CAIH

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES

LOT 3

SÉCURITÉ RÉSEAU, MAINTENANCE ET SERVICES ASSOCIÉS « ESSENTIEL »

Accord-cadre relatif aux infrastructures réseaux et services associés

Version 2026

Table des matières

6. Lot 3 - Sécurité réseau « Essentiel » 3

6.1. Objet et périmètre du lot 3

6.2. Règle de référencement des exigences et cadre de réponse technique 3

6.3. Clarifications générales applicables à la réponse 4

6.4. Fournitures sur catalogues constructeurs 6

6.5. Certifications 8

6.6. Glossaire de lecture 8

6.7. Matrice de synthèse des domaines et références BPU 8

6.8. Exigences techniques et prestations propres au lot 3 10

6.8.1. Pare-feu 10
6.8.1.1. Pare-feu périmétrique 10
6.8.1.2. Pare-feu datacenter 12
6.8.2. Solution de microsegmentation 14
6.8.3. Accès distants, portails et authentification 14
6.8.4. Sécurisation des flux Web et de la messagerie 16
6.8.4.1. Solutions de passerelles de messagerie SMTP 18
6.8.4.2. Solutions de passerelles de grand modèle de langage 20
6.8.4.3. Détection avancée, analyse comportementale et sandboxing 20
6.8.4.4. Publication et sécurisation des applications Web 22
6.8.5. Sécurisation des services d'intelligence artificielle et des flux IA 24
6.8.6. Répartition de charge et commutation applicative L5-L7 25
6.8.7. Portails captifs d'authentification 26
6.8.8. Sécurité multifonction et services de sécurité intégrés 27
6.8.9. Serveur d'authentification sécurisée 30
6.8.10. Solution de contrôle d'accès au réseau 31
6.8.11. DNS, DHCP, IPAM (DDI) et synchronisation temporelle 33
6.8.12. Détection et prévention des intrusions IDS/IPS 35
6.8.13. Protection contre les attaques par déni de service 37
6.8.14. Orchestration et administration des politiques de sécurité 39
6.8.15. Infrastructure de gestion de clés publiques PKI et gestion du cycle de vie des certificats CLM 40
6.8.16. Contrôle USB 42
6.8.17. Chiffrement LAN 43
6.8.18. Administration hors bande OOB 43
6.8.19. Accessoires, gammes constructeurs et outils d'administration 44
6.8.20. La gamme constructeur générale 44
6.8.21. Les outils d'administration constructeur/éditeur 44
6.8.22. Services professionnels, transfert de compétences et automatisation 45
6.8.23. Les prestations d'ingénierie d'audit et d'assistance générale 46
6.8.24. Les prestations d'assistance, d'intégration et d'exploitation 54
6.8.25. Les prestations d'intégration et d'exploitation 55
6.8.26. Les prestations type « Professional Services » constructeur et éditeur 59
6.8.27. Les prestations de transfert de compétences 59
6.8.28. Dispositions communes de maintenance 60
6.8.29. Automatisation 60
6.8.30. Étude de cas 61

6. Lot 3 - Sécurité réseau « Essentiel »

6.1. Objet et périmètre du lot

Le présent lot a pour objet la fourniture, l'intégration, la mise en service et la maintenance de solutions de sécurité réseau, ainsi que la réalisation des prestations d'ingénierie, d'assistance, d'exploitation, d'automatisation et de transfert de compétences associées. Il couvre notamment la protection périmétrique et datacenter, la microsegmentation, les accès distants, la sécurisation des flux Web et de messagerie, la publication applicative, la sécurité des usages d'intelligence artificielle, la répartition de charge, l'authentification, le contrôle d'accès réseau, les services DDI, la synchronisation temporelle, l'IDS/IPS, l'anti-DDoS, l'orchestration des politiques de sécurité, la PKI/CLM, le contrôle des supports USB, le chiffrement LAN et l'administration hors bande.

Le lot comprend également les prestations de maintenance associées. L'ensemble des dispositions relatives à la maintenance, au maintien en condition opérationnelle et de sécurité, au support, aux garanties, aux niveaux de service, aux délais d'intervention et de rétablissement, à la réassurance constructeur ou éditeur, au reporting, à la réversibilité et à la transférabilité est exclusivement défini dans le CCTP commun, le CCAP et les pièces financières.

[ART-301] Articulation avec le CCTP commun. Les dispositions du présent lot complètent les exigences du CCTP commun pour les seules spécificités techniques du lot 3. Le présent lot ne modifie ni ne restreint les règles communes relatives à la maintenance, aux garanties, aux niveaux de service, aux horaires de couverture, aux délais de prise en charge ou de rétablissement, aux modalités d'escalade, au reporting, aux pénalités, à la réversibilité et à la transférabilité. En cas de contradiction, les dispositions du CCTP commun prévalent, sauf dérogation expressément identifiée dans les pièces de la consultation.
Sauf indication explicite contraire, toutes les dispositions relatives à la maintenance, au MCO, au MCS et au support se réfèrent au CCTP commun. Le présent CCTP de lot ne peut qu'en préciser les modalités techniques particulières, sans réduire, remplacer ni contredire les exigences communes applicables.

Maintenance — Sauf indication explicite contraire, toutes les dispositions relatives à la maintenance se réfèrent au CCTP commun. Le présent CCTP de lot ne peut qu'en préciser les modalités techniques particulières, sans réduire, remplacer ni contredire les exigences communes applicables, notamment en matière de maintenance corrective et préventive, de support, de garantie, de niveaux de service, de reporting et de réversibilité.

Une même gamme constructeur/éditeur ne peut pas être présentée dans plus d'une solution technique. Cette variété de propositions permet aux bénéficiaires de mettre en œuvre des solutions combinées distinctes ou d'adapter au mieux la solution technique au besoin spécifique.

6.2. Règle de référencement des exigences et cadre de réponse technique

Afin de faciliter la réponse des candidats, l'analyse de conformité et la comparaison des offres, chaque demande, exigence, fonctionnalité attendue, livrable ou souhait jugé structurant peut être identifié par une référence unique. Cette référence doit être reprise par le candidat dans son cadre de réponse technique et, le cas échéant, dans les documents justificatifs associés.
La codification est construite autour d'un préfixe correspondant au domaine technique concerné, suivi d'un numéro séquentiel sur trois chiffres, selon le format DOMAINE-XXX. À titre d'exemple, les exigences relatives aux pares-feux utilisent le préfixe FW, sous la forme FW-001, FW-002, FW-003, etc. La même logique est appliquée aux autres domaines techniques du lot : MSEG, MFA, WEB, MSG, LLM, SBX, WAF, IA, LB, MULTI, NAC, DDI, IDS, DDOS, ORCH, PKI, USB, CHIFFREMENT, OOB et SERVICES.
Les références n'ont pas pour objet de modifier la portée juridique des exigences du CCTP. Elles constituent un outil de traçabilité permettant d'identifier précisément les points auxquels le candidat doit répondre et de rapprocher les réponses techniques, les éléments du BPU, les justificatifs constructeurs, les engagements de service et les livrables attendus.

Le candidat renseigne obligatoirement le cadre de réponse technique selon le modèle ci-dessous. Lorsque plusieurs solutions techniques sont proposées, le candidat indique clairement la solution concernée par chaque réponse et précise les écarts éventuels entre les solutions.
Le candidat indique pour chaque exigence le niveau de conformité, la solution concernée, la réponse détaillée, les prérequis, dépendances, limites, réserves et preuves documentaires. Une réponse limitée à une mention de conformité sans justification technique n'est pas suffisante.

Référence CCTP	Domaine	Exigence / demande / souhait	Réponse du candidat	Niveau de conformité	Justificatif / référence documentaire	Commentaires / limites éventuelles
FW-001	Pare-feu	Exigence ou fonctionnalité attendue issue du CCTP.	Réponse détaillée du candidat.	Conforme / Partiellement conforme / Non conforme	Référence constructeur, fiche technique, engagement ou annexe.	Précisions utiles à l'analyse.

Pour information, les principaux constructeurs, éditeurs ou acteurs technologiques actuellement présents ou couramment rencontrés dans les infrastructures réseau des bénéficiaires, ou susceptibles de répondre aux besoins couverts par le présent lot, sont notamment les suivants. Cette liste est indicative, non exhaustive et sans caractère prescriptif elle ne constitue ni une restriction du périmètre de réponse, ni une préférence constructeur, ni une exigence de compatibilité exclusive.

- A10
- BlueCoat/Broadcom
- Checkpoint
- Cisco
- Citrix
- F5
- Fortinet
- Hewlett Packard Entreprise/Aruba
- Juniper
- Olféo
- Palo-Alto
- Radware
- Riverbed
- Stormshield
- Systancia
- SkyHigh
- TrendMicro
- UBIKA
- Websense
- Infoblox
- EfficientIP

Les candidats demeurent libres de proposer toute solution équivalente ou alternative conforme aux exigences du CCTP, du CCTP commun et des pièces financières.

6.3. Clarifications générales applicables à la réponse

Périmètre et nombre de solutions techniques.

Le nombre de solutions techniques à présenter pour chaque domaine est défini dans le présent CCTP. Chaque solution demandée constitue une proposition cohérente et autonome, fondée sur une gamme d'un même constructeur ou éditeur et couvrant l'ensemble des besoins, équipements, logiciels, licences, accessoires et services expressément rattachés au domaine concerné. Une gamme ne peut être rattachée à plusieurs solutions d'un même domaine. L'absence d'une solution, d'une gamme ou d'une référence expressément exigée par le CCTP commun constitue un défaut de réponse à l'exigence correspondante et est appréciée selon son caractère obligatoire défini dans les pièces de la consultation.

Statut des exigences.
Sauf mention contraire, les termes « doit », « doivent », « obligatoire », « impérativement » et « a minima » identifient une exigence minimale obligatoire. Les termes « souhaité », « apprécié », « idéalement », « si possible » ou « à la marge » identifient un élément non éliminatoire pris en compte dans l'appréciation de la valeur technique lorsqu'il est rattaché à un critère ou sous-critère annoncé. Les options et exigences conditionnelles ne s'appliquent que dans les cas explicitement prévus. Le candidat indique dans le CRT, pour chaque référence, le niveau de conformité revendiqué et décrit tout écart, réserve, dépendance ou limite.

Équivalences techniques.
Lorsqu'une norme, un protocole, une technologie ou une référence est accompagné de la mention « ou équivalent », l'équivalence peut être fonctionnelle et technique. Le candidat démontre qu'elle permet d'atteindre un niveau au moins équivalent de performance, de sécurité, de disponibilité, d'interopérabilité et d'exploitabilité. La preuve repose sur une documentation officielle du constructeur ou de l'éditeur, une certification, une matrice de compatibilité, une attestation d'engagement ou, lorsque la CAIH le demande, une démonstration ou un POC. Une fonctionnalité uniquement annoncée dans une feuille de route n'est pas réputée disponible à la date limite de remise des offres et doit être signalée comme telle.

Interopérabilité et continuité de service.
L'interopérabilité attendue porte sur l'intégration des solutions proposées aux infrastructures existantes des bénéficiaires au moyen de standards ouverts et documentés. Le candidat identifie les combinaisons effectivement supportées, les éventuelles restrictions et les justificatifs associés. L'exigence de montée de version sans coupure est satisfaite soit par la conception intrinsèque de l'équipement, soit par une architecture redondante maintenant le service pendant l'opération. Toute interruption résiduelle, dépendance ou limitation est décrite dans le CRT avec les mesures compensatoires proposées.

Contenu des prix unitaires.
Le prix unitaire d'un équipement comprend tous les éléments indispensables à son installation, à son alimentation, à son démarrage, à son administration locale et à son fonctionnement nominal, notamment les alimentations et ventilateurs prévus dans la configuration de base, les kits de montage, la visserie, les cordons secteur, les accessoires de console et les licences initiales indispensables. Les cartes, modules, interfaces, extensions, licences optionnelles, abonnements, dispositifs de redondance et accessoires non indispensables à la configuration de base sont chiffrés séparément dans les lignes prévues au BPU. Aucun élément techniquement indispensable ne peut donner lieu à un coût complémentaire non identifié dans l'offre.

Licences et abonnements.
Pour chaque logiciel ou fonctionnalité, le candidat précise la métrique de licence, le périmètre couvert, la durée, le caractère perpétuel ou sous abonnement, les droits d'usage, les mises à jour incluses et les conditions de renouvellement. Lorsque plusieurs durées sont demandées au BPU, chacune fait l'objet d'un prix distinct. Les licences nécessaires au fonctionnement des caractéristiques déclarées conformes sont incluses dans le chiffrage correspondant. Aucun coût de licence ou d'abonnement non déclaré dans l'offre ne peut être facturé pendant l'exécution du marché pour assurer les fonctionnalités commandées.

Catalogues, prix publics et remises.
En complément des références explicitement tarifées au BPU, les fournitures disponibles dans les catalogues officiels des constructeurs proposés peuvent être commandées dans les conditions définies à l'article «

Fournitures sur catalogues constructeurs ». Les prix publics et taux de remise sont établis à la date limite de remise des offres sur la base du tarif officiel en vigueur du constructeur ou de l'éditeur. Le candidat fournit un justificatif daté permettant d'établir le prix public de référence. Pendant l'exécution, les évolutions de catalogue, substitutions de références et nouveaux produits sont traités selon les règles de révision et de mise à jour prévues par les pièces financières et le CCAP. Un produit de remplacement présente des performances et conditions économiques au moins équivalentes à celles du produit remplacé.

Protection des données et journalisation
Les fonctionnalités de journalisation, d'inspection, de déchiffrement ou d'analyse sont paramétrables afin de permettre au bénéficiaire de respecter la réglementation applicable, sa politique de sécurité et les principes de minimisation et de proportionnalité. Le candidat décrit les données traitées, leur localisation, leur durée de conservation, les droits d'accès, les mécanismes de purge et les possibilités d'anonymisation ou de pseudonymisation lorsqu'elles existent.

6.4. Fournitures sur catalogues constructeurs

[CAT-001] Périmètre. En complément des références explicitement tarifées au BPU, le titulaire peut fournir les équipements, logiciels, licences, abonnements, accessoires et composants figurant dans les catalogues officiels des constructeurs retenus dans son offre, dès lors qu'ils relèvent du périmètre du présent marché. Les articles non référencés individuellement au BPU peuvent ainsi faire l'objet d'un bon de commande.

[CAT-002] Catalogues de référence. Le catalogue de référence est le tarif public officiel hors taxes du constructeur ou de l'éditeur, en vigueur à la date d'émission du bon de commande. Le titulaire transmet, à première demande de la CAIH ou du bénéficiaire, tout justificatif officiel, daté et vérifiable permettant d'établir la référence, la désignation, le prix public et la date d'effet du tarif appliqué.

[CAT-003] Remises par constructeur et famille d'articles. Le candidat renseigne obligatoirement dans l'onglet « Catalogues constructeurs » du BPU, pour chaque constructeur proposé et pour chaque famille d'articles concernée, le taux de remise contractuel exprimé en pourcentage. Les familles sont définies de manière homogène et non ambiguë et couvrent notamment, lorsqu'elles existent au catalogue : commutateurs, routeurs, équipements Wi-Fi, contrôleurs, équipements de sécurité, modules et interfaces, optiques, accessoires, logiciels, licences et abonnements. Le candidat peut détailler des sous-familles, sans réduire le périmètre des familles prévues au BPU.

[CAT-004] Détermination du prix. Le prix unitaire hors taxes d'un article sur catalogue est égal au prix public officiel hors taxes applicable à la date du bon de commande, diminué de la remise contractuelle correspondant au constructeur et à la famille d'articles concernés : prix commandé HT = prix public catalogue HT × (1 − taux de remise). Aucun coefficient, frais ou marge supplémentaire ne peut être ajouté, sauf poste expressément prévu au BPU.

[CAT-005] Portée contractuelle. Les taux de remise renseignés au BPU sont fermes quant à leur niveau minimal pendant toute la durée de l'accord-cadre, sous réserve des seules modalités de révision prévues par le CCAP et les pièces financières. Toute remise plus favorable proposée ponctuellement par le constructeur ou le titulaire bénéficie au bénéficiaire. Une évolution du catalogue ne peut entraîner une diminution du taux de remise contractuel.

[CAT-006] Contrôle et traçabilité. Le titulaire fait apparaître sur le devis et, le cas échéant, sur la facture, le constructeur, la référence article, la famille d'articles, le prix public de référence, le taux de remise contractuel et le prix net résultant. Il justifie l'appartenance de l'article à la famille retenue. En cas d'erreur de classement, de divergence ou d'ambiguïté, la condition économiquement la plus favorable au bénéficiaire est appliquée, sans préjudice des stipulations du CCAP.

[CAT-007] Mise à jour des catalogues. Le titulaire informe la CAIH des évolutions de catalogue, suppressions ou substitutions de références. Toute référence de remplacement doit relever du périmètre du marché, présenter des caractéristiques et performances au moins équivalentes et être soumise au taux de remise

applicable à sa famille. La mise à jour d'un catalogue ne modifie pas, à elle seule, les engagements contractuels du titulaire.

Garantie, maintenance et ré-adossement.
La garantie incluse dans le prix d'acquisition couvre, pendant la durée indiquée par le candidat, la conformité, la réparation ou le remplacement du matériel, les frais de transport et de main-d'œuvre associés, sans préjudice des garanties légales. Les extensions de garantie, la maintenance matérielle, la maintenance logicielle et le support constructeur ou éditeur sont chiffrés séparément lorsqu'ils font l'objet de lignes distinctes au BPU. La réassurance constructeur ou éditeur est obligatoire lorsqu'elle conditionne l'accès aux correctifs, aux mises à jour, aux pièces, aux expertises de niveau supérieur ou au respect du niveau de service commandé. Le candidat en précise le contenu, la durée, le bénéficiaire, les modalités d'escalade et la preuve d'activation. Lorsqu'elle est incluse dans la garantie initiale ou dans une prestation de maintenance, elle ne fait pas l'objet d'une facturation supplémentaire. Ces dispositions s'appliquent conformément au CCTP commun, sauf indication explicite contraire.

Niveaux de service.
Les niveaux J+1 en heures ouvrées, 5 jours sur 7, et GTR 4 heures H24, 7 jours sur 7, sont proposés pour les familles de produits auxquelles une ligne de maintenance correspondante est rattachée. Ils ne sont dus qu'en cas de commande de la prestation concernée. Le délai court à compter de l'enregistrement de l'incident par le point de contact prévu au marché, sous réserve de la disponibilité des informations et accès nécessaires au diagnostic. Le candidat précise les exclusions, les modalités de remplacement, les stocks éventuellement mobilisés, les procédures d'escalade et les engagements du constructeur ou de l'éditeur. Ces dispositions s'appliquent conformément au CCTP commun, sauf indication explicite contraire.

Unités d'œuvre et dégressivité.
Chaque unité d'œuvre couvre exclusivement le périmètre, les prérequis et les livrables décrits dans la ligne correspondante du BPU et dans le CCTP. Sauf indication contraire, le prix comprend la préparation, l'exécution, les comptes rendus et livrables, ainsi que les déplacements nécessaires sur le site concerné. Les niveaux : simple, moyen et complexe sont appréciés au regard du nombre d'équipements, du nombre de sites, de l'hétérogénéité technique, des contraintes de disponibilité, des opérations de migration et du niveau d'expertise requis. La dégressivité s'applique uniquement aux prestations homogènes commandées simultanément et réalisées dans des conditions comparables. Une unité d'œuvre « validée par le constructeur ou l'éditeur » comprend la revue formelle du livrable ou de la conception par une entité habilitée, ainsi que la remise d'une preuve écrite de cette validation.

Justificatifs et études de cas.
Les réponses du CRT sont étayées par des pièces permettant de vérifier les caractéristiques annoncées. Les documents officiels du constructeur ou de l'éditeur, certifications, attestations d'engagement, matrices de compatibilité et références documentées sont recevables. La CAIH peut demander une précision, une démonstration ou un POC dans les conditions prévues par le règlement de la consultation, sans permettre la modification substantielle de l'offre. Les études de cas sont traitées selon les hypothèses, livrables et modalités de chiffrage définis dans les pièces de la consultation. Leur prise en compte dans la notation est exclusivement celle annoncée dans le règlement de la consultation.

Cohérence des pièces et références de prix.
Chaque référence de prix correspond à un objet unique décrit de manière concordante dans le CCTP, le CRT, le BPU et, le cas échéant, le DQE. En cas de discordance matérielle entre une référence et son libellé, le candidat la signale dans le délai prévu pour les questions. La CAIH publie, si nécessaire, une rectification applicable à l'ensemble des candidats. Seules les lignes et quantités prévues au scénario de notation financière concourent au calcul du prix évalué, selon les modalités du règlement de la consultation l'ensemble des prix du BPU demeure néanmoins contractuel.

6.5. Certifications

[CERT-001] L'offre indique pour chaque solution technique proposée le niveau de certification française, européenne ou étrangère associée, ainsi que les niveaux de certification de constructeurs tiers obtenus.

6.6. Glossaire de lecture

Terme	Définition
Solution technique	Produit, logiciel, appliance, service ou combinaison cohérente de composants proposé pour un domaine fonctionnel donné.
Gamme	Niveau de capacité ou de dimensionnement attendu elle ne désigne pas nécessairement une gamme commerciale constructeur.
Ensemble	Composition technique cohérente regroupant plusieurs composants nécessaires à la mise en œuvre d'un besoin.
Bundle	Ensemble prédéfini demandé au BPU, comprenant les composants, accessoires, licences et add-ons nécessaires, sauf indication contraire.
Licence	Droit d'usage d'un logiciel, module ou fonctionnalité selon les modalités de l'éditeur.
Variante	Déclinaison technique ou commerciale ne modifiant pas le périmètre fonctionnel attendu, sauf précision explicite.
Référence P	Référence de prix assurant le lien entre le CCTP et le BPU le CCTP décrit l'objet, le BPU porte les éléments financiers.

