sur la PLACE.

4.4.1 L'acquisition d'un module réseau de type carte 4 ports SFP+ pour équipement Skyhigh

Il s'agit d'acquérir un module de commutation enfichable 4 ports SFP+ pour équipement Skyhigh modèle WBG-5500-F.

Référence du matériel	LOT1/ACQ/SKYHIGH/MAP-10G4SR-FBRF
-----------------------	----------------------------------

4.4.2 L'acquisition d'un module de type GBIC SFP+ pour équipement Skyhigh

Il s'agit d'acquérir les adaptateurs pour la cartes module Skyhigh WBG-5500-F.

- 10G SFP+ - short range.

Référence du matériel	LOT1/ACQ/SKYHIGH/10GBASE-SR-SFP+
-----------------------	----------------------------------

4.4.3 L'acquisition d'un module réseau de type carte 8 ports cuivre pour équipement CheckPoint

Il s'agit d'acquérir un module de commutation enfichable 8 ports 10/100/1000 Ethernet type RJ45 pour équipement CheckPoint modèle 6600 ou 26000.

Référence du matériel	LOT1/ACQ/CKP6600/CPAC-8-1C-C
Référence du matériel	LOT1/ACQ/CKP26000/CPAC-8-1C-C

4.4.4 L'acquisition d'un module réseau de type carte 4 ports SFP+ pour équipement CheckPoint

Il s'agit d'acquérir un module de commutation enfichable 4 ports SFP+ pour équipement CheckPoint modèle 6600 ou 26000.

Référence du matériel	LOT1/ACQ/CKP6600/CPAC-4-10F-C
Référence du matériel	LOT1/ACQ/CKP26000/CPAC-4-10F-C

4.4.5 L'acquisition d'un module réseau de type carte 8 ports SFP+ pour équipement CheckPoint

Il s'agit d'acquérir un module de commutation enfichable 8 ports SFP+ pour équipement CheckPoint modèle 19100.

Référence du matériel	LOT1/ACQ/CKP19100/CPAC-8-1-10F-D
-----------------------	----------------------------------

4.4.6 L'acquisition d'un module réseau de type carte 2 ports QSFP28 pour équipement CheckPoint

Il s'agit d'acquérir un module de commutation enfichable 2 ports QSFP28 pour équipement CheckPoint modèle 19100 ou 26000.

Référence du matériel	LOT1/ACQ/CKP19100/CPAC-2-40-100F-D
Référence du matériel	LOT1/ACQ/CKP26000/CPAC-2-40-100F-C

4.4.7 L'acquisition d'un module de type GBIC SFP+ / QSFP+ / QSFP28 pour équipement CheckPoint

Il s'agit d'acquérir différents types d'adaptateur pour les cartes module CheckPoint 6600, 19100 ou 26000.

- 10G SFP+ - short range (CPAC-TR-10SR) ;

- 40G QSFP+ - 300m (CPAC-TR-40SR-QSFP-300m) ;
- 40G QSFP+ - BiDi (CPAC-TR-40SR-QSFP-BiDi) ;
- 100G QSFP28 - short range (CPAC-TR-100SR) ;
- 100G QSFP28 - BiDi (CPAC-TR-100SR-BiDi).

Référence du matériel	LOT1/ACQ/ADAP/CKP6600/CPAC-TR-10SR-C
Référence du matériel	LOT1/ACQ/ADAP/CKP19100/CPAC-TR-10SR-D
Référence du matériel	LOT1/ACQ/ADAP/CKP19100/CPAC-TR-40SR-QSFP-300m-D
Référence du matériel	LOT1/ACQ/ADAP/CKP19100/CPAC-TR-40SR-QSFP-BiDi-D
Référence du matériel	LOT1/ACQ/ADAP/CKP26000/CPAC-TR-40SR-QSFP-300m
Référence du matériel	LOT1/ACQ/ADAP/CKP26000/CPAC-TR-40SR-QSFP-BiDi
Référence du matériel	LOT1/ACQ/ADAP/CKP19100/CPAC-TR-100SR-D
Référence du matériel	LOT1/ACQ/ADAP/CKP19100/CPAC-TR-100SR-BiDi-D
Référence du matériel	LOT1/ACQ/ADAP/CKP26000/CPAC-TR-100SR
Référence du matériel	LOT1/ACQ/ADAP/CKP26000/CPAC-TR-100SR-BiDi

4.4.8 L'acquisition de mémoire pour équipement CheckPoint

Il s'agit d'acquérir des extensions de mémoire pour augmenter la taille totale de mémoire vive embarquée à son maximum pour équipement CheckPoint modèle 6600 ou 19100.

Référence du matériel	LOT1/ACQ/CKP6600/CPAC-RAM16GB-6600
Référence du matériel	LOT1/ACQ/CKP19100/CPAC-RAM32GB-19000

4.4.9 L'acquisition de licence de mise à niveau "virtual systems" pour équipement CheckPoint

Il s'agit d'acquérir une licence autorisant la mise en œuvre de pare-feu virtuels CheckPoint pour équipement CheckPoint modèle 6600, 19100 ou 26000 (10 pare-feu virtuels).

Référence du logiciel	LOT1/ACQ/CKP/LIC/VS-10
-----------------------	------------------------

4.4.10 L'acquisition de licence d'administration pour équipement CheckPoint

Il s'agit d'acquérir des licences autorisant la gestion centralisée de pare-feu CheckPoint (nombre illimité de passerelles de sécurité) :

- en environnement simple ;
- en environnement multi-domaines (10 domaines) ;

- en environnement multi-domaines (10 domaines) virtualisé.

Les licences auront une durée correspondant à celle de la protection des droits d'auteur et seront pour serveurs "open server".

Référence du logiciel	LOT1/ACQ/CKP/LIC/SM
Référence du logiciel	LOT1/ACQ/CKP/LIC/MDM
Référence du logiciel	LOT1/ACQ/CKP/LIC/VS-MDM

4.4.11 L'acquisition d'un module réseau de type carte 8 ports SFP+ pour équipement Cisco

Il s'agit d'acquérir un module de commutation enfichable 8 ports SFP+ pour équipement Cisco modèle FPR-3100, FPR-4100 et FPR-4200.

Référence du matériel	LOT1/ACQ/FPR3100/FPR3K-XNM-8X10G
Référence du matériel	LOT1/ACQ/FPR3100/FPR3K-XNM-8X25G
Référence du matériel	LOT1/ACQ/FPR4100/FPR4K-NM-8X10G
Référence du matériel	LOT1/ACQ/FPR4200/FPR4K-XNM-8X10G
Référence du matériel	LOT1/ACQ/FPR4200/FPR4K-XNM-8X25G

4.4.12 L'acquisition d'un module réseau de type carte 4 ports QSFP+ pour équipement Cisco

Il s'agit d'acquérir un module de commutation enfichable 4 ports QSFP+ pour équipement Cisco modèle FPR-3100, FPR-4100 et FPR-4200.

Référence du matériel	LOT1/ACQ/FPR3100/FPR3K-XNM-4X40G
Référence du matériel	LOT1/ACQ/FPR4100/FPR4K-NM-4X40G
Référence du matériel	LOT1/ACQ/FPR4200/FPR4K-XNM-4X40G

4.4.13 L'acquisition d'un module de type Gbic SFP / SFP+ / QSFP+ pour équipement Cisco

Il s'agit d'acquérir différents types d'adaptateur pour carte commutateur ou pare-feu Cisco ASA / FPR :

- GE SFP, LC connector SX transceiver (GLC-SX-MMD) ;
- GE SFP, LC connector LX/LH transceiver (GLC-LH-SMD) ;
- 1000 BASE-T SFP (GLC-T).
- 10G SR SFP+ (SFP-10G-SR)
- 25G SR SFP+ (SFP-25G-SR-S)

- 40G SR4 QSFP+ (QSFP-40G-SR4)

Référence du matériel	LOT1/ACQ/ADAP/CISCO/GLC-SX-MMD
Référence du matériel	LOT1/ACQ/ADAP/CISCO/GLC-LH-SMD
Référence du matériel	LOT1/ACQ/ADAP/CISCO/GLC-T
Référence du matériel	LOT1/ACQ/ADAP/CISCO/SFP-10G-SR
Référence du matériel	LOT1/ACQ/ADAP/CISCO/SFP-25G-SR-S
Référence du matériel	LOT1/ACQ/ADAP/CISCO/QSFP-40G-SR4

4.4.14 L'acquisition de licence d'activation du VPN SSL pour les pare-feu Cisco

Il s'agit d'acquérir une licence autorisant l'activation de la fonctionnalité VPN SSL avec contrôle du poste client sur les pare-feu Cisco de la gamme FPR-2100, FPR-3100, FPR-4100 et FPR-4200 :

- "Anyconnect Premium" ;
- "Advanced Endpoint Assessment".

L'acquisition des licences se fera par lot de 999 / 9.999 / 49.999 / 99.999 utilisateurs et aura une validité de 5 ans.

Référence du logiciel	LOT1/ACQ/CISCO/LIC/L-AC-APX-LIC-999
Référence du logiciel	LOT1/ACQ/CISCO/LIC/L-AC-APX-LIC-9999
Référence du logiciel	LOT1/ACQ/CISCO/LIC/L-AC-APX-LIC-49999
Référence du logiciel	LOT1/ACQ/CISCO/LIC/L-AC-APX-LIC-99999

4.4.15 L'acquisition de licence d'activation de la fonctionnalité AMP pour les "appliances" Cisco de type sonde active

Il s'agit d'activer les fonctionnalités AMP sur les sondes actives (Cisco FirePower) des pare-feu Cisco de la gamme FPR-3120, FPR-3140 et FPR-4225 :

Référence du logiciel	LOT1/ACQ/CISCO/LIC/L-FPR3120T-AMP
Référence du logiciel	LOT1/ACQ/CISCO/LIC/L-FPR3140T-AMP
Référence du logiciel	LOT1/ACQ/CISCO/LIC/L-FPR4225T-AMP

4.4.16 L'acquisition de solutions d'administration centralisée pour pare-feu et sondes Cisco

Il s'agit d'acquérir une solution d'administration centralisée pour les pare-feu Cisco de la gamme FPR-3100, FPR-4100 et/ou FPR-4200 de type "Firepower Management Center".

- Firepower Management Center 2700 ou équivalent ;
- Firepower Management Center 4700 ou équivalent.

Les équipements posséderont obligatoirement une double alimentation électrique.

Référence du matériel	LOT1/ACQ/CISCO/OAD/FMC2700
Référence du matériel	LOT1/ACQ/CISCO/OAD/FMC4700

4.4.17 L'acquisition d'un module de type Gbic SFP / SFP+ pour pare-feu Fortinet

Il s'agit d'acquérir différents types d'adaptateur pour pare-feu Fortinet FG-200F, FG-501E, FG-800D, FG-1200D et FG-1800F :

- 1 GE SFP SX Transceiver Module (FN-TRAN-SX) ;
- 1 GE SFP LX Transceiver Module (FN-TRAN-LX) ;
- 1 GE SFP RJ45 Transceiver Module (FN-TRAN-GC) ;
- 10 GE SFP+ Transceiver Module, Short Range (FN-TRAN-SFP+SR)
- 40 GE QSFP+ Transceiver Module, Short Range (FN-TRAN-QSFP+SR)

Référence du matériel	LOT1/ACQ/FORTINET/ADAP/FN-TRAN-SX
Référence du matériel	LOT1/ACQ/FORTINET/ADAP/FN-TRAN-LX
Référence du matériel	LOT1/ACQ/FORTINET/ADAP/FN-TRAN-GC
Référence du matériel	LOT1/ACQ/FORTINET/ADAP/FN-TRAN-SFP+SR
Référence du matériel	LOT1/ACQ/FORTINET/ADAP/FN-TRAN-QSFP+SR

4.4.18 L'acquisition de jeton pour équipement Fortinet

Il s'agit d'acquérir deux types de jeton compatibles avec la gamme FortiAuthenticator :

- FortiToken 210 (FTK-210⁷) ;
- FortiToken 310 (FTK-310).

Les FortiTokens auront une durée de vie de 5 ans minimum et ne feront pas l'objet de prestation de maintenance (consommable).

Leur acquisition se fera par lot de 20 / 100 / 200 / 1000 unités selon les modèles

Référence du matériel	LOT1/ACQ/FORTINET/FTK-210-20
Référence du matériel	LOT1/ACQ/FORTINET/FTK-210-100
Référence du matériel	LOT1/ACQ/FORTINET/FTK-210-200

⁷Pour les FortiToken 210, l'activation se fera en mode hors ligne par la fourniture d'un CD d'activation.

Référence du matériel	LOT1/ACQ/FORTINET/FTK-210-1000
Référence du matériel	LOT1/ACQ/FORTINET/FTK-310-20
Référence du matériel	LOT1/ACQ/FORTINET/FTK-310-100
Référence du matériel	LOT1/ACQ/FORTINET/FTK-310-200
Référence du matériel	LOT1/ACQ/FORTINET/FTK-310-1000

L'offre du candidat devra préciser le MTBF.

4.4.19 L'acquisition de licence d'activation de VDOMs supplémentaires pour pare-feu Fortinet

Il s'agit d'acquérir les licences nécessaires pour l'activation de VDOMs supplémentaires pour les pare-feu Fortinet de la gamme FG-1200D et FG-1800F.

L'ajout de VDOMs se fera par 25, 50, 100 et pour le maximum (250).

Référence du logiciel	LOT1/ACQ/FORTINET/LIC/25_VDOM
Référence du logiciel	LOT1/ACQ/FORTINET/LIC/50_VDOM
Référence du logiciel	LOT1/ACQ/FORTINET/LIC/100_VDOM
Référence du logiciel	LOT1/ACQ/FORTINET/LIC/250_VDOM

4.4.20 L'acquisition d'alimentation électrique pour FortiManager FMG-400G

Il s'agit d'acquérir un bloc d'alimentation supplémentaire pour les boîtiers FortiManager de la gamme FMG-400G.

Référence du matériel	LOT1/ACQ/FORTINET/ALIM/FMG-400G
-----------------------	---------------------------------

4.4.21 L'acquisition de solutions d'administration centralisée pour pare-feu Fortinet

Il s'agit d'acquérir une solution d'administration centralisée pour les pare-feu Fortinet de la gamme FG-200F, FG-501E, FG-1200D et FG-1800F et supportant 100 VDOMs et 1000 VDOMs.

L'offre du candidat devra préciser le MTBF et les équipements auront obligatoirement une double alimentation électrique.

Référence du matériel	LOT1/ACQ/FORTINET/OAD/100VDOM
Référence du matériel	LOT1/ACQ/FORTINET/OAD/1000VDOM

4.4.22 L'acquisition de solutions de journalisation centralisée pour pare-feu Fortinet

Il s'agit d'acquérir une solution de journalisation centralisée pour les pare-feu Fortinet de la gamme FG-200F, FG-501E, FG-1200D et FG-1800F et supportant 200 GB par jour et 600 GB par jour.

L'offre du candidat devra préciser le MTBF et les équipements auront obligatoirement une double alimentation électrique.

Référence du matériel	LOT1/ACQ/FORTINET/LOG/200GB
Référence du matériel	LOT1/ACQ/FORTINET/LOG/600GB

4.4.23 L'acquisition d'un module de type Gbic SFP / SFP+ pour équipement Radware

Il s'agit d'acquérir différents types d'adaptateur pour les équipement Radware Alteon 5208, 5280 et 6024 :

- 1 GE SFP Module 1G Base T ;
- 1 GE SFP Module 1G Base SX ;
- 1 GE SFP Module 1G Base LX
- 10 GE SFP+ Module 10G Base T ;
- 10 GE SFP+ Module 10G Base SR ;
- 10 GE SFP+ Module 10G Base LR.

L'offre du candidat devra préciser le MTBF.

Référence du matériel	LOT1/ACQ/RADWARE/ADAP/1G-BaseT
Référence du matériel	LOT1/ACQ/RADWARE/ADAP/1G-BaseSX
Référence du matériel	LOT1/ACQ/RADWARE/ADAP/1G-BaseLX
Référence du matériel	LOT1/ACQ/RADWARE/ADAP/10G-BaseT
Référence du matériel	LOT1/ACQ/RADWARE/ADAP/10G-BaseSR
Référence du matériel	LOT1/ACQ/RADWARE/ADAP/10G-BaseLR

4.4.24 L'acquisition d'extension mémoire pour équipement Radware

Il s'agit d'acquérir des modules d'extension mémoire pour passer de 32 Go ou à 256 Go selon les modèles pour les équipements Radware Alteon 5208 et 6024.

L'offre du candidat devra préciser le MTBF.

Référence du matériel	LOT1/ACQ/RADWARE/Memoire/32G
Référence du matériel	LOT1/ACQ/RADWARE/Memoire/256G

4.4.25 L'acquisition de licence d'activation des fonctionnalités WAF pour équipement Radware

Il s'agit d'acquérir les licences nécessaires pour l'activation de la fonctionnalité WAF pour les équipements Radware Alteon 5208, 5820 et 6024.

Référence du logiciel	LOT1/ACQ/RADWARE/LIC/WAF
-----------------------	--------------------------

4.4.26 L'acquisition de licence d'activation des fonctionnalités GSLB pour équipement Radware

Il s'agit d'acquérir les licences nécessaires pour l'activation de la fonctionnalité GSLB pour les équipements Radware Alteon 5208, 5820 et 6024.

Référence du logiciel	LOT1/ACQ/RADWARE/LIC/GSLB
-----------------------	---------------------------

4.4.27 L'acquisition de licence d'augmentation de bande passante pour équipement Radware

Il s'agit d'acquérir les licences nécessaires pour l'activation de l'augmentation de bande passante à son maximum selon les modèles pour les équipements Radware Alteon 5208, 5820 et 6024.

Référence du logiciel	LOT1/ACQ/RADWARE/LIC/BP_12G
Référence du logiciel	LOT1/ACQ/RADWARE/LIC/BP_26G
Référence du logiciel	LOT1/ACQ/RADWARE/LIC/BP_40G
Référence du logiciel	LOT1/ACQ/RADWARE/LIC/BP_80G

4.4.28 L'acquisition de licence d'activation de vADC supplémentaires pour équipement Radware

Il s'agit d'acquérir les licences nécessaires pour l'activation de vADC supplémentaires pour les équipements Radware Alteon 5208, 5820 et 6024.

L'ajout de vADC se fera par palier de 5.

Référence du logiciel	LOT1/ACQ/RADWARE/LIC/5_vADC
-----------------------	-----------------------------

4.4.29 L'acquisition de licence "Cyber Controller" pour équipement Radware

Il s'agit d'acquérir les licences nécessaires pour l'utilisation de la solution Radware "Cyber Controller" pour l'ensemble des équipements Radware Alteon de la DGFIP.

Référence du logiciel	LOT1/ACQ/RADWARE/LIC/OAD_CyberC
-----------------------	---------------------------------

4.4.30 L'acquisition de licence "Secure Path" pour équipement Radware

Il s'agit d'acquérir les licences nécessaires pour l'utilisation de la solution Radware "Cyber Controller" pour l'ensemble des équipements Radware Alteon de la DGFIP.

Référence du logiciel	LOT1/ACQ/RADWARE/LIC/Secure_Path
-----------------------	----------------------------------

4.4.31 L'acquisition de licence "Bot Manager" pour équipement Radware

Il s'agit d'acquérir les licences nécessaires pour l'utilisation de la fonctionnalité "Bot Manager" intégrée sur les équipements Radware Alteon de la DGFIP et protéger les applications DGFIP exposées aux menaces sur Internet.

