Demande de proposition: Plateforme de service d'accès sécurisé en périphérie (SASE)

Table des matières

1. Introduction et contexte

[Nom de l'entreprise] sollicite des propositions pour une plateforme complète Secure Access Service Edge (SASE) afin de moderniser son infrastructure de réseau et de sécurité. Le présent appel d'offres décrit nos besoins en matière de solution "cloud-native" qui converge la connectivité réseau et les services de sécurité afin de soutenir notre personnel distribué et nos initiatives "cloud-first".

Historique de l'organisation

- [Décrivez votre entreprise/organisation]
- [Exigences industrielles et réglementaires]
- [Taille de l'organisation et de l'infrastructure informatique]

Environnement actuel

- [Architecture actuelle du réseau et de la sécurité]
-

- [Nombre d'utilisateurs et de sites]

Objectifs du projet

- Mise en œuvre d'une architecture SASE unifiée et native dans le nuage
- Amélioration du dispositif de sécurité grâce à des services intégrés
- Optimisation des performances du réseau et de l'expérience des utilisateurs
- Gestion et opérations rationalisées

2. Objectifs du projet

1. Déployer une plateforme SASE complète qui s'intègre :
    - Réseau étendu défini par logiciel (SD-WAN)
    - Composants du Security Service Edge (SSE)
    - Accès au réseau sans confiance (ZTNA)
    - Services de sécurité en nuage
2. Atteindre les résultats suivants :
    - Sécurité unifiée et infrastructure de réseau
    - Visibilité et contrôle accrus
    - Amélioration de l'efficacité opérationnelle
    - Réduction du coût total de possession
    - Architecture cloud-native évolutive

3. L'étendue des travaux

Composants requis

1. Capacités SD-WAN
    - Optimisation du réseau
    - Routage en fonction de l'application
    - Gestion des liaisons WAN

- Contrôles de qualité de service

2. Security Service Edge (SSE)
    - Passerelle Web sécurisée (SWG)
    - Courtier en sécurité de l'accès au nuage (CASB)
    - Accès au réseau sans confiance (ZTNA)
    - Pare-feu en tant que service (FWaaS)
3. Fonctions de sécurité avancées
    - Prévention de la perte de données (DLP)
    - Protection contre les menaces avancées
    - Analyse du comportement des utilisateurs et des entités
    - Renseignements intégrés sur les menaces
4. Gestion et analyse
    - Console de gestion unifiée
    - Contrôle en temps réel
    - Analyse avancée
    - Réponse automatisée aux incidents

Phases de mise en œuvre

1. Planification et conception
    - Évaluation de l'architecture
    - Élaboration d'une stratégie de migration
    - Conception du cadre politique
    - Évaluation de l'infrastructure actuelle du réseau et de la sécurité
    - Formation et planification de la gestion du changement pour le personnel informatique et les utilisateurs finaux

2. Déploiement pilote
    - Mise en œuvre initiale
    - Essais et validation
    - Établissement d'un référentiel de performance
    - Exécution de la preuve du concept (PoC), y compris :
        - Des objectifs et des critères de réussite clairs
        - Essais des principaux cas d'utilisation
        - Critères de performance et scénarios de sécurité
        - Tests d'intégration requis
        - Mesures d'évaluation et exigences en matière de rapports
3. Déploiement complet
    - Déploiement progressif
    - Migration des utilisateurs
    - Intégration avec les systèmes existants
4. Optimisation
    - Optimisation des performances
    - Affinement de la politique
    - Optimisation de l'expérience utilisateur

4. Exigences techniques

Capacités du réseau

1. Caractéristiques du SD-WAN
    - Routage en fonction de l'application
    - Sélection dynamique du chemin
    - Gestion de la qualité de service et de la largeur de bande

- Agrégation de liens et basculement
- Mise en forme du trafic et hiérarchisation

5. Exigences fonctionnelles

A. Exigences fonctionnelles de base

5.1 Architecture native dans les nuages

Conseil : Une architecture "cloud-native" est fondamentale pour une mise en œuvre réussie de SASE. Recherchez des solutions qui démontrent de véritables principes de conception "cloud-first", avec une architecture basée sur des microservices qui permet l'évolutivité, la flexibilité et des opérations résilientes. Tenez compte de la façon dont l'architecture prend en charge le déploiement distribué et maintient des performances cohérentes dans différents environnements cloud.