6.7. Matrice de synthèse des domaines et références BPU

Domaine	Solutions attendues	Références BPU
Pare-feu périmétriques Internet	Au moins 2	P3000 à P3020
Pare-feu datacenter	Au moins 2	P3030 à P3050
Microsegmentation	Au moins 2	P4600 à P4603
Accès distants / portail SSL	Au moins 2	P3060 à P3080
Passerelles Web	Au moins 2	P3090 à P3110
Passerelles SMTP	Au moins 2	P3120 à P3135
Passerelles LLM	Au moins 2	P4520 à P4529
Sandboxing	Au moins 2	P3150 à P3188
Publication Web / WAF	Au moins 2	P3200 à P3220
Firewalls de protection IA	Au moins 2	P4530 à P4539
Répartition de charge L5-L7	Au moins 2	P3230 à P3243
Portails captifs	Au moins 2	P3260 à P3263
Sécurité multifonction	Au moins 2	P3280 à P3300
NAC	Au moins 2	P3320 à P3340
Authentification sécurisée	Au moins 2	P3310 à P3315
DDI	Au moins 2	P3350 à P3360
Synchronisation temporelle	Au moins 2	P3370 à P3371
IDS/IPS	Au moins 2	P3380 à P3390
Anti-DDoS	Au moins 2	P3400 à P3410
Orchestration des politiques	Au moins 2	P3420 à P3430

Domaine	Solutions attendues	Références BPU
PKI / CLM	Au moins 2	P4540 à P4549
Contrôle USB	Au moins 2	P4300 à P4312
Chiffrement LAN	Au moins 2	P4400 à P4411
Administration hors bande	Au moins 2	P4500 à P4511

6.8. Exigences techniques et prestations propres au lot 3

6.8.1. Pare-feu

[FW-003] Pour chaque famille de solutions de pare-feu, le candidat précise les performances garanties avec les fonctions de sécurité activées, les capacités de raccordement, les protocoles pris en charge, les fonctions de filtrage et de protection, l'authentification, les possibilités de virtualisation ou de déploiement cloud/hybride, ainsi que les compléments spécifiques aux exigences communes d'administration, supervision, journalisation, haute disponibilité et MCS définies dans le CCTP commun, auquel il convient de se référer.

6.8.1.1. Pare-feu périmétrique

[FW-001] Les solutions de firewall « internet » existent sur le marché sous forme de logiciels ou d'appliances matérielles. Pour chacune des gammes demandées, l'offre comprend au moins deux solutions techniques matérielles distinctes (appliances).
L'ensemble des gammes demandées offre les fonctionnalités suivantes en plus de celles demandées explicitement pour chaque gamme :

- Persistance de session LAN to LAN et gestion des timeout de session.
- Translation d'adresses IP de type NAT/PAT
- Qualité de service
- Débit théorique IP avec fonction de sécurité avancée (VPN, IPS, AV…) supérieur à 25 % du débit théorique IP
- Intégration automatique de listes de filtrage d'adresses IP, noms de domaine connus comme étant à blacklister au niveau international.
- Protocoles réseau IP spécifiques à gérer :
    - IPv4, IPv6
    - Compatibilité Dicom
- Authentification : compatibilité LDAP et Active Directory, serveur d'authentification sécurisé sur site et dans le cloud (RADIUS, Microsoft Authenticator, Google Authenticator), base locale
- Haute disponibilité (lorsque demandée) : fonctionnement en cluster actif/actif ou actif/passif au choix lors de l'intégration. Synchronisation automatique des nœuds de cluster.

[FW-004] Pour chaque solution concernée, le candidat décrit l'architecture de haute disponibilité proposée, les modes actif/actif et actif/passif disponibles, la synchronisation des nœuds, la conservation des sessions lors d'une bascule, les dépendances techniques, les conditions de fonctionnement en mode dégradé et les licences nécessaires, sans en indiquer le prix dans le CRT.

[FW-005] L'offre comprend 5 gammes de firewalls en fonction de leur capacité de raccordement et de leur puissance de traitement.

Les gammes 1 et 2 correspondent à un type de firewall « basique » et ont notamment pour objectif d'être positionnées sur le LAN afin de protéger des matériels techniques spécifiques non sécurisés à l'état de l'art (matériels biomédicaux, services de gestion de bâtiments, caméras ou autres périphériques…).

Le candidat complète une fiche par famille et par gamme demandée, précisant le nombre de solutions, le positionnement, le dimensionnement, les performances minimales, les fonctionnalités incluses ou optionnelles, la haute disponibilité, l'administration et les écarts éventuels au CCTP.

Le candidat répond à chaque exigence du CCTP en indiquant sa référence, son intitulé, le niveau de conformité, la réponse détaillée, les limites, les prérequis, les options et le document justificatif associé. Les références [PXXXXX] sont conservées pour assurer le lien avec le BPU.

Règle de lecture des références de prix : chaque référence [Pxxxx] renvoie au BPU. Le BPU porte exclusivement les prix, remises, licences, abonnements, accessoires, options, variantes, tranches, durées et

frais associés. Le présent CCTP conserve l'objet technique, les performances, les quantités de solutions demandées et les conditions d'exécution.

- **[P**3000] Gamme 1 : 4 firewalls de 2 ports à 6 ports Ethernet 100/1000 Mbps minimum
    - Débit théorique IP : 1 Gbps minimum
    - Nombre de VLAN par interface Ethernet : 4
- **[P**3001] Gamme 2 : 4 firewalls de 4 ports à 6 ports Ethernet 100/1000 Mbps minimum avec au moins une interface 10 Gbps :
    - Débit théorique IP : 2 Gbps minimum
    - Nombre de VLAN par interface Ethernet : 4
- **[P**3002] Gamme 3 : 4 firewalls dont au moins deux permettant une architecture en haute disponibilité
    - 4 ports à 8 ports en Ethernet 100/1000 Mbps minimum
    - Débit théorique IP : 8 Gbps minimum
    - Fonctions de sécurité avancées :
        - Réseaux privés virtuels (VPN) de type IPsec
    - Nombre minimal de sessions en simultané : 1 000 000
    - Nombre minimal de nouvelles sessions par seconde : 40 000
    - Nombre de VLAN par interface Ethernet : 8
    - Protocoles réseau IP spécifiques à gérer :
        - RIP, OSPF
        - Compatibilité H323 et SIP, MGCP
- **[P**3003] Gamme 4 : 4 firewalls dont au moins trois permettant une architecture en haute disponibilité
    - 6 ports à 12 ports en Ethernet 100/1000 Mbps minimum dont 2 ports 10 Gbps au minimum (SFP/SFP+/QSFP)
    - Débit théorique IP hors fonction de sécurité avancée : 10 Gbps minimum
    - Fonctions de sécurité avancées :
        - Réseaux privés virtuels (VPN) de type IPsec
        - Système de Prévention d'Intrusion (IPS)
        - Analyse antivirus (AV)
    - Nombre minimal de sessions en simultané : 2 000 000
    - Nombre minimal de nouvelles sessions par seconde : 50 000
    - Nombre de VLAN par interface Ethernet : 16
    - Protocoles réseau IP spécifiques à gérer :
        - RIP, OSPF, BGP
        - Compatibilité H323 et SIP, MGCP
- [P3004] Gamme 5 : 4 firewalls en haute disponibilité dont au moins 2 doivent permettre de créer plusieurs instances indépendantes les unes des autres avec paramétrage et fonctionnement spécifique à chaque instance
    - 8 ports à 24 ports en Ethernet 1 Gbps minimum dont 4 ports 10 Gbps au minimum (SFP/SFP+/QSFP)
    - Débit théorique IP hors fonction de sécurité avancée : 40 Gbps minimum
    - Fonctions de sécurité avancées :
        - Réseaux privés virtuels (VPN) de type IPsec
        - Système de Prévention d'Intrusion (IPS)
        - Analyse antivirus (AV)
    - Protection DDoS optionnelle
    - Gestion de restrictions d'accès et de filtrage par plage horaire
    - Nombre minimal de sessions en simultané : 4 000 000
    - Nombre minimal de nouvelles sessions par seconde : 60 000
    - Nombre de VLAN par interface Ethernet : 32
    - Protocoles réseau IP spécifiques à gérer :
        - RIP, OSPF, BGP,

- IPv4, IPv6

En complément des gammes unitaires ci-dessus, l'offre fera apparaitre les gammes de bundle ci-dessous. Les gammes de bundle doivent impérativement être construites sur la base des gammes de solutions techniques ci-dessus. Les bundles comprennent les accessoires, licences et add-ons nécessaires à leur mise en œuvre.

- **[P**3010] Bundle 1 : gamme de 2 ensembles comprenant chacun
  - 2 solutions de la gamme 3 en haute disponibilité disposant des fonctionnalités de base
- **[P**3011] Bundle 2 : gamme de 3 ensembles comprenant chacun
  - 2 solutions de la gamme 4 en haute disponibilité disposant des fonctionnalités de base
- **[P**3012] Bundle 3 : gamme de 4 ensembles comprenant chacun
  - 2 solutions de la gamme 5 en haute disponibilité disposant des fonctionnalités de base

Le titulaire fournit l'une des modalités d'accès VPN suivantes :

1. Un client IPsec compatible Windows, avec indication de la compatibilité Linux et macOS toute licence associée est illimitée et forfaitaire.
2. Une compatibilité avec les clients embarqués des systèmes d'exploitation Windows, avec indication de la compatibilité Linux, macOS, Android et iOS.

[FW-006] Pour les pares-feux périmétriques, les exigences communes d'administration, supervision, journalisation, diagnostic, haute disponibilité et MCS définies dans le CCTP commun, auquel il convient de se référer s'appliquent. Le candidat précise en complément les tableaux de bord, exports, API, fonctions de diagnostic et spécificités d'administration propres aux gammes proposées.
Dans le cadre de firewall sous forme de cartes en châssis, est proposé en complément le châssis le plus petit possible permettant d'héberger ce type de firewall.
Dans le cadre de firewall fortement scalable, est proposé le "répartiteur" de firewall le plus petit avec les firewalls les plus petits compatibles. Les évolutions possibles permettant d'augmenter les capacités globales seront décrites.
[P3020] Licences, abonnements et variantes associés à la solution, selon tranches et durées définies au BPU.

6.8.1.2. Pare-feu datacenter

[FW-002] Les solutions de firewall « datacenter » existent sur le marché sous forme de logiciels ou d'appliances matérielles. Pour chacune des gammes demandées, l'offre comprend au moins deux solutions techniques matérielles distinctes (appliances).
L'ensemble des gammes demandées offre les fonctionnalités suivantes en plus de celles demandées explicitement pour chaque gamme :

- Nombre de VLAN par interface Ethernet : 256
- Persistance de session LAN to LAN et gestion des timeout de session.
- Translation d'adresses IP de type NAT/PAT
- Qualité de service
- Débit théorique IP avec fonction de sécurité avancée (VPN, IPS, AV…) supérieur à 25 % du débit théorique IP
- Nombre de sessions VPN (IPsec et SSL) simultanées minimum : 1 000
- Protocoles réseau IP spécifiques à gérer :
  - IPv4, IPv6
  - RIP, OSPF
  - Compatibilité H323 et SIP, MGCP, ICA.
  - Compatibilité Dicom
- Authentification : compatibilité LDAP et Active Directory, serveur d'authentification sécurisé sur site et dans le cloud (RADIUS, Microsoft Authenticator, Google Authenticator), base locale
- Haute disponibilité : fonctionnement en cluster actif/actif ou actif/passif au choix lors de l'intégration. Synchronisation automatique des nœuds de cluster.

[FW-007] L'offre comprend 3 gammes de firewalls en fonction de leur capacité de raccordement et de leur puissance de traitement :

- **[P**3030] Gamme 1 : 4 firewalls dont au moins 2 doivent permettre de créer plusieurs instances indépendantes les unes des autres avec paramétrage et fonctionnement spécifique à chaque instance
    - 3 ports à 7 ports avec 25% minimum des ports en Ethernet 10 Gbps (SFP/SFP+/QSFP), les autres ports en Ethernet 100/1000 Mbps minimum.
    - Débit théorique IP : 8 à 40 Gbps minimum
- **[P**3031] Gamme 2 : 4 firewalls :
    - De 6 ports à 12 ports avec 25% minimum des ports en Ethernet 25 Gbps, les autres ports en Ethernet 1/10 Gbps :
    - Débit théorique IP sans fonctionnalités de sécurité : 40 Gbps minimum
    - Fonctions de sécurité spécifiques :
        - Détection d'intrusion IDS/IPS
        - Gestion de restrictions d'accès et de filtrage par plage horaire
    - Nombre minimal de sessions en simultané : 4 000 000
    - Nombre minimal de nouvelles sessions par seconde : 150 000
    - Possibilité de créer plusieurs instances de firewall indépendantes les unes des autres avec paramétrages et fonctionnement spécifiques à chaque instance.
    - Capacité de 5 instances au minimum
- **[P**3032] Gamme 3 : 4 firewalls
    - De 6 ports à 12 ports avec 50% minimum des ports en Ethernet 40 Gbps, les autres ports en Ethernet 1/10 Gbps (SFP/SFP+/QSFP)
    - Débit théorique IP sans fonctionnalités de sécurité : 16 à 100 Gbps minimum
    - Fonctions de sécurité spécifiques :
        - Détection d'intrusion IDS/IPS
        - Gestion de restrictions d'accès et de filtrage par plage horaire
    - Nombre minimal de sessions en simultané : 50 000 000
    - Nombre minimal de nouvelles sessions par seconde : 750 000
    - Possibilité de créer plusieurs instances de firewall indépendantes les unes des autres avec paramétrages et fonctionnement spécifiques à chaque instance.
    - Capacité de 5 instances au minimum

En complément des gammes unitaires ci-dessus, l'offre fera apparaitre les gammes de bundle ci-dessous. Les gammes de bundle doivent impérativement être construites sur la base des gammes de solutions techniques ci-dessus. Les bundles comprennent les accessoires, licences et add-ons nécessaires à leur mise en œuvre.

- **[P**3040] Bundle 1 : gamme de 4 ensembles comprenant chacun
    - 2 solutions de la gamme 1 en haute disponibilité disposant des fonctionnalités de base
- **[P**3041] Bundle 2 : gamme de 4 ensembles comprenant chacun
    - 2 solutions de la gamme 2 en haute disponibilité disposant des fonctionnalités de base
- **[P**3042] Bundle 3 : gamme de 4 ensembles comprenant chacun
    - 2 solutions de la gamme 3 en haute disponibilité disposant des fonctionnalités de base

L'ensemble des gammes applique les exigences communes d'administration, supervision, journalisation, diagnostic, haute disponibilité et MCS définies dans le CCTP commun, auquel il convient de se référer.
La version logicielle de la solution inclut la fourniture du système d'exploitation lorsque celui-ci n'est pas standard et présente des caractéristiques spécifiques implémentées par l'éditeur.
Dans le cadre de firewall sous forme de cartes en châssis, est proposé en complément le châssis le plus petit possible permettant d'héberger ce type de firewall.
[P3050] Licences, abonnements et variantes associés à la solution, selon tranches et durées définies au BPU.

6.8.2. Solution de microsegmentation

[MSEG-001] Les solutions de microsegmentation existent sur le marché sous forme de logiciels. Pour chacune des gammes demandées, l'offre comprend au moins deux solutions techniques distinctes. Ces solutions peuvent être aussi disponibles avec un management on premise ou dans le cloud.
Les solutions attendues permettent la mise en œuvre d'une segmentation logique fine des charges de travail, applications et conteneurs selon une approche Zero Trust. Elles sont indépendantes de l'architecture réseau sous-jacente et peuvent, le cas échéant, s'intégrer à des infrastructures SDN ou Software Defined Datacenter existantes.

L'ensemble des gammes demandées offre les fonctionnalités suivantes :

- Interface de management centralisée
- Configuration des règles de filtrage orientée applications
- Agnostique de l'architecture réseau
- Déploiement en mode visibilité seule pour accompagner la création des matrices de flux
- Gestion granulaire des flux nord/sud et est/ouest
- Définition des règles en fonction des adresses IP source, destination, ports, processus
- Avec ou sans agent
- Compatible avec les systèmes d'exploitation serveur Microsoft et diverses distributions Linux communément répandues, notamment Red Hat, Ubuntu, Debian et SUSE.
- Compatible avec les solutions de conteneurisation type Kubernetes
- Extension possible sur les systèmes d'exploitation client
- La compatibilité avec des systèmes d'exploitation qui ne sont plus supportés par leur éditeur est appréciée
- Intégration dans l'écosystème client via API
- Traçabilité des évènements
- Authentification : compatibilité LDAP et Active Directory, Serveur d'authentification sécurisé On Premise et dans le Cloud (Radius, Microsoft Authenticator, Google Authenticator), base locale
- Haute disponibilité.
- Cartographie applicative dynamique

Gammes et références associées à la microsegmentation
Définition d'une charge de travail : une charge de travail désigne toute ressource informatique pouvant faire l'objet de politiques de microsegmentation, notamment les serveurs physiques, machines virtuelles, conteneurs et instances cloud supportés par la solution.

[P4600] Gamme 1 : jusqu'à 500 charges de travail (workload)
[P4601] Gamme 2 : jusqu'à 5 000 charges de travail.
[P4602] Gamme 3 : jusqu'à 20 000 charges de travail.
[P4603] Gamme 4 : plus de 20 000 charges de travail.

6.8.3. Accès distants, portails et authentification

[MFA-001] Le candidat décrit les services applicatifs accessibles à distance, les navigateurs et systèmes d'exploitation compatibles, les mécanismes de contrôle de conformité du poste, les annuaires et protocoles d'authentification pris en charge, l'authentification forte, les certificats, les cartes professionnelles de santé, les accès sans agent et les capacités maximales en sessions simultanées.
Les solutions de portail SSL existent sur le marché sous forme d'appliances matérielles. Pour chacune des gammes demandées, sont proposées au moins deux solutions techniques.
L'offre comprend trois gammes de portail extranet ayant pour caractéristiques et fonctionnalités communes :

- Ergonomie de présentation sous forme d'un portail web pour les utilisateurs
- Services applicatifs disponibles :
    - Web, TSE, Full IP, bureau virtuel, Microsoft Outlook Web Access, outils de prise de main à distance.

    - Support HTML 5
    - Reverse proxy Active Sync
    - Application spécifique par redirection de ports
    - Toute autre application standard du SIH nécessitant un accès à distance.
- Possibilité d'accès TSE sans installation de plugin sur le poste client sera appréciée
    - Possibilité de tester le niveau de sécurité et d'intégrité du poste client avant ouverture de connexion :
    - Version de système d'exploitation et niveau de patch système
    - Version de logiciel anti-virus et état des mises à jour
    - Présence ou absence de logiciel spécifique prédéfini
- Compatibilité avec les principaux navigateurs du marché :
    - Microsoft Edge
    - Firefox
    - Safari
    - Chrome
    - Opéra
- Authentification :
    - Compatibilité LDAP et Active Directory, serveur d'authentification sécurisé sur site et dans le cloud (RADIUS, Microsoft Authenticator, Google Authenticator), TACACS+ multiples, base locale
    - Filtrage d'accès IP en VPN par authentification via serveur d'authentification sécurisé sur site et dans le cloud (RADIUS, Microsoft Authenticator, Google Authenticator) et TACACS+
    - Compatibilité avec la gestion de l'authentification forte par carte à jeton et Carte Professionnelle de Santé (CPS) ou carte sécurisée hébergeant le certificat CPS
    - Authentification par certificat embarqué sur le client
- Contrôle des adresses publiques entrantes
- Haute disponibilité : fonctionnement en cluster actif/actif, ou actif/passif. Synchronisation automatique des nœuds de cluster.

[MFA-006] L'offre comprend 3 gammes de portail extranet en fonction de leur puissance de traitement :
[P3060] Gamme 1 de 4 solutions : capacité 500 sessions simultanées
[P3061] Gamme 2 de 4 solutions : capacité 2500 sessions simultanées
[P3062] Gamme 3 de 4 solutions : capacité 5000 sessions simultanées

En complément des gammes unitaires ci-dessus, l'offre fera apparaitre les gammes de bundle ci-dessous. Les gammes de bundle doivent impérativement être construites sur la base des gammes de solutions techniques ci-dessus. Les bundles comprennent les accessoires, licences et add-ons nécessaires à leur mise en œuvre.

- **[P**3070] Bundle 1 : gamme de 4 ensembles comprenant chacun
  2 solutions de la gamme 1 en haute disponibilité disposant des fonctionnalités de base du produit
- **[P**3071] Bundle 2 : gamme de 4 ensembles comprenant chacun
  2 solutions de la gamme 2 en haute disponibilité disposant des fonctionnalités de base du produit
- **[P**3072] Bundle 3 : gamme de 4 ensembles comprenant chacun
  2 solutions de la gamme 3 en haute disponibilité disposant des fonctionnalités de base du produit

L'ensemble des gammes proposées dispose des fonctionnalités communes suivantes :

- Une ergonomie et capacité d'administration avancées, grâce à une interface graphique accessible via interface Web, y compris pour la gestion de la haute disponibilité. L'interface d'administration est unique pour les deux gammes.
- Des fonctionnalités de supervision temps réel telles que :
    - Suivi de l'utilisation applicative
    - Compteurs d'usage par application
- Une gestion des logs :
    - Traçabilité complète des flux, des erreurs.

    - Export pour stockage et analyse vers une solution de supervision externe des journaux de logs. L'offre précise les outils nécessaires à leur gestion.
    - L'offre comprend les tableaux de bord de base disponibles (trafic par protocole, source et destinataire, alarmes, sites les plus utilisés…)
- Des fonctionnalités d'aide au diagnostic tel qu'un debug des fonctionnalités et protocoles, une visualisation des processus utilisant la CPU, une visualisation de l'utilisation de la mémoire... Les fichiers de debug peuvent être exportés pour stockage et analyse dans un environnement micro-informatique. L'offre précise les outils nécessaires à leur gestion.
- La version logicielle de la solution inclut la fourniture du système d'exploitation lorsque celui-ci n'est pas standard et présente des caractéristiques spécifiques implémentées par l'éditeur.

[P3080] Licences, abonnements et variantes associés à la solution, selon tranches et durées définies au BPU.

6.8.4. Sécurisation des flux Web et de la messagerie

[WEB-006] Le candidat décrit les protocoles, le filtrage URL et contenu, le déchiffrement SSL, les protections antivirus, antimalware, anti ransomware, anti-hameçonnage et antispam, l'analyse MIME, les quarantaines, la décompression, les mises à jour de signatures, les profils utilisateurs, les notifications, les performances et l'intégration avec une sandbox.

[WEB-001] Les passerelles web peuvent être proposées sous forme matérielle, logicielle, virtuelle, sur site, cloud ou hybride. Pour chaque gamme demandée, l'offre présente au moins deux solutions et, le cas échéant, les variantes logicielles ou virtuelles associées.

Les solutions de cette catégorie sont destinées principalement à la sécurisation des flux utilisateurs sortants vers Internet. Les fonctions de publication d'applications, de répartition de charge et de protection applicative relèvent des catégories dédiées correspondantes.