Référence du logiciel	LOT1/ACQ/RADWARE/LIC/Bot_Manager
-----------------------	----------------------------------

4.4.32 L'acquisition de licence pour module Secure Track+ pour équipement Tufin

Il s'agit d'acquérir les licences nécessaires pour l'ajout de pare-feu supplémentaires sous gestion de la solution Secure Track+ :

- cluster de pare-feu physiques ;
- cluster de pare-feu virtuels

Référence du logiciel	LOT1/ACQ/TUFIN/LIC/TF-SECTRK-FW-CLS
Référence du logiciel	LOT1/ACQ/TUFIN/LIC/TF-SECTRK-FWVS-CLS

4.4.33 L'acquisition de licence pour module Secure Change+ pour équipement Tufin

Il s'agit d'acquérir les licences nécessaires pour l'ajout de pare-feu supplémentaires sous gestion de la solution Secure Change+ :

- cluster de pare-feu physiques ;
- cluster de pare-feu virtuels

Référence du logiciel	LOT1/ACQ/TUFIN/LIC/TF-SCWF-FW-CLS
Référence du logiciel	LOT1/ACQ/TUFIN/LIC/TF-SCWF-FWVS-CLS

4.4.34 L'acquisition d'un abonnement pour la mise à jour des signatures SNORT

Il s'agit d'acquérir une licence autorisant le téléchargement des dernières signatures SNORT pour leur installation sur 1 serveur, 5 serveurs ou 10 serveurs.

L'abonnement aura une durée d'un an.

Référence du logiciel	LOT1/ACQ/SNORT/ABMT/1_SERVEUR
-----------------------	-------------------------------

Référence du logiciel	LOT1/ACQ/SNORT/ABMT/5_SERVEURS
Référence du logiciel	LOT1/ACQ/SNORT/ABMT/10_SERVEURS

4.4.35 L'acquisition de licence de complément de parc pour la solution EDR HarfangLab

Il s'agit d'acquérir une licence autorisant l'extension de l'utilisation de la solution EDR d'HarfangLab à l'ensemble des postes de la DGFIP.

L'acquisition des licences se fera par lot de 100 / 1.000 / 10.000 / 50.000 postes.

Référence du logiciel	LOT1/ACQ/EDR/LIC/HarfangLab-100
Référence du logiciel	LOT1/ACQ/EDR/LIC/HarfangLab-1000
Référence du logiciel	LOT1/ACQ/EDR/LIC/HarfangLab-10000
Référence du logiciel	LOT1/ACQ/EDR/LIC/HarfangLab-50000

4.4.36 L'acquisition d'un abonnement pour la mise à jour de la solution ADACIS ARIMES Standalone

Il s'agit d'acquérir une licence autorisant l'utilisation pour plus de cinq utilisateurs de la solution d'analyse de risques labellisée conforme à la méthodologie EBIOS Risk Manager par l'ANSSI.

L'abonnement aura une durée d'un an.

Référence du logiciel	LOT1/ACQ/ADACIS/ABMT/ARIMES_Standalone
-----------------------	--

4.4.37 L'acquisition d'un abonnement pour la mise à jour de la solution ADACIS AGRIOS

Il s'agit d'acquérir une licence autorisant l'utilisation pour plus de cinq utilisateurs de la solution "On Premise" de suivi des risques cyber et de la mise en place des mesures de sécurité nécessaires.

L'abonnement aura une durée d'un an.

Référence du logiciel	LOT1/ACQ/ADACIS/ABMT/AGRIOS
-----------------------	-----------------------------

4.4.38 L'acquisition d'un abonnement pour la mise à jour de la solution HACK THE BOX

Il s'agit d'acquérir une licence autorisant l'utilisation des solutions "HACK THE BOX - Workforce Development Plan 1 (Academy/Dedicated Labs/ Professional Labs)" et "HACK THE BOX - Workforce Development Plan 2 (Academy/Dedicated Labs/ Professional Labs)" pour 1 utilisateurs, 5 utilisateurs ou 10 utilisateurs

L'abonnement aura une durée d'un an.

Référence du logiciel	LOT1/ACQ/HACKTHEBOX/ABMT/WRKF1/1_UTILISATEUR
Référence du logiciel	LOT1/ACQ/HACKTHEBOX/ABMT/WRKF1/5_UTILISATEURS
Référence du logiciel	LOT1/ACQ/HACKTHEBOX/ABMT/WRKF1/10_UTILISATEURS
Référence du logiciel	LOT1/ACQ/HACKTHEBOX/ABMT/WRKF2/1_UTILISATEUR
Référence du logiciel	LOT1/ACQ/HACKTHEBOX/ABMT/WRKF2/5_UTILISATEURS
Référence du logiciel	LOT1/ACQ/HACKTHEBOX/ABMT/WRKF2/10_UTILISATEURS

4.5 MAINTENANCE DE L'EXISTANT ET DES NOUVELLES EXTENSIONS

4.5.1 La maintenance standard (en période HO)

4.5.1.1 La description de la prestation

La fourniture de prestations consiste en la maintenance sur site du parc de matériels et de logiciels de sécurité existant au jour de la notification du marché⁸. Cet inventaire, qui indique la fin de support ou de maintenance en cours pour certains éléments du parc, pourra cependant être modifié de manière peu significative du fait des acquisitions des extensions mentionnées au premier titre de ce lot et des remplacements ou abandons des matériels et logiciels obsolètes.

Le parc intégrera en plus les quelques acquisitions réalisées, sur les marchés actuels, entre la date de publication du présent CCTP et la date effective de fin de ces marchés.

Les extensions feront l'objet d'UO de maintenance répertoriées dans l'annexe financière pour l'année de leur acquisition. Pour les années suivantes elles seront intégrées dans le parc existant pour le même coût.

La maintenance comprendra :

- pour le matériel :
 - l'intervention sur site d'un ou plusieurs techniciens qualifiés en cas de panne avec le remplacement s'il y a lieu des éléments défectueux et la reconfiguration, si nécessaire, de l'équipement concerné ;
- pour les logiciels :
 - la maintenance corrective du système d'exploitation des matériels et des logiciels embarqués (fourniture de patchs correctifs avec possibilité d'avoir une solution de contournement dans un premier temps). La mise en œuvre de cette correction doit prendre en compte des impacts sur les autres éléments de l'architecture dans la quelle l'équipement est intégré. Les autres incidences (sur les fonctionnalités, sur les performances) doivent être documentées. L'intervention du titulaire sur site sera laissée à l'appréciation de l'administration qui jugera le risque ou la difficulté à installer la solution ;
 - la maintenance évolutive avec la fourniture des dernières versions dès leur disponibilité et après l'accord de l'administration. L'administration peut refuser cette livraison et le titulaire s'engage à maintenir au maximum deux versions sur la durée du marché.

La maintenance porte sur un engagement de résultats et débutera dès la notification du marché, sous réserve des bons de commande correspondants.

⁸ Le parc est détaillé dans les fichiers "DGFIP-DGS-2500013_pas5_lot1_annexe_financiere_maintenance_parc_logiciels.ods" et "DGFIP-DGS-2500013_pas5_lot1_annexe_financiere_maintenance_parc_materiels.ods".

Dans le cas où les éditeurs ou les constructeurs des logiciels et matériels concernés décideraient de leur fin de support ou fin de vie, le titulaire restera tenu par une garantie de réparation, de remplacement et de support.

Le périmètre de cette prestation couvre l'ensemble des anomalies, à savoir bloquantes et non bloquantes lesquelles seront qualifiées par l'administration.

Degré de gravité de l'anomalie	Définition
Bloquante	<p>Un équipement ou une des fonctionnalités de la solution est indisponible de façon permanente ou régulière.</p> <p>Ce contexte correspond notamment au blocage de la solution et/ou de l'équipement et/ou d'une fonctionnalité majeure, avec une conséquence de blocage significatif, dont un service inopérant, un nombre d'accès impossible significatif, une sécurisation non assurée, ou encore la non-exploitabilité technique d'une fonctionnalité intégrée à la solution.</p> <p>Une anomalie bloquante pour laquelle le titulaire a proposé une solution de contournement provisoire devient non bloquante.</p>
Non bloquante	<p>Une des fonctions de la solution est en mode dégradé.</p> <p>Il s'agit de la non-conformité empêchant l'utilisation de tout ou partie des fonctionnalités de la solution et/ou de l'équipement et/ou d'une fonctionnalité majeure, tout en permettant l'obtention du résultat par une solution de contournement acceptée par la DGFIP.</p> <p>Cette notion recouvre par exemple la gêne significative pour l'utilisateur ou l'exploitant due à l'anomalie, ou une documentation incomplète ou non exploitable.</p>

Le processus de traitement doit comporter les étapes suivantes :

- l'administration (maximum 15 interlocuteurs différents) appelle le service concerné du titulaire entre 8h et 19h, les jours ouvrés du lundi au vendredi⁹ (par téléphone (numéro vert) de préférence, par mail ou via une interface Web) ;
- le titulaire procède à l'ouverture d'un ticket d'incident (début du délai de proposition d'un plan d'action) ;
- le support rappelle l'administration et soumet une proposition de résolution ;
- l'acceptation par l'administration du plan d'action marque la fin du délai de proposition du plan d'action ;
- le titulaire intervient sur site (l'arrivée sur site marque la fin du délai d'intervention) ;
- la clôture de l'incident intervient après la phase de tests (fin du délai de solution de contournement ou de réparation).

Chaque délai débute à compter de l'ouverture du ticket chez le titulaire mais n'est décompté que sur les périodes effectives d'intervention¹⁰

⁹ Les heures ouvrées (HO) s'envisagent au sens du calendrier de l'administration.

¹⁰ La période d'intervention en jour ouvré est de 8 heures à 19 heures.

Synthèse des délais :

MAINTENANCE STANDARD	DÉLAIS MAXIMUM EN HEURES OUVRÉES			
	Proposition d'un plan d'action	Intervention	Solution de contournement	Réparation
Maintenance matériels (Pièces et main d'œuvre)	30 mn	2 h		4 h
Maintenance logiciels				
Anomalie non bloquante	8 h	3 jours	4 jours	
Anomalie bloquante	4 h	8 h	10 h	

Le titulaire met à la disposition un outil Web extranet de suivi des incidents et de partage d'informations avec la DGFIP disposant d'accès authentifiés et chiffrés et garantissant l'isolement des données propres à la DGFIP.

Le site Web doit être à jour et consulté uniquement par une liste de bénéficiaires (maximum 15 personnes) déterminée au plus tard un mois après la date de notification du marché¹¹.

Les soumissionnaires expliciteront les modalités d'application de la maintenance.

4.5.1.2 La fourniture de l'administration

L'administration fournit :

- la description de l'incident ;
- les éléments techniques permettant la résolution de ce dernier.

4.5.1.3 Les livrables de la prestation

Le livrable est la résolution de l'incident et le rapport d'activité (état des incidents, des dossiers clos et en-cours) sera communiqué après la clôture d'incident (5 jours au plus tard) et, en fin de prestation et/ou mensuellement (selon le nombre d'unités d'œuvre commandées) à l'administration.

4.5.1.4 La définition d'unités d'œuvre

Le tableau ci-après reprend, pour chaque matériel ou logiciel (/N°PDT¹² ou référence de l'extension acquise), l'UO de maintenance (incluant les frais de déplacement, les pièces ainsi que la main d'œuvre) et précise la durée d'exécution. Pour chacune d'entre elle, le soumissionnaire distinguera la période où il existe une garantie constructeur ou éditeur et celle où cette garantie n'existe plus. Les garanties constructeur ou éditeur seront détaillées.

¹¹ La liste pourra être mise à jour par l'administration.

¹² Les numéros de série ne pouvant pas être publiés, un numéro (N°PDT) est attribué à chaque produit (matériel ou logiciel) à maintenir (liste dans les fichiers "DGFIP-DGS-2500013_pas5_lot1_annexe_financiere_maintenance_parc_logiciels.ods" et "DGFIP-DGS-2500013_pas5_lot1_annexe_financiere_maintenance_parc_materiels.ods").

Unités d'œuvre	Sous garantie constructeur	Hors garantie constructeur
Référence	LOT1/MAINT/STD/AVECG/3M /N°PDT	LOT1/MAINT/STD/HORSG/3M /N°PDT
Référence	LOT1/MAINT/STD/AVECG/3M /référence de l'extension	LOT1/MAINT/STD/HORSG/3M /référence de l'extension
Durée d'exécution	3 mois	3 mois

4.5.2 L'extension de maintenance (en période HNO)

4.5.2.1 La description de la prestation

C'est une extension de la maintenance de type standard. Elle possède les mêmes caractéristiques que cette dernière, avec cependant une couverture horaire complémentaire (HNO, soit 19h-8h les jours ouvrés et 24h/24 les jours non ouvrés, soit week-end et jours fériés) et des délais de réactivité plus court.

Concernant la maintenance logicielle, l'intervention du titulaire sur site sera laissée à l'appréciation de l'administration qui jugera le risque ou la difficulté à installer la solution.

Le périmètre de cette prestation couvre l'ensemble des anomalies, à savoir bloquantes et non bloquantes lesquelles seront qualifiées par l'administration.

Les notions d'anomalies bloquante et non-bloquante sont définies au 4.5.1.1 du présent document.

Synthèse des délais :

EXTENSION DE MAINTENANCE	DÉLAIS MAXIMUM 7J/7, 24h/24			
	Proposition d'un plan d'action	Intervention	Solution de contournement	Réparation
Maintenance matériels (Pièces et main d'œuvre)	15 mn	1 h		4 h
Maintenance logiciels				
Anomalie non bloquante	1 h	2 h	10 h	
Anomalie bloquante	15 mn	1 h	1 h 30	

Chaque délai débute à compter de l'ouverture du ticket chez le titulaire.

Les soumissionnaires expliciteront les modalités d'application, spécifiques à cette extension de maintenance.

Les délais de la prestation d'extension de maintenance s'appliquent 24h/24, 7j/7.

4.5.2.2 La fourniture de l'administration

L'administration fournit :

- la description de l'incident ;
- les éléments techniques permettant la résolution de ce dernier.

4.5.2.3 Les livrables de la prestation

Le livrable est la résolution de l'incident et le rapport d'activité (état des incidents, des dossiers clos et en-cours) sera communiqué après la clôture d'incident (5 jours au plus tard) et, en fin de prestation et/ou mensuellement (selon le nombre d'unités d'œuvre commandées) à l'administration.

4.5.2.4 La définition d'unités d'œuvre

Le tableau ci-après reprend, pour chaque matériel ou logiciel (/N°PDT¹³ ou référence de l'extension), l'UO d'extension de maintenance (incluant les frais de déplacement, les pièces ainsi que la main d'œuvre) et précise la durée d'exécution.

Unités d'œuvre	Sous garantie constructeur	Hors garantie constructeur
Référence	LOT1/MAINT/EXT/AVECG/2S /N°PDT	LOT1/MAINT/EXT/HORSG/2S /N°PDT
Référence	LOT1/MAINT/EXT/AVECG/2S /référence de l'extension	LOT1/MAINT/EXT/HORSG/2S /référence de l'extension
Durée d'exécution	2 semaines	2 semaines
Référence	LOT1/MAINT/EXT/AVECG/1M /N°PDT	LOT1/MAINT/EXT/HORSG/1M /N°PDT
Référence	LOT1/MAINT/EXT/AVECG/1M /référence de l'extension	LOT1/MAINT/EXT/HORSG/1M /référence de l'extension
Durée d'exécution	1 mois	1 mois

¹³ Les numéros de série ne pouvant pas être publiés, un numéro (N°PDT) est attribué à chaque produit (matériel ou logiciel) à maintenir (liste dans les fichiers "DGFIP-DGS-2500013_pas5_lot1_annexe_financiere_maintenance_parc_logiciels.ods" et "DGFIP-DGS-2500013_pas5_lot1_annexe_financiere_maintenance_parc_materiels.ods").

4.5.3 Le support de la solution antivirus DGFiP

4.5.3.1 Périmètre

La DGFiP utilise la solution WithSecure Client Security et son administration centralisée WithSecure Policy Manager (console et serveur) pour protéger les postes de travail sous les systèmes d'exploitation Windows (7, 10 et 11) et Linux Ubuntu, en version 32 bits et 64 bits, ainsi que les serveurs sous Windows Server 20xx. La version en production est actuellement la version 16.

La version des Antivirus utilisée par la DGFiP fait l'objet d'un document annexe intitulé "DGFIP-DGS-2500013_pas5_cctp_annexe_version_Antivirus.odt".

Ce fichier confidentiel sera joint dans une archive séparée dont le mot de passe devra être demandé par les candidats sur la PLACE.

La DGFiP possède une licence de type « licence de parc » permettant l'utilisation du logiciel sur l'ensemble des postes, soit 160.000 unités au maximum dans l'ensemble de ses services. La DGFiP ne suit pas le nombre exact de logiciels installés, car le nombre de postes de travail actifs varie quasi-quotidiennement.

La licence permet l'utilisation de l'antivirus sur des environnements virtualisés.

La plateforme de gestion et d'administration est composée d'un serveur PMS, de seize serveurs PMP¹⁴ et un serveur PMC¹⁵ qui seront virtualisés en 2025. Cette configuration pourra évoluer en fonction des besoins de la DGFiP et des recommandations d'architecture de WithSecure.

La plate-forme de production est installée à l'ESI de Marseille. La plate-forme de secours installée sur le site sécurisé du SPS.

L'administration et le premier niveau de support de la solution sont assurés par l'ESI de Marseille.

4.5.3.2 les acteurs

- L'équipe antivirus de l'ESI de Marseille gère l'exploitation et l'administration des serveurs de la solution antivirus, la mise en oeuvre de la politique antivirus, la diffusion des mises à jour du logiciel, la qualification et la diffusion quotidienne des signatures, le suivi du déploiement de la solution, le suivi des infections virales et la diffusion de consignes et de solutions de désinfections ainsi que la tenue d'un Intranet dédié. L'administration et le premier niveau de support de la solution sont assurés par l'ESI de Marseille.
- L'équipe poste de travail du bureau SI-3 (Bureau des infrastructures et de la sécurité au sein du service du système d'information) assure les rôles de MOA et de MOE du projet.
- Le titulaire du présent marché : Les intervenants devront avoir suivi une formation approfondie au système de protection antivirus WithSecure. Ils devront également avoir l'expérience de missions de réalisation de prestations de maintenance logicielle dans des environnements organisationnels, fonctionnels et technologiques les plus proches possibles de ceux couverts par le marché.

Les exigences fixées par l'Administration reposent sur des niveaux d'expérience élevés et une expertise forte dans les domaines techniques couverts par ce marché de support logiciel. Les demandes de support adressées

¹⁴Policy Manager Proxy

¹⁵Policy Manager Console

par l'Administration proviennent d'équipes techniques dont le personnel est qualifié. Le relais attendu de la prestation de support doit donc se positionner d'emblée à un niveau d'expertise fort.

Le candidat décrira dans son offre les compétences des personnels chargés de la réalisation des prestations : description par profil-type (qualifications, expérience, références). Le prestataire est responsable de la formation et de la mise à niveau des compétences indispensables pour son personnel sur l'ensemble des sujets relevant des prestations demandées. Il en assume l'incidence sur l'organisation de la prestation et prend en charge l'intégralité des coûts associés.

Le titulaire privilégiera la continuité des prestations commandées par la pérennité de ses intervenants, sur la durée du marché. Le titulaire s'engage ainsi à une stabilité de ces intervenants et à un remplacement à profil équivalent en cas d'indisponibilité de ces derniers selon les modalités définies ci-après :

- En cas d'absence ou de départ d'une personne affectée à l'exécution de la prestation, le titulaire, dès qu'il en a connaissance, doit en aviser la personne responsable du marché et prendre toutes les dispositions pour que la bonne exécution des prestations ne s'en trouve pas compromise.

Pour respecter cette dernière obligation, le titulaire doit désigner un remplaçant d'un niveau au moins équivalent et assurer en interne le transfert de connaissance sur le projet et sur la prestation en cours. Il communiquera le nom et les titres au pouvoir adjudicateur dans un délai maximal de huit (8) jours calendaires à compter du premier jour ouvré d'absence ou de départ de la personne affectée à l'exécution des prestations du marché.

Ce remplacement est subordonné à l'accord exprès du pouvoir adjudicateur. Le silence gardé par la personne publique dans un délai de quinze (15) jours calendaires à compter de la réception de la lettre ou du courriel vaut acceptation du remplacement.