[WEB-002] L'offre comprend cinq gammes de passerelles web ayant pour caractéristiques et fonctionnalités communes :

- Dans le cas d'une solution matérielle : 2 ports Ethernet 1000 Mbps au minimum à 2 ports Ethernet 10 Gbps.
- Fonctions de filtrage temps réel, soit de base, soit sous forme de briques applicatives optionnelles :
    - Filtrage URL :
        - Sur contenu : listes noires, listes blanches, mots clés…
        - Sur adresses IP ou nom de domaine destinataire.
        - Sur adresse de site à partir d'une banque de données :
        - Filtrage par profil utilisateur
        - Filtrage par classification thématique des sites
    - Décryptage de flux SSL pour filtrage
    - Filtrage de fichiers de type MIME
    - Horaire par instance et par profils utilisateur.
    - Filtrage de protocole (streaming)
    - Analyse des flux ICAP pour le filtrage http/ /VIRUS/URL
    - Analyse de contenu
    - Filtrage anti-virus :
        - Protection contre les virus, malware/spyware, ransomware
        - Protection contre l'hameçonnage
        - Sur contenu : listes noires, listes blanches, mots clés…
        - Sur adresses IP ou nom de domaine (émetteur et destinataire)
        - Décompression des fichiers téléchargés pour analyse (5 niveaux minimum)
    - Compatibilité avec les principaux navigateurs du marché :
        - Microsoft Edge
        - Firefox
        - Safari
        - Chrome
        - Opéra

- Mise à jour des fichiers de signatures (virus, spywares, malwares…), de listes noires, banque de données d'URL et des moteurs logiciels associés automatiques et paramétrables avec une granularité au minimum de l'ordre de 30 minutes.
- Gestion de profils
- Authentification :
  - Annuaire local
  - Compatibilité LDAP et Active Directory, serveur d'authentification sécurisé sur site et dans le cloud (RADIUS, Microsoft Authenticator, Google Authenticator), TACACS+ multiples
- Notifications multiples activables/désactivables des actions réalisées sur les flux vers les destinataires et/ou administrateurs.
- Haute disponibilité lorsqu'elle est demandée :
  - Fonctionnement en cluster actif/actif ou actif/passif. Synchronisation automatique des nœuds de cluster.
- Fonctionnalités proxy lorsqu'elle est demandée :
  - Protocoles à gérer http, ftp, https, smtp, Citrix, LDAP et Active Directory
  - Possibilité de transférer les protocoles ci-dessus sur d'autres ports que les ports normalisés
  - Réexpédition de flux smtp et http sur nom de domaine.
  - Routage en fonction de profils liés à des groupes d'utilisateurs
  - Analyse des flux ICAP pour le filtrage http/SMTP/VIRUS/URL
  - Fonction cache

[WEB-005] Les 5 gammes de passerelles internet-web :

- **[P**3090] Gamme 1 : 4 passerelles web dont au moins 2 doivent permettre la haute disponibilité :
  - Capacités de 250 sessions simultanées
  - Bande passante de 100 Mbps
- **[P**3091] Gamme 2 : 4 passerelles web permettant la haute disponibilité dont au moins 2 proposant des fonctions de « proxyfication »
  - Capacité de 5 000 sessions simultanées
  - Bande passante de 400 Mbps
- **[P**3092] Gamme 3 : 4 passerelles web permettant la haute disponibilité dont au moins 2 permettent le déchiffrement SSL et le filtrage de fuites de données
  - Capacité de 10 000 sessions simultanées
  - Bande passante de 1 Gbps
- **[P**3093] Gamme 4 : 4 passerelles web permettant la haute disponibilité dont au moins 2 proposant des fonctions de « proxyfication »
  - Capacité de 20 000 sessions simultanées
  - Bande passante de 1,15 Gbps
- **[P3094**] Gamme 5 de 4 passerelles web permettant la haute disponibilité dont au moins 2 proposant des fonctions de « proxyfication »
  - Capacité de 50 000 sessions simultanées
  - Bande passante de 2,5 Gbps

En complément des gammes unitaires ci-dessus, l'offre fera apparaitre les gammes de bundle ci-dessous. Les gammes de bundle doivent impérativement être construites sur la base des gammes de solutions techniques ci-dessus. Les bundles comprennent les accessoires, licences et add-ons nécessaires à leur mise en œuvre.

- **[P**3100] Bundle 1 : gamme de 2 ensembles comprenant chacun
  2 solutions de la gamme 1 en haute disponibilité disposant des fonctionnalités de base du produit
- **[P**3101] Bundle 2 : gamme de 4 ensembles comprenant chacun
  2 solutions de la gamme 2 en haute disponibilité disposant des fonctionnalités de base du produit
- **[P**3102] Bundle 3 : gamme de 4 ensembles comprenant chacun
  2 solutions de la gamme 3 en haute disponibilité disposant des fonctionnalités de base du produit

- [P3103] Bundle 4 : gamme de 4 ensembles comprenant chacun
  2 solutions de la gamme 4 en haute disponibilité disposant des fonctionnalités de base du produit
- [P3104] Bundle 5 : gamme de 4 ensembles comprenant chacun
  2 solutions de la gamme 5 en haute disponibilité disposant des fonctionnalités de base du produit

[WEB-003] L'ensemble de la gamme dispose des fonctionnalités suivantes :

- Une ergonomie et capacité d'administration avancées, grâce à une interface graphique accessible via interface Web, y compris pour la gestion de la haute disponibilité. L'interface d'administration est unique pour toute la gamme.
- Une gestion des logs :
  - Le contenu des logs doit respecter la législation française en vigueur
  - Traçabilité complète des flux, des erreurs.
  - Export pour stockage et analyse vers une solution de supervision externe des journaux de logs. L'offre précise les outils nécessaires à leur gestion.
  - L'offre comprend les tableaux de bord de base disponibles (trafic par protocole, source et destinataire, alarmes, sites les plus utilisés, trafic par utilisateur, sites par utilisateur…)
- Des fonctionnalités d'aide au diagnostic tel qu'un debug des fonctionnalités et protocoles, une visualisation des processus utilisant la CPU, une visualisation de l'utilisation de la mémoire... Les fichiers de debug doivent pouvoir être exportés pour stockage et analyse dans un environnement micro-informatique. L'offre précise les outils nécessaires à leur gestion.
- La version logicielle de la solution inclut la fourniture du système d'exploitation lorsque celui-ci n'est pas standard et présente des caractéristiques spécifiques implémentées par l'éditeur.

[WEB-004] L'offre détaille les modes de catégorisation des sites pour le filtrage anti-virus et filtrage d'URL, ainsi que la fréquence de mise à jour des fichiers de signatures (virus, spywares, malwares), de listes noires, des banques de données d'URL et des moteurs logiciels associés.
L'offre comprend le niveau de performance de la solution proposée (débit et flux simultanés…).
[P3110] Licences, abonnements et variantes associés à la solution, selon tranches et durées définies au BPU.

6.8.4.1. Solutions de passerelles de messagerie SMTP

[MSG-001] Les passerelles SMTP peuvent être proposées sous forme logicielle, matérielle ou cloud. Pour chaque gamme demandée, l'offre présente au moins deux solutions et, le cas échéant, les variantes logicielles, virtuelles, sur site, cloud ou hybrides associées.

[MSG-002] L'offre comprend six gammes de passerelles smtp ayant pour caractéristiques et fonctionnalités :

- Dans le cas d'une solution matérielle : 2 ports Ethernet 100/1000 Mbps au minimum
- Protocoles supportés SMTP, SMTPs IMAP, IMAPs, POP3, POP3s
- Fonctions de filtrage temps réel :
  - Type MIME
  - Par profils utilisateur.
  - Sur adresse IP ou nom de domaine émetteur ou destinataire.
  - Filtrage anti-virus :
    - Protection contre les virus, malware/spyware
    - Sur contenu : listes noires, listes blanches, mots clés…
  - Filtrage anti-spam avec niveau de sensibilité définie sur la base de critères multiples. L'offre précise la souplesse de définition de la sensibilité disponible.
  - Filtrage sur requête DNS inverse
  - Décompression des pièces jointes pour analyse (5 niveaux minimum)
  - Gestion des quarantaines :
    - Outil de recherche multicritère ergonomique
    - Possibilité de délégation de la gestion/recherche de la quarantaine à d'autres utilisateurs que l'administrateur, tels que les destinataires.

- Mise à jour des fichiers de signatures (virus, spywares, malwares), de listes noires, et des moteurs logiciels associés automatiques et paramétrables avec une granularité au minimum de l'ordre de 30 minutes
- Authentification :
  - Annuaire local
  - Compatibilité LDAP et Active Directory, Serveur d'authentification sécurisé On Premise et dans le Cloud (Radius, Microsoft Authenticator, Google Authenticator), Tacacs multiples
- Notifications multiples activables/désactivables des actions réalisées sur les messages vers les émetteurs et/ou destinataires et/ou administrateurs.
- Haute disponibilité lorsqu'elle est demandée :
  - Fonctionnement en cluster actif/actif ou actif/passif. Synchronisation automatique des nœuds de cluster.
- Mode transparent possible pour les architectures avec Sandbox lorsque cette dernière fonction n'est plus disponible afin de ne pas bloquer les flux de messagerie.

[MSG-003] Les 6 gammes de passerelles de messagerie SMTP :

- **[P**3120] Gamme 1 de 4 passerelles de messagerie dont au moins deux permettent la haute disponibilité
  - Capacité de 4000 mails par heure
- **[P**3121] Gamme 2 de 4 passerelles de messagerie permettant la haute disponibilité dont au moins 2 permettent le filtrage en sandbox (déporté ou non)
  - Capacité de 10 000 mails par heure
- **[P**3122] Gamme 3 de 4 passerelles de messagerie permettant la haute disponibilité dont au moins 2 permettent le filtrage en sandbox (déporté ou non)
  - Capacité de 100 000 mails par heure
- **[P**3123] Gamme 4 de 4 passerelles de messagerie permettant la haute disponibilité dont au moins 2 permettent le filtrage en sandbox (déporté ou non)
  - Capacité de 500 000 mails par heure
- **[P**3124] Gamme 5 de 4 passerelles de messagerie permettant la haute disponibilité dont au moins 2 permettent le filtrage en sandbox (déporté ou non)
  - Capacité de 1 000 000 de mails par heure
- **[P**3125] Gamme 6 de 4 passerelles de messagerie permettant la haute disponibilité dont au moins 2 permettent le filtrage en sandbox (déporté ou non)
  - Capacité de 1 500 000 mails par heure

En complément des gammes unitaires ci-dessus, l'offre fera apparaitre les gammes de bundle ci-dessous. Les gammes de bundle doivent impérativement être construites sur la base des gammes de solutions techniques ci-dessus. Les bundles comprennent les accessoires, licences et add-ons nécessaires à leur mise en œuvre.

- **[P**3130] Bundle 1 : gamme de 2 ensembles comprenant chacun
  2 solutions de la gamme 1 en haute disponibilité disposant des fonctionnalités de base du produit
- **[P**3131] Bundle 2 : gamme de 4 ensembles comprenant chacun
  2 solutions de la gamme 2 en haute disponibilité disposant des fonctionnalités de base du produit
- **[P**3132] Bundle 3 : gamme de 4 ensembles comprenant chacun
  2 solutions de la gamme 3 en haute disponibilité disposant des fonctionnalités de base du produit
- **[P**3133] Bundle 4 : gamme de 4 ensembles comprenant chacun
  2 solutions de la gamme 4 en haute disponibilité disposant des fonctionnalités de base du produit
- **[P**3134] Bundle 5 : gamme de 4 ensembles comprenant chacun
  2 solutions de la gamme 5 en haute disponibilité disposant des fonctionnalités de base du produit
- **[P**3135] Bundle 6 : gamme de 4 ensembles comprenant chacun
  2 solutions de la gamme 6 en haute disponibilité disposant des fonctionnalités de base du produit

[MSG-004] Pour l'ensemble des passerelles de messagerie, les exigences communes d'administration, supervision, journalisation, export des traces, diagnostic, haute disponibilité, MCS et fourniture du système d'exploitation spécifique le cas échéant sont celles définies dans le CCTP commun, auquel il convient de se référer. Le candidat précise uniquement les compléments propres aux flux de messagerie, aux quarantaines, aux mises à jour de signatures et aux performances attendues.

6.8.4.2. Solutions de passerelles de grand modèle de langage

[LLM-001] Pour chaque passerelle de grand modèle de langage proposée, le candidat décrit les modes de déploiement disponibles, les modèles pris en charge, les fonctions de routage, de mise en cache et de limitation de débit, les mécanismes de contrôle d'accès, les capacités d'observabilité et les modalités d'application des règles de gouvernance de l'IA du bénéficiaire.
La solution permet au bénéficiaire de centraliser et sécuriser les usages des modèles de langage, qu'ils soient internes, hébergés sur site, fournis en mode cloud ou accessibles via des services externes. Elle précise les conditions d'interconnexion avec les applications clientes, les API et les plateformes d'IA utilisées par le bénéficiaire.
Les solutions de cette catégorie assurent principalement le contrôle, la gouvernance et la sécurisation des échanges entre les utilisateurs, applications ou agents et les modèles d'intelligence artificielle. Les fonctions de protection des modèles IA peuvent être complémentaires.
La passerelle prend en charge plusieurs modèles et permet, selon les règles définies, le routage des requêtes vers le modèle le plus approprié, la mise en cache des réponses autorisées, le suivi des consommations, la limitation de débit et l'application de politiques d'accès par profil, rôle ou application.
Pour les passerelles de grand modèle de langage, les exigences communes d'observabilité, journalisation, audit, reporting, alerte, supervision et MCS sont celles définies dans le CCTP commun, auquel il convient de se référer. Le candidat précise uniquement les compléments propres aux usages IA, notamment le suivi des requêtes, des modèles sollicités, des coûts, des erreurs, des accès et des événements de sécurité associée aux échanges avec les modèles de langage.

- [P4520] Gamme 1 : passerelle LLM destinée aux usages initiaux ou maîtrisés, couvrant le contrôle des accès, le routage des requêtes, les journaux d'usage et les politiques de gouvernance IA de base.
- [P4521] Gamme 2 : passerelle LLM destinée aux usages intermédiaires ou mutualisés, intégrant des capacités renforcées de supervision, de limitation de débit, de suivi des consommations et de contrôle par profil, application ou rôle.
- [P4522] Gamme 3 : passerelle LLM destinée aux usages avancés ou critiques, intégrant des fonctions étendues de gouvernance, d'observabilité, de journalisation, de contrôle des modèles sollicités, de gestion des erreurs et d'intégration avec l'écosystème de sécurité du bénéficiaire.

[P4529] Licences, abonnements et variantes associés aux passerelles LLM, selon tranches, métriques et durées définies au BPU.

6.8.4.3. Détection avancée, analyse comportementale et sandboxing

[SBX-004] Le candidat décrit les flux analysés, les environnements d'exécution disponibles, les capacités d'analyse simultanée, les volumes de fichiers traités, la décompression, le suivi des URL, l'analyse comportementale, les mécanismes anti-évasion, les règles YARA, les listes d'adresses et d'empreintes, la soumission manuelle, les notifications et l'intégration avec les passerelles Web, les passerelles de messagerie et les pares-feux.

[SBX-001] Les solutions de bac à sable et analyse comportementale existent sur le marché sous forme de logiciels ou d'appliances matérielles ou de services dans le cloud. Pour chacune des gammes de bac à sable demandées, sont proposées au moins deux solutions techniques matérielles (appliance) ou sous formes logicielles lorsqu'elles sont intégrées à des solutions de type passerelle de messagerie, passerelle Internet ou firewall périmétrique.

[SBX-002] L'offre comprend huit gammes de solution de bac à sable ayant pour caractéristiques et fonctionnalités communes :

- Dans le cas d'une solution matérielle : 2 ports Ethernet 100/1000 Mbps au minimum
- Filtrage des flux de messagerie

Hébergement de machines virtuelles représentatives de l'environnement de l'établissement (compatibilité avec les versions actuellement maintenues de Windows)

- Exécution de contenu en environnements virtuels cloisonnés
- Décompression des fichiers pour analyse (5 niveaux minimum)
- Suivi des URL et téléchargement des fichiers si nécessaire lors de l'exécution du contenu
- *Analyse comportementale de l'exécution du contenu
    - Écriture sur le disque
    - Modification de la base de registre
    - Accès internet (serveurs de commande et contrôle)
    - Installation de virus
- *Mécanismes de leurre permettant de dissimuler l'environnement d'exécution en sandbox pour le contenu en cours d'analyse
- *Possibilité de soumettre du contenu manuellement
- *Filtrage sur listes noires :
    - D'adresses IP
    - D'empreintes
    - De règles YARA
- *Notifications multiples activables/désactivables des actions réalisées vers les administrateurs.
- *Haute disponibilité lorsqu'elle est demandée :
    - Fonctionnement en cluster actif/actif ou actif/passif. Synchronisation automatique des nœuds de cluster.
    - Possibilité d'installation des passerelles en mode multi-machines sans redondance des achats de licence (coût de licence non lié au nombre de machines installées)

[SBX-003] Les solutions de bac à sable peuvent analyser les fichiers sur les flux de type messagerie (SMTP) et navigation web (HTTP). Deux types de gammes seront demandés : les gammes spécifiques pour les flux de messagerie et les gammes permettant de traiter les deux types de flux.

Gammes spécifiques pour les flux de messagerie :

- **[P**3150] Gamme 1 : Capacité de 4 analyses simultanées ou 500 fichiers/heure
- **[P**3151] Gamme 2 : Capacité de 8 analyses simultanées ou 1000 fichiers/heure
- **[P**3152] Gamme 3 : Capacité de 20 analyses simultanées ou 5000 fichiers/heure
- **[P**3153] Gamme 4 : Capacité de 50 analyses simultanées ou 12.000 fichiers/heure

Gammes permettant de traiter les flux de messagerie et les flux de navigation web :

- **[P**3160] Gamme 5 : Capacité de 4 analyses simultanées ou 500 fichiers/heure
- **[P**3161] Gamme 6 : Capacité de 8 analyses simultanées ou 1000 fichiers/heure
- **[P**3162] Gamme 7 : Capacité de 20 analyses simultanées ou 5.000 fichiers/heure
- **[P**3163] Gamme 8 : Capacité de 50 analyses simultanées ou 12.000 fichiers/heure

[SBX-006] En complément des gammes de bac à sable, l'offre comprend également une gamme d'au moins deux solutions techniques d'analyse comportementale dont la principale fonctionnalité est la détection de signaux faibles sur les flux réseau :
[P3170] Gamme de deux solutions d'analyse comportementale permettant la détection de signaux faibles

- Capacité de 10 Gigabits par seconde

En complément des gammes unitaires ci-dessus, l'offre fera apparaitre, lorsqu'elles existent, les gammes de bundle ci-dessous.
Les gammes de bundle doivent impérativement être construites sur la base des gammes de solutions techniques ci-dessus. Les bundles comprennent les accessoires, licences et add-ons nécessaires à leur mise en œuvre.

- **[P**3180] Bundle 1 : gamme de 4 ensembles comprenant chacun
  2 solutions de la gamme 1 en haute disponibilité disposant des fonctionnalités de base du produit

- **[P**3181] Bundle 2 : gamme de 4 ensembles comprenant chacun
  2 solutions de la gamme 2 en haute disponibilité disposant des fonctionnalités de base du produit
- **[P**3182] Bundle 3 : gamme de 4 ensembles comprenant chacun
  2 solutions de la gamme 3 en haute disponibilité disposant des fonctionnalités de base du produit
- **[P**3183] Bundle 4 : gamme de 4 ensembles comprenant chacun
  2 solutions de la gamme 4 en haute disponibilité disposant des fonctionnalités de base du produit
- **[P**3184] Bundle 5 : gamme de 4 ensembles comprenant chacun
  2 solutions de la gamme 5 en haute disponibilité disposant des fonctionnalités de base du produit
- **[P**3185] Bundle 6 : gamme de 4 ensembles comprenant chacun
  2 solutions de la gamme 6 en haute disponibilité disposant des fonctionnalités de base du produit
- **[P**3186] Bundle 7 : gamme de 4 ensembles comprenant chacun
  2 solutions de la gamme 7 en haute disponibilité disposant des fonctionnalités de base du produit
- **[P**3187] Bundle 8 : gamme de 4 ensembles comprenant chacun
  2 solutions de la gamme 8 en haute disponibilité disposant des fonctionnalités de base du produit
- **[P**3188] Bundle 9 : gamme de 2 ensembles comprenant chacun
  2 solutions de la gamme de solutions d'analyse comportementale en haute disponibilité disposant des fonctionnalités de base du produit

[SBX-005] Pour l'ensemble des solutions de sandboxing et d'analyse comportementale, les exigences communes d'administration, supervision, journalisation, export des traces, diagnostic, haute disponibilité, MCS et fourniture du système d'exploitation spécifique le cas échéant sont celles définies dans le CCTP commun, auquel il convient de se référer. Le candidat précise uniquement les compléments propres aux environnements d'analyse, aux mécanismes anti-évasion, aux soumissions manuelles, aux notifications et aux capacités de traitement.

6.8.4.4. Publication et sécurisation des applications Web

[WAF-002] Le candidat décrit, pour chaque solution de publication Web ou de répartition de charge, les protocoles pris en charge, les fonctions de reverse proxy, de chiffrement et de déchiffrement, les protections applicatives, les algorithmes de répartition, la persistance des sessions, les contrôles de disponibilité, les performances HTTP/S et L4-L7, ainsi que les compléments spécifiques aux exigences communes d'administration, supervision, journalisation, diagnostic, haute disponibilité et MCS définies dans le CCTP commun, auquel il convient de se référer.

[WAF-001] Les solutions de portails de publication et de sécurisation d'applications web existent sur le marché sous forme de logiciels ou d'appliances matérielles. L'offre comprend au moins deux solutions techniques distinctes. Pour chacune des gammes demandées, l'offre présente soit une solution technique matérielle (appliance), soit une solution sous forme logicielle. La version logicielle de la solution inclut la fourniture du système d'exploitation lorsque celui-ci n'est pas standard et présente des caractéristiques spécifiques implémentées par l'éditeur, conformément au CCTP commun.
La présente section couvre à la fois les fonctions de publication sécurisée d'applications Web, notamment de type reverse proxy, et les fonctions de protection applicative avancée de type WAF. Les solutions attendues peuvent donc assurer l'exposition contrôlée d'applications vers des utilisateurs externes ainsi que leur protection contre les attaques applicatives. Les fonctions éventuelles de répartition de charge ou d'optimisation du trafic sont considérées comme complémentaires et ne constituent pas le périmètre principal de cette section.

[WAF-004] Les fonctionnalités communes aux 3 gammes de portails demandés sont :

- Compatibilité avec les principaux navigateurs du marché :
  - Microsoft Edge
  - Firefox
  - Safari
  - Chrome
  - Opéra

    - Indiquer la compatibilité avec les OS et navigateurs de terminaux mobiles (smartphones, tablettes…)
- Services applicatifs disponibles :
    - Entièrement compatible avec tout le protocole IP V4 et V6
- Haute disponibilité : fonctionnement en cluster actif/actif ou actif/passif.
- Possibilité d'installation des portails en mode multi-machines sans redondance des achats de licence (coût de licence non lié au nombre de machines installées)

L'ensemble des gammes dispose des fonctionnalités suivantes :

- Une ergonomie et capacité d'administration avancées, grâce à une interface graphique accessible via interface Web, y compris pour la gestion de la haute disponibilité. L'interface d'administration est unique pour toute la gamme. Elle permet un rendu graphique des résultats des optimisations.
- Une gestion des logs :
    - Traçabilité complète des flux, des erreurs.
    - Export pour stockage et analyse vers une solution de supervision externe des journaux de logs. L'offre précise les outils nécessaires à leur gestion.
    - L'offre comprend les tableaux de bord de base disponibles (trafic par protocole, source et destinataire, alarmes, trafic par utilisateur…)
- Des fonctionnalités d'aide au diagnostic tel qu'un debug des fonctionnalités et protocoles, une visualisation des processus utilisant la CPU, une visualisation de l'utilisation de la mémoire... Les fichiers de debug doivent pouvoir être exportés pour stockage et analyse dans un environnement micro-informatique. L'offre précise les outils nécessaires à leur gestion.

[WAF-003] Pour leur administration, les solutions proposées supportent les standards :

- SSHv2
- SNMP v3
- NTP
- TFTP
- Serveur d'authentification sécurisé On Premise et dans le Cloud (Radius, Microsoft Authenticator, Google Authenticator) et Tacacs

Les comptes administrateurs peuvent être gérés à travers un serveur AAA et plusieurs niveaux d'administration sont supportés.

Une interface web ainsi qu'une interface en ligne de commande permettent de configurer l'ensemble des fonctionnalités des équipements.

- **[P**3200] Gamme 1 : solution de publication d'applications web n'intégrant pas de fonctions de sécurité avancées, communément appelés reverse proxy :
    - Au moins 3 configurations de densité de 2 ports Ethernet 1 Gbps minimum
    - Débit théorique de traitement HTTP/S : de 100 Mbps à 250 Mbps
    - Nombre de transactions : de 250 à 1 000 transactions HTTP/S par seconde minimum
- **[P**3201] Gamme 2 : solution de publication d'applications web intégrant des fonctions de chiffrement/déchiffrement :
    - Au moins 3 configurations de densité de 2 ports Ethernet 1 Gbps minimum
    - Débit théorique de traitement HTTP/S : de 250 Mbps à 1 Gbps
    - Nombre de transactions : de 1 000 à 10 000 transactions HTTP/S par seconde minimum
- **[P**3202] Gamme 3 : solution de publication d'applications web intégrant des fonctions de sécurité avancées, communément appelés pares-feux applicatifs :
    - Au moins 3 configurations de densité de 2 ports Ethernet 1 Gbps à 2 ports 10 Gbps minimum
    - Débit théorique de traitement HTTP/S : de 1 Gbps à 10 Gbps
    - Nombre de transactions : de 10 000 à 30 000 transactions HTTP/S par seconde minimum
    - Protection contre les attaques de type web, dont à minima :
    - Détection d'attaques connues par consultation d'une base de signatures
    - Détection d'attaques connues par analyse comportementale des requêtes HTTP
    - Détection d'injections de codes
    - Détection de balises cachées ou interdites
    - Détection de valeurs non autorisées dans les champs de formulaires

- **[P**3210] Bundle 1 : ensemble comprenant :
    - 2 solutions de la gamme 1 en haute disponibilité
    - 2 ports Ethernet 1 Gbps chacun
    - Débit théorique de traitement HTTP/S : de 100 Mbps à 250 Mbps
    - Nombre de transactions : de 250 à 1 000 transactions HTTP/S par seconde minimum
- **[P**3211] Bundle 2 : ensemble comprenant :
    - 2 solutions de la gamme 2 en haute disponibilité
    - 2 ports Ethernet 1 Gbps chacun
    - Débit théorique de traitement HTTP/S : de 250 Mbps à 1 Gbps
    - Nombre de transactions : de 1 000 à 10 000 transactions HTTP/S par seconde minimum
- **[P**3212] Bundle 3 : ensemble comprenant :
    - 2 solutions de la gamme 3 en haute disponibilité
    - 2 ports Ethernet de 1 Gbps à 10 Gbps chacun
    - Débit théorique de traitement HTTP/S : de 1 Gbps à 10 Gbps
    - Nombre de transactions : de 10 000 à 30 000 transactions HTTP/S par seconde minimum

[P3220] Licences, abonnements et variantes associés à la solution, selon tranches et durées définies au BPU.

6.8.5. Sécurisation des services d'intelligence artificielle et des flux IA

[IA-001] Le titulaire devra proposer des solutions permettant de sécuriser les infrastructures, services, applications et flux reposant sur des technologies d'intelligence artificielle (IA), d'intelligence artificielle générative (IAG), de grands modèles de langage (LLM), de systèmes RAG (Retrieval-Augmented Generation) ou d'agents autonomes. Les solutions devront contribuer à la protection des communications, des traitements et des ressources exposées par ces technologies au sein du système d'information.

[IA-002] Les solutions de cette catégorie ont pour vocation principale la protection des modèles, agents et applications d'intelligence artificielle contre les attaques, abus ou usages malveillants. Les fonctions de routage ou de gouvernance des flux IA relèvent prioritairement de la catégorie « Passerelles LLM ».

[IA-003] Catégories de produits attendus
- AI Gateway
- LLM Firewall / Prompt Firewall
- Solutions de sécurisation des architectures RAG
- Solutions de sécurisation des agents IA
- Solutions d'AI Detection & Response
- Solutions d'AI Security Posture Management (AI-SPM)
- Fonctionnalités de sécurité IA intégrées à des plateformes WAF, API Security, SSE ou CNAPP.

[IA-004] Fonctionnalités principales - Les solutions devront permettre :
- L'identification et la supervision des flux à destination ou en provenance de services d'intelligence artificielle
- Le contrôle des communications entre applications, agents IA, API, modèles et sources de données
- La protection contre les tentatives de prompt injection, de contournement des mécanismes de sécurité et d'utilisation malveillante des modèles
- L'inspection et le filtrage des requêtes et réponses échangées avec les moteurs d'IA
- La sécurisation des architectures RAG, notamment des bases vectorielles, référentiels documentaires et interfaces de recherche
- La gestion et la sécurisation des communications initiées par des agents autonomes
- La segmentation et la microsegmentation des infrastructures IA
- La détection d'anomalies, de comportements suspects ou d'usages non autorisés
- La traçabilité et la journalisation des échanges associés aux services IA

- L'intégration avec les solutions de sécurité existantes de l'établissement, notamment les NGFW, WAF, API Gateway, SIEM, XDR et plateformes de supervision.

  - [P4530] Gamme 1 : firewall de protection IA destiné aux usages initiaux ou maîtrisés, couvrant l'identification des flux IA, le filtrage des requêtes et réponses, la protection contre les attaques de type prompt injection et la journalisation des événements associés.
  - [P4531] Gamme 2 : firewall de protection IA destiné aux usages intermédiaires ou mutualisés, intégrant des capacités renforcées de contrôle des communications entre applications, agents IA, API, modèles et sources de données, ainsi que des fonctions de détection d'anomalies et d'usages non autorisés.
  - [P4532] Gamme 3 : firewall de protection IA destiné aux usages avancés ou critiques, intégrant des fonctions étendues de protection des modèles, agents et applications IA, de sécurisation des architectures RAG, de contrôle des bases vectorielles et de supervision des comportements suspects.

[P4539] Licences, abonnements et variantes associés aux firewalls de protection IA, selon tranches, métriques et durées définies au BPU.

6.8.6. Répartition de charge et commutation applicative L5-L7

[LB-001] Pour chacune des gammes demandées, l'offre comprend au moins deux solutions techniques matérielles (appliance).
Les solutions de cette catégorie ont pour vocation principale la distribution du trafic et la haute disponibilité des services applicatifs. Les fonctions de sécurité applicative ou de publication sécurisée sont considérées comme complémentaires.

[LB-002] L'offre comprend quatre gammes de solutions de commutateur L5/L7 (répartition de charge) ayant pour caractéristiques et fonctionnalités communes :

- Services applicatifs disponibles :
  - Tous protocoles IP
  - Application spécifique par filtrage par port
- Capacité de mettre en œuvre des flux sans translation d'adresses du client.
- Fonctionnalités d'équilibrage de charge :
  - « Round Robin » : chaque nouvelle connexion est dirigée sur le serveur suivant dans la ferme)
  - « Le moins de connexion » : chaque nouvelle connexion est dirigée sur le serveur de la ferme gérant le moins de connexion
  - « Le moins de trafic » : chaque nouvelle connexion est dirigée sur le serveur de la ferme gérant le moins de trafic
  - « Temps de réponse » : chaque nouvelle connexion est dirigée sur le serveur de la ferme présentant le meilleur temps de réponse
  - « Hashing » : pour chaque nouvelle connexion une empreinte, Hashing, est calculée, assurant que les flux d'un même utilisateur seront toujours dirigés sur le même serveur de la ferme
  - « SNMP » : l'équipement doit pouvoir requêter en SNMP les serveurs de la ferme (par exemple, charge CPU ou niveau mémoire) et chaque nouvelle connexion est dirigée sur le serveur de la ferme présentant les meilleurs résultats
- Pour chacun de ces algorithmes de répartitions, il doit être possible de mettre en place une pondération des serveurs (« poids » d'un serveur reflétant sa capacité de traitement).
- Fonctions d'optimisation des flux
- Persistance de sessions en cours (gestion des cookies) :
  - En mode de haute disponibilité : pas de réinitialisation de sessions en cas de bascule de cluster.
  - Entre serveurs applicatifs destinataires et postes clients
- Haute disponibilité : fonctionnement en cluster actif/actif ou actif/passif. Synchronisation automatique des nœuds de cluster.

[LB-004] L'offre comprend quatre gammes de solutions de commutateur L5/L7 en fonction des performances attendues, des capacités de haute disponibilité et des usages de répartition de charge applicative décrits ci-après.

- **[P**3230] Gamme 1 : solutions de commutateur L5/L7, dont au moins 2 permettent la haute disponibilité :
    - Débit théorique de traitement L7 : de 1 Gbps
    - Nombre de requêtes L4 par seconde : 1000
- **[P**3231] Gamme 2 : solutions de commutateur L5/L7, dont au moins 2 permettent la haute disponibilité :
    - Débit théorique de traitement L7 : de 5 Gbps
    - Nombre de requêtes L4 par seconde : 10.000
- **[P**3232] Gamme 3 : solutions de commutateur L5/L7, dont au moins 2 permettent la haute disponibilité :
    - Débit théorique de traitement L7 : de 10 Gbps
    - Nombre de requêtes L4 par seconde : 100.000
- **[P**3233] Gamme 4 : solutions de commutateur L5/L7, dont au moins 2 permettent la haute disponibilité :
    - Débit théorique de traitement L7 : de 40 Gbps
    - Nombre de requêtes L4 par seconde : 1M

En complément des gammes unitaires ci-dessus, l'offre fera apparaitre les gammes de bundle ci-dessous. Les gammes de bundle doivent impérativement être construites sur la base des gammes de solutions techniques ci-dessus. Les bundles comprennent les accessoires, licences et add-ons nécessaires à leur mise en œuvre.

- **[P**3240] Bundle 1 : gamme de 2 ensembles comprenant chacun : 2 solutions de la gamme 1 en haute disponibilité
- **[P**3241] Bundle 2 : gamme de 4 ensembles comprenant chacun : 2 solutions de la gamme 2 en haute disponibilité
- **[P**3242] Bundle 3 : gamme de 4 ensembles comprenant chacun : 2 solutions de la gamme 3 en haute disponibilité
- **[P**3243] Bundle 4 : gamme de 4 ensembles comprenant chacun : 2 solutions de la gamme 4 en haute disponibilité

[LB-003] Pour l'ensemble des répartiteurs de charge et commutateurs applicatifs L5-L7, les exigences communes d'administration, supervision, journalisation, export des traces, diagnostic, haute disponibilité, MCS et authentification des administrateurs sont celles définies dans le CCTP commun, auquel il convient de se référer. Le candidat précise uniquement les compléments propres aux algorithmes de répartition, aux contrôles de disponibilité, à la persistance de session, aux performances L4-L7 et aux interfaces d'administration spécifiques.

6.8.7. Portails captifs d'authentification

[MFA-002] Les solutions de portails captifs d'authentification ou portails d'accès internet existent sur le marché sous forme de logiciels ou d'appliances matérielles. L'offre comprend au moins deux solutions techniques distinctes. Pour chacune des gammes demandées, l'offre présente soit une solution technique matérielle (appliance), soit une solution sous forme logicielle. La version logicielle de la solution inclut la fourniture du système d'exploitation lorsque celui-ci n'est pas standard et présente des caractéristiques spécifiques implémentées par l'éditeur, conformément au CCTP commun.

[MFA-007] L'offre comprend quatre gammes de portails captifs ayant pour fonctionnalités communes :

- Possibilité de mise en œuvre de plusieurs portails web pour plusieurs profils d'utilisateurs (Solution Multi portail)
- Ergonomie de présentation pour les utilisateurs, bénéficiant d'une interface multi-langues
- Personnalisation de la page d'accueil du portail, intégration de charte graphique spécifique au bénéficiaire et intégration d'une charte d'utilisation

- Compatibilité avec les principaux navigateurs du marché dans leur dernière version :
  - Microsoft Edge
  - Firefox
  - Safari
  - Chrome
  - Opéra
  - Indiquer la compatibilité avec les OS et navigateurs de terminaux mobiles (smartphones, tablettes…) pour la configuration automatique et le portail.
- Services applicatifs disponibles :
  - Entièrement compatible avec tout le protocole IP V4 et V6
  - Application spécifique par filtrage par port UDP et TCP
- Service de configuration automatique du client sans paramétrage préalable
- Validation de clauses d'utilisation avant ouverture d'accès.
- Possibilité de mettre à disposition des accès internet sans authentification :
  - Accès internet complet
  - Filtrage sur certaines URL uniquement
- Authentification :
  - Compatibilité Serveur d'authentification sécurisé On Premise et dans le Cloud (Radius, Microsoft Authenticator, Google Authenticator), Tacacs (RFC 1492), annuaire local, LDAP et Active Directory.
  - Indication de la compatibilité Gestion de l'authentification forte carte à jeton
- Possibilité de délégation des fonctions de gestion des utilisateurs et de leurs droits à des groupes d'utilisateurs
- Haute disponibilité : fonctionnement en cluster actif/actif. Synchronisation automatique des nœuds de cluster.
- Possibilité d'installation des portails en mode multi-machines sans redondance des achats de licence (coût de licence non lié au nombre de machines installées)

En fonctionnalité complémentaire :

- Possibilité de tester le niveau de sécurité et d'intégrité du poste client avant ouverture de connexion :
  1. Version de système d'exploitation et niveau de patch système
  2. Version de logiciel anti-virus et état des mises à jour
  3. Présence ou absence de logiciel spécifique

L'offre précise le mode de licence de la solution proposée. Le candidat précise si une licence site est disponible cette caractéristique est appréciée dans les conditions fixées au règlement de la consultation.

- **[P**3260] Gamme 1 : capacité de 250 sessions simultanées
- **[P**3261] Gamme 2 : capacité de 1000 sessions simultanées
- **[P**3262] Gamme 3 : capacité de 3000 sessions simultanées
- **[P**3263] Gamme 4 : capacité de 5000 sessions simultanées

[MFA-005] Pour l'ensemble des portails captifs, les exigences communes d'administration, supervision, journalisation, export des traces, diagnostic, haute disponibilité, MCS et fourniture du système d'exploitation spécifique le cas échéant sont celles définies dans le CCTP commun, auquel il convient de se référer. Le candidat précise uniquement les compléments propres à la personnalisation des portails, à la délégation des droits, aux parcours utilisateurs et aux modalités d'authentification.

6.8.8. Sécurité multifonction et services de sécurité intégrés

[MULTI-001] Pour chaque solution multifonction, le candidat précise les domaines couverts, les fonctions incluses ou optionnelles, les performances avec plusieurs fonctions actives, les limites de mutualisation, les possibilités d'acquisition séparée et les compléments spécifiques aux exigences communes d'administration, journalisation, haute disponibilité et MCS définies dans le CCTP commun, auquel il convient de se référer. Les solutions multifonctions peuvent couvrir tout ou partie des domaines ci-dessous la couverture fonctionnelle est explicitement indiquée dans l'offre.

- Firewalls « périmétriques »
- Portail extranet SSL
- Passerelles internet-web
- Passerelles de messagerie électronique
- Solutions de bac à sable (Sandboxing)
- Solution de publication d'applications web sécurisée
- Solution de commutation L5/L7 (répartition de charge)
- Portail captif d'authentification

[MULTI-002] L'offre couvre les gammes multifonctions ci-dessous, selon leur périmètre fonctionnel, leur capacité de raccordement et leur puissance de traitement.

- **[P**3280] Gamme 1 : 4 solutions firewall multifonctions dont au moins 2 proposent la haute disponibilité :
    - Fonctionnalités attendues :
        - Firewall périmétrique avec fonction Antivirus : 2 Gbps théorique
        - VPN : 250 sessions en simultané
        - Passerelle de messagerie : 4000 mails par heure
        - Passerelle internet-web si disponible
- **[P**3281] Gamme 2 : 4 solutions firewall multifonctions proposant la haute disponibilité
    - Fonctionnalités attendues :
        - Firewall périmétrique avec fonctions IPS et Antivirus : 10 Gbps théorique
        - VPN : 500 sessions en simultané
        - Passerelle internet-web : 1000 sessions simultanées
        - Passerelle de messagerie : 10.000 mails par heure
        - Portail d'accès internet si disponible
        - Fonction bac à sable si disponible
- **[P**3282] Gamme 3 : 4 solutions firewall multifonctions proposant la haute disponibilité
    - Fonctionnalités attendues :
        - Firewall périmétrique avec fonctions IPS et Antivirus : 10 Gbps théorique
        - VPN : 1000 sessions en simultané
        - Passerelle internet-web : 3000 sessions simultanées
        - Passerelle de messagerie : 100.000 mails par heure
        - Portail d'accès internet si disponible
        - Fonction bac à sable si disponible
- **[P**3283] Gamme 4 : 4 solutions firewall multifonctions proposant la haute disponibilité dont au moins 2 doivent permettre de créer plusieurs instances indépendantes les unes des autres avec paramétrage et fonctionnement spécifique à chaque instance
    - Fonctionnalités attendues :
        - Firewall périmétrique avec fonctions IPS et Antivirus : 40 Gbps théorique
        - VPN : 2500 sessions en simultané
        - Passerelle internet-web : 5000 sessions simultanées
        - Passerelle de messagerie : 1 000 000 de mails par heure
        - Portail d'accès internet si disponible
        - Fonction bac à sable si disponible
- **[P**3284] Gamme 5 : 4 solutions de publication d'applications web multifonctions dont au moins 2 proposent la haute disponibilité
    - Fonctionnalités attendues :
        - Publication d'applications web : 2000 requêtes HTTPS/s
        - Portail extranet SSL : 500 sessions simultanées
        - Firewall périmétrique si disponible
        - Passerelle de messagerie si disponible
- **[P**3285] Gamme 6 : 4 solutions de publication d'applications web multifonctions proposant la haute disponibilité
    - Fonctionnalités attendues :

        - Publication d'applications web : 10.000 requêtes HTTPS/s
        - Portail extranet SSL : 1000 sessions simultanées
        - Firewall périmétrique si disponible
        - Passerelle de messagerie si disponible
        - Passerelle internet-web si disponible
- **[P**3286] Gamme 7 : 4 solutions de passerelle Internet multifonctions dont au moins 2 proposent la haute disponibilité
    - Fonctionnalités attendues :
        - Passerelle internet-web : 1000 sessions simultanées
        - Passerelle de messagerie : 10.000 mails par heure
- **[P**3287] Gamme 8 : 4 solutions de passerelle Internet multifonctions proposant la haute disponibilité
    - Fonctionnalités attendues :
        - Passerelle internet-web : 3000 sessions simultanées
        - Passerelle de messagerie : 100.000 mails par heure
        - Fonction bac à sable si disponible
- **[P**3288] Gamme 9 : 4 solutions de passerelle Internet multifonctions proposant la haute disponibilité
    - Fonctionnalités attendues :
        - Passerelle internet-web : 5000 sessions simultanées
        - Passerelle de messagerie : 1 000 000 de mails par heure
        - Fonction bac à sable si disponible
- **[P**3290] Bundle 1 : gamme de 2 ensembles comprenant chacun :
  2 solutions de la gamme 1 en haute disponibilité et proposant l'ensemble des fonctionnalités demandées, sans autres fonctionnalités additionnelles
- **[P**3291] Bundle 2 : gamme de 4 ensembles comprenant chacun :
  2 solutions de la gamme 2 en haute disponibilité et proposant l'ensemble des fonctionnalités demandées, sans autres fonctionnalités additionnelles
- **[P**3292] Bundle 3 : gamme de 4 ensembles comprenant chacun :
  2 solutions de la gamme 3 en haute disponibilité et proposant l'ensemble des fonctionnalités demandées, sans autres fonctionnalités additionnelles
- **[P**3293] Bundle 4 : gamme de 4 ensembles comprenant chacun :
  2 solutions de la gamme 4 en haute disponibilité et proposant l'ensemble des fonctionnalités demandées, sans autres fonctionnalités additionnelles
- **[P**3294] Bundle 5 : gamme de 2 ensembles comprenant chacun :
  2 solutions de la gamme 5 en haute disponibilité et proposant l'ensemble des fonctionnalités demandées, sans autres fonctionnalités additionnelles
- **[P**3295] Bundle 6 : gamme de 4 ensembles comprenant chacun :
  2 solutions de la gamme 6 en haute disponibilité et proposant l'ensemble des fonctionnalités demandées, sans autres fonctionnalités additionnelles
- **[P**3296] Bundle 7 : gamme de 2 ensembles comprenant chacun :
  2 solutions de la gamme 7 en haute disponibilité et proposant l'ensemble des fonctionnalités demandées, sans autres fonctionnalités additionnelles
- **[P**3297] Bundle 8 : gamme de 4 ensembles comprenant chacun :
  2 solutions de la gamme 8 en haute disponibilité et proposant l'ensemble des fonctionnalités demandées, sans autres fonctionnalités additionnelles
- **[P**3298] Bundle 9 : gamme de 4 ensembles comprenant chacun :
  2 solutions de la gamme 9 en haute disponibilité et proposant l'ensemble des fonctionnalités demandées, sans autres fonctionnalités additionnelles

Selon les domaines effectivement couverts, la solution multifonction reprend les exigences applicables des sections correspondantes du CCTP, ainsi que les exigences communes d'administration, d'authentification, de journalisation, de diagnostic, de haute disponibilité, de MCS et de fourniture du système d'exploitation spécifique le cas échéant définies dans le CCTP commun, auquel il convient de se référer.
Lorsque la solution multifonction est proposée sous forme de carte en châssis, l'offre comprend le plus petit châssis compatible et précise les conditions d'évolution de capacité.