- La personne publique dispose également d'un droit de récusation des intervenants proposés qui ne correspondraient pas au profil annoncé dans l'offre initiale du titulaire. Pendant toute la durée d'exécution de la prestation, la personne publique se réserve le droit de récuser à ce titre :
 - ceux des intervenants qui s'avéreraient inadaptés à l'exécution des prestations, soit pour des motifs d'ordre professionnel liés aux résultats attendus, soit pour des motifs liés aux conditions d'exécution des prestations. Le titulaire procédera alors au remplacement des personnels refusés, dans les mêmes conditions et délais mentionnés supra.
 - ceux des intervenants proposés par le titulaire pour remplacer les intervenants principaux dont l'absence, le départ ou la défaillance ont été préalablement déclarés à la personne publique.

En cas de récusation, le titulaire dispose de quinze (15) jours calendaires pour proposer un autre remplaçant.

A défaut de proposition de remplaçant par le titulaire ou en cas de récusation des remplaçants par le pouvoir adjudicateur et plus globalement en cas de non-respect de ses obligations contractuelles relatives au remplacement du personnel, le marché pourra être résilié dans les conditions prévues à l'article 50 du CCAG-TIC .

En aucun cas, le remplacement du personnel ne peut justifier une augmentation du prix du marché.

4.5.3.3 Le support du logiciel

Le support comprendra :

- la fourniture sans délai des mises à jour de signatures fournies par l'éditeur WithSecure, à partir de son site web ;
- la fourniture sans délai des mises à jour, mineures et majeures, de l'ensemble des produits ;
- le support technique (cf. § 4.5.3.3.1) ;
- le suivi technique du bon fonctionnement des progiciels ;
- les interventions nécessaires pour déterminer l'origine des anomalies entraînant le non fonctionnement des progiciels. Ces interventions pourront nécessiter des déplacements sur site (essentiellement sur les sites de Noisy-le-Grand, Marseille ou Bussy)¹⁶ ;
- la mise à disposition de la documentation en français ;
- la fourniture, pour une nouvelle version, d'une documentation détaillée de la nouvelle version, qui présentera les évolutions du logiciel et décrira les possibles avantages à déployer cette nouvelle version dans le contexte de l'administration ;
- la tenue à jour de la documentation ;
- la maintenance corrective qui comprend les interventions demandées par la personne publique en cas d'anomalies, c'est-à-dire de difficultés de fonctionnement du progiciel (répétitives et reproductibles).

Le titulaire devra proposer également sur son site de support en ligne (cf. § 4.5.3.3.1) :

- le téléchargement des solutions/corrections aux problèmes connus ;
- le téléchargement des versions les plus récentes de la documentation technique ;
- des informations précises, actualisées et en langue française.

Le titulaire devra être partenaire de l'éditeur du logiciel et indiquer alors de quel niveau d'agrément il dispose. Il devra opter pour le contrat « premium » proposé par WithSecure. Une attestation de l'éditeur sera demandée annuellement.

4.5.3.3.1 Modalités de mise en œuvre du support du logiciel

Les interlocuteurs chargés au sein de la DGFIP de l'administration de l'antivirus disposeront d'un support du titulaire, assuré du lundi au vendredi de 8h à 18h, sur l'ensemble des logiciels déployés.

➤ Premier niveau de support

La DGFIP assurera le premier niveau de support pour les utilisateurs du logiciel de protection virale. Un à cinq interlocuteurs « privilégiés » désignés par la DGFIP assureront l'interface avec le niveau deux de support assuré par le titulaire.

➤ Second niveau de support

Le titulaire assure le second niveau de support du logiciel de protection virale. Un support proactif mis en place par le titulaire permettra :

¹⁶ En cas de déplacements, les frais de déplacement, d'hébergement et de nourriture des intervenants du titulaire seront à sa charge.

- la réception par la DGFIP des informations liées aux alertes virales ;
- le suivi technique du bon fonctionnement du logiciel fourni ;
- les interventions nécessaires pour déterminer l'origine et corriger les anomalies entraînant un fonctionnement non satisfaisant du logiciel, et en particulier les réponses aux demandes relatives au paramétrage de l'ensemble de la solution.

La DGFIP pourra accéder au support suivant les modalités ci-dessous :

- par téléphone, au moyen d'un seul et unique numéro national non surtaxé ;
- via un site Internet dédié permettant l'enregistrement et la mise à jour un ticket d'incident ainsi que le suivi de son évolution. Le titulaire mettra à disposition tous les moyens nécessaires à l'enregistrement et au suivi des demandes.
- par courriel : une adresse dédiée est mise à la disposition de l'administration.

Toute saisine devra faire l'objet d'un accusé de réception avec les informations relatives au ticket incident (heure d'appel ou de saisine, référence, description sommaire de l'incident...). Les conditions suivantes, au minimum, devront être remplies :

- pas d'appel téléphonique sans suite ;
- temps de réponse d'une journée dans le cas d'un courriel.

Le support est assuré en français, quel que soit le canal sollicité.

Intervenant en second niveau du dispositif, l'équipe support du titulaire devra disposer d'un niveau de compétence élevé sur les produits concernés. Ce support pourra intégrer le recours à l'expertise de l'éditeur.

➤ Livrables associés à la prestation de support technique

L'Administration fournit :

- la description de l'incident ;
- les éléments techniques permettant la résolution de ce dernier.

Le livrable est constitué de la résolution de l'incident et d'un rapport mensuel d'activité (état des incidents, des dossiers clos et en-cours) qui sera communiqué au plus tard deux jours ouvrés avant chaque comité de suivi (COSUIV, cf. § 4.5.3.3.3).

4.5.3.3.2 Délais de résolution

Les délais attendus en matière de support dépendent de :

- la gravité, bloquante ou non bloquante, de l'anomalie ;
- la nature de la réponse qui apporte une solution définitive ou de contournement.

Ils sont indépendants du canal utilisé pour la saisine.

Degré de gravité de l'anomalie	Définition
Bloquante	Une des fonctionnalités de la solution est indisponible de façon permanente ou régulière ; cela correspond notamment au blocage de la plate-forme de distribution des mises à jour antivirus, au blocage d'un nombre significatif de postes utilisateurs suite à un faux-positif, à la non-exploitabilité technique d'une fonctionnalité intégrée. Une anomalie bloquante pour laquelle le titulaire a proposé une solution de contournement provisoire devient non bloquante.
Non bloquante	Une des fonctions de la solution est en mode dégradé. Il s'agit de non-conformité empêchant l'utilisation de tout ou partie des fonctionnalités du logiciel tout en permettant l'obtention du résultat par une solution de contournement acceptée par la DGFIP. Cette notion recouvre par exemple la gêne significative pour l'utilisateur ou l'exploitant due à l'anomalie, ou une documentation incomplète ou non exploitable.

L'appréciation du caractère bloquant ou non de l'anomalie est du ressort de la DGFIP.

Actions	Anomalie bloquante délais maximums	Anomalie non bloquante délais maximums
Rappel de l'utilisateur	1 HO	4 HO
Réponse à une demande d'information	1 JO	5 JO
Fourniture d'une solution de contournement	1 JO	5 JO
Fourniture d'une solution définitive	5 JO	10 JO

HO : Heure Ouvrée – JO : Jour Ouvré

En ce qui concerne la prise en compte d'un nouveau code malveillant transmis par l'Administration, les délais maximums d'intervention attendus sont les suivants :

Actions	Délais maximums
Rappel de l'utilisateur	1 HO
Fourniture d'une solution de contournement	4 HO
Transmission à WithSecure	1 HO

Un rapport mensuel sur l'activité de support est fourni mensuellement par le titulaire en comité de suivi (COSUIV, cf. § 4.5.3.3.3). Il contient :

- un état de l'activité du support technique sur le mois écoulé (nombre de demandes ouvertes, fermées en cours de traitement, etc.) ;
- un rapport mensuel de suivi et d'information.

Le respect de ces délais de résolution constitue une obligation de résultat. En cas de dépassement de ces délais, le titulaire encourt les pénalités de retard telles qu'elles sont définies à l'article 18-1 du CCAP.

4.5.3.3 Les instances de suivi et de pilotage de l'exécution des prestations de support

Le suivi de l'exécution des services du § 4.5.3 sera inclus dans le prix des prestations de support.

Le titulaire organise et documente la phase d'initialisation du marché en préparant les réunions qui seront nécessaires à la finalisation du plan qualité qui constituera le livrable de cette phase. Celui-ci précise les intervenants et leur responsabilité dans les différentes instances et activités. Il décrit les méthodes et processus appliqués pour garantir le respect des exigences contractuelles après la notification du marché, il est validé lors du premier comité de suivi et mis à jour aussi souvent que nécessaire.

Le titulaire devra désigner un gestionnaire de compte, dédié à l'administration, chargé du suivi technique du marché.

Des réunions de travail pourront être convoquées à la demande de la DGFIP ou du titulaire pour examiner en détail toute question relative à l'exécution du marché, sans périodicité définie. La liste des participants est fonction des thèmes examinés.

Pour le suivi de l'exécution des prestations, une instance sera mise en place : le comité de suivi (COSUIV).

Le comité de suivi est constitué de la maîtrise d'ouvrage, de la maîtrise d'œuvre et des exploitants de la solution. Il se réunira mensuellement. Le secrétariat du comité et la rédaction des comptes rendus sont assurés par le titulaire.

4.5.3.4 Unité d'oeuvre

L'unité d'oeuvre suivante sera employée pour le support du logiciel WithSecure décrit ci-dessus. Il s'agit d'une prestation forfaitaire trimestrielle.

Unité d'oeuvre	
Référence	LOT1/MAINT/SUPP-TRIM-WS
Durée d'exécution	3 mois

4.6 PRESTATIONS D'ASSISTANCE ANNEXES

4.6.1 La veille et le conseil

4.6.1.1 La description de la prestation

La prestation de veille et de conseil consiste à :

- informer, dans la limite des heures ouvrées du jour ouvré suivant, l'administration de l'existence de failles de sécurité des systèmes d'exploitation et des logiciels des équipements présents dans une configuration ;
- informer, dans les 10 jours, l'administration de l'existence de nouvelles versions de système d'exploitation et des logiciels des équipements présents dans une configuration ;
- présenter la nature des correctifs ;
- mesurer, dans le cas d'un passage à une nouvelle version, les impacts de cette évolution en garantissant la cohérence de l'ensemble des versions des logiciels d'une configuration et des équipements périphériques ;
- préciser la procédure à appliquer pour changer de version logicielle (système d'exploitation, configurations) et les outils utilisés pour cet usage (s'il y en a).

La veille et le conseil permettront à l'administration de saisir le service réalisant la prestation de maintenance.

Les soumissionnaires doivent s'engager à maintenir les versions logicielles durant toute la durée du marché. L'administration, quant à elle, n'est pas tenue de faire évoluer ces mêmes versions mais peut avoir intérêt à la faire réaliser.

4.6.1.2 La fourniture de l'administration

L'administration fournit les versions et logiciels des équipements périphériques à la configuration.

4.6.1.3 Les livrables de la prestation

Le livrable est un dossier de veille, en langue française, remis en fin d'exécution d'UO.

Une présentation de ce rapport à l'administration (en Île-de-France) aura lieu dans un délai de 5 jours à l'issue de la fin de l'UO.

Les soumissionnaires fourniront un exemple de dossier de veille dans leur offre.

4.6.1.4 La définition d'unités d'œuvre

Le tableau ci-après reprend l'UO et précise la durée d'exécution.

Unité d'œuvre	Veille
Référence	LOT1/VEIL/6M
Durée d'exécution	6 mois

4.6.2 Le transfert de compétences

4.6.2.1 La description de la prestation

Le titulaire réalise un transfert de compétences pour permettre au personnel de l'administration de maîtriser les évolutions réalisées (installation d'une nouvelle configuration).

Les bénéficiaires de cette prestation sont supposés être déjà familiarisés aux technologies mises en œuvre sur le projet.

Les soumissionnaires doivent proposer un processus de transfert de compétences pouvant s'inspirer des étapes suivantes :

- établir un bilan rapide des compétences des participants et une analyse détaillée des besoins pour affiner le plan de formation ;
- définir la forme, le contenu, et le déroulement de la formation en fonction du domaine et du niveau du transfert, du profil des personnes concernées et des objectifs souhaités ;
- réaliser la formation théorique et pratique au domaine cité dans la demande ;
- établir une synthèse de l'enquête de satisfaction réalisée auprès des bénéficiaires du transfert de compétences.

Le titulaire fournit le matériel sur lequel s'effectue le transfert de compétences.

4.6.2.2 La fourniture de l'administration

L'administration fournit :

- le profil des bénéficiaires et leur niveau de connaissance ;
- le nombre exact de bénéficiaires (6 personnes maximum) ;
- les objectifs du transfert de compétences ;
- le périmètre du transfert ;
- le lieu du transfert de compétences (et la logistique associée dans les locaux de l'administration).

4.6.2.3 Les livrables de la prestation

Les livrables sont :

- un support en français sous forme papier et dématérialisé ;
- un bilan détaillé du transfert de compétences.

4.6.2.4 La définition des unités d'œuvre et la localisation

Le tableau ci-après reprend les unités d'œuvre et précise les durées d'exécution.

Unités d'œuvre	Transfert de compétences		
	Niveau simple	Niveau moyen	Niveau expert
	Mise en œuvre d'une nouvelle fonctionnalité en exploitation	Mise en œuvre d'un nouveau produit en exploitation	Transfert aux architectes maîtrise d'œuvre
Référence	LOT1/TRANS /SIMP/1J	LOT1/TRANS /MOY/3J	LOT1/TRANS /EXP/5J
Durée d'exécution	1 jour	3 jours	5 jours

Le délai de remise du bilan correspond à 5 jours (au plus tard) à partir de la fin de la durée d'exécution.

Le délai contractuel correspond au délai d'exécution additionné du délai de remise des livrables.

4.6.3 Solution antivirus WithSecure : Prestation de transfert de connaissances

La DGFIP souhaite pouvoir bénéficier d'un transfert de connaissances vers les exploitants DGFIP et les responsables du projet dans le cadre d'un changement de version des logiciels fournis.

Cette prestation s'effectuera dans les locaux de la DGFIP : à Noisy-le-Grand ou à Marseille.

Pour chaque commande, la DGFIP fournira les informations suivantes :

- date de début d'intervention souhaitée ;
- date de fin d'intervention souhaitée.

La prestation de transfert de connaissances fait l'objet des deux unités d'œuvre suivantes (contenu identique, seul le site d'exécution est différent) :

Noms	LOT1/TRANS/TR-COMP-FS13 (sur le site de Marseille) LOT1/TRANS/TR-COMP-FS93 (sur le site de Noisy le Grand)
Contexte	Utilisateurs disposant de compétences informatiques
Travaux à assurer	Formation portant sur les points suivants : - transfert de connaissances dans le cadre d'un changement de version
Durée	2 jours
Livrables	<ul style="list-style-type: none"> • prestation de transfert de connaissances • support(s) comprenant la documentation en français

Les frais de déplacement, d'hébergement et de nourriture des intervenants du titulaire devront être inclus dans les prix des UO.

4.6.4 La désinstallation, le déplacement et la réinstallation de matériel

4.6.4.1 La description de la prestation

Cette prestation consiste à désinstaller (retirer de l'armoire à racks proprement), déménager et réinstaller (mise en rack et mise en service) d'un équipement d'un site vers un autre site de l'administration.

Ce déménagement concernera soit un élément rackable ou non, pris isolément, soit un ensemble d'éléments inclus dans un rack ainsi que ce dernier.

Le titulaire prend obligatoirement à sa charge l'assurance des matériels.

4.6.4.2 La fourniture de l'administration

L'administration fournit :

- la liste des équipements à déménager ;
- les contraintes de planification de l'opération (horaires des sites concernés, périodes d'indisponibilité du service) ;
- le calendrier du déménagement.

4.6.4.3 Les livrables de la prestation

Les livrables attendus sont :

- le compte rendu du déménagement comprenant notamment les éléments suivants :
 - date et heure de prise en charge ;
 - difficultés éventuelles rencontrées ;
 - date et heure de livraison sur site cible ;
 - liste et références des éléments livrés.
- le procès-verbal de livraison sur site cible.

4.6.4.4 La définition d'unités d'œuvre

Cette prestation est réalisée sous la forme d'une UO correspondant au déménagement d'un matériel d'un site vers un autre site de l'administration.

Le tableau ci-après reprend les unités d'œuvre et précise les délais d'exécution.

Désinstallation, déplacement et réinstallation					
Unités d'œuvres	Pour un élément				
	Intra Ile-de-France	Province vers province		Ile-de-France vers province (ou l'inverse)	
		Inférieur à 500 kms	Supérieur à 500 kms	Inférieur à 500 kms	Supérieur à 500 kms
Référence	LOT1/DEPL /ELT /IDF/5J	LOT1/DEPL /ELT /PRO-PRO/ INF-500/5J	LOT1/DEPL /ELT /PRO-PRO/ SUP-500/5J	LOT1/DEPL /ELT /IDF-PRO/ INF-500/5J	LOT1/DEPL /ELT /IDF-PRO/ SUP-500/5J
Délai d'exécution	5 jours	5 jours	5 jours	5 jours	5 jours
Unités d'œuvres	Pour plusieurs éléments				
	Intra Ile-de-France	Province vers province		Ile-de-France vers province (ou l'inverse)	
		Inférieur à 500 kms	Supérieur à 500 kms	Inférieur à 500 kms	Supérieur à 500 kms
Référence	LOT1/DEPL /CONF /IDF/5J	LOT1/DEPL /CONF /PRO-PRO/ INF-500/5J	LOT1/DEPL /CONF /PRO-PRO/ SUP-500/5J	LOT1/DEPL /CONF /IDF-PRO/ INF-500/5J	LOT1/DEPL /CONF /IDF-PRO/ SUP-500/5J
Délai d'exécution	5 jours	5 jours	5 jours	5 jours	5 jours

Le délai de remise des livrables correspond à 5 jours (au plus tard) à partir de la fin du délai d'exécution.

Le délai contractuel correspond au délai d'exécution additionné du délai de remise des livrables.

4.6.5 L'installation de matériel

4.6.5.1 La description de la prestation

Cette prestation consiste à installer un matériel sur un site de l'administration ou désigné par cette dernière. Ce matériel sera soit un élément rackable ou non, pris isolément, soit un ensemble d'éléments inclus dans un rack ainsi que ce dernier.

4.6.5.2 La fourniture de l'administration

L'administration fournit :

- la liste des équipements à installer et à paramétrer ;
- les contraintes de planification de l'opération (horaires des sites concernés, périodes d'indisponibilité du service) ;
- le calendrier d'installation et de paramétrage.

4.6.5.3 Le livrable de la prestation

Le livrable est le compte rendu d'installation ainsi que la fin de la prestation proprement dite.

4.6.5.4 La définition d'unités d'œuvre

Le tableau ci-après reprend, pour chaque prestation, l'UO d'installation sur un site de l'administration ou désigné par cette dernière.

Unités d'œuvre	Installation	Installation et paramétrage	Paramétrage
Pour un élément			
Référence	LOT1/INST/ELT /TYP1/1J	LOT1/INST/ELT /TYP2/1J	LOT1/INST/ELT /TYP3/1J
Délai d'exécution	1 jour	1 jour	1 jour
Pour un ensemble d'éléments			
Référence	LOT1/INST/ELTS /TYP1/1J	LOT1/INST/ELTS /TYP2/1J	LOT1/INST/ELTS /TYP3/1J
Délai d'exécution	1 jour	1 jour	1 jour

Le délai de remise des livrables correspond à 5 jours (au plus tard) à partir de la fin du délai d'exécution.

Le délai contractuel correspond au délai d'exécution additionné du délai de remise des livrables.

5 LOT 2 : PAS - ACQUISITIONS

5.1 OBJET DU LOT

L'objet du présent lot est l'acquisition, l'installation et la maintenance de matériels spécifiques de sécurité, ainsi que la réalisation de prestations d'assistance associées, afin de renouveler et de créer des infrastructures de sécurité.