[P3300] Licences, abonnements et variantes associés à la solution, selon tranches et durées définies au BPU.

6.8.9. Serveur d'authentification sécurisée

[MFA-004] Les solutions d'authentification sécurisée existent sur le marché sous forme de solutions logicielles ou d'appliances matérielles. L'offre comprend :

- Deux solutions couvrant les cas de déploiements purement on-premise permettant un fonctionnement déconnecté d'Internet
- Deux solutions couvrant les cas de déploiement on-premise avec la possibilité de l'étendre en mode hybride (on-premise + cloud)

Pour chacun des types de déploiements demandés, l'offre comprend soit une solution technique hautement disponible soit matérielle (appliance) soit purement logicielle. La version logicielle de la solution inclut la fourniture du système d'exploitation lorsque celui-ci n'est pas standard et présente les caractéristiques spécifiques implémentées par l'éditeur.
Les fonctionnalités attendues, communes aux deux types de déploiement, sont :

- Annuaire d'authentification local à la solution, annuaire externe LDAP et annuaire externe Active Directory
- Prise en charge de la norme 802.1x
- Gestion des autorisations basée sur des profils et des rôles
- Ergonomie et capacité d'administration avancée grâce à une interface graphique
- Gestion des traces :
  - Traçabilité complète des flux d'ouverture et de fermeture de sessions utilisateurs ainsi que des trafics associés, et des erreurs.
  - Traçabilité complète des flux d'ouverture et de fermeture de sessions administrateurs ainsi que le contenu des actions qu'ils ont réalisées
  - Export pour stockage et analyse vers une solution tierce de corrélation des traces. L'offre précise les outils nécessaires à leur gestion et les protocoles d'export pris en charge.
  - L'offre décrit la possibilité de produire les tableaux de bord standards ainsi que la possibilité de les personnaliser et d'en créer de nouveaux
- Des fonctionnalités d'aide au diagnostic (fonctionnalités, protocoles …)
- Des fonctionnalités de supervision des ressources utilisées (CPU, mémoire, stockage...)

[MFA-003] Pour les serveurs d'authentification sécurisée, les exigences communes d'administration, supervision, journalisation, export des traces, diagnostic, haute disponibilité et MCS sont celles définies dans le CCTP commun, auquel il convient de se référer. Les moyens d'authentification offerts aux utilisateurs intègrent un ou plusieurs facteurs suivants :

- Authentification d'un utilisateur sur une machine attribuée avec un mot de passe
- Authentification par certificat de sécurité délivré par l'autorité de certification privée du bénéficiaire ou par une autorité de certification publique.
- Authentification par mot de passe à usage unique, envoi de ce mot de passe via un service d'émission de SMS ou par messagerie électronique. Dans le cas de systèmes de génération de mot de passe à usage unique matériel ou logiciel, il conviendra de préciser lesquels
- Pour le type de déploiement hybride, authentification par service Cloud tel que Microsoft Authenticator ou Google Authenticator

Parmi les standards pris en charge, le support de la norme FIDO2 est **un atout apprécié**. Dans le cas où ce standard n'est actuellement pas pris en charge par la solution, la feuille de route pour son support sera décrite.
L'offre précise le mode de licence de la solution proposée. Le candidat précise si une licence site est disponible cette caractéristique est appréciée dans les conditions fixées au règlement de la consultation.
L'offre comprend 2 gammes de serveurs d'authentification sécurisée :

- **[P**3310] Gamme 1 : déploiement purement on-premise
- **[P**3311] Gamme 2 : déploiement on-premise avec la possibilité de l'étendre en mode hybride

Licences, abonnements et variantes associés à la solution, selon tranches et durées définies au BPU :

- [P3312] de 1 à 99 utilisateurs simultanés
- [P3313] de 100 à 999 utilisateurs simultanés
- [P3314] de 1000 à 4999 utilisateurs simultanés
- [P3315] plus de 5000 utilisateurs simultanés

6.8.10. Solution de contrôle d'accès au réseau

[NAC-001] Les solutions de contrôle d'accès réseau existent sur le marché sous forme de logiciels ou d'appliances matérielles. L'offre comprend au moins deux solutions techniques distinctes. Pour la solution demandée, l'offre comprend soit une solution technique matérielle (appliance) soit une solution sous forme logicielle. La version logicielle de la solution inclut la fourniture du système d'exploitation lorsque celui-ci n'est pas standard et présente des caractéristiques spécifiques implémentées par l'éditeur.

Les fonctionnalités attendues sont les suivantes. Les exigences communes d'administration, supervision, journalisation, diagnostic, haute disponibilité et MCS sont celles définies dans le CCTP commun, auquel il convient de se référer les éléments ci-dessous précisent uniquement les compléments propres au contrôle d'accès réseau.

- Authentification – identification :
  - Norme 802.1x
- Solution d'authentification sécurisée, déployable **On-Premise et/ou dans le Cloud**, compatible avec les mécanismes d'authentification **RADIUS**, **Microsoft Authenticator** et **Google Authenticator**
- Prendre en charge l'authentification des terminaux et des utilisateurs via les protocoles **802.1X / EAP (Extensible Authentication Protocol)** sur les réseaux filaires (EAPOL - EAP over LAN) et sans fil (WLAN).
- S'appuyer sur les identités suivantes :
  - Compte utilisateur
  - Compte machine
  - Certificat X.509
  - Adresse MAC
  - Adresse IP.
  - Type du client (profiling) L'identification à minima des types de clients suivants :
    - Ordinateurs avec leur système d'exploitation
    - Imprimantes et copieurs multifonction
    - Équipements mobiles (tablettes, smartphones)
    - Téléphones IP
    - Terminaux connectés via un IP phone
    - Bornes wifi
    - Caméras IP
    - IOT
    - Empreintes de type :
      1. Adresse MAC
      2. Entête http
      3. Requêtes DHCP, SNMP
      4. Autres
  - L'identification de la conformité (posture) des terminaux sur la base de leur identité :
    - Version de système d'exploitation et niveau de patch système
    - Version de logiciel anti-virus et état des mises à jour
    - Présence ou absence de logiciel spécifique (Firewall, …)

- Application de règles de sécurité :

- En fonction de l'authentification, de l'identité, de la conformité du client et de ses composants et de son profil calculé :
    - Affectation de VLAN (VLAN dynamique)
    - Autoconfiguration d'ACL
    - Autoconfiguration du port Ethernet (débit, duplex et PoE)
    - Mise en quarantaine
    - Accueil des terminaux non authentifiés sur un portail captif d'authentification disposant des fonctionnalités demandées au chapitre « Portail captif d'authentification »

- Administration, délégation et reporting :
    - Ergonomie et capacité d'administration avancée, grâce à une interface graphique accessible via interface Web, y compris pour la gestion de la haute disponibilité.
    - Gestion des logs :
        - Traçabilité complète des flux d'ouverture et de fermeture de sessions, ainsi que des trafics associés, et des erreurs.
        - Export pour stockage et analyse vers une solution de supervision externe des journaux de logs. L'offre précise les outils nécessaires à leur gestion.
    - Possibilité de délégation des fonctions de gestion des utilisateurs et de leurs droits à des groupes d'utilisateurs
    - L'offre comprend les tableaux de bords de base disponibles (ouvertures/fermeture de session, source et destinataire, alarmes…)
    - Des fonctionnalités d'aide au diagnostic tel qu'un debug des fonctionnalités et protocoles, une visualisation des processus utilisant la CPU, une visualisation de l'utilisation de la mémoire... Les fichiers de debug peuvent être exportés pour stockage et analyse dans un environnement micro-informatique. L'offre précise les outils nécessaires à leur gestion.

- Haute disponibilité :
    - Fonctionnement en cluster actif/actif ou actif/passif au choix lors de l'intégration. Synchronisation automatique des nœuds de cluster.

L'offre comprend un prix unitaire pour chacune des gammes proposées ainsi que les prix unitaires de tous les accessoires, fonctionnalités et add-ons associés à cette gamme (licences…). En particulier, l'offre mentionnera les éventuels clients d'authentification disponibles et leur tarification par tranche en fonction du nombre de clients.

L'offre précise le mode de licence de la solution proposée. Le candidat précise si une licence site perpétuelle est disponible cette caractéristique est appréciée dans les conditions fixées au règlement de la consultation.

[NAC-002] L'offre comprend au moins 3 gammes de solution de contrôle d'accès réseau en fonction du nombre de clients réseau :
- [P3320] Gamme 1 : capacité de 1 à 5000 clients 802.1x
- [P3321] Gamme 2 : capacité de 5001 à 10 000 clients 802.1x
- [P3322] Gamme 3 : capacité de 10001 à 25 000clients 802.1x
- [P3323] Gamme 4 : capacité au-delà de 25 001 clients 802.1x

En complément des gammes unitaires ci-dessus, l'offre fera apparaitre les gammes de bundle ci-dessous.

Les gammes de bundle doivent impérativement être construites sur la base des gammes de solutions techniques ci-dessus. Elles contiennent dans leur prix unitaire tous les accessoires, licences et add-ons nécessaires à leur mise en œuvre. Par ailleurs, l'optimisation des coûts de licence sur les bundles sera particulièrement appréciée.

- [P3330] Bundle 1 : ensemble comprenant :
    - Au moins 2 appliance en cluster haute disponibilité

    - 500 clients profilés ou invités
    - 250 clients en contrôle de conformité
    - 250 clients provisionnés
    - Évolutif jusqu'à triplement des quantités de clients
- [P3331] Bundle 2 : ensemble comprenant :
    - Au moins 2 appliance en cluster haute disponibilité
    - 5000 clients profilés ou invités
    - 1000 clients en contrôle de conformité
    - 1000 clients provisionnés
    - Évolutif jusqu'à doublement des quantités de clients
- [P3332] Bundle 3 : ensemble comprenant :
    - Au moins 2 appliance en cluster haute disponibilité
    - 10000 clients profilés ou invités
    - 5000 clients en contrôle de conformité
    - 5000 clients provisionnés
    - Évolutif jusqu'à doublement des quantités de clients
- [P3333] Bundle 4 : ensemble comprenant :
    - Au moins 2 appliance en cluster haute disponibilité
    - 25000 clients profilés ou invités
    - 10000 clients en contrôle de conformité
    - 10000 clients provisionnés
    - Évolutif jusqu'à doublement des quantités de clients

[P3340] L'offre comprend aussi les prix unitaires et en quantités des ajouts de licences. Ces prix sont déclinés par tranche d'utilisateurs simultanés ainsi que par durée d'utilisation (1 an, 2 ans, 3 ans et 4 ans, à vie).
Les mises à jour logicielles, correctifs, évolutions mineures ou majeures et composants nécessaires au maintien en condition opérationnelle et de sécurité relèvent des exigences communes définies dans le CCTP commun, auquel il convient de se référer.

6.8.11. DNS, DHCP, IPAM (DDI) et synchronisation temporelle

[DDI-001] Les solutions de gestion de plan d'adressage, DNS et DHCP existent sur le marché sous forme de logiciels ou d'appliances matérielles. Pour la gamme demandée, l'offre comprend soit DEUX solutions techniques matérielles (appliance) soit DEUX solutions sous forme logicielle et si techniquement possible les deux formes. Les versions logicielles des solutions incluent la fourniture du système d'exploitation lorsque celui-ci n'est pas standard et présente des caractéristiques spécifiques implémentées par l'éditeur
L'intégration des trois fonctions DNS/DHCP/gestion de plan d'adressage IP dans une même solution technique est fortement souhaitable.

[DDI-002] Les principales fonctionnalités attendues sont les suivantes. Les exigences communes d'administration, supervision, journalisation, export des traces, diagnostic, haute disponibilité et MCS sont celles définies dans le CCTP commun, auquel il convient de se référer les éléments ci-dessous précisent uniquement les compléments propres aux fonctions DNS, DHCP et IPAM.

- Capacité de traitement minimale de 5000 à 100000 requêtes DNS et de 100 à 3000 requêtes DHCP par seconde
- Gestion d'au moins 500 sous-réseaux IP et VLAN,
- Service DNS pour la zone DNS technique Active Directory, ainsi que pour les zones DNS des postes, imprimantes, serveurs, équipements d'infrastructure, téléphones IP et appareils biomédicaux qui représentent un total de 50000 enregistrements DNS
- Services DNS permettant :
    - La résolution de nom IP<>host et sa résolution inverse
    - Le relayage de requêtes DNS
    - La résolution sélective ou conditionnelle en fonction de critères liés aux postes clients de tous types à l'origine de la demande

    - Partage de charge en round-robin de résolution
    - Fonction de cache de résultats de résolution à la suite de requêtes relayées avec paramétrage de la durée de vie des entrées du cache.
    - Support des enregistrements de type SRV pour le support de domaines Microsoft Windows.
    - Intégration à une architecture Microsoft Windows en lieu et place des services serveurs DNS/DHCP disponibles en standard sur les serveurs Microsoft.
    - Transfert de zone vers d'autres serveurs DNS
- Services DHCP disponibles, avec une capacité d'enregistrement minimale de 30000 entrées, statiques ou dynamiques.
- Services DHCP permettant la gestion de la téléphonie sur IP et la déclaration des postes téléphoniques IP clients de tous constructeurs.
- Services DHCP permettant :
    - Allocation d'adresses DHCP et BOOTP statiques et dynamiques, complétées des adresses de passerelles, des configurations DNS, Wins, ToIP.
    - Réservation et affectation de plages d'adresses sur un critère précis tel que l'adresse MAC du client et indiqué dans la requête DHCP émise.
    - Options DHCP conformes aux normes RFC 2132
    - Gestion de l'option 128 (TFTP server IP address)
    - Mise à jour dynamique des enregistrements DNS à la suite des allocations d'adresses DHCP/BOOTP
- Gestion de plans d'adressages :
    - Visualisation des attributions, des réservations des adresses, par adresse, par blocs d'adresses.
    - Visualisation des noms/types des clients usagés d'adresses IP.
    - Recherche d'adresses, de clients, d'adresses MAC…
    - Historisation des allocations et des baux DHCP
    - Aide à l'optimisation du plan d'adressage et à la gestion des manques d'adresses
    - Gestion d'alertes en cas d'un dysfonctionnement quelconque d'allocation d'adresses.
- Compatibilité complète IPv4/IPv6.
- Géolocalisation des adresses IP et Mac utilisées :
    - Prise en charge de requêtes SNMP vers les éléments actifs de réseau
    - Analyse des tables d'adresses
    - Liste des adresses IP et MAC par port d'élément actif de réseau
- Autoprotection contre les attaques DNS et DHCP :
    - DDoS
    - Vulnérabilités Zero Day
    - Malwares DNS/DHCP
- Compatibilité SNMP et envoi de trap vers une station de supervision externe.
- Ergonomie et capacité d'administration avancées, grâce à une interface graphique accessible via interface Web, y compris pour la gestion de la haute disponibilité, pour l'ensemble des fonctionnalités demandées.
- L'interface d'administration permet :
    - Le contrôle d'intégrité de toute modification ou ajout
    - L'annulation totale ou partielle d'un ajout ou d'une modification
    - La délégation totale ou partielle de la gestion d'une plage d'adresses
- Haute disponibilité : fonctionnement en cluster actif/actif ou actif/passif. L'offre précise le temps de bascule entre deux nœuds et les méthodes de réplication des données permettant d'assurer une continuité de service et une synchronisation des données en temps réel. L'offre précise également les possibilités d'intégration en haute disponibilité à travers un cluster à plus de deux nœuds.
- Gestion des logs :
    - Traçabilité complète des flux de requêtes, des erreurs.
    - Export pour stockage et analyse vers une solution de supervision externe des journaux de logs. L'offre précise les outils nécessaires à leur gestion.

- L'offre comprend les tableaux de bord de base disponibles (ouvertures/fermeture de session, source et destinataire, alarmes…)

[DDI-004] L'offre est basée sur une licence site. Le nombre d'adresses gérées par la solution ne doit être limité que par la capacité matérielle des appliances ou des serveurs d'hébergement.

- **[P**3350] L'offre comprend une gamme matérielle et logicielle :
  - D'une capacité de traitement minimale de 5000 à 100000 requêtes DNS et de 100 à 3000 requêtes DHCP par seconde
  - Gérant au moins 500 sous-réseaux IP et VLAN

[P3360] Licences, abonnements et variantes associés à la solution, selon tranches et durées définies au BPU.
Solutions de boîtiers de synchronisation de l'heure

[DDI-003**]** L'offre comprend DEUX solutions techniques matérielles distinctes permettant de couvrir les caractéristiques suivantes :

- Permettre la synchronisation du temps de différents équipements informatiques ou non informatiques basée sur l'utilisation de protocoles standards. A minima, les solutions doivent supporter le protocole NTP (« Network Time Protocol »). Optionnellement, les solutions supportent PTP (« Precision Time Protocol »). La feuille de route du support de protocole « SCP Time » sera appréciée.
- La fourniture de l'heure UTC (« Universal Time Coordinator ») est assurée par une synchronisation satellitaire apportée par la solution. La solution doit comporter les matériels et accessoires permettant de capter l'information satellite.
- Afin d'être résiliente vis-à-vis de l'information satellite, la nature et le nombre de satellites utilisés par la solution doivent être précisés.
- La connexion au réseau local du bénéficiaire doit accepter de multiples interfaces 100 Mbps base-T à minima. Le nombre d'interfaces et leurs caractéristiques seront spécifiés dans l'offre.

L'offre comprend deux solutions matérielles de synchronisation de temps :

- **[P**3370] Solution 1 : solutions matérielles de synchronisation de temps
- **[P**3371] Solution 2 : solutions matérielles de synchronisation de temps

6.8.12. Détection et prévention des intrusions IDS/IPS

[IDS-001] Les sondes autonomes IDS/IPS existent sur le marché sous forme de logiciels ou d'appliances matérielles. Pour chacune des gammes demandées, l'offre comprend au moins deux solutions techniques matérielles distinctes (appliances). Les exigences communes d'administration, supervision, journalisation, diagnostic, haute disponibilité et MCS sont celles définies dans le CCTP commun, auquel il convient de se référer les éléments propres aux signatures, politiques de détection et modes de prévention sont précisés ci-après.

[IDS-002] L'offre comprend 4 gammes de sondes en fonction de leur puissance de traitement :

- **[P**3380] Gamme 1 : au minimum 4 sondes IDS/IPS dont au moins une permettant une architecture en haute disponibilité
  - Débit IP : 100 Mbps minimum
  - Détection d'attaques sur les couches 3 à 7
    - Sur la base des signatures d'attaques connues
    - Par analyse comportementale
  - Catégorisation des signatures d'attaque selon :
    - La criticité de l'attaque
    - Le niveau de confiance de la signature
    - Le niveau de performance matérielle requis pour activer la signature
  - Implémentation de deux niveaux de filtrage :
    - Détection qui génère une alerte
    - Prévention qui bloque les requêtes

- Mise à jour automatique et régulière de la base de signatures
- Activation automatique des signatures selon une politique prédéfinie
- Paramétrage d'exceptions sur une politique ou une signature
- Authentification : compatibilité LDAP et Active Directory, Serveur d'authentification sécurisé On Premise et dans le Cloud (Radius, Microsoft Authenticator, Google Authenticator), base locale
- Si Haute disponibilité : fonctionnement en cluster actif/actif ou actif/passif au choix lors de l'intégration. Synchronisation automatique des nœuds de cluster.

- **[P**3381] Gamme 2 : au minimum 4 sondes IDS/IPS permettant une architecture en haute disponibilité
  - Débit IP : 1 Gbps minimum
  - Détection d'attaques sur les couches 3 à 7
    - Sur la base des signatures d'attaques connues
    - Par analyse comportementale
  - Catégorisation des signatures d'attaque selon :
    - La criticité de l'attaque
    - Le niveau de confiance de la signature
    - Le niveau de performance matérielle requis pour activer la signature
  - Implémentation de deux niveaux de filtrage :
    - Détection qui génère une alerte
    - Prévention qui bloque les requêtes
  - Mise à jour automatique et régulière de la base de signatures
  - Activation automatique des signatures selon une politique prédéfinie
  - Paramétrage d'exceptions sur une politique ou une signature
  - Authentification : Compatibilité LDAP et Active Directory, Serveur d'authentification sécurisé On Premise et dans le Cloud (Radius, Microsoft Authenticator, Google Authenticator), Tacacs multiples, base locale
  - Haute disponibilité : fonctionnement en cluster actif/actif ou actif/passif au choix lors de l'intégration. Synchronisation automatique des nœuds de cluster.
- **[P**3382] Gamme 3 : au minimum 4 sondes IDS/IPS permettant une architecture en haute disponibilité
  - Débit IP : 10 Gbps minimum
  - Détection d'attaques sur les couches 3 à 7
    - Sur la base des signatures d'attaques connues
    - Par analyse comportementale
  - Catégorisation des signatures d'attaque selon :
    - La criticité de l'attaque
    - Le niveau de confiance de la signature
    - Le niveau de performance matérielle requis pour activer la signature
  - Implémentation de deux niveaux de filtrage :
    - Détection qui génère une alerte
    - Prévention qui bloque les requêtes
  - Mise à jour automatique et régulière de la base de signatures
  - Activation automatique des signatures selon une politique prédéfinie
  - Paramétrage d'exceptions sur une politique ou une signature
  - Authentification : Compatibilité LDAP et Active Directory, Serveur d'authentification sécurisé On Premise et dans le Cloud (Radius, Microsoft Authenticator, Google Authenticator), Tacacs multiples, base locale
  - Haute disponibilité : fonctionnement en cluster actif/actif ou actif/passif au choix lors de l'intégration. Synchronisation automatique des nœuds de cluster.
- **[P**3383] Gamme 4 : au minimum 4 sondes IDS/IPS permettant une architecture en haute disponibilité
  - Débit IP : 40 Gbps minimum
  - Détection d'attaques sur les couches 3 à 7

        - Sur la base des signatures d'attaques connues
        - Par analyse comportementale
    - Catégorisation des signatures d'attaque selon :
        - La criticité de l'attaque
        - Le niveau de confiance de la signature
        - Le niveau de performance matérielle requis pour activer la signature
    - Implémentation de deux niveaux de filtrage :
        - Détection qui génère une alerte
        - Prévention qui bloque les requêtes
    - Mise à jour automatique et régulière de la base de signatures
    - Activation automatique des signatures selon une politique prédéfinie
    - Paramétrage d'exceptions sur une politique ou une signature
    - Authentification : Compatibilité LDAP et Active Directory, Serveur d'authentification sécurisé On Premise et dans le Cloud (Radius, Microsoft Authenticator, Google Authenticator), Tacacs multiples, base locale
    - Haute disponibilité : fonctionnement en cluster actif/actif ou actif/passif au choix lors de l'intégration. Synchronisation automatique des nœuds de cluster.

[P3390] Licences, abonnements et variantes associés à la solution, selon tranches et durées définies au BPU.

6.8.13. Protection contre les attaques par déni de service

[DDOS-001] Les solutions autonomes anti DDoS existent sur le marché sous forme de logiciels ou d'appliances matérielles. Pour chacune des gammes demandées, l'offre comprend au moins deux solutions techniques matérielles distinctes (appliances).

[DDOS-002] L'offre comprend 4 gammes de solutions anti DDoS en fonction de leur puissance de traitement :

- **[P**3400] Gamme 1 : au minimum 4 solutions anti DDoS dont au moins une permettant une architecture en haute disponibilité
    - Débit IP : 100 Mbps minimum
    - Détection d'attaques de type déni de service volumétriques sur les couches 3 à 7 : SYN, ICMP, TCP, UDP, HTTP, DNS, etc.
    - Détection d'attaques de type déni de service protocolaire :
        - Épuisement des tables d'état de session
        - Fragmentation IP
    - Détection d'attaques de type déni de service applicatives :
        - Invoquant des délais d'expiration ou des changements d'état de session
        - Sollicitant des ressources mémoire ou processeur
        - Exploitant des vulnérabilités
    - Utilisation de seuils de détection :
        - En nombre de paquets par seconde
        - En nombre de transaction par seconde
    - Mécanismes de détection avancés :
        - Base de signatures
        - Base de réputation d'adresses IP
        - Analyse comportementale
    - Implémentation de mécanismes de mitigation (RTBH, uRPF, dispersion géographique, etc.)
    - Authentification : compatibilité LDAP et Active Directory, Serveur d'authentification sécurisé On Premise et dans le Cloud (Radius, Microsoft Authenticator, Google Authenticator), base locale
    - Si Haute disponibilité : fonctionnement en cluster actif/actif ou actif/passif au choix lors de l'intégration. Synchronisation automatique des nœuds de cluster.

- **[P**3401] Gamme 2 : au minimum 4 solutions anti DDoS permettant une architecture en haute disponibilité
    - Débit IP : 1 Gbps minimum
    - Détection d'attaques de type déni de service volumétriques sur les couches 3 à 7 : SYN, ICMP, TCP, UDP, HTTP, DNS, etc.
    - Détection d'attaques de type déni de service protocolaire :
        - Épuisement des tables d'état de session
        - Fragmentation IP
    - Détection d'attaques de type déni de service applicatives :
        - Invoquant des délais d'expiration ou des changements d'état de session
        - Sollicitant des ressources mémoire ou processeur
        - Exploitant des vulnérabilités
    - Utilisation de seuils de détection :
        - En nombre de paquets par seconde
        - En nombre de transaction par seconde
    - Mécanismes de détection avancés :
        - Base de signatures
        - Base de réputation d'adresses IP
        - Analyse comportementale
    - Implémentation de mécanismes de mitigation (RTBH, uRPF, dispersion géographique, etc.)
    - Authentification : compatibilité LDAP et Active Directory, Serveur d'authentification sécurisé On Premise et dans le Cloud (Radius, Microsoft Authenticator, Google Authenticator), base locale
    - Si Haute disponibilité : fonctionnement en cluster actif/actif ou actif/passif au choix lors de l'intégration. Synchronisation automatique des nœuds de cluster.
- **[P**3402] Gamme 3 : au minimum 4 solutions anti DDoS permettant une architecture en haute disponibilité
    - Débit IP : 10 Gbps minimum
    - Détection d'attaques de type déni de service volumétriques sur les couches 3 à 7 : SYN, ICMP, TCP, UDP, HTTP, DNS, etc.
    - Détection d'attaques de type déni de service protocolaire :
        - Épuisement des tables d'état de session
        - Fragmentation IP
    - Détection d'attaques de type déni de service applicatives :
        - Invoquant des délais d'expiration ou des changements d'état de session
        - Sollicitant des ressources mémoire ou processeur
        - Exploitant des vulnérabilités
    - Utilisation de seuils de détection :
        - En nombre de paquets par seconde
        - En nombre de transaction par seconde
    - Mécanismes de détection avancés :
        - Base de signatures
        - Base de réputation d'adresses IP
        - Analyse comportementale
    - Implémentation de mécanismes de mitigation (RTBH, uRPF, dispersion géographique, etc.)
    - Authentification : compatibilité LDAP et Active Directory, Serveur d'authentification sécurisé On Premise et dans le Cloud (Radius, Microsoft Authenticator, Google Authenticator), base locale
    - Si Haute disponibilité : fonctionnement en cluster actif/actif ou actif/passif au choix lors de l'intégration. Synchronisation automatique des nœuds de cluster.
- **[P**3403] Gamme 4 : au minimum 4 solutions anti DDoS permettant une architecture en haute disponibilité
    - Débit IP : 40 Gbps minimum

- Détection d'attaques de type déni de service volumétriques sur les couches 3 à 7 : SYN, ICMP, TCP, UDP, HTTP, DNS, etc.
- Détection d'attaques de type déni de service protocolaire :
  - Épuisement des tables d'état de session
  - Fragmentation IP
- Détection d'attaques de type déni de service applicatives :
  - Invoquant des délais d'expiration ou des changements d'état de session
  - Sollicitant des ressources mémoire ou processeur
  - Exploitant des vulnérabilités
- Utilisation de seuils de détection :
  - En nombre de paquets par seconde
  - En nombre de transaction par seconde
- Mécanismes de détection avancés :
  - Base de signatures
  - Base de réputation d'adresses IP
  - Analyse comportementale
- Implémentation de mécanismes de mitigation (RTBH, uRPF, dispersion géographique, etc.)
- Authentification : compatibilité LDAP et Active Directory, Serveur d'authentification sécurisé On Premise et dans le Cloud (Radius, Microsoft Authenticator, Google Authenticator), base locale
- Si Haute disponibilité : fonctionnement en cluster actif/actif ou actif/passif au choix lors de l'intégration. Synchronisation automatique des nœuds de cluster.

[P3410] Licences, abonnements et variantes associés à la solution, selon tranches et durées définies au BPU.

6.8.14. Orchestration et administration des politiques de sécurité

[ORCH-001] Les solutions d'orchestration de politique de filtrage, permettant la gestion automatisée de la politique de sécurité réseau du bénéficiaire, existent sur le marché soit sous forme de solution technique matérielle (appliance) soit sous forme logicielle. La version logicielle de la solution inclut la fourniture du système d'exploitation lorsque celui-ci n'est pas standard et présente des caractéristiques spécifiques implémentées par l'éditeur.

L'offre comprend DEUX solutions techniques distinctes.

[ORCH-002] Pour chaque solution technique, les principales fonctionnalités attendues sont les suivantes :

- Administration dans un environnement de firewalls hétérogène (multi constructeurs), les firewalls pouvant être des appliances et/ou des firewalls virtuels.
- Cartographie du réseau
- Validation de la conformité des règles par rapport à la politique de sécurité du bénéficiaire
- Cycle de vie des firewalls : révision de la politique de sécurité sur les firewalls permettant d'éliminer les mauvaises configurations, les objets et règles non utilisés.
- Audit de la politique de sécurité réseau
- Optimisation des règles de filtrage pour éviter les doublons et failles de sécurité.
- Génération de rapports à destination des responsables sécurité et directions.
- Workflow, selon un processus de validation défini, pour les demandes et réalisation de changements
- Granularité de profils permettant d'adapter les droits en fonction des rôles et du périmètre de gestion.
- Découverte/cartographie des flux pour les applications métiers définies. Corrélation avec les matrices de flux associées.
- Cartographie des flux entre applications.
- Authentification LDAP des administrateurs
- Traçabilité et historisation des demandes et modifications effectuées.
- Export des logs vers un outil tiers de consolidation de logs

[ORCH-003] La possibilité d'interfaçage avec des solutions tierces, telles que des solutions ITSM/Ticketing, de gestion des adresses IP ou de CMDB, constitue un atout apprécié dans les conditions fixées par les pièces de la consultation.
[ORCH-004] L'offre précise le mode de licence de la solution proposée, les métriques applicables, les limites éventuelles, les prérequis d'intégration et les modalités d'évolution.

[P3420] Gamme 1 : suite logicielle pour une capacité de 1 à 100 devices
[P3421] Gamme 2 : suite logicielle pour une capacité de 101 à 500 devices
[P3422] Gamme 3 : suite logicielle pour une capacité de plus de 500 devices

[P3430] Licences, abonnements et variantes associés à la solution, selon tranches et durées définies au BPU.

6.8.15. Infrastructure de gestion de clés publiques PKI et gestion du cycle de vie des certificats CLM

[PKI-001] Les solutions de PKI et de gestion du cycle de vie des certificats existent sur le marché sous forme de logiciels, d'appliances matérielles, de services managés, de services cloud ou de déploiements hybrides. L'offre comprend au moins deux solutions techniques distinctes permettant de couvrir les besoins de création, d'administration, de protection, de publication, de renouvellement, de révocation, de supervision et d'audit des certificats numériques utilisés par le système d'information du bénéficiaire.
[PKI-007] La solution couvre les usages liés aux certificats serveurs, certificats utilisateurs, certificats machines, certificats d'équipements réseau, certificats applicatifs, certificats utilisés pour l'authentification 802.1x, le chiffrement des communications, la signature, les accès distants, les services web, les API, les équipements de sécurité, les objets connectés et les environnements hybrides ou cloud lorsque ceux-ci sont utilisés par le bénéficiaire.

[PKI-002] Le candidat décrit l'architecture proposée, les composants inclus, les autorités de certification prises en charge, les autorités d'enregistrement, les modules de publication, les référentiels, les connecteurs, les interfaces d'administration, les mécanismes de haute disponibilité, les dépendances techniques, les prérequis d'intégration et les modalités de maintien en condition opérationnelle et de sécurité.
[PKI-008] Les exigences communes d'administration, de supervision, de journalisation, d'export des traces, de diagnostic, de haute disponibilité, de sauvegarde, de restauration, de MCO, de MCS, de réversibilité et de transférabilité sont celles définies dans les pièces communes du marché. Le présent paragraphe précise uniquement les exigences propres aux fonctions PKI et CLM.

[PKI-003] Les fonctionnalités minimales attendues sont les suivantes :

- Création, renouvellement, suspension, révocation et archivage des certificats
- Gestion des modèles de certificats, profils d'usage, politiques de certification et règles d'approbation
- Prise en charge des formats, protocoles et standards usuels, notamment X.509, CSR, OCSP, CRL, SCEP, EST, ACME ou équivalent
- Publication des informations de révocation et de validation des certificats
- Inventaire centralisé des certificats internes et externes
- Découverte automatique des certificats présents sur les serveurs, équipements réseau, applications, services exposés, équilibreurs de charge, pare-feu, passerelles, annuaires et plateformes cloud
- Alertes avant expiration, tableaux de bord de conformité et suivi des risques liés aux certificats expirés, faibles, non conformes ou inconnus
- Traçabilité complète des demandes, validations, émissions, renouvellements, révocations et actions d'administration
- Gestion des rôles, habilitations, circuits de validation et séparation des fonctions
- Intégration avec les annuaires, solutions IAM, serveurs d'authentification, équipements réseau, solutions NAC, EDR, SIEM, ITSM et outils d'automatisation

- Interfaces d'administration, API et mécanismes d'automatisation documentés
- Export des journaux vers une solution tierce de supervision ou de corrélation
- Mécanismes de sauvegarde, restauration, reprise d'activité et continuité de service adaptés au caractère critique de l'infrastructure de confiance.

[PKI-004] La solution permet au bénéficiaire de définir des politiques différenciées selon les usages, les populations, les équipements, les durées de validité, les niveaux d'assurance, les autorités émettrices, les circuits d'approbation et les exigences de sécurité applicables. Le candidat précise les limites éventuelles liées au nombre d'autorités, de certificats, de modèles, de connecteurs, de flux automatisés, d'utilisateurs administrateurs, de workflows et de certificats supervisés.

[PKI-005] Lorsque la solution intègre ou s'interface avec des modules matériels de sécurité, le candidat précise les HSM compatibles, les modes de raccordement, les exigences de certification, les mécanismes de protection des clés privées, les modalités de rotation, de sauvegarde, de séquestre lorsqu'il est applicable, de destruction et de restitution des clés en fin de prestation.

[PKI-006] Le candidat précise les modalités de déploiement disponibles : sur site, cloud, hybride, service managé ou combinaison de ces modes. Il indique les données traitées, leur localisation, les conditions d'accès aux données, les mécanismes de chiffrement, les garanties de réversibilité, les modalités d'export et les dépendances à des services tiers.

- [P4540] Gamme 1 :

[PKI-009] La gamme 1 couvre les besoins de mise en place, d'administration et de supervision d'une infrastructure de gestion de certificats pour des usages maîtrisés ou de périmètre limité. Elle permet notamment de gérer les certificats internes et externes, d'assurer leur renouvellement, leur révocation, leur supervision et leur traçabilité.

  - Gestion centralisée des certificats et de leur cycle de vie
  - Inventaire des certificats connus et découverte des certificats sur les périmètres déclarés
  - Alertes avant expiration et tableaux de bord de suivi
  - Gestion des demandes, validations, émissions et révocations
  - Intégration avec un annuaire d'entreprise et les principaux systèmes d'exploitation serveur
  - Publication CRL et/ou OCSP ou mécanisme équivalent
  - Rôles d'administration différenciés et journalisation des actions
  - API ou mécanismes d'automatisation pour les opérations courantes
  - Export des journaux vers une solution de supervision ou de corrélation
  - Documentation d'exploitation, d'administration et de réversibilité.

- [P4541] Gamme 2 :

[PKI-010] La gamme 2 couvre les besoins avancés ou critiques nécessitant une infrastructure de confiance étendue, fortement automatisée, interconnectée avec l'écosystème de sécurité et adaptée aux environnements multisites, hybrides, cloud, conteneurisés ou à forte volumétrie. Elle inclut les fonctionnalités de la gamme 1 et les complète par des capacités renforcées d'automatisation, de gouvernance, d'intégration, de conformité et de résilience.

  - Gestion multi-autorités, multi-entités ou multi-bénéficiaires avec séparation logique des périmètres
  - Automatisation avancée des demandes, renouvellements et révocations via API, connecteurs, workflows ou protocoles standards
  - Découverte étendue des certificats sur les environnements sur site, cloud, hybrides, équipements réseau, plateformes applicatives, conteneurs et services exposés
  - Intégration avec les solutions ITSM, SIEM, SOAR, IAM, PAM, NAC, MDM, EDR, passerelles applicatives, WAF, répartiteurs de charge et plateformes cloud
  - Gestion de politiques de certification différenciées par usage, périmètre, niveau d'assurance, criticité ou population
  - Prise en charge de chaînes de validation complexes et de circuits d'approbation personnalisables

- Fonctionnalités avancées de conformité, audit, reporting, cartographie des risques et remédiation
- Prise en charge de déploiements haute disponibilité, plan de reprise d'activité et mécanismes de continuité de service renforcés
- Intégration avec HSM, coffre-fort de secrets ou solution de gestion de clés lorsque nécessaire
- Capacités de délégation outillée permettant à plusieurs équipes ou entités de gérer leurs certificats dans un cadre gouverné.

[P4549] Licences, abonnements, connecteurs, modules complémentaires, services managés, options HSM, options d'automatisation, tranches de certificats, tranches d'équipements supervisés, tranches d'utilisateurs administrateurs et variantes associés aux solutions PKI/CLM sont renseignés selon les métriques, durées et modalités définies au BPU.
[PKI-011] Le candidat précise, pour chaque gamme, les métriques de licence applicables, notamment le nombre de certificats gérés, le nombre de certificats découverts, le nombre d'autorités de certification, le nombre de connecteurs, le nombre d'environnements couverts, le nombre d'administrateurs, le volume d'événements journalisés, les durées d'abonnement, ainsi que les éventuelles limites techniques ou contractuelles.

6.8.16. Contrôle USB

[USB-001] Contrôle et restrictions d'usage. La solution autorise, bloque ou restreint l'usage des supports amovibles selon des politiques centralisées et l'identification des périphériques.

[USB-002] Chiffrement et traçabilité. La solution assure le chiffrement, la traçabilité des opérations, le contrôle des copies et l'analyse antimalware des supports concernés.

[USB-003] Administration, exceptions et intégration. La solution permet la gestion des exceptions, le fonctionnement hors connexion, l'administration déléguée et l'intégration avec les annuaires et outils de sécurité.

Gammes et capacités minimales
[USB-004] Le candidat propose au moins deux solutions techniques distinctes et indique, pour chaque gamme, les limites de capacité, les prérequis de dimensionnement, les performances garanties, les modalités d'évolution et les conditions de haute disponibilité.

Gamme	Capacité minimale	Périmètre minimal
Gamme 1	1 000 postes administrés	Politiques centralisées, chiffrement et traçabilité des opérations.
Gamme 2	5 000 postes administrés	Administration déléguée, fonctionnement hors connexion et intégration annuaire.
Gamme 3	20 000 postes administrés	Architecture distribuée et haute disponibilité.

[USB-005] Les capacités indiquées constituent des minima. Toute limitation liée au mode de déploiement, aux fonctions activées, à la conservation des données ou à la haute disponibilité est explicitement précisée dans le CRT.

Gammes et licences associées aux supports amovibles USB
- [P4300] Gamme 1 : solution standard de contrôle des supports amovibles.
- [P4301] Gamme 2 : solution de contrôle avec chiffrement.
- [P4302] Gamme 3 : solution avec gestion centralisée avancée.
- [P4310] Licences pour 1 à 500 postes.
- [P4311] Licences pour 501 à 5 000 postes.
- [P4312] Licences pour plus de 5 000 postes.

6.8.17. Chiffrement LAN

[CHIFFREMENT-001] Chiffrement des flux et protocoles. La solution chiffre les flux du réseau local entre équipements, sites ou segments selon les standards et protocoles pris en charge.

[CHIFFREMENT-002] Gestion des clés et déploiement. La solution assure la gestion et la rotation des clés et précise les modes de déploiement ainsi que la transparence pour les applications.

[CHIFFREMENT-003] Performances, résilience et intégration. Le candidat précise les performances avec chiffrement activé, la haute disponibilité, la supervision, la journalisation et les conditions d'intégration dans les architectures existantes.

Gammes et capacités minimales
[CHIFFREMENT-004] Le candidat propose au moins deux solutions techniques distinctes et indique, pour chaque gamme, les limites de capacité, les prérequis de dimensionnement, les performances garanties, les modalités d'évolution et les conditions de haute disponibilité.

Gamme	Capacité minimale	Périmètre minimal
Gamme 1	Débit chiffré de 1 Gbit/s minimum	Deux interfaces réseau minimum chiffrement entre équipements ou segments.
Gamme 2	Débit chiffré de 10 Gbit/s minimum	Quatre interfaces réseau minimum gestion centralisée et rotation des clés.
Gamme 3	Débit chiffré de 40 Gbit/s minimum	Interfaces 10/25/40 Gbit/s haute disponibilité supervision et journalisation.

[CHIFFREMENT-005] Les capacités indiquées constituent des minima. Toute limitation liée au mode de déploiement, aux fonctions activées, à la conservation des données ou à la haute disponibilité est explicitement précisée dans le CRT.

Gammes et bundles associés au chiffrement LAN
- [P4400] Gamme 1 : chiffrement LAN à l'échelle d'un site.
- [P4401] Gamme 2 : chiffrement LAN intersites.
- [P4402] Gamme 3 : chiffrement LAN pour datacenter.
- [P4410] Bundle 1 : paire de solutions en haute disponibilité.
- [P4411] Bundle 2 : solution redondée multisites.

6.8.18. Administration hors bande OOB

[OOB-001] Accès d'administration sécurisés. La solution fournit des accès console et réseau sécurisés, indépendants du réseau de production, en situation nominale ou dégradée.

[OOB-002] Authentification forte et traçabilité. La solution assure l'authentification forte, la gestion des rôles, le chiffrement, la traçabilité et, le cas échéant, l'enregistrement des sessions et des actions.

[OOB-003] Résilience, supervision et intégration. La solution fournit les mécanismes de rebond, la redondance, l'alimentation secourue, l'administration centralisée et l'intégration avec les annuaires, bastions et outils de supervision.

Gammes et capacités minimales
[OOB-004] Le candidat propose au moins deux solutions techniques distinctes et indique, pour chaque gamme, les limites de capacité, les prérequis de dimensionnement, les performances garanties, les modalités d'évolution et les conditions de haute disponibilité.

Gamme	**Capacité minimale**	**Périmètre minimal**
Gamme 1	**Jusqu'à 32 équipements administrés**	Jusqu'à 32 ports console ou équivalent au moins deux accès réseau sécurisés indépendants alimentation redondante appréciée adaptée aux établissements de petite taille ou aux sites isolés.

Gamme 2	**De 33 à 128 équipements administrés**	Jusqu'à 128 ports console ou équivalent authentification forte (MFA) journalisation centralisée des sessions et actions administrateur adaptée aux établissements de taille intermédiaire.
Gamme 3	**De 129 à 256 équipements administrés**	Jusqu'à 256 ports console ou équivalent haute disponibilité enregistrement des sessions mécanismes de rebond (jump host) supervision centralisée adaptée aux grands établissements et établissements supports de GHT.
Gamme 4	**Plus de 256 équipements administrés**	Architecture distribuée ou multisite haute disponibilité administration centralisée gestion de plusieurs centaines d'équipements adaptée aux CHU, grands GHT et infrastructures critiques multisites.

[OOB-005] Les capacités indiquées constituent des minima. Toute limitation liée au mode de déploiement, aux fonctions activées, à la conservation des données ou à la haute disponibilité est explicitement précisée dans le CRT.
[OOB-006] Chaque solution technique est autonome, peut être acquise seule et peut être combinée avec d'autres solutions dans l'environnement du bénéficiaire.
Une offre logicielle et/ou matérielle proposée peut répondre éventuellement à plusieurs des solutions techniques demandées. C'est alors une solution multifonction.
[OOB-007] Les propositions techniques doivent être adaptées au besoin de chaque domaine et de chaque gamme. Les réponses surdimensionnées ou couvrant largement au-delà du domaine demandé ne seront pas valorisées.
Dans le cas d'une solution multifonction :

- L'offre est déclinée pour chaque solution technique afin de permettre une acquisition et une mise en œuvre des fonctionnalités individuellement
- L'offre est proposée sous forme de bundles en tant que solutions multifonction pour permettre une acquisition et une mise en œuvre de tout ou partie des fonctionnalités proposées au sein d'une même solution technique

Gammes et bundles associés au management hors bande OOB

- [P4500] Gamme 1 : jusqu'à 32 équipements administrés.
- [P4501] Gamme 2 : jusqu'à 128 équipements administrés.
- [P4502] Gamme 3 : jusqu'à 256 équipements administrés.
- [P4503] Gamme 4 : plus de 256 équipements administrés.
- [P4510] Bundle 1 : architecture OOB en haute disponibilité.
- [P4511] Bundle 2 : architecture OOB multisites.