5.2 ACQUISITIONS DE MATÉRIELS, DE LOGICIELS

Il s'agit de l'acquisition de matériels et de logiciels de sécurité. Les soumissionnaires tiendront compte du fait que toutes les caractéristiques mentionnées sont des minima obligatoires. Ainsi, toute offre présentant des performances inférieures ou incompatibles avec ceux-ci sera écartée. Les caractéristiques de performance demandées sont en IP v4 mais devront être compatibles en IP v6.

Tous les équipements proposés par les soumissionnaires seront au format rack standard (exprimé en U).

Les différents équipements à fournir par le soumissionnaire doivent se décliner sous forme d'Appliance ou de châssis.

Les prix comprendront la livraison.

Le marché vise au renforcement de la sécurité des ressources de la DGFIP.

Les produits à acquérir sont de type :

- pare-feu ;
- accélérateurs de flux ;
- serveur mandataire ;
- TAP réseau ;
- agrégateur de liens ;
- solution d'effacement des données ;
- scanner de vulnérabilité ;
- serveur mandataire pour des tests de sécurité ;
- boîtier de cryptographie ;
- solution de prise de main à distance ;
- solution de chiffrement ;
- tokens USB PKI ;
- solution SIEM souveraine avec CTI intégrée ;
- solution de géolocalisation d'adresses IP avec détermination d'ASN ;
- solution de détection d'adresses IP utilisant des mécanismes de masquage (proxies, VPN, Tor, etc.) ;
- solution anti-DDOS de niveau 3 à 7 sans déchiffrement SSL ;

- solution SaaS anti-DDOS souveraine de niveau 3 à 7 ;
- solution de Bot Manager ;
- solution d'annuaire inversée ;
- solution de reconnaissance faciale et d'image.

5.2.1 L'acquisition d'un pare-feu

Il s'agit de l'acquisition d'un pare-feu et d'outils de gestion et d'administration de ce matériel.

5.2.1.1 Caractéristiques minimales du pare-feu

Les normes exigées pour les grandes fonctionnalités demandées ci-dessous sont synthétisées dans l'annexe " DGFIP-DGS-2500013_pas5_cctp_lot2_annexe_caracteristiques ".

Ce fichier confidentiel sera joint dans une archive séparée dont le mot de passe devra être demandé par les candidats sur la PLACE.

L'offre du candidat devra répondre à deux besoins distincts dans l'architecture de sécurité du réseau de la DGFIP :

- un pare-feu de type "appliance" ;
- un pare-feu "nouvelle génération".

5.2.1.2 Caractéristiques du pare-feu de type "appliance"

La fonctionnalité demandée est celle de filtrage réseau de niveaux 3 et 4 (couche ISO) de type "filtrage de paquet avec état"¹⁷ qui travaille principalement avec des réseaux Ethernet/IP.

Le pare-feu gère des règles, afférentes au triplet "adresse source, adresse destination, protocole" permettant d'autoriser ou de refuser la connexion réseau décrite par cette règle. Une règle permet aussi de définir des traductions d'adresses (NAT) ou des traductions de ports (PAT). Tous les types de traductions d'adresses¹⁸ et ports¹⁹ doivent être supportés par le pare-feu. Le pare-feu peut traduire simultanément les adresses source et destination dans une même règle.

Le pare-feu doit avoir la capacité de réaliser des statistiques d'utilisation (par exemple le nombre de paquets réseau traités, le nombre de paquets réseau rejetés) et des informations de sécurité (par exemple, fournir une trace des paquets réseau qui ont été rejetés par le pare-feu). Les soumissionnaires devront évaluer en pourcentage l'impact de ces statistiques sur les performances globales du pare-feu (influence de l'activation des journaux sur les performances).

Les protocoles à inspecter seront à minima les suivants : HTTP, LDAP, DNS, SMTP, SNMP, FTP, Telnet, NTP.

¹⁷ "stateful inspection".

¹⁸ NAT source, NAT destination, NAT statique, NAT dynamique.

¹⁹ PAT source, PAT destination, PAT statique, PAT dynamique.

Le pare-feu est équipé d'interfaces réseau 1Gbps cuivre RJ45 et/ou 1Gbps/10Gbps/40Gbps fibre optique (connecteurs SC ou ST / LC duplex ou MTP/MPO 12 fibres) et des accessoires nécessaires à son fonctionnement (logiciels, cartes, câbles, fibre, extension)²⁰.

Le pare-feu doit avoir plusieurs niveaux d'administration (par exemple : lecture seule, accès restreint, accès complet). Les soumissionnaires devront décrire le processus permettant de réaliser ces niveaux d'administration, ainsi que l'accès au pare-feu. Les accès SSH v2 sont privilégiés.

Le pare-feu devra pouvoir s'insérer dans un environnement de type SDN²¹ ou OpenStack et être configurable par l'intermédiaire d'API²².

Le pare-feu devra pouvoir offrir la possibilité d'être utilisé en mode multi-contexte tout en garantissant à minima :

- l'étanchéité entre les contextes ;
- le contrôle des ressources entre les contextes empêchant un contexte saturé de saturer les autres contextes.

5.2.1.2.1 Caractéristiques générales

Le soumissionnaire proposera 5 configurations distinctes et de dimensionnements différents correspondant à une "très petite"²³, "petite", "moyenne", "grande" et "très grande" configuration.

CARACTÉRISTIQUES GÉNÉRALES	MINIMUM EXIGE					REMARQUES
MATÉRIEL PARE-FEU						
CONFIGURATIONS	C0	C1	C2	C3	C4	
Matériel "rackable" dans une armoire standard	Impératif					Préciser le nombre de U
Double alimentation électrique	optionnelle ²⁴		obligatoire			Préciser la consommation électrique maximale (W) et le dégagement calorifique (BTU/h)
Administration du boîtier	Administrable à distance					Par interface Web sécurisée, par client léger et/ou par SSH
	Configuration par API					Préciser les méthodes et les éventuelles limitations
Interfaces Ethernet 1Gbps CU de management (minimum)	1	1	1	1	1	Si le support proposé est de type SFP alors il faudra fournir un connecteur compatible
Interfaces Ethernet 1Gbps CU (minimum)	8	8	8	-	-	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Interfaces Giga-Ethernet SFP (minimum)	2	8	8	-	-	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques

²⁰ Cette remarque s'applique à tous les pare-feu.

²¹ Software Defined Network

²² Application Programming Interface (interface de programmation)

²³ environnement maquette, test des fonctionnalités toutes options (la solution proposée pourra être virtualisée (compatible avec KVM))

²⁴ si l'équipement offre la possibilité d'avoir une deuxième alimentation alors celle-ci devra être fournie

Interfaces 10 Giga-Ethernet SFP+ (minimum)	2	8	8	16	16	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Interfaces 40 Giga-Ethernet QSFP+ (minimum)	-	-	-	4	4	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Ajout d'interface Ethernet (CU / SFP / SFP+ / QSFP+)	Optionnel					Préciser le nombre d'interfaces supplémentaires maximum et leur débit.
Débit de traitement pare-feu multi-protocole (minimum)	4,5 Gbps	16 Gbps	40 Gbps	90 Gbps	95 Gbps	Préciser le débit maximum
Nombre de connexions concurrentes ²⁵ (minimum)	600k	4M	10M	40M	90M	Préciser le total de connexions supportées
Nombre de nouvelles connexions par seconde (minimum)	150k	500k	1M	1,4M	1,7M	Préciser le nombre maximum de sessions par seconde
Débit VPN AES (minimum)	1,7 Gbps	10 Gbps	16 Gbps	50 Gbps	60 Gbps	Préciser le débit maximum de traitement VPN (chiffrement AES)
Tunnel VPN IPSec ²⁶ (minimum)	800	5 000	15 000	20 000	20 000	Préciser le nombre maximum de tunnel VPN IPSec
Connexions VPN SSL simultanées (minimum)	800	5 000	15 000	20 000	20 000	Préciser le nombre maximum de connexion VPN SSL
Nombre de multi-contextes (minimum)	2	2	2	10	10	Préciser le nombre maximum de contextes
Haute disponibilité	oui	oui	oui	oui	oui	active/active ; active/passive
Codification d'UO	LOT2/ ACQ/ PFEU/ STD /C0	LOT2/ ACQ/ PFEU/ STD /C1	LOT2/ ACQ/ PFEU/ STD /C2	LOT2/ ACQ/ PFEU/ STD /C3	LOT2/ ACQ/ PFEU/ STD /C4	

L'offre du candidat devra préciser le MTBF.

Le pare-feu de type "appliance" devra être évolutif et pouvoir proposer l'ajout de fonctionnalités par simple activation de licence.

5.2.1.2.2 Fonctionnalités VPN

Les fonctionnalités attendues sont :

- VPN Tunneling ;
- authentification par mot de passe et/ou certificat ;
- intégrité.

Elles doivent être réalisées dans un environnement utilisant des autorités de certification publiques et/ou internes aux ministères financiers.

L'utilisation du client VPN du constructeur devra permettre de contrôler la conformité du poste de travail (système d'exploitation, correctif de sécurité, solution Antivirus, ...), permettre la connexion du poste de manière automatique sans authentification de l'utilisateur autorisant ainsi la mise à jour du poste à distance.

²⁵unité : k : kilo (1.000) / M : méga (1.000.000)

²⁶un tunnel IPSec peut être de type "site à site" ou de type utilisateurs (client)

La licence aura une durée correspondant à celle de la protection des droits d'auteur et permettra d'activer le VPN SSL avec les minimum en pré-requis et les fonctionnalités du client VPN souhaitées.

Référence du logiciel	LOT2/ACQ/PFEU/STD/LIC/VPN/C0
Référence du logiciel	LOT2/ACQ/PFEU/STD/LIC/VPN/C1
Référence du logiciel	LOT2/ACQ/PFEU/STD/LIC/VPN/C2
Référence du logiciel	LOT2/ACQ/PFEU/STD/LIC/VPN/C3
Référence du logiciel	LOT2/ACQ/PFEU/STD/LIC/VPN/C4

5.2.1.2.3 Adaptateurs multimodes SFP / SFP+ / QSFP+

Les adaptateurs nécessaires pour les interfaces SFP / SFP+ / QSFP+ feront l'objet des UO suivants :

Référence du matériel	LOT2/ACQ/PFEU/STD/ADAP/SFP
Référence du matériel	LOT2/ACQ/PFEU/STD/ADAP/SFP+
Référence du matériel	LOT2/ACQ/PFEU/STD/ADAP/QSFP+

5.2.1.2.4 Augmentation de la capacité multi-contexte

Il s'agit ici d'acquérir des licences augmentant le nombre de "contextes" disponibles sur le pare-feu lorsque cela est possible.

En fonction du modèle de licence du constructeur, il sera demandé l'ajout d'un contexte, de 10 contextes ou de la totalité des contextes (maximum).

Référence du logiciel	LOT2/ACQ/PFEU/STD/MC/1C
Référence du logiciel	LOT2/ACQ/PFEU/STD/MC/10C
Référence du logiciel	LOT2/ACQ/PFEU/STD/MC/MAX

5.2.1.2.5 Administration centralisée

L'outil d'administration centralisée qui pourrait venir en supplément de l'appliance sera détaillé.

Il devra autoriser l'administration à minima d'un cluster de pare-feu avec la totalité des contextes activés et fera l'objet de l'UO suivante :

Référence du matériel	LOT2/ACQ/PFEU/STD/OAD
-----------------------	-----------------------

L'offre du candidat devra préciser le MTBF.

Si la solution existe sous forme virtualisée²⁷ (VM), celle-ci pourra être proposée et dans ce cas fera l'objet de deux UO, l'une pour la partie VM, l'autre pour l'hyperviseur faisant fonctionner cette VM.

²⁷ KVM à privilégier mais la DGFIP a une préférence pour l'appliance physique

L'hyperviseur sera fourni avec toutes les licences nécessaires.

Référence du matériel	LOT2/ACQ/PFEU/STD/OAD_VM
Référence du matériel	LOT2/ACQ/PFEU/STD/OAD_Hyperviseur

5.2.1.3 **Caractéristiques du pare-feu "nouvelle génération"**

5.2.1.3.1 Analyse applicative et prévention d'intrusion

Le pare-feu doit proposer à minima les fonctionnalités et pré-requis du pare-feu de type "appliance".

Les protocoles à inspecter seront à minima les suivants : IP, TCP, HTTP, UDP, SIP, RTP/RTCP, H.323, POP3, IMAP4, NNTP, SSL, MGCP, SSH, LDAP, DNS, SMTP, SNMP, FTP, Telnet, NTP.

Le pare-feu proposé doit particulièrement gérer les fonctions suivantes :

- décontamination antivirale ;
- déchiffrement SSL ;
- authentification des flux ;
- authentification des utilisateurs ;
- détection des chevaux de Troie ;
- protection contre les attaques DOS (deni de service) ;
- protection contre l'usurpation de sessions et l'évasion des sessions ;
- protection contre les injections SQL ;
- IDS (Intrusion Detection System) / IPS (Intrusion Prevention System) ;
- filtrage de contenu (URL) ;
- haute disponibilité.

Le pare-feu est équipé d'interfaces réseau 1Gbps cuivre RJ45 et/ou 1Gbps/10Gbps/40Gbps fibre optique (connecteurs SC ou ST / LC duplex ou MTP/MPO 12 fibres) et des accessoires nécessaires à son fonctionnement (logiciels, cartes, câbles, fibre, extension).

Le pare-feu devra pouvoir éventuellement (option) offrir la possibilité d'être utilisé en mode multi-contexte tout en garantissant à minima :

- l'étanchéité entre les contextes ;
- le contrôle des ressources entre les contextes empêchant un contexte saturé de saturer les autres contextes.

Le pare-feu devra pouvoir s'insérer dans un environnement de type SDN ou OpenStack et être configurable par l'intermédiaire d'API.

Pour respecter les bonnes pratiques et les recommandations de l'ANSSI, le soumissionnaire proposera trois constructeurs différents dont l'un au moins devra être certifié par l'ANSSI.

Les constructeurs devront être différents de celui retenu pour l'UO pare-feu de type "appliance".

5.2.1.3.2 Fonctions VPN

Les fonctionnalités attendues sont :

- VPN Tunneling ;
- authentification par mot de passe et/ou certificat ;
- intégrité.

Elles doivent être réalisées dans un environnement utilisant des autorités de certification publiques et/ou internes aux ministères financiers.

5.2.1.3.3 Caractéristiques générales

Le soumissionnaire proposera pour chaque constructeur 5 configurations distinctes et de dimensionnements différents correspondant à une " très petite²⁸ ", " petite ", " moyenne ", " grande " et " très grande " configuration.

CARACTERISTIQUES GENERALES	MINIMUM EXIGE					REMARQUES
MATERIEL PARE-FEU NOUVELLE GENERATION						
CONFIGURATIONS	C0	C1	C2	C3	C4	
Matériel "rackable" dans une armoire standard	Impératif					Préciser le nombre de U
Double alimentation électrique	optionnelle ²⁹		obligatoire			Préciser la consommation électrique maximale (W) et le dégagement calorifique (BTU/h)
Administration du boîtier	Administrable à distance					Par interface Web sécurisée, par client léger et/ou par SSH
	Configuration par API					Préciser les méthodes et les éventuelles limitations
Interfaces Ethernet 1Gbps CU de management (minimum)	1	1	1	1	1	Si le support proposé est de type SFP alors il faudra fournir un connecteur compatible
Interfaces Ethernet 1Gbps CU (minimum)	8	8	8	-	-	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Interfaces Giga-Ethernet SFP (minimum)	-	-	-	-	-	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Interfaces 10 Giga-Ethernet SFP+ (minimum)	8	8	8	8	8	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Interfaces 40 Giga-Ethernet QSFP+ (minimum)	-	-	-	4	6	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques

²⁸environnement maquette, test des fonctionnalités toutes options (la solution proposée pourra être virtualisée (compatible avec KVM))

²⁹Si l'équipement offre la possibilité d'avoir une deuxième alimentation alors celle-ci devra être fournie

Ajout d'interface Ethernet (CU / SFP / SFP+ / QSFP+)	Optionnel					Préciser le nombre d'interfaces supplémentaires maximum et leur débit.
Débit de traitement pare-feu (UDP 1518) (minimum)	39 Gbps	55 Gbps	72 Gbps	190 Gbps	245 Gbps	Préciser le débit maximum
Débit de traitement pare-feu NGFW ³⁰ (minimum)	7 Gbps	10 Gbps	15 Gbps	17 Gbps	34 Gbps	Préciser le débit maximum
Nombre de connexions concurrentes ³¹ (minimum)	1,8M	5M	7M	12M	25M	Préciser le total de connexions supportées
Nombre de nouvelles connexions par seconde (minimum)	90k	190k	250k	335k	335k	Préciser le nombre maximum de sessions par seconde
Débit VPN AES (minimum)	7,5 Gbps	15 Gbps	25 Gbps	34 Gbps	60 Gbps	Préciser le débit maximum de traitement VPN (chiffrement AES)
Tunnel VPN IPSec (minimum)	500	1 000	5 000	10 000	10 000	Préciser le nombre maximum de tunnel VPN IPSec
Connexions VPN SSL simultanées (minimum)	500	1 000	2 000	10 000	10 000	Préciser le nombre maximum de connexions VPN SSL ("tunnel mode")
Optionnelle - Nombre de multi-contextes (minimum)	10	10	10	10	25	Préciser le nombre maximum de contextes
Haute disponibilité	oui	oui	oui	oui	oui	active/active ; active/passive
Codification d'UO	LOT2/ACQ/PFEU/NGx ³² /C0	LOT2/ACQ/PFEU/NGx/C1	LOT2/ACQ/PFEU/NGx/C2	LOT2/ACQ/PFEU/NGx/C3	LOT2/ACQ/PFEU/NGx/C4	

L'offre du candidat devra préciser le MTBF.

5.2.1.3.4 Adaptateurs multimodes SFP / SFP+ / QSFP+

Les adaptateurs nécessaires pour les interfaces SFP / SFP+ / QSFP+ font l'objet des UO suivants :

Référence du matériel	LOT2/ACQ/PFEU/NGx/ADAP/SFP
Référence du matériel	LOT2/ACQ/PFEU/NGx/ADAP/SFP+
Référence du matériel	LOT2/ACQ/PFEU/NGx/ADAP/QSFP+

5.2.1.3.5 Augmentation de la capacité multi-contexte

Si l'équipement propose un mode multi-contexte³³, il s'agit ici d'acquérir des licences augmentant le nombre de "contextes" disponibles sur le pare-feu.

En fonction du modèle de licence du constructeur, il sera demandé l'ajout d'un contexte, de 10 contextes ou de la totalité des contextes (maximum).

³⁰NGFW : Next Gen FireWall - pare-feu + module IPS + contrôle Applicatifs

³¹unité : k : kilo (1.000) / M : méga (1.000.000)

³²où x représente le numéro de constructeur (1, 2 ou 3)

³³dans la négative, l'UO ne sera pas renseignée et le soumissionnaire le précisera dans sa réponse

Référence du logiciel	LOT2/ACQ/PFEU/NGx/MC/1C
Référence du logiciel	LOT2/ACQ/PFEU/NGx/MC/10C
Référence du logiciel	LOT2/ACQ/PFEU/NGx/MC/MAX

5.2.1.3.6 Administration centralisée

L'outil d'administration centralisée qui pourrait venir en supplément de l'appliance sera détaillé.

Il devra autoriser l'administration à minima d'un cluster de pare-feu avec la totalité des contextes activés et fera l'objet de l'UO suivante :

Référence du matériel	LOT2/ACQ/PFEU/NGx/OAD
-----------------------	-----------------------

L'offre du candidat devra préciser le MTBF.

Si la solution existe sous forme virtualisée³⁴ (VM), celle-ci pourra être proposée et dans ce cas fera l'objet de deux UO, l'une pour la partie VM, l'autre pour l'hyperviseur faisant fonctionner cette VM.

L'hyperviseur sera fourni avec toutes les licences nécessaires.

Référence du matériel	LOT2/ACQ/PFEU/NGx/OAD_VM
Référence du matériel	LOT2/ACQ/PFEU/NGx/OAD_Hyperviseur

5.2.2 L'acquisition d'un pare-feu Web applicatif

Les normes exigées pour les grandes fonctionnalités demandées ci-dessous sont synthétisées dans l'annexe " DGFIP-DGS-2500013_pas5_cctp_lot2_annexe_caracteristiques ".

Ce fichier confidentiel sera joint dans une archive séparée dont le mot de passe devra être demandé par les candidats sur la PLACE.

Il s'agit d'acquérir un pare-feu de type WAF³⁵ répondant aux fonctionnalités suivantes :

- respect du protocole HTTP ;
- prévention contre les attaques de type XSS, injection SQL et OWASP Top 10 ;
- protection des services Web (XML/SOAP, ...) ;
- haute-disponibilité ;
- option permettant de cloisonner différents environnements, avec une séparation forte des instances virtuelles de pare-feu applicatif.

Le pare-feu est équipé d'interfaces réseau 1Gbps cuivre RJ45 et/ou 1Gbps/10Gbps/40Gbps fibre optique (connecteurs SC ou ST / LC duplex ou MTP/MPO 12 fibres) et des accessoires nécessaires à son fonctionnement (logiciels, cartes, câbles, fibre, extension).

Le pare-feu devra pouvoir s'insérer dans un environnement de type SDN ou OpenStack et être configurable par l'intermédiaire d'API.

³⁴ KVM à privilégier mais la DGFIP a une préférence pour l'appliance physique

³⁵ Web Application Firewall

Le soumissionnaire proposera 5 configurations distinctes et de dimensionnements différents correspondant à une "très petite"³⁶, "petite", "moyenne", "grande" et "très grande" configuration.

CARACTERISTIQUES GENERALES	MINIMUM EXIGE					REMARQUES
MATERIEL PARE-FEU WEB APPLICATIF						
CONFIGURATIONS	C0	C1	C2	C3	C4	
Matériel "rackable" dans une armoire standard	optionnelle		Impératif			Préciser le nombre de U
Double alimentation électrique	optionnelle		obligatoire			Préciser la consommation électrique maximale (W) et le dégagement calorifique (BTU/h)
Administration du boîtier	Administrable à distance					Par interface Web sécurisée, par client léger et/ou par SSH
	Configuration par API					Préciser les méthodes et les éventuelles limitations
Interface d'administration dédiée	option	option	oui	oui	oui	impératif
Interfaces Ethernet 1Gbps CU (minimum)	2	2	2	4	-	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Interfaces Giga-Ethernet SFP (minimum)	-	-	-	-	-	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Interfaces 10 Giga-Ethernet SFP+ (minimum)	-	-	-	4	-	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Interfaces 40 Giga-Ethernet QSFP+ (minimum)	-	-	-	-	4	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Ajout d'interface Ethernet (CU / SFP / SFP+ / QSFP+)	Optionnel					Préciser le nombre d'interfaces supplémentaires maximum et leur débit.
Débit réseau (applicatif) (minimum)	50 Mbps	200 Mbps	1 Gbps	3 Gbps	10 Gbps	Préciser le débit maximum
Haute disponibilité	oui	oui	oui	oui	oui	active/active ; active/passive
Virtualisation	-	-	oui	oui	oui	impératif
Solution logicielle	possible	possible	non	non	non	La solution pourra être logicielle et s'exécuter sur un serveur

³⁶ environnement maquette, test des fonctionnalités toutes options (la solution proposée pourra être virtualisée (compatible avec KVM))

						x86_64
Codification d'UO	LOT2/ ACQ/ PFEU/ WAF /C0	LOT2/ ACQ/ PFEU/ WAF /C1	LOT2/ ACQ/ PFEU/ WAF /C2	LOT2/ ACQ/ PFEU/ WAF /C3	LOT2/ ACQ/ PFEU/ WAF /C4	

L'offre du candidat devra préciser le MTBF.

5.2.2.1 Adaptateurs multimodes SFP / SFP+ / QSFP+

Les adaptateurs nécessaires pour les interfaces SFP / SFP+ / QSFP+ font l'objet des UO suivants :

Référence du matériel	LOT2/ACQ/PFEU/WAF/ADAP/SFP
Référence du matériel	LOT2/ACQ/PFEU/WAF/ADAP/SFP+
Référence du matériel	LOT2/ACQ/PFEU/WAF/ADAP/QSFP+

L'offre du candidat devra préciser le MTBF.

5.2.2.2 Administration centralisée

L'outil d'administration centralisée qui pourrait venir en supplément du pare-feu WAF sera détaillé.

Il devra autoriser l'administration à minima d'un cluster de pare-feu avec la totalité des contextes activés et fera l'objet de l'UO suivante :

Référence du matériel	LOT2/ACQ/PFEU/WAF/OAD
-----------------------	-----------------------

L'offre du candidat devra préciser le MTBF.

Si la solution existe sous forme virtualisée³⁷ (VM), celle-ci pourra être proposée et dans ce cas fera l'objet de deux UO, l'une pour la partie VM, l'autre pour l'hyperviseur faisant fonctionner cette VM.

L'hyperviseur sera fourni avec toutes les licences nécessaires.

Référence du matériel	LOT2/ACQ/PFEU/WAF/OAD_VM
Référence du matériel	LOT2/ACQ/PFEU/WAF/OAD_Hyperviseur

5.2.3 L'acquisition d'un équipement de type accélérateur de flux

Les normes exigées pour les grandes fonctionnalités demandées ci-dessous sont synthétisées dans l'annexe " DGFIP-DGS-2500013_pas5_cctp_lot2_annexe_caracteristiques ".

Ce fichier confidentiel sera joint dans une archive séparée dont le mot de passe devra être demandé par les candidats sur la PLACE.

Il s'agit d'acquérir un accélérateur de flux permettant de délester les fonctions d'authentification et de chiffrement des données SSL des serveurs à un appareil dédié à cet effet.

³⁷ KVM à privilégier mais la DGFIP a une préférence pour l'appliance physique

Le soumissionnaire fournira un équipement répondant aux fonctionnalités suivantes :

- cache ;
- authentification ;
- compression de contenus web en fonction des capacités des navigateurs connectés ;
- répartition de charge et haute disponibilité ;
- pare-feu applicatif (WAF) ;
- fonctionnalités de protection (syn flood...) et de sécurité contre les attaques de robots et par déni de services avancées (niveau 7) ;
- compression de plusieurs types de documents (HTML, javascript, MIME, doc, ppt, xls) cachés ou non transmis en HTTP ou HTTPS ;
- option multi-contexte permettant de cloisonner différents environnements, avec une séparation forte des instances virtuelles entre zones de sécurité et une possibilité de re-cloisonnement au sein d'une même zone de sécurité.

L'équipement est équipé d'interfaces réseau 1Gbps cuivre RJ45 et/ou 1Gbps/10Gbps/40Gbps/100Gbps fibre optique (connecteurs base-T ou LC duplex ou MTP/MPO 12 fibres) et des accessoires nécessaires à son fonctionnement (logiciels, cartes, câbles, fibre, extension).

Le soumissionnaire proposera 5 configurations distinctes et de dimensionnements différents correspondant à une " virtuelle³⁸ " (C0), " petite " (C1), " moyenne " (C2), " grande " (C3) et " très grande " (C4) configuration.

Les configurations C3 et C4 devront être déclinées en deux sous-configurations :

- l'une dite "standard" (std), orientée essentiellement répartition de charge sans fonctionnalités de sécurité avancées exigées de base ;
- l'autre dite "secure" (sec) comprenant de base les fonctionnalités de sécurité, de protection avancées et aux capacités de traitement SSL accrues (cartes d'accélération matérielles...).

Caractéristiques minimales								
CONFIGURATIONS	C0	C1	C2	C3		C4		Remarques
				standard	secure	standard	secure	
Matériel "rackable" dans une armoire standard	-	Impératif						Préciser le nombre de U
Double alimentation électrique	-	obligatoire						Préciser la consommation électrique maximale (W) et le dégagement calorifique (BTU/h)

³⁸ environnement maquette, test des fonctionnalités toutes options (la solution proposée devra être virtualisée (compatible avec KVM et/ou Openstack))

Système d'exploitation propriétaire ou ouvert	Oui							Avec maintenance de l'éditeur
Administration du boîtier et/ou des instances virtuelles	Oui							Par interface Web sécurisée, par client léger et/ou par SSH
Ensemble des fonctions disponibles via interface Web	Oui							De préférence ou par client léger
Interfaces Ethernet 1Gbps CU (minimum)	-	8	-	-	-	-	-	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Interfaces Giga-Ethernet SFP (minimum)	-	-	8	-	-	-	-	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Interfaces 10 Giga-Ethernet SFP+ (minimum)	-	2	4	8	8	8	8	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Interfaces 40 Giga-Ethernet QSFP+ ou QSFP28 (minimum)	-	-	-	2	2	4	4	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Interfaces 100 Giga-Ethernet QSFP28 (minimum)	-	-	-	-	-	2	2	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Ajout d'interface Ethernet (CU / SFP / SFP+ / SFP28 / QSFP+ / QSFP28)	Optionnel							Préciser le nombre d'interfaces supplémentaires maximum et leur débit.
Load balancing	oui	oui	oui	oui	oui	oui	oui	Impératif
SSL Offload & Acceleration	oui	oui	oui	oui	oui	oui	oui	Impératif
Authentification	oui	oui	oui	oui	oui	oui	oui	Impératif
TCP multiplexing	oui	oui	oui	oui	oui	oui	oui	Impératif

Filtrage applicatif (WAF)	facultatif	facultatif	oui	facultatif	oui	facultatif	oui	Pour les configurations où il est indiqué facultatif, la fonctionnalité doit pouvoir être ajoutée via licence
Compression	oui	oui	oui	oui	oui	oui	oui	Indiquer la limite en bande passante
Redirection de Cache	oui	oui	oui	oui	oui	oui	oui	
Bande passante L4/L7 en Gbps (minimum)	1	10	20	50	50	150	150	Augmentation par licence
Connexions ³⁹ L4/seconde (minimum)	-	180k	500k	1M	1M	3M	3M	
Requêtes HTTP/seconde (minimum)	-	280k	900k	2,5M	2,5M	5M	5M	
Connexions L4 concurrentes (minimum)	-	20M	50M	70M	70M	90M	90M	
SSL/TLS connexions/seconde (CPS) RSA (clé 2K) (minimum)	-	7k	20k	30k	80k	60k	150k	
SSL/TLS connexions/seconde (CPS) ECC (EC-P256) (minimum)	-	4k	9k	20k	40k	30k	100k	
Capacité de traitement SSL en Gbps (minimum)	-	3	10	20	40	40	60	
Multi-contexte (minimum)	-	-	5	20	20	40	40	
Codification d'UO	LOT2/ ACQ/ ACCL/ C0	LOT2/ ACQ/ ACCL/ C1	LOT2/ ACQ/ ACCL/ C2	LOT2/ ACQ/ ACCL/ C3_STD	LOT2/ ACQ/ ACCL/ C3_SEC	LOT2/ ACQ/ ACCL/ C4_STD	LOT2/ ACQ/ ACCL/ C4_SEC	

L'offre du candidat devra préciser le MTBF.

5.2.3.1 Adaptateurs SFP / SFP+ / SFP28 / QSFP+ / QSFP28

Les adaptateurs nécessaires pour les interfaces Base-T / SFP / SFP+ / SFP28 / QSFP+ / QSFP28 font l'objet des UO suivants :

Référence du matériel	LOT2/ACQ/ACCL/ADAP/Base-T
-----------------------	---------------------------

³⁹unité : k : kilo (1.000) / M : méga (1.000.000)

Référence du matériel	LOT2/ACQ/ACCL/ADAP/SFP
Référence du matériel	LOT2/ACQ/ACCL/ADAP/SFP+
Référence du matériel	LOT2/ACQ/ACCL/ADAP/SFP28
Référence du matériel	LOT2/ACQ/ACCL/ADAP/QSFP+
Référence du matériel	LOT2/ACQ/ACCL/ADAP/QSFP28

L'offre du candidat devra préciser le MTBF.

5.2.3.2 Connectique spécifique

Il s'agit ici d'acquérir ici, lorsqu'ils existent, les câbles à attache directe (DAC), optiques actifs (AOC) et "breakout" de tout type et de toutes les longueurs, compatibles avec l'ensemble des matériels de configurations C1 à C4.

Chaque référence de câble se traduira par une UO.

Référence du matériel	LOT2/ACQ/ACCL/CONNECT/ref_cable
-----------------------	---------------------------------

5.2.3.3 Augmentation de la capacité multi-contexte

Il s'agit ici d'acquérir des licences augmentant le nombre de "contextes" disponibles sur l'équipement.

En fonction du modèle de licence du constructeur et des modèles de matériels, il sera demandé l'ajout d'un contexte, de 5 contextes, de 10 contextes ou de la totalité des contextes de façon à pouvoir atteindre la limite maximale supportable par les équipements proposés.

Référence du logiciel	LOT2/ACQ/ACCL/MC/1C
Référence du logiciel	LOT2/ACQ/ACCL/MC/5C
Référence du logiciel	LOT2/ACQ/ACCL/MC/10C
Référence du logiciel	LOT2/ACQ/ACCL/MC/MAX

5.2.3.4 Augmentation de bande passante

Il s'agit d'acquérir des licences permettant d'augmenter la capacité de bande passante des équipements.

L'augmentation de bande passante se traduira par l'acquisition d'une UO pour passer au palier immédiatement supérieur⁴⁰ selon la solution proposée par le constructeur.

Référence du logiciel	LOT2/ACQ/ACCL/BP/C0
Référence du logiciel	LOT2/ACQ/ACCL/BP/C1
Référence du logiciel	LOT2/ACQ/ACCL/BP/C2

⁴⁰exemple : si la solution C0 offre un débit initial de 1G et que les possibilités d'augmentation du constructeur sont ensuite de 2G puis 5G alors pour passer de 1G à 5G, il faudra 2 UO (le coût restant fixe pour une UO).

Référence du logiciel	LOT2/ACQ/ACCL/BP/C3_STD
Référence du logiciel	LOT2/ACQ/ACCL/BP/C3_SEC
Référence du logiciel	LOT2/ACQ/ACCL/BP/C4_STD
Référence du logiciel	LOT2/ACQ/ACCL/BP/C4_SEC

5.2.3.5 Augmentation de la mémoire

Le candidat proposera pour les modèles qui le permettent, les extensions de mémoire (RAM). Chaque extension se traduira par une UO et il conviendra de préciser à quelle configuration elle pourra s'appliquer.

Référence du matériel	LOT2/ACQ/ACCL/MEMOIRE/Cx
-----------------------	--------------------------

L'offre du candidat devra préciser le MTBF.

5.2.3.6 Fonctionnalités soumises à licences

Le candidat proposera l'ensemble des fonctionnalités optionnelles complémentaires soumises à licences pour les différents équipements (ex : pare-feu applicatif, protection contre les robots, GSLB...) qui ne seraient pas incluses et/ou exigées de base dans les configurations matérielles demandées.

Chaque fonctionnalité se traduira par une UO spécifique.

Référence du logiciel	LOT2/ACQ/ACCL/LIC/Nom_Fonctionnalité
-----------------------	--------------------------------------

5.2.3.7 Administration centralisée

L'outil d'administration centralisée qui pourrait venir en supplément des solutions d'accélération de flux sera détaillé.

Il devra autoriser l'administration à minima d'un cluster d'équipements avec la totalité des contextes activés et fera l'objet de l'UO suivante :

Référence du matériel	LOT2/ACQ/ACCL/OAD
-----------------------	-------------------

L'offre du candidat devra préciser le MTBF.

Si la solution existe sous forme virtualisée⁴¹ (VM), celle-ci pourra être proposée et dans ce cas fera l'objet de deux UO, l'une pour la partie VM, l'autre pour l'hyperviseur faisant fonctionner cette VM.

L'hyperviseur sera fourni avec toutes les licences nécessaires.

Référence du matériel	LOT2/ACQ/ACCL/OAD_VM
Référence du matériel	LOT2/ACQ/ACCL/OAD_Hyperviseur

⁴¹ KVM à privilégier mais la DGFIP a une préférence pour l'appliance physique

5.2.4 L'acquisition d'un serveur mandataire

Les normes exigées pour les grandes fonctionnalités demandées ci-dessous sont synthétisées dans l'annexe " DGFIP-DGS-2500013_pas5_cctp_lot2_annexe_caracteristiques ".

Ce fichier confidentiel sera joint dans une archive séparée dont le mot de passe devra être demandé par les candidats sur la PLACE.

Il s'agit d'acquérir un serveur mandataire permettant le filtrage avancé des accès de type navigation Internet pour l'ensemble des agents de la DGFIP.

Le soumissionnaire fournira un équipement répondant aux fonctionnalités suivantes :

- Filtrage applicatif : Prise en charge des protocoles HTTP, HTTPS, FTP, DNS, etc. ;
- Déchiffrement SSL/TLS : Capacité à inspecter le trafic chiffré (avec gestion des exceptions) ;
- Contrôle des accès : Politiques granulaires par utilisateur, groupe ou appareil (adresse IP) ;
- Méthodes d'authentification :
 - utilisateur/mot de passe ;
 - LDAP ;
 - Kerberos.
- Protection contre les menaces :
 - Analyse anti-malware (sandboxing, signatures, IA) ;
 - Détection du phishing et des sites malveillants ;
 - Prévention des fuites de données (DLP).
- Journalisation et reporting :
 - Conservation des journaux pendant 1 mois (au minimum) ;
 - Export des journaux vers un SIEM ;
 - Rapports personnalisables sur l'activité et les incidents.
- S'insérer dans une architecture en haute disponibilité :
 - Architecture redondante⁴² (actif/passif, actif/actif ou cluster)

Le soumissionnaire proposera 3 configurations distinctes et de dimensionnements différents correspondant à une " virtuelle⁴³", "petite " et " grande " configuration.

CARACTERISTIQUES GENERALES	MINIMUM EXIGE			REMARQUES
MATERIEL SERVEUR MANDATAIRE (PROXY)				
CONFIGURATIONS	C0	C1	C2	
Matériel "rackable" dans une armoire standard	-	Impératif		Préciser le nombre de U

⁴²La répartition de charge n'est pas demandée par la solution, c'est un plus si elle sait le faire

⁴³ environnement maquette, test des fonctionnalités toutes options (la solution proposée devra être virtualisée (compatible avec KVM et/ou Openstack))

Double alimentation électrique	-	obligatoire		Préciser la consommation électrique maximale (W) et le dégagement calorifique (BTU/h)
Administration de la solution	Administrable à distance			Par interface Web sécurisée, par client léger et/ou par SSH
	Configuration par API			Préciser les méthodes et les éventuelles limitations
Interfaces Ethernet 1Gbps CU de management (minimum)	-	1	1	Si le support proposé est de type SFP alors il faudra fournir un connecteur compatible
Interfaces Ethernet 1Gbps CU (minimum)	-	4	-	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Interfaces 10 Giga-Ethernet SFP+ (minimum)	-	-	4	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Ajout d'interface Ethernet (CU / SFP / SFP+ / QSFP+)	Optionnel			Préciser le nombre d'interfaces supplémentaires maximum et leur débit.
Haute disponibilité	oui	oui	oui	active/active active/passive cluster
Codification d'UO	LOT2/ ACQ/ PRX/ C0	LOT2/ ACQ/ PRX/ C1	LOT2/ ACQ/ PRX/ C2	

L'offre du candidat devra préciser le MTBF.

5.2.4.1 Administration centralisée

L'outil d'administration centralisée qui pourrait venir en supplément des solutions d'accélération de flux sera détaillé.

Il devra autoriser l'administration à minima d'un cluster d'équipements pouvant couvrir l'usage pour 100.000 utilisateurs et fera l'objet de l'UO suivante :

Référence du matériel	LOT2/ACQ/PRX/OAD
-----------------------	------------------

L'offre du candidat devra préciser le MTBF.

Si la solution existe sous forme virtualisée⁴⁴ (VM), celle-ci pourra être proposée et dans ce cas fera l'objet de deux UO, l'une pour la partie VM, l'autre pour l'hyperviseur faisant fonctionner cette VM.