6.8.19. Accessoires, gammes constructeurs et outils d'administration

[P3440] L'offre comprend les prix unitaires d'une gamme complète de modules optiques de tous types et de marques compatibles avec les gammes de matériels des constructeurs proposés au BPU.
[ACC-001] Le titulaire et les constructeurs concernés garantissent le fait que l'usage des modules optiques compatibles proposés ne limite en aucun cas l'accès au support et autres garanties souscrites par un bénéficiaire.

6.8.20. La gamme constructeur générale

[P3450] En complément des gammes de matériels demandés dans les paragraphes ci-dessus et représentant la majorité des besoins des bénéficiaires, l'offre comprend l'ensemble de la gamme matérielle des constructeurs/éditeurs retenus en firewalls, passerelles internet et de messagerie, portail extranet. Tous les accessoires et add-ons de ces gammes complémentaires sont proposés. L'offre indique les taux de remise sur prix publics pour chacun des éléments de ces gammes.

6.8.21. Les outils d'administration constructeur/éditeur

[ADMIN-001] Les équipements installés sont supervisés et administrés par un logiciel pour chaque solution technique demandée, le logiciel pouvant être commun à plusieurs solutions techniques, et couvrant les

fonctionnalités principales de configuration, sauvegarde, gestion de versions, haute disponibilité, règles de filtrage, historique, alarmes, incidents, statistiques, diagnostic, authentification et agent SNMP.

- Configuration des équipements via une interface graphique unique,
- Gestion des configurations : téléchargement, sauvegarde…
- Gestion des versions logicielles : téléchargement, sauvegarde….
- Configuration et gestion centralisée des configurations et de la haute disponibilité,
- Configuration et gestion centralisée des règles de filtrage et de sécurité,
- Historique des actions d'administration (configuration).
- Interface conviviale
- Gestion des alarmes via la remontée de traps SNMP ou de surveillance (polling),
- Redirection des alarmes vers d'autres supports tels sur messagerie, SMS…
- Historique des incidents
- Statistiques sur l'état de la QoS, sur les règles de filtrage et sur le transit des données.
- Aide au diagnostic par l'interprétation des traps, la capitalisation des incidents précédents.
- Procédure de login des utilisateurs,
- Droits associés en fonction des différents niveaux d'utilisateurs.
- Pour tous les équipements : agent SNMP

[ADMIN-002] Il est souhaitable que l'outil dispose d'un assistant, de type wizard, pour les opérations les plus courantes.

[P3460] Briques logicielles d'administration constructeur ou éditeur, selon le détail du BPU.

6.8.22. Services professionnels, transfert de compétences et automatisation

Ces prestations sont en conformité avec le paragraphe 3.7 du présent CCTP. Leur description générale est indiquée ci-dessous et le bénéficiaire précise le détail exact de la prestation lors de l'émission d'un bon de commande.

[SERVICES-001] Ces prestations sont regroupées en deux principaux types :

- Ingénierie, audit et assistance générale
- Intégration, implémentation et exploitation

[SERVICES-003] L'offre précise systématiquement pour chaque prestation le curriculum vitae type de l'intervenant, son niveau de qualification ou d'expertise, le nombre de jours d'intervention envisagé, les éventuels prérequis à fournir par le bénéficiaire et toute autre information nécessaire à la bonne qualification et réalisation de la prestation.

- Le curriculum vitae type de l'intervenant, ainsi que son niveau de qualification ou d'expertise
- Le nombre de jours d'intervention envisagé
- Les éventuels prérequis à fournir par le bénéficiaire
- Toute autre information nécessaire à la bonne qualification et réalisation de la prestation

[SERVICES-004] Afin d'adapter au mieux la prestation à la taille des réseaux existants dans les bénéficiaires, l'unité d'œuvre des prestations d'ingénierie, d'audit et d'assistance générale est calculée sur la base d'une fonction sécurité type comprenant, selon les projets, une paire de solutions fonctionnelles décrites dans le présent paragraphe.

- Une paire de solutions fonctionnelles décrites dans le présent paragraphe :
  - Une paire de firewall contenant 300 règles et 6 interfaces en HA
  - Ou une paire de passerelles internet/SMTP en HA
  - Ou une paire de solutions d'analyse comportementales type « Bac à sables » :
  - Ou une paire de portail extranet en HA
  - Ou une paire de solutions d'applications web
  - Ou une paire de commutateurs L5-L7

- Une paire de portails captifs (cluster haute disponibilité).
- Ou une paire de serveurs d'authentification (cluster haute disponibilité),
- Ou une paire de solutions de contrôle d'accès réseau (cluster haute disponibilité)
- Ou une paire de commutateurs applicatifs
- Ou une paire de sondes IDS/IPS
- Ou une paire de sondes anti-DDoS
- Une paire d'appliance ou de serveurs DNS/DHCP
- Toutes solutions en configuration standard (toutes fonctionnalités incluses)

[SERVICES-005] Pour les infrastructures de taille supérieure, ce qui est souvent le cas dans les bénéficiaires, la prestation est évaluée sur la base d'un multiple et/ou de la somme des unités d'œuvre de base indiquée dans le présent paragraphe.

[SERVICES-006] Les firewalls basiques P3000 et P3001 ne sont pas concernés par les prestations d'ingénierie, d'audit et d'assistance générale.

[SERVICES-007] La dégressivité des coûts en quantité des UOE d'intégration s'applique lorsque l'ensemble des matériels concernés est à intégrer sur un même site géographique et que les bâtiments hébergeant les locaux techniques concernés ne sont pas distants de plus de 300 mètres les uns des autres.

- L'ensemble des matériels concernés est à intégrer sur un même site géographique
- Les bâtiments hébergeant les locaux techniques concernés ne sont pas distants de plus de 300 mètres les uns des autres.

[SERVICES-008] Les prestations attendues sont toujours encadrées par les prérequis imposés par le bénéficiaire dont le titulaire tient obligatoirement compte, notamment le budget, le planning du projet et les délais de prestations.

6.8.23. Les prestations d'ingénierie d'audit et d'assistance générale

Les prestations couvrent les audits, inventaires, études d'évolution, rénovations, plans de continuité et missions de gestion de projet décrits ci-dessous.
Dispositions communes : le bénéficiaire fournit les documents, configurations et accès nécessaires. Sauf précision contraire, chaque prestation comprend l'analyse de l'existant, la définition de la cible, les recommandations, la méthode de mise en œuvre, le planning, les contraintes et le chiffrage fondé sur le présent marché.
Les livrables sont remis dans des formats modifiables et comprennent uniquement les éléments adaptés à la prestation : rapport, inventaire, synoptique, matrice de flux, dossier de cible, méthode de mise en œuvre, planning ou compte rendu.
Les prestations relatives aux infrastructures de taille supérieure sont valorisées par addition ou multiplication des unités d'œuvre. Les références P3000 et P3001 sont exclues de ce dispositif. La dégressivité des UOE d'intégration s'applique lorsque les équipements sont installés sur un même site et que les bâtiments concernés sont distants de 300 mètres au plus.

- [P3500] Firewalls, portails, passerelles : Bilan d'infrastructure sécurité existante
    - Prérequis bénéficiaire : toutes documentations, configurations
    - Synoptique de l'infrastructure (tous les éléments de l'infrastructure)
    - Synoptique fonctionnel
    - Photographie du plan d'adressage utilisé (privé, publique) et de la translation d'adresses
    - Cohérence des règles de sécurité
    - Photographie des VPN implantés
    - Photographie du routage et de l'interconnexion avec l'infrastructure de réseau interne et publique.
    - Matrice de flux tous domaines applicatifs confondus
    - Fonctionnalités implémentées

- Écarts avec l'état de l'art sur les services implémentés
- Livrables : synoptiques, inventaire IP/translation d'adresses, VPN, règles de sécurité, filtrages, rapport explicatif.

- [P3501] Toutes solutions techniques : Inventaire d'infrastructure sécurité existante :
  - Prérequis bénéficiaire : accès aux infrastructures réseau
  - Liste exhaustive de tous les matériels et logiciels en production sur le réseau
  - N° de série, types et version de système d'exploitation par matériel
  - Sauvegarde centralisée des configurations et des systèmes d'exploitation
  - Livrables : tableau Excel comprenant toutes les informations demandées, CD/DVD comprenant toutes les configurations des matériels et logiciels.
- [P3502] Toutes solutions techniques : Mise à jour d'inventaire d'infrastructure sécurité existante (correction <50%) :
  - Prérequis bénéficiaire : document d'inventaires existants, schémas d'infrastructures, accès aux infrastructures réseau
  - Liste exhaustive de tous les matériels et logiciels en production sur le réseau
  - N° de série, types et version de système d'exploitation par matériel
  - Sauvegarde centralisée des configurations et des systèmes d'exploitation
  - Livrables : tableau Excel comprenant toutes les informations demandées, CD/DVD comprenant toutes les configurations des matériels.
- [P3503] Bilan d'infrastructure IPAM existante comprenant
  - Prérequis bénéficiaire : toutes documentations, configurations
  - Synoptique de l'infrastructure réseau
  - Photographie du plan d'adressage utilisé
  - Bilan de l'utilisation du plan d'adressage
  - Fonctionnalités implémentées
  - Écarts avec l'état de l'art sur les services implémentés
  - Livrables : synoptiques, inventaire IP/adresses MAC, rapport explicatif.
- [P3504] Évolution d'infrastructure de firewall de tous types (périmétriques et Datacenter) :
  - Prérequis bénéficiaire : synoptiques réseau, schémas et fonctionnalités de sécurité implémentées, règles de sécurité, translation d'adressage, règles de filtrages, cible recherchée
  - Proposition d'évolution matérielle et ou logicielle d'une fonctionnalité sécurité vétuste
  - Optimisation des matériels et logiciels en production et description détaillée de l'architecture cible
  - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.
- [P3505] Évolution d'infrastructure de portail extranet :
  - Prérequis bénéficiaire : synoptiques réseau, schémas et fonctionnalités de sécurité implémentées, règles de sécurité, translation d'adressage, règles de filtrages, cible recherchée
  - Proposition d'évolution matérielle et ou logicielle d'une fonctionnalité sécurité vétuste
  - Optimisation des matériels et logiciels en production et description détaillée de l'architecture cible
  - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.
- [P3506] Évolution d'infrastructure de passerelles internet de tous types :
  - Prérequis bénéficiaire : synoptiques réseau, schémas et fonctionnalités de sécurité implémentées, règles de sécurité, translation d'adressage, règles de filtrages, cible recherchée
  - Proposition d'évolution matérielle et ou logicielle d'une fonctionnalité sécurité vétuste
  - Optimisation des matériels et logiciels en production et description détaillée de l'architecture cible
  - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.

- [P3507] Évolution d'infrastructure de solutions d'analyse comportementales type « Bac à sables » :
    - Prérequis bénéficiaire : synoptiques réseau, schémas et fonctionnalités de sécurité implémentées, règles de sécurité, règles de filtrages, cible recherchée, environnements clients types
    - Proposition d'évolution matérielle et ou logicielle d'une fonctionnalité sécurité vétuste
    - Optimisation des matériels et logiciels en production et description détaillée de l'architecture cible
    - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.
- [P3508] Évolution d'infrastructure de solutions de serveur d'authentification :
    - Prérequis bénéficiaire : Liste exhaustive et état des lieux des annuaires de tous types, état du parc client (tous types de terminaux), cahier de spécifications techniques générales de la solution en production, cible recherchée détaillée par utilisateur/terminal.
    - Proposition d'évolution matérielle et ou logicielle d'une fonctionnalité sécurité vétuste
    - Optimisation des matériels et logiciels en production et description détaillée de l'architecture cible
    - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.
- [P3509] Évolution d'infrastructure d'une solution de contrôle d'accès :
    - Prérequis bénéficiaire : Liste exhaustive et état des lieux des annuaires de tous types, état du parc client (tous types de terminaux), cahier de spécifications techniques générales de la solution en production, cible recherchée détaillée par utilisateur/terminal.
    - Proposition d'évolution matérielle et ou logicielle d'une fonctionnalité sécurité vétuste
    - Optimisation des matériels et logiciels en production et description détaillée de l'architecture cible
    - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.
- [P3510] Évolution d'infrastructure d'une solution de publication d'applications web :
    - Prérequis bénéficiaire : Synoptiques réseau, schémas et fonctionnalités de sécurité implémentées, application concernées, cible recherchée détaillée.
    - Proposition d'évolution technique et fonctionnelle
    - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire
- [P3511] Évolution d'infrastructure d'une solution de commutateurs applicatifs :
    - Prérequis bénéficiaire : Synoptiques réseau, schémas et fonctionnalités de sécurité implémentées, application concernées, cible recherchée détaillée.
    - Ingénierie, analyse des flux, fonctionnalités implémentées
    - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.
- [P3512] Évolution d'infrastructure de sondes IDS/IPS :
    - Prérequis bénéficiaire : synoptiques réseau, schémas et fonctionnalités de sécurité implémentées, règles de sécurité, règles de filtrages, cible recherchée
    - Proposition d'évolution matérielle et ou logicielle d'une fonctionnalité sécurité vétuste
    - Optimisation des matériels et logiciels en production et description détaillée de l'architecture cible
    - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.
- [P3513] Évolution d'infrastructure de sondes Anti-DDoS :

    - Prérequis bénéficiaire : synoptiques réseau, schémas et fonctionnalités de sécurité implémentées, règles de sécurité, règles de filtrages, cible recherchée
    - Proposition d'évolution matérielle et ou logicielle d'une fonctionnalité sécurité vétuste
    - Optimisation des matériels et logiciels en production et description détaillée de l'architecture cible
    - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.
- [P3514] Évolution fonctionnelle de firewall de tous types :
    - Prérequis bénéficiaire : synoptiques réseau, schémas et fonctionnalités de sécurité implémentées, règles de sécurité, translation d'adressage, règles de filtrages, cible recherchée
    - Proposition d'évolution fonctionnelle (plan d'adressage, règles/filtres, haute disponibilité…)
    - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.
- [P3515] Évolution fonctionnelle de portail extranet :
    - Prérequis bénéficiaire : synoptiques réseau, schémas et fonctionnalités de sécurité implémentées, règles de sécurité, translation d'adressage, règles de filtrages, cible recherchée
    - Proposition d'évolution fonctionnelle (plan d'adressage, règles/filtres, haute disponibilité…)
    - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.
- [P3516] Évolution fonctionnelle de passerelles internet de tous types :
    - Prérequis bénéficiaire : synoptiques réseau, schémas et fonctionnalités de sécurité implémentées, règles de sécurité, translation d'adressage, règles de filtrages, cible recherchée
    - Proposition d'évolution fonctionnelle (plan d'adressage, règles/filtres, haute disponibilité…)
    - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.
- [P3517] Évolution fonctionnelle de solutions d'analyse comportementales type « Bac à sables » :
    - Prérequis bénéficiaire : synoptiques réseau, schémas et fonctionnalités de sécurité implémentées, règles de sécurité, translation d'adressage, règles de filtrages, cible recherchée, environnement client type.
    - Proposition d'évolution fonctionnelle (capacité d'environnements clients, règles/filtres, haute disponibilité…)
    - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.
- [P3518] Rénovation complète d'une infrastructure de sécurité (matériel et fonctionnel) de firewall de tous types :
    - Prérequis bénéficiaire : synoptiques réseau, schémas et fonctionnalités de sécurité implémentées, règles de sécurité, translation d'adressage, règles de filtrages, cible recherchée
    - Proposition d'évolution matérielle
    - Proposition d'évolution fonctionnelle
    - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.
- [P3519] Rénovation complète d'une infrastructure de sécurité (matériel et fonctionnel) de portail extranet :
    - Prérequis bénéficiaire : synoptiques réseau, schémas et fonctionnalités de sécurité implémentées, règles de sécurité, translation d'adressage, règles de filtrages, cible recherchée
    - Proposition d'évolution matérielle
    - Proposition d'évolution fonctionnelle

    - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.
- [P3520] Rénovation complète d'une infrastructure de sécurité (matériel et fonctionnel) de passerelles internet de tous types :
    - Prérequis bénéficiaire : synoptiques réseau, schémas et fonctionnalités de sécurité implémentées, règles de sécurité, translation d'adressage, règles de filtrages, cible recherchée
    - Proposition d'évolution matérielle
    - Proposition d'évolution fonctionnelle
    - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.
- [P3521] Rénovation complète d'une infrastructure de gestion IP (matériel et fonctionnel) :
    - Prérequis bénéficiaire : synoptiques réseau, schémas et fonctionnalités implémentées niveau 2 et 3, plan d'adressage, cible recherchée
    - Proposition d'évolution matérielle
    - Proposition d'évolution fonctionnelle
    - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning théorique, contraintes de mises en œuvre pour le bénéficiaire.
- [P3522] Évolution et rénovation d'un portail captif d'authentification :
    - Prérequis bénéficiaire : Liste exhaustive et état des lieux des annuaires de tous types, état du parc client (tous types de terminaux), cahier de spécifications techniques générales de la solution en production, cible recherchée détaillée par utilisateur/terminal.
    - Ingénierie d'authentification
    - Définition des scénarii à mettre en œuvre
    - Proposition d'évolution technique et fonctionnelle
    - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.
- [P3523] Évolution et rénovation d'un serveur d'authentification sécurisée :
    - Prérequis bénéficiaire : Liste exhaustive et état des lieux des annuaires de tous types, méthodologie d'authentification, cahier de spécifications techniques générales de la solution en production, cible recherchée détaillée par utilisateur/terminal.
    - Ingénierie d'authentification
    - Définition des scénarii à mettre en œuvre
    - Proposition d'évolution technique et fonctionnelle
    - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.
- [P3524] Évolution et rénovation d'une solution de contrôle d'accès :
    - Prérequis bénéficiaire : Liste exhaustive de tous les matériels réseaux en production, état des lieux des annuaires de tous types, état du parc client (tous types de terminaux), cahier de spécifications techniques générales de la solution en production, cible recherchée détaillée par utilisateur/terminal.
    - Ingénierie d'authentification, de profilage et de posture des clients
    - Définition des scénarii à mettre en œuvre
    - Proposition d'évolution technique et fonctionnelle
    - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.
    - Coût unitaire dégressif par profil utilisateur/terminal à l'unité, par [2 à 4], par [5 à 9], par [10 et plus].
- [P3525] Évolution et rénovation d'une solution de publication d'applications web :

    - Prérequis bénéficiaire : Synoptiques réseau, schémas et fonctionnalités de sécurité implémentées, application concernées, cible recherchée détaillée.
    - Proposition d'évolution technique et fonctionnelle
    - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.
- [P3526] Évolution et rénovation d'une solution de commutateurs applicatifs :
    - Prérequis bénéficiaire : Synoptiques réseau, schémas et fonctionnalités de sécurité implémentées, application concernées, cible recherchée détaillée.
    - Ingénierie, analyse des flux, fonctionnalités implémentées
    - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.
- [P3527] Rénovation complète de sondes IDS/IPS :
    - Prérequis bénéficiaire : synoptiques réseau, schémas et fonctionnalités de sécurité implémentées, règles de sécurité, règles de filtrages, cible recherchée
    - Proposition d'évolution matérielle
    - Proposition d'évolution fonctionnelle
    - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.
- [P3528] Rénovation complète de sondes anti-DDoS :
    - Prérequis bénéficiaire : synoptiques réseau, schémas et fonctionnalités de sécurité implémentées, règles de sécurité, règles de filtrages, cible recherchée
    - Proposition d'évolution matérielle
    - Proposition d'évolution fonctionnelle
    - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.
- [P3529] Plan de continuité d'activité des solutions de sécurité :
    - Prérequis bénéficiaire : synoptiques réseau, schémas et fonctionnalités de sécurité implémentées, règles de sécurité, translation d'adressage, règles de filtrages, cible recherchée
    - Bilan de la haute-disponibilité existante
    - Proposition d'évolution matérielle et/ou logicielle
    - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.
- [P3530] Plan de continuité d'activité de toutes les solutions d'authentification et de contrôle d'accès :
    - Prérequis bénéficiaire : Cahier de spécifications techniques générales de la solution en production, cible recherchée.
    - Bilan de la haute-disponibilité existante
    - Proposition d'évolution matérielle et/ou logicielle
    - Livrables : description détaillée de la cible, synoptiques, méthodologie détaillée de mise en œuvre, évaluation du coût sur la base du présent marché public, planning, contraintes de mises en œuvre pour le bénéficiaire.
- [P3531] Assistance générale gestion de projet d'une solution de sécurité de type Firewall :
    - Prérequis bénéficiaire : définition des objectifs et finalités du projet, liste des fournitures commandées, documentation infrastructure existante en cas de remplacement
    - Suivi de projet et de toutes ses étapes
    - Coordination des intervenants (du titulaire et du bénéficiaire)
    - Planification globale du projet
    - Accompagnement au changement
    - Gestion des risques
    - Résolution des difficultés techniques

    - Organisation des comités de pilotage et rédaction des comptes-rendus
    - Livrables : plannings, comptes-rendus de réunion, suivi de projet.
- [P3532] Assistance générale gestion de projet d'une solution de sécurité de type portail extranet :
    - Prérequis bénéficiaire : définition des objectifs et finalités du projet, liste des fournitures commandées, documentation infrastructure existante en cas de remplacement
    - Suivi de projet et de toutes ses étapes
    - Coordination des intervenants (du titulaire et du bénéficiaire)
    - Planification globale du projet
    - Accompagnement au changement
    - Gestion des risques
    - Résolution des difficultés techniques
    - Organisation des comités de pilotage et rédaction des comptes-rendus
    - Livrables : plannings, comptes-rendus de réunion, suivi de projet.
- [P3533] Assistance générale gestion de projet d'une solution de sécurité de type passerelle internet/SMTP :
    - Prérequis bénéficiaire : définition des objectifs et finalités du projet, liste des fournitures commandées, documentation infrastructure existante en cas de remplacement
    - Suivi de projet et de toutes ses étapes
    - Coordination des intervenants (du titulaire et du bénéficiaire)
    - Planification globale du projet
    - Accompagnement au changement
    - Gestion des risques
    - Résolution des difficultés techniques
    - Organisation des comités de pilotage et rédaction des comptes-rendus
    - Livrables : plannings, comptes-rendus de réunion, suivi de projet.
- [P3534] Assistance générale gestion de projet d'une solution d'analyse comportementale type « bac à sable » :
    - Prérequis bénéficiaire : définition des objectifs et finalités du projet, liste des fournitures commandées, documentation infrastructure existante en cas de remplacement
    - Suivi de projet et de toutes ses étapes
    - Coordination des intervenants (du titulaire et du bénéficiaire)
    - Planification globale du projet
    - Accompagnement au changement
    - Gestion des risques
    - Résolution des difficultés techniques
    - Organisation des comités de pilotage et rédaction des comptes-rendus
    - Livrables : plannings, comptes-rendus de réunion, suivi de projet.
- [P3535] Assistance générale gestion de projet d'une solution de portail captif d'authentification :
    - Prérequis bénéficiaire : définition des objectifs et finalités du projet, liste des fournitures commandées, documentation infrastructure existante en cas de remplacement.
    - Suivi de projet et de toutes ses étapes
    - Coordination des intervenants (du titulaire et du bénéficiaire)
    - Planification globale du projet
    - Accompagnement au changement
    - Gestion des risques
    - Résolution des difficultés techniques
    - Organisation des comités de pilotage et rédaction des comptes-rendus
    - Livrables : plannings, comptes-rendus de réunion, suivi de projet.
- [P3536] Assistance générale gestion de projet d'une solution d'authentification sécurisée :
    - Prérequis bénéficiaire : définition des objectifs et finalités du projet, liste des fournitures commandées, documentation infrastructure existante en cas de remplacement.
    - Suivi de projet et de toutes ses étapes
    - Coordination des intervenants (du titulaire et du bénéficiaire)
    - Planification globale du projet

    - Accompagnement au changement
    - Gestion des risques
    - Résolution des difficultés techniques
    - Organisation des comités de pilotage et rédaction des comptes-rendus
    - Livrables : plannings, comptes-rendus de réunion, suivi de projet.
    -
- [P3537] Assistance générale gestion de projet d'une solution de contrôle d'accès physique :
    - Prérequis bénéficiaire : définition des objectifs et finalités du projet, liste des fournitures commandées, documentation infrastructure existante en cas de remplacement.
    - Suivi de projet et de toutes ses étapes
    - Coordination des intervenants (du titulaire et du bénéficiaire)
    - Planification globale du projet
    - Accompagnement au changement
    - Gestion des risques
    - Résolution des difficultés techniques
    - Organisation des comités de pilotage et rédaction des comptes-rendus
    - Livrables : plannings, comptes-rendus de réunion, suivi de projet.
- [P3538] Assistance générale gestion de projet d'une solution de publication d'applications web :
    - Prérequis bénéficiaire : définition des objectifs et finalités du projet, liste des fournitures commandées, documentation infrastructure existante en cas de remplacement.
    - Suivi de projet et de toutes ses étapes
    - Coordination des intervenants (du titulaire et du bénéficiaire)
    - Planification globale du projet
    - Accompagnement au changement
    - Gestion des risques
    - Résolution des difficultés techniques
    - Organisation des comités de pilotage et rédaction des comptes-rendus
    - Livrables : plannings, comptes-rendus de réunion, suivi de projet.
- [P3539] Assistance générale gestion de projet d'une solution de type IPAM :
    - Prérequis bénéficiaire : définition des objectifs et finalités du projet, liste des fournitures commandées, documentation infrastructure existante en cas de remplacement
    - Suivi de projet et de toutes ses étapes
    - Coordination des intervenants (du titulaire et du bénéficiaire)
    - Planification globale du projet
    - Accompagnement au changement
    - Gestion des risques
    - Résolution des difficultés techniques
    - Organisation des comités de pilotage et rédaction des comptes-rendus
    - Livrables : plannings, comptes-rendus de réunion, suivi de projet.
- [P3540] Assistance générale gestion de projet d'une solution de commutation applicative L5/L7 :
    - Prérequis bénéficiaire : définition des objectifs et finalités du projet, liste des fournitures commandées, documentation infrastructure existante en cas de remplacement.
    - Suivi de projet et de toutes ses étapes
    - Coordination des intervenants (du titulaire et du bénéficiaire)
    - Planification globale du projet
    - Accompagnement au changement
    - Gestion des risques
    - Résolution des difficultés techniques
    - Organisation des comités de pilotage et rédaction des comptes-rendus
    - Livrables : plannings, comptes-rendus de réunion, suivi de projet.
- [P3541] Assistance générale gestion de projet d'une solution de sondes IDS/IPS ou anti-DDoS :
    - Prérequis bénéficiaire : définition des objectifs et finalités du projet, liste des fournitures commandées, documentation infrastructure existante en cas de remplacement
    - Suivi de projet et de toutes ses étapes

- Coordination des intervenants (du titulaire et du bénéficiaire)
- Planification globale du projet
- Accompagnement au changement
- Gestion des risques
- Résolution des difficultés techniques
- Organisation des comités de pilotage et rédaction des comptes-rendus
- Livrables : plannings, comptes-rendus de réunion, suivi de projet.

6.8.24. Les prestations d'assistance, d'intégration et d'exploitation

[SERVICES-002] Les prestations d'intégration et d'exploitation sont directement liées à l'installation ou la modification de matériel ou de logiciels existants. L'offre précise le cas échéant les coûts dégressifs en quantité.

Remarque : Le temps de gestion interne au titulaire lié à son fonctionnement tel que le temps de planification des ressources, l'organisation des livraisons ou le suivi administratif des commandes n'est pas refacturable à un bénéficiaire par une prestation de service en UOE.

Sont incluses les prestations suivantes :

- **[P**3600] Assistance cahier de spécifications techniques générales
  - Prérequis bénéficiaire : Documentation infrastructure concernée existante en cas de remplacement, définition de la cible recherchée
  - Rédaction du cahier de spécifications techniques générales
  - Livrables : cahier de spécifications techniques générales
- **[P**3601] Assistance à la réalisation de maquette de mise en œuvre :
  - Prérequis bénéficiaire : cahier de spécifications techniques générales
  - Réalisation de maquettes à partir du matériel livré
  - Application des spécifications techniques générales
  - Exécution des cahiers de réception sur la maquette
  - Livrables : maquette conforme aux spécifications techniques générales
- **[P**3602] Assistance cahier de réception
  - Prérequis bénéficiaire : cahier de spécifications techniques générales
  - Rédaction du cahier de réception
  - Livrables : cahier de réception
- **[P**3603] Assistance cahier de déploiement.
  - Prérequis bénéficiaire : cahier de spécifications techniques générales, cahier de réception
  - Rédaction du cahier de déploiement
  - Livrables : cahier de déploiement
- [P3604] Assistance cahier d'exploitation.
  - Prérequis bénéficiaire : cahier de spécifications techniques générales, cahier de réception
  - Rédaction du cahier d'exploitation
  - Livrables : cahier d'exploitation
- **[P**3605] Assistance au déploiement :
  - Prérequis bénéficiaire : cahier de spécifications techniques générales, cahier de réception, cahier de déploiement, cahier d'exploitation.
  - Exécution du cahier de déploiement sur l'installation
  - Livrables : cahiers de déploiement exécutés avec succès.
- **[P**3606] Assistance à la réception :
  - Prérequis bénéficiaire : cahier de spécifications techniques générales, cahier de réception
  - Exécution des cahiers de réception sur l'installation
  - Livrables : cahiers de réception exécutés avec succès et conformité de l'installation au cahier de spécifications techniques générales.

6.8.25. Les prestations d'intégration et d'exploitation

[P3700] Intégration d'un firewall « internet »
- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Installation physique
- Système d'exploitation et configuration, reprise de règles et configurations existantes
- Authentification
- Application cahier de déploiement et du cahier de réception
- Tests et validation

[P3701] Intégration d'un firewall « datacenter »
- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Installation physique
- Système d'exploitation et configuration, reprise de règles et configurations existantes
- Authentification
- Application cahier de déploiement et du cahier de réception
- Tests et validation

[P3702] Intégration d'un portail extranet :
- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Installation physique
- Système d'exploitation et configuration, reprise de règles et configurations existantes
- Authentification
- Application cahier de déploiement et du cahier de réception
- Tests et validation

[P3703] Intégration d'une passerelle internet-web :
- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Installation physique
- Système d'exploitation et configuration
- Authentification
- Application cahier de déploiement et du cahier de réception
- Tests et validation

[P3704] Intégration d'une passerelle de messagerie SMTP :
- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Installation physique
- Système d'exploitation et configuration
- Authentification
- Application cahier de déploiement et du cahier de réception
- Tests et validation

[P3705] Intégration d'une solution d'analyse comportementale type « bac à sable » :
- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Installation physique
- Système d'exploitation et configuration
- Authentification
- Installation des masters
- Application cahier de déploiement et du cahier de réception
- Tests et validation

[P3706] Intégration d'une solution multifonctions internet périmétrique :
- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Installation physique
- Système d'exploitation et configuration
- Authentification
- Application cahier de déploiement et du cahier de réception
- Tests et validation

[P3707] Intégration d'un portail captif d'authentification :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Installation physique
- Système d'exploitation et configuration
- Authentification
- Application cahier de déploiement
- Tests et validation

[P3708] Intégration d'un serveur d'authentification Serveur d'authentification sécurisé On Premise et dans le Cloud (Radius, Microsoft Authenticator, Google Authenticator) :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Installation physique
- Système d'exploitation et configuration
- Authentification
- Application cahier de déploiement
- Tests et validation

[P3709] Intégration d'une solution de contrôle d'accès réseau :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Installation physique
- Système d'exploitation et configuration
- Authentification
- Application cahier de déploiement
- Tests et validation

[P3710] Intégration d'une solution de gestion de plan d'adressage :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Installation physique
- Système d'exploitation et configuration, reprise de règles et configurations existantes, reprise des entrées DNS/DHCP existantes, intégration de tous les plans d'adressage du réseau, et tous les paramètres par plage d'adresses.
- Intégration à l'environnement DNS/DHCP/Domaines Windows du bénéficiaire (LDAP/Active Directory)
- Intégration fonction d'administration
- Application cahier de déploiement
- Tests et validation

[P3711] Intégration de boîtiers de synchronisation de l'heure :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Installation physique
- Système d'exploitation et configuration
- Application cahier de déploiement
- Tests et validation
- Coût dégressif à l'unité et par 2 (haute disponibilité).

[P3712] Intégration d'une solution de publication d'applications web :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Installation physique
- Système d'exploitation et configuration
- Application cahier de déploiement
- Tests et validation
- Coût dégressif à l'unité et par 2 (haute disponibilité).

[P3713] Intégration d'une solution de commutation applicative L5/L7 :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Installation physique
- Système d'exploitation et configuration
- Authentification
- Application cahier de déploiement

- Tests et validation
- Coût dégressif à l'unité et par 2 (haute disponibilité).

[P3714] Intégration d'une solution de sondes IDS/IPS :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Installation physique
- Système d'exploitation et configuration, reprise de règles et configurations existantes
- Authentification
- Application cahier de déploiement et du cahier de réception
- Tests et validation

[P3715] Intégration d'une solution de sondes anti-DDoS :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Installation physique
- Système d'exploitation et configuration, reprise de règles et configurations existantes
- Authentification
- Application cahier de déploiement et du cahier de réception
- Tests et validation

[P3716] Mise à jour de systèmes d'exploitation d'un firewall :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Système d'exploitation et configuration
- Application cahier de déploiement
- Tests et validation

[P3717] Mise à jour de systèmes d'exploitation d'un portail extranet :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Système d'exploitation et configuration
- Application cahier de déploiement
- Tests et validation

[P3718] Mise à jour de systèmes d'exploitation d'une passerelle internet-web :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Système d'exploitation et configuration
- Application cahier de déploiement
- Tests et validation

[P3719] Mise à jour de systèmes d'exploitation d'une passerelle de messagerie SMTP :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Système d'exploitation et configuration
- Application cahier de déploiement
- Tests et validation

[P3720] Mise à jour de systèmes d'exploitation d'une solution d'analyse comportementale type « bac à sable » :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Système d'exploitation et configuration
- Application cahier de déploiement
- Tests et validation

[P3721] Mise à jour de systèmes d'exploitation d'une solution multifonctions internet périmétrique :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Système d'exploitation et configuration
- Application cahier de déploiement
- Tests et validation

[P3722] Mise à jour de systèmes d'exploitation d'un portail captif d'authentification :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Système d'exploitation et configuration
- Application cahier de déploiement
- Tests et validation

- Coût dégressif à l'unité et par 2.

[P3723] Mise à jour de systèmes d'exploitation d'un serveur d'authentification Serveur d'authentification sécurisé On Premise et dans le Cloud (Radius, Microsoft Authenticator, Google Authenticator) :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Système d'exploitation et configuration
- Application cahier de déploiement
- Tests et validation
- Coût dégressif à l'unité et par 2.

[P3724] Mise à jour de systèmes d'exploitation d'un serveur de gestion de plan d'adressage :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Système d'exploitation et configuration
- Application cahier de réception
- Tests et validation

[P3725] Mise à jour de systèmes d'exploitation d'une solution de contrôle d'accès réseau :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Système d'exploitation et configuration
- Application cahier de déploiement
- Tests et validation
- Coût dégressif à l'unité et par 2.

[P3726] Mise à jour système d'une solution de publication d'applications web :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Système d'exploitation et configuration
- Tests et validation
- Coût dégressif à l'unité et par 2 (haute disponibilité).

[P3727] Mise à jour système d'une solution de commutation applicative L5/L7 :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Système d'exploitation et configuration
- Tests et validation
- Coût dégressif à l'unité et par 2 (haute disponibilité).

[P3728] Mise à jour de systèmes d'exploitation d'une solution de sondes IDS/IPS :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Système d'exploitation et configuration
- Application cahier de déploiement
- Tests et validation

[P3729] Mise à jour de systèmes d'exploitation d'une solution de sondes anti-DDoS :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Système d'exploitation et configuration
- Application cahier de déploiement
- Tests et validation

[P3730] Pour les firewalls : Modification de configuration :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- ACL, translation d'adresses, règles, filtrages, profils, authentification…
- Tests et validation

[P3731] Pour les passerelles internet : Modification de configuration :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- ACL, règles, filtrages, profils, authentification…
- Tests et validation

[P3732] Modification/création de VPN sur un firewall :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- ACL, translation d'adresses, règles, VPN.
- Tests et validation

[P3733] Pour les contrôleurs d'accès au réseau : Modification de configuration :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Modification profilage, authentification, provisionning…
- Tests et validation

[P3734] Pour les sondes IDS/IPS ou anti-DDoS : Modification de configuration :

- Prérequis bénéficiaire : cahier de déploiement et de configuration, cahier de réception
- Modification règles de filtrages, des seuils de détection…
- Tests et validation

En complément de l'ensemble des prestations ci-dessus, l'offre comprend les coûts forfaitaires journaliers pour des intervenants ayant les profils ci-dessous. Dans chaque cas l'offre comprend un coût unitaire dégressif à l'unité, par [2 à 4] journées, par [5 à 9] journées, par mois, par trimestre et par année d'interventions. Ces journées sont forfaitaires avec obligation de moyens. Les prestations à réaliser n'entrent pas dans la liste des prestations standards décrites ci-dessus. Ces prestations sont détaillées et définies par le bénéficiaire et actées par le titulaire lors de la commande.

Au minimum les intervenants disposent de l'un des profils suivants :

- **[P**3800] Technicien réseau confirmé : intégration matérielle et logicielle standard
- **[P**3801] Ingénieur réseau confirmé : certifié, expérience de déploiement de solutions de sécurité avancées
- **[P**3802] Ingénieur réseau expert : certifié, expérience de déploiement et de migration de solutions de sécurité avancées.
- **[P**3803] Chef de projet/coordonnateur : multi-compétences techniques, coordonnateur, organisation et suivi de projet, rigueur.
- [P3804] Frais de déplacement 1er jour (déplacement > 50 km du siège et des agences locales)
- [P3805] Frais de déplacement jours suivant, intervenant déjà sur place (déplacement > 50 km du siège et des agences locales)

Remarque : Les déplacements hors France métropolitaine seront facturés sur devis

6.8.26. Les prestations type « Professional Services » constructeur et éditeur

L'offre comprend les coûts forfaitaires journaliers pour des interventions de type « Professional Services » exécutées par chacun des constructeurs et éditeurs proposés dans l'offre du titulaire. Dans chaque cas l'offre comprend un coût unitaire dégressif à l'unité, par [2 à 4], par [5 à 9] et par [10 à 49] journées d'interventions. Ces journées sont forfaitaires avec obligation de moyens. Les prestations à réaliser n'entrent pas dans la liste des prestations standards décrites ci-dessus. Ces prestations sont définies de manière détaillée par le bénéficiaire et actées par le titulaire lors de la commande.

Ingénieur « PS » constructeur et éditeur :

- **[P**3820] Coût unitaire dégressif par journée d'intervention de [2 à 4] jours
- **[P**3821] Coût unitaire dégressif par journée d'intervention de [5 à 9] jours
- **[P**3822] Coût unitaire dégressif par journée d'intervention de [10 à 49] jours

[P3821] Frais de déplacement « PS » 1er jour (déplacement > 50 km du siège et des agences locales)
[P3822] Frais de déplacement « PS » jours suivant, intervenant déjà sur place (déplacement > 50 km du siège et des agences locales)

Remarque : Les déplacements hors France métropolitaine seront facturés sur devis

6.8.27. Les prestations de transfert de compétences

Est incluse la réalisation de transferts de compétences conformément au CCTP commun, sous forme de prix unitaires :

- [P3830] : Coût unitaire dégressif par journée d'intervention 1 jour
- [P3831] : Coût unitaire dégressif par journée d'intervention 2 jours
- [P3832] : Coût unitaire dégressif par journée d'intervention 5 jours

- [P3833] : Coût unitaire dégressif par journée d'intervention 10 jours

[SERVICES-009] Les prestations sont composées d'un transfert de compétences sur l'ensemble des produits et technologies mises à disposition dans le présent lot.
Les coûts sont indiqués pour un groupe de 3 à 6 personnes :

- Pour chaque gamme de matériels/logiciel fournis
- Pour chaque technologie mise en œuvre
- Coût dégressif à la journée, par 2 journées, par 5 et par 10.
- Sur le site des bénéficiaires et dans les locaux du titulaire.

Les prestations ci-dessous complètent les prestations générales d'ingénierie, d'intégration, de migration, de paramétrage, de mise à jour, de tests et de validation prévues au présent CCTP. Les prérequis, livrables et conditions de réception sont précisés par le candidat dans sa réponse.

[P4613] Mise à jour de la solution.
[P4612] Évolution des politiques de microsegmentation.
[P4611] Migration d'une solution de microsegmentation.
[P4610] Déploiement d'une solution de microsegmentation.
[P4423] Mise à jour de la solution.
[P4422] Rotation ou renouvellement des clés.
[P4421] Migration d'une solution de chiffrement LAN.
[P4420] Déploiement d'une solution de chiffrement LAN.
[P4323] Mise à jour de la solution.
[P4322] Paramétrage des politiques de contrôle et de chiffrement.
[P4321] Migration d'une solution de contrôle des supports amovibles.
[P4320] Déploiement d'une solution de contrôle des supports amovibles.
[P4033] Mise à jour logicielle d'une solution NAC.
[P4032] Évolution des politiques NAC.
[P4031] Migration d'une solution NAC.
[P4030] Intégration d'une solution NAC.

6.8.28. Dispositions communes de maintenance

Les prestations de maintenance, de maintien en condition opérationnelle et de sécurité, de support, de gestion des incidents, de maintenance préventive et corrective, de gestion des versions, de réassurance constructeur ou éditeur, de reporting, de réversibilité, de transférabilité, ainsi que les niveaux de service, horaires de couverture et délais d'intervention ou de rétablissement applicables au présent lot sont définis dans le CCTP commun, le CCAP et les pièces financières.
Le présent lot ne comporte aucune disposition spécifique venant modifier ou restreindre ces exigences communes. Les équipements, logiciels, licences, abonnements et infrastructures relevant du présent lot peuvent bénéficier de ces prestations lorsqu'elles sont commandées par un bénéficiaire.

6.8.29. Automatisation

Descriptions des prestations
Les infrastructures IT des établissements sont de plus en plus complexes et requièrent de plus en plus d'expertise. Tout changement sur ces infrastructures demande beaucoup de temps de préparation et de mise en œuvre. Les changements deviennent par conséquent critiques à gérer avec un risque accru d'incident. Pour abstraire cette complexité de l'infrastructure et garantir une gestion des changements fiable, maîtrisée et rapide, le recours à l'automatisation et à l'orchestration des réseaux devient une nécessité.
La prestation du titulaire consiste à conseiller et à accompagner l'établissement dans l'étude, la conception, la mise en œuvre et le maintien opérationnel de sa politique d'automatisation.

Pour la phase d'étude et de conception, la prestation du titulaire consiste notamment à :

- Recueillir les besoins de l'établissement
- Analyser et prendre connaissance des différents systèmes composant l'infrastructure IT de l'établissement
- Prendre connaissance de l'organisation de l'établissement
- Proposer une modélisation du workflow d'automatisation et un plan de mise en œuvre.

À l'issue de cette phase, les livrables attendus sont :

- La synthèse de l'expression de besoin et de l'analyse des systèmes et organisation de l'établissement
- Le dossier de modélisation et du plan de déploiement

Pour la phase de conception et mise en œuvre, le titulaire propose si besoin des prestations de :

- Développement d'outils (ex : connecteurs) pour l'intégration des solutions IT de l'établissement.
- Qualification de ces outils et des workflows en environnement de tests.
- Assistance et accompagnement à la prise en main de ces outils.
- Maintien opérationnel de ces outils pour suivre l'évolution des solutions IT de l'établissement

Les livrables attendus, associés à cette phase, sont :

- La documentation des outils mis en œuvre
- Les procédures d'utilisation des outils mis en œuvre

Coûts des prestations d'automatisation
L'offre comprend les coûts journaliers pour des intervenants ayant les profils ci-dessous.

- [P6080] Journée d'un consultant junior, tarification dégressive à l'unité, par [2 à 9], par [10 à 29], par [30 et plus] journées d'interventions
- [P6081] Journée d'un consultant sénior, tarification dégressive à l'unité, par [2 à 9], par [10 à 29], par [30 et plus] journées d'interventions
- [P6082] Journée d'un consultant chef de projet, tarification dégressive à l'unité, par [2 à 9], par [10 à 29], par [30 et plus] journées d'interventions
- [P6083] Journée d'un consultant directeur de projet, tarification dégressive à l'unité, par [2 à 9], par [10 à 29], par [30 et plus] journées d'interventions
- [P6084] Frais de déplacement 1er jour (déplacement > 50 km du siège et des agences locales)
- [P6085] Frais de déplacement jours suivant, intervenant déjà sur place (déplacement > 50 km du siège et des agences locales)

Remarque : Les déplacements hors France métropolitaine seront facturés sur devis

6.8.30. Étude de cas

[ETUDE-001] Afin d'illustrer l'intégration des gammes de matériels et les prestations proposées dans le présent lot, l'offre comprend une étude complète décrivant la migration de l'existant vers une architecture technique aboutie et sécurisée.