L'hyperviseur sera fourni avec toutes les licences nécessaires.

Référence du matériel	LOT2/ACQ/PRX/OAD_VM
-----------------------	---------------------

⁴⁴ KVM à privilégier mais la DGFIP a une préférence pour l'appliance physique

Référence du matériel	LOT2/ACQ/PRX/OAD_Hyperviseur
-----------------------	------------------------------

5.2.5 L'acquisition de TAP réseau

Il s'agit d'acquérir un équipement de type TAP réseau "fibre" pour le monitoring du trafic réseau dans le cadre d'une utilisation avec une appliance 2 ports ou un logiciel d'analyse ou d'agrégation de liens sur des réseaux à 1G / 10G / 40G / 100G .

Le système de type passif fourni doit offrir les fonctionnalités suivantes :

- absence d'alimentation électrique ;
- monitoring en ligne non intrusif ;
- liens de production opérationnels en permanence ;
- copie de tous les niveaux protocolaires ;
- pas de perte de paquets ;
- absence de point de rupture ;
- compatible FO multimode OM3/OM4 connecteur LC.

Le soumissionnaire proposera 3 configurations distinctes et de dimensionnements différents correspondant à une " petite ", " moyenne " et " grande " configuration.

CARACTERISTIQUES GENERALES	MINIMUM EXIGE			REMARQUES
MATÉRIEL AGRÉGATEUR RÉSEAU				
CONFIGURATIONS	C1	C2	C3	
Matériel "rackable" dans une armoire standard	Impératif			Préciser le nombre de U
aucune alimentation électrique	obligatoire			
Nombre de ports monitorés ⁴⁵	1	4	8	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Possibilité d'ajouter plusieurs modules sur une même ligne de rack	Optionnel			Préciser le nombre proposé
Garantie des traitements (IPS)	Système de garantie de trafic			
Codification d'UO	LOT2/ ACQ/ TAP/ C1	LOT2/ ACQ/ TAP/ C2	LOT2/ ACQ/ TAP/ C3	

L'offre du candidat devra préciser le MTBF et la perte maximale d'insertion (dB).

5.2.6 L'acquisition d'un agrégateur de liens réseaux

Il s'agit d'acquérir un équipement de type agrégateur de liens réseaux "fibre" pour le monitoring du trafic réseau.

⁴⁵1 port correspond à une entrée et deux sorties (liaison entre deux équipements avec réplique du trafic)

Le système fourni doit offrir les fonctionnalités suivantes :

- très faible latence ;
- chaque port peut recevoir ou renvoyer le trafic ;
- agrégation, réplication et duplication de trafic réseau ;
- copie de tous les niveaux protocolaires ;
- pas de perte de paquets.

L'agrégateur est équipé d'interfaces réseau 1Gbps cuivre RJ45 et/ou 1Gbps/10Gbps/40Gbps fibre optique (connecteurs SC ou ST / LC duplex ou MTP/MPO 12 fibres) et des accessoires nécessaires à son fonctionnement (logiciels, cartes, câbles, fibre, extension).

Le soumissionnaire proposera 3 configurations distinctes et de dimensionnements différents correspondant à une " petite ", " moyenne " et " grande " configuration.

CARACTERISTIQUES GENERALES	MINIMUM EXIGE			REMARQUES
MATÉRIEL AGRÉGATEUR DE LIENS RÉSEAUX				
CONFIGURATIONS	C1	C2	C3	
Matériel "rackable" dans une armoire standard	Impératif			Préciser le nombre de U
Double alimentation électrique	obligatoire			Préciser la consommation électrique maximale (W) et le dégagement calorifique (BTU/h)
Administration du boîtier	Administrable à distance			Par interface Web sécurisée, par client léger et/ou par SSH
Interfaces Ethernet 1Gbps CU (minimum)	24	-	-	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Interfaces Giga-Ethernet SFP (minimum)	-	-	-	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Interfaces 10 Giga-Ethernet SFP+ (minimum)	-	24	48	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Interfaces 40 Giga-Ethernet QSFP+ (minimum)	4	4	4	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Ajout d'interface Ethernet (CU / SFP / SFP+ / QSFP+)	Optionnel			Préciser le nombre d'interfaces supplémentaires maximum et leur débit.
Codification d'UO	LOT2/ ACQ/ AGG/ C1	LOT2/ ACQ/ AGG/ C2	LOT2/ ACQ/ AGG/ C3	

L'offre du candidat devra préciser le MTBF.

5.2.6.1 Adaptateurs SFP / SFP+ / QSFP+

Les adaptateurs nécessaires pour les interfaces SFP / SFP+ / QSFP+ font l'objet des UO suivants :

Référence du matériel	LOT2/ACQ/AGG/ADAP/SFP
Référence du matériel	LOT2/ACQ/AGG/ADAP/SFP+
Référence du matériel	LOT2/ACQ/AGG/ADAP/QSFP+

L'offre du candidat devra préciser le MTBF.

5.2.7 L'acquisition d'une solution d'effacement de données

Les normes exigées pour les grandes fonctionnalités demandées ci-dessous sont synthétisées dans l'annexe " DGFIP-DGS-2500013_pas5_cctp_lot2_annexe_caracteristiques ".

Ce fichier confidentiel sera joint dans une archive séparée dont le mot de passe devra être demandé par les candidats sur la PLACE.

Il s'agit d'acquérir une solution d'effacement de données fondée sur la démagnétisation du disque ou l'effacement de données pour les supports de type SSD.

L'offre du candidat devra préciser le MTBF.

5.2.7.1 La démagnétisation du disque

Le soumissionnaire fournira une solution de type "démagnétiseur" qui consistera à soumettre le disque à un champ magnétique intense. La solution devra pouvoir fournir une force de "démagnétisation" minimale de **7000 Gauss**.

Les médias supportés par la solution seront de divers ordres :

- disques durs : 2½", 3½" et 5¼" PC ;
- DLT Tapes⁴⁶ : Super DLT I, II & III, DLT IV-VSL, S-DLT ;
- LTO Tapes⁴⁷ : LTO1, LTO2, LTO3, LTO4, LTO5.

Référence du matériel	LOT2/ACQ/EFF/DEM
-----------------------	------------------

5.2.7.2 L'effacement de données

Le soumissionnaire fournira une solution complète de type matérielle permettant l'effacement par "surcharge" ou formatage des disques durs. Il n'y aura pas de surcoût de licence lié au nombre de disque effacé.

La solution devra prendre en charge à minima les disques durs au format NVMe, SSD, SAS, SATA, Fibre Channel et SCSI.

⁴⁶ "Digital Linear Tape (ou DLT) est une technique de sauvegarde de données informatiques sur bande magnétique"

⁴⁷ "Linear Tape-Open (ou LTO) est une technique de stockage sur bande magnétique au format ouvert »

Référence du matériel	LOT2/ACQ/EFF/FORMATAGE
-----------------------	------------------------

5.2.8 L'acquisition d'un scanner de vulnérabilité

Les normes exigées pour les grandes fonctionnalités demandées ci-dessous sont synthétisées dans l'annexe " DGFIP-DGS-2500013_pas5_cctp_lot2_annexe_caracteristiques ".

Ce fichier confidentiel sera joint dans une archive séparée dont le mot de passe devra être demandé par les candidats sur la PLACE.

Il s'agit d'acquérir deux types de logiciel de scanner de vulnérabilités qui obéiront aux fonctionnalités et caractéristiques déclinées ci-dessous.

5.2.8.1 Scanner de vulnérabilité de type 1

Les fonctionnalités attendues de ce logiciel sont les suivantes :

- recherche de vulnérabilités Web ;
- recherche de vulnérabilités de type "Injection SQL" et "XSS" en profondeur ;
- analyse des scripts, contenus Javascript / Ajax / Flash ;
- réalisation du Fuzzing ;
- réalisation de scan de ports et test des protocoles associés ;
- réalisation d'une liste de sous domaines d'un site.

La licence aura une durée correspondant à celle de la protection des droits d'auteur, avec support et mise à jour.

Référence du logiciel	LOT2/ACQ/SCAN/TYP1
-----------------------	--------------------

5.2.8.2 Scanner de vulnérabilité de type 2

Les fonctionnalités attendues de ce logiciel sont les suivantes :

- réalisation de scans de ports ;
- analyse des services afin de déceler ceux qui sont vulnérables ;
- analyse des erreurs de configuration ;
- analyse des patchs de sécurité non appliqués (avec un compte root / admin) ;
- recherche de mots de passe faibles ou de mots de passe par défaut ;
- report des services jugés déconseillés (Telnet) ;
- analyse de la pile TCP (Recherche de dénis de service) ;
- planification des scans de vulnérabilités ;
- création de rapports, en mode détaillé ou non ;
- support des plugins.

Le logiciel fourni sera en deux parties distinctes :

- un démon / service qui exécute les requêtes et communique avec la cible ;
- une application client qui récupère les données et affiche le résultat.

La licence aura une durée correspondant à celle de la protection des droits d'auteur, avec support et mise à jour.

Référence du logiciel	LOT2/ACQ/SCAN/TYP2
-----------------------	--------------------

5.2.9 L'acquisition d'un serveur mandataire pour des tests de sécurité

Les normes exigées pour les grandes fonctionnalités demandées ci-dessous sont synthétisées dans l'annexe " DGFIP-DGS-2500013_pas5_cctp_lot2_annexe_caracteristiques ".

Il s'agit d'acquérir un logiciel de type serveur mandataire applicatif HTTP

Ce fichier confidentiel sera joint dans une archive séparée dont le mot de passe devra être demandé par les candidats sur la PLACE.P/HTTPS interactif.

Les fonctionnalités de ce logiciel devront être déclinées comme suit :

- recherche automatisée de vulnérabilités dans une application Web ;
- serveur mandataire applicatif opérant en mode "man in the middle" (MITM) entre un navigateur et le serveur Web analysé ;
- interception et modification de requêtes (GET, POST) ;
- création d'un inventaire du contenu et des fonctionnalités d'un site Web (fichiers, dossiers) ;
- automatisation d'attaques sur une application Web (fuzzing, tests d'injections sql, buffer overflow) ;
- analyse des token de session (session ID) afin de vérifier s'ils sont prédictibles ;
- outil permettant de décoder des requêtes (décodage de caractères), et de les comparer ;
- possibilité d'enregistrer / restaurer la configuration des différents outils.

La licence associée au logiciel sera une version professionnelle, d'une durée correspondant à celle de la protection des droits d'auteur, avec support et mise à jour.

Référence du logiciel	LOT2/ACQ/SMAND
-----------------------	----------------

L'offre du candidat devra préciser le MTBF.

5.2.10 L'acquisition d'un boîtier de cryptographie

Les normes exigées pour les grandes fonctionnalités demandées ci-dessous sont synthétisées dans l'annexe " DGFIP-DGS-2500013_pas5_cctp_lot2_annexe_caracteristiques ".

Ce fichier confidentiel sera joint dans une archive séparée dont le mot de passe devra être demandé par les candidats sur la PLACE.

Il s'agit d'acquérir un boîtier de cryptographie, conforme au RGS⁴⁸ ou eIDAS⁴⁹, si possible qualifié par l'ANSSI, répondant aux fonctionnalités suivantes :

- chiffrement et intégrité ;
- authentification (utilisateurs ou données) ;
- gestion des clés de signature (stockage et informations de sécurité) ;
- signature ;
 - des applications de gestion de titres électroniques sécurisées ;
 - des applications de eServices ;
 - des applications d'infrastructures de gestion de clés publiques (IGC).

Le boîtier disposera de circuits spécifiques autorisant la détection d'attaques et qui permettent, en fonction de sa configuration, l'effacement des données critiques de sécurité.

Des API devront être disponibles afin de permettre aux éditeurs et aux intégrateurs de logiciels d'intégrer le boîtier cryptographique à leur application en gérant tout ou partie du protocole d'échange. Les API minimales proposées seront :

- une API Java ;
- une API PKCS#11.

Des extensions de l'API PKCS#11 permettront d'accéder aux fonctions cryptographiques et aux fonctions spécifiques du boîtier.

Les objectifs de sécurité pris en compte par ce boîtier :

- support de divers systèmes d'exploitations dont Windows, Linux, HP-UX ;
- gérer un fichier d'événements ;
- assurer la confidentialité et l'intégrité des clés durant toute leur durée de vie ;
- exécuter des opérations cryptographiques de manière sécurisée en utilisant des algorithmes et des paramètres conformes au RGS. Le boîtier devra supporter les algorithmes suivants :
 - AES 128, 192 et 256 bits ;
 - RSA 2048 à 4096 bits ;
 - ECC courbe elliptique conforme à NIST P-256 ;
 - Algorithmes post-quantiques.
- pouvoir identifier et authentifier les utilisateurs ;
- restreindre l'accès à des services, en fonction du rôle de l'utilisateur, aux services explicitement assignés à ce rôle ;
- détecter toute tentative d'attaques physiques et entrer dans un état d'erreur en cas de détection d'attaque ;

⁴⁸Référentiel Général de Sécurité

⁴⁹electronic IDentification, Authentication and trust Services - l'identification électronique et les services de confiance pour les transactions électroniques

- supporter la sauvegarde et la restauration des clés en préservant leur confidentialité et leur intégrité ;
- supporter un mécanisme de mise à jour sécurisé de son code embarqué ;
- initialisation par un mécanisme sécurisé basé sur des techniques de secrets partagés ;
- pouvoir s'intégrer avec différentes PKI :
 - RSA 2048 à 4096 bits ;
 - Microsoft Certificate Services ;
 - RSA Certificate Manager ;
 - PKI Opentrust ATOS/IDNOMIC ;
 - Oracle Database ;
 - EJBCA.

Le soumissionnaire proposera 3 configurations distinctes et de dimensionnements différents correspondant à une "petite", "moyenne" et "grande" configuration.

CARACTÉRISTIQUES GÉNÉRALES	MINIMUM EXIGE			REMARQUES
BOÎTIER CRYPTOGRAPHIE				
CONFIGURATIONS	C1	C2	C3	
Matériel "rackable" dans une armoire standard	Impératif			
Ventilateur redondant	Impératif			
Double alimentation électrique	obligatoire			Préciser la consommation électrique maximale (W) et le dégagement calorifique (BTU/h)
Nombre de clés basées sur les courbes elliptiques NIST P-256 (TPS ⁵⁰)	500	1200	2400	
Vitesse (TPS RSA 2048 bits)	450	3500	8500	
Nombre maximum de Clients	10	20	100	
Codification d'UO	LOT2/ACQ /CRYPTO /C1	LOT2/ACQ /CRYPTO /C2	LOT2/ACQ /CRYPTO /C3	

L'offre du candidat devra préciser le MTBF.

5.2.11 L'acquisition d'une solution de chiffrement

Les normes exigées pour les grandes fonctionnalités demandées ci-dessous sont synthétisées dans l'annexe " DGFIP-DGS-2500013_pas5_cctp_lot2_annexe_caracteristiques ".

Ce fichier confidentiel sera joint dans une archive séparée dont le mot de passe devra être demandé par les candidats sur la PLACE.

⁵⁰ Transactions par seconde

5.2.11.1 Chiffrement des échanges de fichiers

Il s'agit d'acquérir une solution logicielle de chiffrement des échanges de fichiers qualifiée par l'ANSSI et répondant aux fonctionnalités suivantes :

- utilisation d'un conteneur chiffré pour le transport de fichier (messagerie, support amovible, transfert de fichiers, etc...) ;
- chiffrement à la volée, transparent pour les utilisateurs ;
- mécanisme de recouvrement d'entreprise ;
- compatibles avec les systèmes d'exploitation Windows, Linux et Mac OS X ;
- solution "gratuite" pour lire le conteneur et récupérer les fichiers.

L'offre du candidat devra proposer une licence d'une durée correspondante à celle de la protection des droits d'auteur que la DGFIP souhaite acquérir par tranche (10 postes, 100 postes, 1000 postes et 5000 postes).

Référence du logiciel	LOT2/ACQ/ENC/LIC/10_CTNR
Référence du logiciel	LOT2/ACQ/ENC/LIC/100_CTNR
Référence du logiciel	LOT2/ACQ/ENC/LIC/1000_CTNR
Référence du logiciel	LOT2/ACQ/ENC/LIC/5000_CTNR

5.2.11.2 Chiffrement de partages réseaux

Il s'agit d'acquérir une solution logicielle de chiffrement de partage réseaux qualifiée par l'ANSSI et répondant aux fonctionnalités suivantes :

- chiffrement de fichiers sur partages réseaux entre utilisateurs et groupe de travail ;
- chiffrement à la volée, transparent pour les utilisateurs ;
- mécanisme de recouvrement d'entreprise ;
- gestion du chiffrement sur les supports amovibles (clé mémoire, disque externe, etc.).

L'offre du candidat devra proposer une licence d'une durée correspondante à celle de la protection des droits d'auteur.

Référence du logiciel	LOT2/ACQ/ENC/PARTAGE
-----------------------	----------------------

5.2.12 L'acquisition de token USB PKI

Les normes exigées pour les grandes fonctionnalités demandées ci-dessous sont synthétisées dans l'annexe " DGFIP-DGS-2500013_pas5_cctp_lot2_annexe_caracteristiques ".

Ce fichier confidentiel sera joint dans une archive séparée dont le mot de passe devra être demandé par les candidats sur la PLACE.

Il s'agit d'acquérir des tokens USB PKI pour un usage d'authentification forte, de signature électronique et/ou de chiffrement.

Les tokens USB devront répondre aux normes et fonctionnalités suivantes :

- compatible avec les systèmes d'exploitations Microsoft Windows 10/11, Linux ;
- conformité à la norme FIPS 140-2 (niveau 3 minimum) ;
- compatibilité avec les standards PKCS#11, Microsoft CSP/KSP, OpenSSL
- stockage des certificats au format X509 v3 ;
- capacité de stockage EEPROM de 64 Ko minimum pour les certificats ;
- support des algorithmes de sécurité : RSA 2048, AES (128/192/256), SHA-1, SHA-256, SHA-384, SHA-512, P-256 ECDSA ;
- génération des clés sur le token (pas d'export possible) ;
- verrouillage de la clé après plusieurs tentatives ;
- connectique de type USB-A ;
- authentification d'une session Windows en lien avec un AD⁵¹ Samba 4 ou Microsoft ;
- accès aux applications depuis les navigateurs Microsoft Edge, Firefox
- accès à une connexion VPN avec certificat (optionnel).

La couche logicielle ("Middleware") sera fournie et documentée.

Les "Tokens" auront une durée de vie de 5 ans minimum et ne feront pas l'objet de prestation de maintenance (consommable).

Leur acquisition se fera par lot de 1.000 ou 10.000 unités

Référence du matériel	LOT2/ACQ/TOKEN/USB-1000
Référence du matériel	LOT2/ACQ/TOKEN/USB-10000

L'offre du candidat devra préciser le MTBF.

5.2.13 L'acquisition d'une solution SIEM souveraine avec CTI intégrée

Les normes exigées pour les grandes fonctionnalités demandées ci-dessous sont synthétisées dans l'annexe " DGFIP-DGS-2500013_pas5_cctp_lot2_annexe_caracteristiques ".

Ce fichier confidentiel sera joint dans une archive séparée dont le mot de passe devra être demandé par les candidats sur la PLACE.

Il s'agit de l'acquisition d'une solution de type SIEM ("Security Information and Event Management"), accompagnée de ses outils de gestion, d'administration, et intégrant nativement une capacité CTI ("Cyber Threat Intelligence").

La solution devra répondre aux exigences de souveraineté (éditeurs, traitement, stockage des données en conformité avec les réglementations françaises / européennes).

La solution devra répondre aux besoins suivants dans l'architecture de sécurité du réseau de la DGFIP :

⁵¹Active Directory

- Collecte centralisée et corrélation d'événements de sécurité issus de sources hétérogènes (systèmes, équipements réseau, applications, antivirus, etc.) ;
- Intégration native ou interopérable avec une base CTI (Cyber Threat Intelligence) actualisée en continu ;
- Fonctionnalités avancées de détection, d'investigation, d'alerte et d'automatisation (SOAR en option).

La solution devra également répondre aux spécifications suivantes :

- Collecte d'événements multi-source :
 - prise en charge des formats standardisés (syslog, CEF, JSON, LEEF, etc.),
 - avec agent ou "agentless" ;
 - capacité à collecter en temps réel et en différé.
- Moteur de corrélation permettant de construire des règles dynamiques, adaptables, avec possibilité de corrélation contextuelle (temps, géolocalisation, utilisateurs, signatures).
- Base CTI intégrée ou interopérable, avec mise à jour automatique quotidienne ou en temps réel. Les flux CTI doivent provenir de sources certifiées ou référencées (ex. : ANSSI, MISP, CIRCL, etc.). Le moteur doit permettre l'enrichissement automatique des événements avec les éléments issus de la CTI (adresses IP, domaines, hachages, etc.).
- Tableau de bord personnalisable (par rôle, par périmètre) incluant des visualisations dynamiques, alertes en temps réel, rapports périodiques, et indicateurs clés de performance (KPI⁵² sécurité).
- Mécanisme d'alerte temps réel configurable (seuils, règles, scénarios) avec notification multicanal (mail, syslog, webhook, etc.).
- Capacité d'investigation (analyse post-incident) avec fonctions de recherche full-text, pivotage, visualisation des timelines et chaînes d'attaque (kill chain, MITRE ATT&CK).
- Interopérabilité via API RESTful pour l'intégration dans un SOC existant ou des outils tiers (ex. : ticketing, SOAR, plateformes de supervision).

Il est demandé une **conformité souveraine** :

- Les données collectées et stockées doivent rester sur le territoire français ou européen ;
- L'éditeur de la solution devra être français ou européen, non soumis à des législations extraterritoriales (type CLOUD Act).
- La solution doit pouvoir être hébergée en interne (on-premise) ou sur un cloud certifié SecNumCloud.

Exploitabilité et administration

- L'interface d'administration doit permettre une gestion fine des rôles et des accès (RBAC), incluant des profils : lecture seule, analyste, administrateur.
- Toutes les actions d'administration doivent être journalisées (journaux d'administration accessibles dans le SIEM lui-même).
- L'administration distante doit être possible via interface web sécurisée (HTTPS avec authentification forte) ou via accès SSH.

⁵²Key Performance Indicators

Le soumissionnaire devra fournir une documentation technique complète (architecture, guide d'installation, d'administration, de maintien en condition opérationnelle).

La solution devra être extensible (ajout de connecteurs, montée en charge horizontale/verticale).

Référence du matériel	LOT2/ACQ/SIEM
-----------------------	---------------

5.2.14 L'acquisition d'une solution de géolocalisation d'adresses IP avec détermination d'ASN

Les normes exigées pour les grandes fonctionnalités demandées ci-dessous sont synthétisées dans l'annexe " DGFIP-DGS-2500013_pas5_cctp_lot2_annexe_caracteristiques ".

Ce fichier confidentiel sera joint dans une archive séparée dont le mot de passe devra être demandé par les candidats sur la PLACE.

Il s'agit de l'acquisition d'un service ou d'un outil permettant la géolocalisation d'adresses IP publiques et la détermination de leur ASN ("Autonomous System Number") d'appartenance.

La solution devra s'intégrer aisément aux environnements de supervision et d'analyse de la sécurité existants (SIEM, SOC, outils réseau, etc.).

Les fonctionnalités attendues sont détaillées dans l'annexe "DGFIP-DGS-2500013_pas5_cctp_lot2_annexe_caracteristiques".

La solution devra permettre :

- La résolution d'adresses IP en informations géographiques (pays, région, ville, latitude/longitude approximative).
- L'identification de l'ASN, du nom de l'organisation associée, du bloc IP d'origine et du registre d'attribution (RIPE, ARIN, APNIC, etc.).

L'exploitation via une interface web, une API ou un outil en ligne de commande.

La solution devra également répondre aux spécifications suivantes :

- Géolocalisation IP : la solution doit restituer les informations suivantes à partir d'une IP :
 - Pays (nom et code ISO) ;
 - Région et ville (si disponibles) ;
 - Coordonnées approximatives (latitude/longitude)
- Identification ASN :
 - récupération du numéro ASN,
 - récupération de l'organisation détentrice,
 - récupération du registre d'origine et des plages IP associées.
- Requêtes en masse : possibilité de traiter des lots d'adresses IP (fichiers ou via API).
- Historique de requêtes : consultation des recherches précédentes avec possibilité d'export (optionnel).
- Interfaces disponibles :

- Interface web sécurisée (HTTPS) ;
- API RESTful (format JSON ou XML), avec documentation technique ;
- outils en ligne de commande ou bibliothèques (Python, Bash, etc.) en option
- Intégration et interopérabilité :
 - la solution devra pouvoir s'intégrer dans un écosystème de sécurité existant (SIEM, outils de supervision, scripts d'automatisation) ;
 - L'API devra permettre des appels automatisés depuis des outils tiers (par exemple enrichissement automatique dans un flux CTI ou une alerte SIEM).

Référence du matériel	LOT2/ACQ/GEOLOC
-----------------------	-----------------

5.2.15 L'acquisition d'une solution de détection d'adresses IP utilisant des mécanismes de masquage (proxies, VPN, Tor, etc.)

Les normes exigées pour les grandes fonctionnalités demandées ci-dessous sont synthétisées dans l'annexe " DGFIP-DGS-2500013_pas5_cctp_lot2_annexe_caracteristiques ".

Ce fichier confidentiel sera joint dans une archive séparée dont le mot de passe devra être demandé par les candidats sur la PLACE.

Il s'agit de l'acquisition d'une solution permettant de détecter si une adresse IP publique est associée à un mécanisme de masquage d'identité ou de localisation tel qu'un proxy ouvert, un VPN commercial, un nœud Tor, ou un service d'anonymisation similaire.

L'objectif est d'améliorer les capacités d'évaluation de la fiabilité des connexions réseaux et des événements de sécurité.

La solution devra permettre d'obtenir, pour toute adresse IP publique, les informations suivantes :

- Type de technologie de masquage détectée (proxy, VPN, réseau Tor, etc.) ;
- Niveau de fiabilité de la détection ;
- Informations contextuelles complémentaires (par exemple : datacenter, usage mobile, fournisseur d'accès, etc.).

La solution devra également répondre aux spécifications suivantes :

- Détection multi-catégories : la solution doit identifier et catégoriser les technologies de masquage parmi les suivantes (au minimum) :
 - Proxy ouvert ou anonyme ;
 - VPN commerciaux ;
 - Nœuds d'entrée ou de sortie Tor ;
 - Hébergement en datacenter (cloud public, hébergement web) ;
 - Adresses IP mobiles ou résidentielles (optionnel)
- Base de données IP actualisée : la solution doit s'appuyer sur une base actualisée au moins hebdomadairement (idéalement quotidienne), sans intervention manuelle requise.

- Formats d'accès :
 - API RESTful (retours en JSON ou XML)
 - Interface web pour consultation manuelle
 - Intégration possible dans des scripts automatisés (CLI, Python, etc.)
- Résultat de la requête IP :
 - Type de service identifié (ex : "VPN", "Tor", "Open Proxy")
 - Nom ou type d'organisation associée si disponible
 - Fiabilité de la détection (score, flag booléen ou indicateur de confiance)
 - Informations complémentaires (ex : hébergement cloud connu, mobile ISP, etc.)
- Intégration et compatibilité
 - La solution devra être intégrable dans les outils de cybersécurité existants (SIEM, moteurs CTI, solutions d'analyse d'événements).
 - Les appels API devront pouvoir être automatisés dans des scénarios de corrélation ou d'enrichissement de logs.
- La documentation technique devra inclure des exemples d'usage et les spécifications complètes de l'API.
- Exploitabilité et administration
 - Accès via interface web sécurisée (HTTPS) et API avec authentification (clé API ou token).
 - Mise à disposition d'un tableau de bord (optionnel) pour la visualisation statistique des types d'IP détectées.
 - Export possible des résultats ou historiques en formats standards (CSV, JSON).

Référence du matériel	LOT2/ACQ/DETECT_IP
-----------------------	--------------------

5.2.16 L'acquisition d'une solution anti-DDOS de niveau 3 à 7 sans déchiffrement SSL

Les normes exigées pour les grandes fonctionnalités demandées ci-dessous sont synthétisées dans l'annexe " DGFIP-DGS-2500013_pas5_cctp_lot2_annexe_caracteristiques ".

Ce fichier confidentiel sera joint dans une archive séparée dont le mot de passe devra être demandé par les candidats sur la PLACE.

Il s'agit de l'acquisition d'une solution anti-DDOS⁵³ de niveau 3 à 7 Hybride (On-Premise + Cloud).

La solution anti-DDOS, de niveau 3 à 7 volumétrique, permettra de protéger le SI DGFIP contre les attaques par Deni de Services Distribués et volumétriques, allant de la couche 3 à la couche 7 du modèle OSI.

Cette solution devra être multi-protocolaire (Exemple : HTTP, HTTPS, DNS, SMTP, etc.). Elle devra pouvoir protéger sans déchiffrer les flux et avec une analyse comportementale. La technologie utilisée "On-Premise" doit être la même que celle utilisée dans le cloud.

⁵³Distributed Denial of Service attack (attaque par déni de service distribuée)

La solution devra pouvoir s'interconnecter avec l'environnement existant sans régression sur la visibilité que pourrait avoir un SOC, notamment la récupération d'adresse IP source réelle de bout en bout.

Le soumissionnaire fournira un équipement répondant aux fonctionnalités suivantes :

- Détection et mitigation sans déchiffrement TLS ;
- Extraction/Exploitation de l'adresse IP source réelle de bout en bout sans déchiffrement TLS ;
- Protection anti-DDOS de la couche 3 à la couche 7 ;
- Génération des empreintes TLS ;
- Protection contres attaques ciblant des API ;
- Protection contre les attaques de type "zero day" ;
- Analyse comportementale (ML) en temps réel ;
- Protection basée sur des Signatures ;
- Accès aux contenus des signatures (lors d'un blocage) ;
- Interopérable avec d'autres solutions de type WAF/WAAP ;
- Proposer différents mode de déploiement : transparent ou actif ;
- Blocage par Géolocalisation ;
- Blocage par ISP/ASNs ;
- Blocage/Déblocage en Masse ;
- Mécanisme de challenge adaptatif (tcp, dns, http) ;
- Protection efficace des applications non web (DNS, SMTP ..) ;
- Protection comportementale DNS ;
- Déploiement : Hybride (même technologie utilisée dans le cloud et "On-Premise").

Le soumissionnaire proposera 2 configurations distinctes et de dimensionnements différents correspondant à une "très petite" et " très grande " configuration.

CARACTERISTIQUES GENERALES	MINIMUM EXIGE		REMARQUES
MATERIEL Anti-DdoS niveau 3 à 7 hybride sans déchiffrement SSL			
CONFIGURATIONS	C1	C2	
Matériel "rackable" dans une armoire standard	Impératif		1 U, modulable
Double alimentation électrique	optionnelle	obligatoire	Préciser la consommation électrique maximale (W) et le dégagement calorifique (BTU/h)
Administration du boîtier	Administrable à distance		Par interface Web sécurisée, par client léger et/ou par SSH
	Configuration par API		Préciser les méthodes et les éventuelles limitations

Interface d'administration dédiée	oui	oui	impératif
Interfaces Ethernet 1Gbps CU (minimum)	2	2	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Interfaces Giga-Ethernet SFP (minimum)	2	4	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Interfaces 10 Giga-Ethernet SFP+ (minimum)	2	4	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Interfaces 40 Giga-Ethernet QSFP+ (minimum)	-	2	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Ajout d'interface Ethernet (CU / SFP / SFP+ / QSFP+)	optionnelle		Préciser le nombre d'interfaces supplémentaires maximum et leur débit.
Débit trafic légitime	5 Gbps	40 Gbps	Préciser le débit maximum
Débit trafic de Mitigation (minimum)	2 Gbps	30 Gbps	
Haute disponibilité	oui	oui	active/active ; active/passive
Débit de prévention DDOS (en Paquet Par Seconde) (minimum)	10 Mpps	40 Mpps	
Codification d'UO	LOT2/ ACQ/ ADDOS /C1	LOT2/ ACQ/ ADDOS /C2	

L'offre du candidat devra préciser le MTBF.

5.2.16.1 Adaptateurs SFP / SFP+ / QSFP+

Les adaptateurs nécessaires pour les interfaces SFP / SFP+ / QSFP+ font l'objet des UO suivants :

Référence du matériel	LOT2/ACQ/ADDOS/ADAP/SFP
Référence du matériel	LOT2/ACQ/ADDOS/ADAP/SFP+
Référence du matériel	LOT2/ACQ/ADDOS/ADAP/QSFP+

L'offre du candidat devra préciser le MTBF.

5.2.16.2 Administration centralisée

L'outil d'administration centralisée qui pourrait venir en supplément de la solution sera détaillé et fait l'objet de l'UO suivante :

Référence du matériel	LOT2/ACQ/ADDOS/OAD
-----------------------	--------------------

L'offre du candidat devra préciser le MTBF.

5.2.17 L'acquisition d'une solution SaaS⁵⁴ anti-DDOS souveraine de niveau 3 à 7

Les normes exigées pour les grandes fonctionnalités demandées ci-dessous sont synthétisées dans l'annexe " DGFIP-DGS-2500013_pas5_cctp_lot2_annexe_caracteristiques ".

Ce fichier confidentiel sera joint dans une archive séparée dont le mot de passe devra être demandé par les candidats sur la PLACE.

Il s'agit de l'acquisition d'une solution anti-DDOS de niveau 3 à 7 souveraine.

La solution anti-DDOS souveraine de niveau 3 à 7 volumétrique, permettra de protéger le SI DGFIP contre les attaques par Deni de Services Distribués volumétriques, allant de la couche 3 à la couche 7 du modèle OSI.

Cette solution devra être multi-protocolaire (Exemple : HTTP, HTTPS, DNS, SMTP et etc.), la solution devra pouvoir protéger sans déchiffrer les flux, et avec une analyse comportementale.

Le soumissionnaire fournira un équipement répondant aux fonctionnalités suivantes :

- Protection anti-DDOS de la couche 3 à la couche 7 ;
- Génération des empreintes TLS ;
- Protection contres attaques ciblant des API ;
- Capable de protéger sans déchiffrement TLS ;
- Protection contre les attaques de type "zero day" ;
- Protection contre des robots ;
- Analyse comportementale (ML) en temps réel ;
- Protection basée sur des Signatures ;
- Proposer différents mode de déploiement : transparent ou actif ;
- Blocage par Géolocalisation ;
- Blocage par ISP/ASNs ;
- Blocage/Déblocage en Masse ;
- Mécanisme de challenge adaptatif (tcp, dns, http) ;
- Protection avancée des applications non web (DNS, SMTP ..) ;
- Déploiement : **Cloud Souverain**

Référence du logiciel	LOT2/ACQ/SaaSADDOS
-----------------------	--------------------

5.2.18 L'acquisition d'une solution de Bot Manager

Les normes exigées pour les grandes fonctionnalités demandées ci-dessous sont synthétisées dans l'annexe " DGFIP-DGS-2500013_pas5_cctp_lot2_annexe_caracteristiques ".

⁵⁴software as a service (SaaS) ou logiciel en tant que service

Ce fichier confidentiel sera joint dans une archive séparée dont le mot de passe devra être demandé par les candidats sur la PLACE.

Il s'agit de l'acquisition d'une solution de Bot Manager capable de détecter et de catégoriser des bots avancés et en temps réel.

La solution de Bot Manager devra être capable de détecter et de catégoriser des bots avancés et en temps réel.

La solution devra pouvoir faire du challenge adaptatif (challenge sans captcha au captcha simple et évolutif).

En mode Hybride la solution doit pouvoir déchiffrer les flux en "On-Premise" et de faire une analyse dans le cloud, si l'offre SaaS de la solution n'est pas souveraine.

La solution devra pouvoir s'interconnecter avec l'environnement existant sans régression sur la visibilité que pourrait avoir un SOC, notamment la récupération d'adresse IP source réelle de bout en bout.

Le soumissionnaire proposera deux configurations distinctes et de dimensionnements différents correspondant à une "très petite" et "très grande" configuration (Environnement de préproduction et de production).

CARACTERISTIQUES GENERALES	MINIMUM EXIGE		REMARQUES
Bot Manager			
CONFIGURATIONS	C1	C2	
Matériel "rackable" dans une armoire standard	Impératif		1 U, modulable
Double alimentation électrique	optionnelle	obligatoire	Préciser la consommation électrique maximale (W) et le dégagement calorifique (BTU/h)
Administration du boîtier	Administrable à distance		Par interface Web sécurisée, par client léger et/ou par SSH
	Configuration par API		Préciser les méthodes et les éventuelles limitations
Interface d'administration dédiée	oui	oui	impératif
Interfaces Ethernet 1Gbps CU (minimum)	2	2	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Interfaces Giga-Ethernet SFP (minimum)	-	-	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Interfaces 10 Giga-Ethernet SFP+ (minimum)	2	2	Préciser le nombre maximum d'interfaces en standard et ses caractéristiques
Interfaces 40 Giga-	-	-	Préciser le nombre maximum

Ethernet QSFP+ (minimum)			d'interfaces en standard et ses caractéristiques
Ajout d'interface Ethernet (CU / SFP / SFP+ / QSFP+)	Optionnel		Préciser le nombre d'interfaces supplémentaires maximum et leur débit.
Débit réseau (minimum)	1 Gbps	10 Gbps	Préciser le débit maximum
Haute disponibilité	oui	oui	active/active ; active/passive
Nombre de requêtes minimum mensuel à traiter	500 Millions	10 Milliards	
Solution logicielle	-		
Codification d'UO	LOT2/ ACQ/ BOT/ C1	LOT2/ ACQ/ BOT/ C2	

L'offre du candidat devra préciser le MTBF.

5.2.18.1 Adaptateurs SFP / SFP+ / QSFP+

Les adaptateurs nécessaires pour les interfaces SFP / SFP+ / QSFP+ font l'objet des UO suivants :

Référence du matériel	LOT2/ACQ/BOT/ADAP/SFP
Référence du matériel	LOT2/ACQ/BOT/ADAP/SFP+
Référence du matériel	LOT2/ACQ/BOT/ADAP/QSFP+

L'offre du candidat devra préciser le MTBF.

5.2.18.2 Administration centralisée

L'outil d'administration centralisée qui pourrait venir en supplément des solutions d'accélération de flux sera détaillé et fait l'objet de l'UO suivante :

Référence du matériel	LOT2/ACQ/BOT/OAD
-----------------------	------------------

L'offre du candidat devra préciser le MTBF.

5.2.19 L'acquisition d'une solution d'annuaire inversée

Les normes exigées pour les grandes fonctionnalités demandées ci-dessous sont synthétisées dans l'annexe " DGFIP-DGS-2500013_pas5_cctp_lot2_annexe_caracteristiques ".

Ce fichier confidentiel sera joint dans une archive séparée dont le mot de passe devra être demandé par les candidats sur la PLACE.

Il s'agit de l'acquisition d'un service ou d'un outil permettant de rechercher la présence en ligne d'adresse mails ou encore de numéro de téléphone. La solution devra répondre aux exigences d'anonymisation des recherches et lister les sources des résultats.

La solution devra répondre aux besoins suivants :

- Ne doit pas stocker les informations soumises (soumissions anonymisées) ;
- Doit permettre de faire des recherches inversées de numéros de téléphone ;
- Doit permettre de faire des recherches inversées d'adresses mails ;
- Les recherches ne doivent pas être intrusives (OSINT) ;
- Recherche personnalisé sur des plateformes précises (Github, Gmail, Google Maps...) (en option) ;
- Possibilité d'exporter facilement les informations et sources ;
- Recherche par API (en option).

La solution devra également répondre aux spécifications suivantes :

- Récupération d'informations à partir de sources web, réseaux sociaux, base de données publiques et dark web.
- Vérification de la validité ou de l'existence du numéro ou de l'adresse email.
- Recherche des informations de l'adresse mail ou du numéro de téléphone dans des fuites de données connus.
- Trouver des informations associées comme des comptes de réseaux sociaux, des domaines ou des profils en ligne.
- Pas de journalisation des recherches de la part de la solution.
- Recherche passive sans notification vers l'utilisateur (OSINT).
- Interfaces disponibles :
 - Interface web sécurisée (HTTPS).
 - API REST (format JSON ou XML), avec documentation technique (en option).
- Exploitabilité et administration
 - Le système d'authentification doit être fort et l'interface doit permettre la recherche multiple par différents acteurs sur le même compte.

Référence du logiciel	LOT2/ACQ/ANNUAIRE_INV
-----------------------	-----------------------

5.2.20 L'acquisition d'une solution de reconnaissance faciale et d'image

Les normes exigées pour les grandes fonctionnalités demandées ci-dessous sont synthétisées dans l'annexe " DGFIP-DGS-2500013_pas5_cctp_lot2_annexe_caracteristiques ".

Ce fichier confidentiel sera joint dans une archive séparée dont le mot de passe devra être demandé par les candidats sur la PLACE.

Il s'agit de l'acquisition d'un service ou d'un outil permettant la reconnaissance d'image incorporant également la reconnaissance faciale en parcourant différentes sources sur internet (blog, réseaux sociaux, site web...). La solution devra répondre aux exigences d'anonymisation des recherches ainsi qu'une possibilité de suppression des résultats.

La solution devra répondre aux besoins suivants :

- Ne doit pas stocker les informations soumises (soumissions anonymisées) ;
- Doit permettre de faire des recherches faciales sur diverses plateformes d'images et blogs ;
- Les recherches ne doivent pas être intrusives (OSINT) ;
- Veille d'utilisation d'images (utilisation d'images pour de faux profils de fraude ou de redteam...) (en option) ;
- Capacité de demande de suppression d'images des résultats publiques ;
- Possibilité d'exporter facilement les informations et sources ;
- Recherches personnalisées sur des plateformes précises (en option) ;
- Recherche par API (en option) ;

La solution devra également répondre aux spécifications suivantes :

- Reconnaissance faciale avancée avec une analyse des traits faciaux pour identifier les correspondances, même si les angles ou la qualité des images varient.
- Affichages des vignettes des images correspondantes pour une navigation rapide ainsi que les liens vers les sites web externes ou les images sont trouvées.
- Recherche restreinte sur certaines périodes ou domaines spécifiques.
- Capacité de suppression des résultats sur l'outil ou sur le site web hébergeant l'image.
- Exportation rapide et facile d'un rapport de résultats au format PDF.
- Suivi en ligne d'une image avec système de notification ou d'API afin de suivre les traces d'un utilisateur spécifique en ligne.
- Interfaces disponibles :
 - Interface web sécurisée (HTTPS).
 - API REST (format JSON ou XML), avec documentation technique (en option).
 - Notification par Email.
- Exploitabilité et administration :
 - Le système d'authentification doit être fort et l'interface doit permettre la recherche multiple par différents acteurs sur le même compte.

Référence du logiciel	LOT2/ACQ/REC_FACIALE
-----------------------	----------------------

5.3 MAINTENANCE DES ACQUISITIONS

5.3.1 La maintenance standard (en période HO)

5.3.1.1 La description de la prestation

La fourniture de prestations consiste en la maintenance sur site des matériels et logiciels acquis dans le cadre du présent lot.

La maintenance comprendra :

- pour le matériel, l'intervention sur site d'un ou plusieurs techniciens qualifiés en cas de panne avec le remplacement s'il y a lieu des éléments défectueux et la reconfiguration, si nécessaire, de l'équipement concerné ;
- pour les logiciels :
 - la maintenance corrective du système d'exploitation des matériels et des logiciels embarqués (fourniture de patchs correctifs avec possibilité d'avoir une solution de contournement dans un premier temps). La mise en œuvre de cette correction doit prendre en compte des impacts sur les autres éléments de l'architecture dans la quelle l'équipement est intégré. Les autres incidences (sur les fonctionnalités, sur les performances) doivent être documentés. L'intervention du titulaire sur site sera laissée à l'appréciation de l'administration qui jugera le risque ou la difficulté à installer la solution ;
 - la maintenance évolutive avec la fourniture des dernières versions dès leur disponibilité et après l'accord de l'administration. L'administration peut refuser cette livraison et le titulaire s'engage à maintenir au maximum deux versions sur la durée du marché.

La maintenance porte sur un engagement de résultats.

La date de réception de la livraison ou, le cas échéant, de la prestation de service de configuration vaut point de départ.

Dans le cas où les éditeurs ou les constructeurs des logiciels et matériels concernés décideraient de leur fin de support ou fin de vie, le titulaire restera tenu par une garantie de réparation, de remplacement et de support.

Le périmètre de cette prestation couvre l'ensemble des anomalies, à savoir bloquantes et non bloquantes, lesquelles seront qualifiées par l'administration.

Les notions d'anomalies bloquante et non-bloquante sont définies au 4.5.1.1 du présent document.

Le processus de traitement doit comporter les étapes suivantes :

- l'administration (maximum 15 bénéficiaires) appelle le service concerné du titulaire entre 8h et 19h, les jours ouvrés du lundi au vendredi⁵⁵ (par téléphone (numéro vert) de préférence, par mail ou via une interface Web) ;
- le titulaire procède à l'ouverture d'un ticket d'incident (début du délai de proposition d'un plan d'action) ;
- le support rappelle l'administration et soumet une proposition de résolution ;
- l'acceptation par l'administration du plan d'action marque la fin du délai de proposition du plan d'action ;
- le titulaire intervient sur site (l'arrivée sur site marque la fin du délai d'intervention) ;
- la clôture de l'incident intervient après la phase de tests (fin du délai de solution de contournement ou de réparation).

Chaque délai débute à compter de l'ouverture du ticket chez le titulaire mais n'est décomptée que sur les périodes effectives d'intervention.⁵⁶

Synthèse des délais :

GARANTIE	DÉLAIS MAXIMUM EN HEURES OUVRÉES			
	Proposition d'un plan d'action	Intervention	Solution de contournement	Réparation
Pièces et main d'œuvre	30 mn	2 h		4 h
Garantie logicielle				
Anomalie non bloquante	8 h	3 jours	4 jours	
Anomalie bloquante	4 h	8 h	10 h	

Le titulaire met à la disposition un outil Web extranet de suivi des incidents et de partage d'informations avec la DGFIP disposant d'accès authentifiés et chiffrés et garantissant l'isolement des données propres à la DGFIP.

Le site Web doit être à jour et consulté uniquement par une liste de bénéficiaires (maximum 15 personnes) déterminée au plus tard un mois après la date de notification du marché⁵⁷.

Les soumissionnaires expliciteront les modalités d'application de la maintenance.

5.3.1.2 La fourniture de l'administration

L'administration fournit :

- la description de l'incident ;

⁵⁵ Les heures ouvrées (HO) s'envisagent au sens du calendrier de l'administration.

⁵⁶ La période d'intervention en jour ouvré est de 8 heures à 19 heures.

⁵⁷ La liste pourra être mise à jour par l'administration.

- les éléments techniques permettant la résolution de ce dernier.

5.3.1.3 Les livrables de la prestation

Le livrable est la résolution de l'incident et le rapport d'activité (état des incidents, des dossiers clos et en-cours) sera communiqué après la clôture d'incident (5 jours au plus tard) et, en fin de prestation et/ou mensuellement (selon le nombre d'unités d'œuvre commandées) à l'administration.

5.3.1.4 La définition d'unités d'œuvre

Le tableau ci-après reprend, pour chaque matériel ou logiciel, l'UO de maintenance (incluant les frais de déplacement, les pièces ainsi que la main d'œuvre) et précise la durée d'exécution. Pour chacune d'entre elle, le soumissionnaire distinguera la période où il existe une garantie constructeur ou éditeur et celle où cette garantie n'existe plus. Les garanties constructeur ou éditeur seront détaillées.

Unités d'œuvre	Sous garantie constructeur	Hors garantie constructeur
Référence	LOT2/MAINT/STD/AVECG/3M	LOT2/MAINT/SDT/HORSG/3M
Durée d'exécution	3 mois	3 mois

5.3.2 L'extension de maintenance (en période HNO)

5.3.2.1 La description de la prestation

C'est une extension de la maintenance de type standard. Elle possède les mêmes caractéristiques que cette dernière, avec cependant une couverture horaire complémentaire (HNO, soit 19h-8h, les jours ouvrés et 24h/24 les jours non ouvrés, soit week-end et jours fériés) et des délais de réactivité plus courts.

Concernant la maintenance logicielle, l'intervention du titulaire sur site sera laissée à l'appréciation de l'administration qui jugera le risque ou la difficulté à installer la solution.

Le périmètre de cette prestation couvre l'ensemble des anomalies, à savoir bloquantes et non bloquantes lesquelles seront qualifiées par l'administration.

Les notions d'anomalies bloquante et non-bloquante sont définies au 4.5.1.1 du présent document.

Synthèse des délais :

EXTENSION DE GARANTIE	DÉLAIS MAXIMUM 7J/7, 24h/24			
	Proposition d'un plan d'action	Intervention	Solution de contournement	Réparation
Pièces et main d'œuvre	15 mn	1 h		4 h
Garantie logicielle				
Anomalie bloquante non	1 h	2 h	10 h	
Anomalie bloquante	15 mn	1 h	1 h 30	

Chaque délai débute à compter de l'ouverture du ticket chez le titulaire.

Les soumissionnaires expliciteront les modalités d'application, spécifiques à cette extension de maintenance.

Les délais de la prestation d'extension de maintenance s'appliquent 24h/24, 7j/7.

5.3.2.2 La fourniture de l'administration

L'administration fournit :

- la description de l'incident ;
- les éléments techniques permettant la résolution de ce dernier.

5.3.2.3 Les livrables de la prestation

Le livrable est la résolution de l'incident et le rapport d'activité (état des incidents, des dossiers clos et en-cours) sera communiqué après la clôture d'incident (5 jours au plus tard) et, en fin de prestation et/ou mensuellement (selon le nombre d'unités d'œuvre commandées) à l'administration.

5.3.2.4 La définition d'unités d'œuvre

Le tableau ci-après reprend, pour chaque matériel ou logiciel, l'UO d'extension de maintenance (incluant les frais de déplacement, les pièces ainsi que la main d'œuvre) et précise la durée d'exécution. Pour chacune d'entre elle, le soumissionnaire distinguera la période où il existe une garantie constructeur ou éditeur et celle où cette garantie n'existe plus. Les garanties constructeur ou éditeur seront détaillées.

Unités d'œuvre	Sous garantie constructeur	Hors garantie constructeur
Référence	LOT2/MAINT/EXT/AVECG/2S	LOT2/MAINT/EXT/HORSG/2S
Durée d'exécution	2 semaines	2 semaines
Référence	LOT2/MAINT/EXT/AVECG/1M	LOT2/MAINT/EXT/HORSG/1M
Durée d'exécution	1 mois	1 mois

5.4 PRESTATIONS D'ASSISTANCE ANNEXES

5.4.1 La veille et le conseil

5.4.1.1 La description de la prestation

La prestation de veille et de conseil consiste à :

- informer, dans la limite des heures ouvrées du jour ouvré suivant, l'administration de l'existence de failles de sécurité des systèmes d'exploitation et des logiciels des équipements présents dans une configuration ;
- informer, dans les 10 jours, l'administration de l'existence de nouvelles versions de systèmes d'exploitation et des logiciels des équipements présents dans une configuration ;
- présenter la nature des correctifs ;
- mesurer, dans le cas d'un passage à une nouvelle version, les impacts de cette évolution en garantissant la cohérence de l'ensemble des versions des logiciels d'une configuration et des équipements périphériques ;
- préciser la procédure à appliquer pour changer de version logicielle (système d'exploitation, configurations) et les outils utilisés pour cet usage (s'il y en a).

La veille et le conseil permettront à l'administration de saisir le service réalisant la prestation de maintenance.

Les soumissionnaires doivent s'engager à maintenir les versions logicielles durant toute la durée du marché. L'administration, quant à elle, n'est pas tenue de faire évoluer ces mêmes versions mais peut avoir intérêt à la faire réaliser.

5.4.1.2 La fourniture de l'administration

L'administration fournit les versions et logiciels des équipements périphériques à la configuration.

5.4.1.3 Les livrables de la prestation

Le livrable est un dossier de veille, en langue française, remis en fin d'exécution d'UO.

Une présentation de ce rapport à l'administration (en Île-de-France) aura lieu dans un délai de 5 jours à l'issue de la fin de l'UO.

Les soumissionnaires fourniront un exemple de dossier de veille dans leur offre.

5.4.1.4 La définition d'unités d'œuvre

Le tableau ci-après reprend l'UO et précise la durée d'exécution.

Unité d'œuvre	Veille
Référence	LOT2/VEIL/6M
Durée d'exécution	6 mois

5.4.2 Le transfert de compétences

5.4.2.1 La description de la prestation

Le titulaire réalise un transfert de compétences pour permettre au personnel de l'administration de maîtriser les évolutions réalisées (installation d'une nouvelle configuration).

Les bénéficiaires de cette prestation sont supposés être déjà familiarisés aux technologies mises en œuvre sur le projet.

Les soumissionnaires doivent proposer un processus de transfert de compétences pouvant s'inspirer des étapes suivantes :

- établir un bilan rapide des compétences des participants et une analyse détaillée des besoins pour affiner le plan de formation ;
- définir la forme, le contenu, et le déroulement de la formation en fonction du domaine et du niveau du transfert, du profil des personnes concernées et des objectifs souhaités ;
- réaliser la formation théorique et pratique au domaine cité dans la demande ;
- établir une synthèse de l'enquête de satisfaction réalisée auprès des bénéficiaires du transfert de compétences.

Le titulaire fournit le matériel sur lequel s'effectue le transfert de compétences.

5.4.2.2 La fourniture de l'administration

L'administration fournit :

- le profil des bénéficiaires et leur niveau de connaissance ;
- le nombre exact de bénéficiaires (6 personnes maximum) ;
- les objectifs du transfert de compétences ;
- le périmètre du transfert ;
- le lieu du transfert de compétences (et la logistique associée dans les locaux de l'administration).

5.4.2.3 Les livrables de la prestation

Les livrables sont :

- un support en français sous forme papier et dématérialisé ;
- un bilan détaillé du transfert de compétences.

5.4.2.4 La définition des unités d'œuvre et la localisation

Le tableau ci-après reprend les unités d'œuvre et précise les durées d'exécution.

Unités d'œuvre	Transfert de compétences		
	Niveau simple	Niveau moyen	Niveau expert
	Mise en œuvre d'une nouvelle fonctionnalité en exploitation	Mise en œuvre d'un nouveau produit en exploitation	Transfert aux architectes maîtrise d'œuvre
Référence	LOT2/TRANS /SIMP/1J	LOT2/TRANS /MOY/3J	LOT2/TRANS /EXP/5J
Durée d'exécution	1 jour	3 jours	5 jours

Le délai de remise du bilan correspond à 5 jours (au plus tard) à partir de la fin de la durée d'exécution.

Le délai contractuel correspond au délai d'exécution additionné du délai de remise des livrables.

5.4.3 La désinstallation, le déplacement et la réinstallation de matériel

5.4.3.1 La description de la prestation

Cette prestation consiste à désinstaller physiquement (retirer de l'armoire à racks proprement), déménager et réinstaller (mise en rack et mise en service) d'un équipement d'un site vers un autre site de l'administration.

Ce déménagement concernera soit un élément rackable ou non, pris isolément, soit un ensemble d'éléments inclus dans un rack ainsi que ce dernier.

Le titulaire prend obligatoirement à sa charge l'assurance des matériels.

5.4.3.2 La fourniture de l'administration

L'administration fournit :

- la liste des équipements à déménager ;
- les contraintes de planification de l'opération (horaires des sites concernés, périodes d'indisponibilité du service) ;
- le calendrier du déménagement.

5.4.3.3 Les livrables de la prestation

Les livrables attendus sont :

- le compte rendu du déménagement comprenant notamment les éléments suivants :
 - date et heure de prise en charge ;
 - difficultés éventuelles rencontrées ;
 - date et heure de livraison sur site cible ;
 - liste et références des éléments livrés.
- le procès-verbal de livraison sur site cible.

5.4.3.4 La définition d'unités d'œuvre

Cette prestation est réalisée sous la forme d'une UO correspondant au déménagement d'un matériel d'un site vers un autre site de l'administration.

Le tableau ci-après reprend les unités d'œuvre et précise les délais d'exécution.

Désinstallation, déplacement et réinstallation					
Unités d'œuvres	Pour un élément				
	Intra Île-de-France	Province vers province		Île-de-France vers province (ou l'inverse)	
		Inférieur à 500 kms	Supérieur à 500 kms	Inférieur à 500 kms	Supérieur à 500 kms
Référence	LOT2/DEPL /ELT /IDF/5J	LOT2/DEPL/ELT /PRO-PRO/ INF-500/5J	LOT2/DEPL/ELT /PRO-PRO/ SUP-500/5J	LOT2/DEPL/ELT /IDF-PRO/ INF-500/5J	LOT2/DEPL/ELT /IDF-PRO/ SUP-500/5J
Délai d'exécution	5 jours	5 jours	5 jours	5 jours	5 jours
Unités d'œuvres	Pour plusieurs éléments				
	Intra Île-de-France	Province vers province		Île-de-France vers province (ou l'inverse)	
		Inférieur à 500 kms	Supérieur à 500 kms	Inférieur à 500 kms	Supérieur à 500 kms
Référence	LOT2/DEPL /CONF /IDF/5J	LOT2/DEPL /CONF /PRO-PRO/ INF-500/5J	LOT2/DEPL /CONF /PRO-PRO/ SUP-500/5J	LOT2/DEPL /CONF /IDF-PRO/ INF-500/5J	LOT2/DEPL /CONF /IDF-PRO/ SUP-500/5J
Délai d'exécution	5 jours	5 jours	5 jours	5 jours	5 jours

Le délai de remise des livrables correspond à 5 jours (au plus tard) à partir de la fin du délai d'exécution.

Le délai contractuel correspond au délai d'exécution additionné du délai de remise des livrables.

5.4.4 L'installation de matériel

5.4.4.1 La description de la prestation

Cette prestation consiste à installer un matériel sur un site de l'administration ou désigné par cette dernière. Ce matériel sera soit un élément rackable ou non, pris isolément, soit un ensemble d'éléments inclus dans un rack ainsi que ce dernier.

5.4.4.2 La fourniture de l'administration

L'administration fournit :

- la liste des équipements à installer et à paramétrer ;
- les contraintes de planification de l'opération (horaires des sites concernés, périodes d'indisponibilité du service) ;
- le calendrier d'installation et de paramétrage.

5.4.4.3 Le livrable de la prestation

Le livrable est le compte rendu d'installation ainsi que la fin de la prestation proprement dite.

5.4.4.4 La définition d'unités d'œuvre

Le tableau ci-après reprend, pour chaque prestation, l'UO d'installation sur un site de l'administration ou désigné par cette dernière.

Unités d'œuvre	Installation	Installation et paramétrage	Paramétrage
Pour un élément			
Référence	LOT2/INST/ELT /TYP1/1J	LOT2/INST/ELT /TYP2/1J	LOT2/INST/ELT /TYP3/1J
Délai d'exécution	1 jour	1 jour	1 jour
Pour un ensemble d'éléments			
Référence	LOT2/INST/ELTS /TYP1/1J	LOT2/INST/ELTS /TYP2/1J	LOT2/INST/ELTS /TYP3/1J
Délai d'exécution	1 jour	1 jour	1 jour

Le délai de remise des livrables correspond à 5 jours (au plus tard) à partir de la fin du délai d'exécution.

Le délai contractuel correspond au délai d'exécution additionné du délai de remise des livrables.

FIN DU DOCUMENT