Exigence	Sous-exigence	O/N	Notes
Architecture Cloud-Native	Conception "cloud-first" avec architecture microservices		
	Capacités de déploiement basées sur des conteneurs		
	Mise à l'échelle automatique et gestion des ressources élastiques		
	Prise en charge de l'architecture multi-locataires		
	Intégration de fournisseurs de services en nuage natifs		

5.2 Capacités SD-WAN intégrées

Conseil : Une intégration SD-WAN efficace est cruciale pour optimiser les performances du réseau et garantir une connectivité fiable entre les sites distribués. Privilégiez les solutions qui offrent des fonctions complètes d'optimisation du réseau étendu et des capacités de routage intelligent du trafic, tout en maintenant des performances applicatives constantes.

Exigence	Sous-exigence	O/N	Notes

Intégration SD-WAN	Capacités de routage en fonction de l'application		
	Sélection et optimisation dynamiques des chemins		
	Équilibrage et agrégation de la charge des liaisons WAN		
	Contrôles de la qualité de service (QoS)		
	Gestion et optimisation de la bande passante		

5.3 Services de sécurité complets

Conseil : les services de sécurité constituent l'épine dorsale de l'architecture SASE. Évaluez les solutions en fonction de leur capacité à fournir des contrôles de sécurité intégrés, fournis dans le nuage, qui protègent tous les bords du réseau tout en conservant la simplicité de gestion et de déploiement.

Exigence	Sous-exigence	O/N	Notes
Services de sécurité	Fonctionnalité de pare-feu de nouvelle génération		
	Capacités de prévention des menaces avancées		
	Fonctions de prévention des pertes de données (DLP)		
	Mise en œuvre de l'accès au réseau de confiance zéro		
	Services de passerelle web sécurisée		

5.4 Interface de gestion unifiée

Conseil : Une interface de gestion centralisée est essentielle pour des opérations SASE efficaces. Recherchez des solutions offrant un contrôle intuitif et complet par le biais d'une interface unique qui permet une gestion unifiée des politiques, une surveillance et des rapports, tout en s'adaptant aux différents rôles administratifs et niveaux d'accès.

Exigence	Sous-exigence	O/N	Notes
Interface de gestion	Console unique pour toutes les fonctions du SASE		
	Gestion du contrôle d'accès basé sur les rôles		
	Tableaux de bord et rapports personnalisables		
	Gestion intégrée des politiques		
	Capacités de configuration en temps réel		

5.5 Application de la politique

Conseil : L'application cohérente des politiques sur l'ensemble des bords du réseau et des fonctions de sécurité est essentielle au maintien de la posture de sécurité. Les solutions doivent être évaluées en fonction de leur capacité à mettre en œuvre des politiques granulaires de manière uniforme tout en permettant des ajustements dynamiques en fonction du contexte et des risques.

Exigence	Sous-exigence	O/N	Notes
Application de la politique	Création et contrôle granulaires des politiques		
	Gestion des politiques basées sur les utilisateurs et les groupes		
	Mise en œuvre de politiques tenant compte de la localisation		
	Application de règles spécifiques à une application		
	Déploiement automatisé des politiques		

5.6 Optimisation du trafic

Conseil : les capacités d'optimisation du trafic ont un impact direct sur l'expérience de l'utilisateur et les performances de l'application. Privilégiez les solutions qui offrent des fonctions d'optimisation complètes tout en maintenant la sécurité et la visibilité sur l'ensemble des flux de trafic.

Exigence	Sous-exigence	O/N	Notes
Optimisation du trafic	Optimisation du trafic WAN		
	Accélération des performances des applications		
	Contrôle de l'allocation de la bande passante		
	Mécanismes de priorisation du trafic		
	Capacités de mise en œuvre de la qualité de service		

5.7 Évolutivité

Conseil : L'évolutivité garantit que votre solution SASE peut grandir avec votre organisation. Prenez en compte les capacités de mise à l'échelle horizontale et verticale, ainsi que la capacité à maintenir les performances au fur et à mesure de l'expansion du déploiement.

Exigence	Sous-exigence	O/N	Notes
Évolutivité	Prise en charge de la mise à l'échelle horizontale		
	Gestion des ressources élastiques		
	Optimisation des performances à grande échelle		
	Planification automatisée des capacités		
	Équilibrage dynamique de la charge		

5.8 Capacités d'intégration

Conseil : les capacités d'intégration déterminent dans quelle mesure la solution SASE fonctionne avec votre infrastructure existante. Évaluez l'étendue et la profondeur des options d'intégration, en vous concentrant sur les API et les connecteurs prédéfinis pour les systèmes d'entreprise courants.

Exigence	Sous-exigence	O/N	Notes

Intégration	Disponibilité de l'API et documentation		
	Intégration du système SIEM		
	Connectivité du fournisseur d'identité		
	Intégration d'outils de sécurité tiers		
	Capacités d'intégration personnalisées		

5.9 Protection contre les menaces avancées

Conseil : La protection contre les menaces avancées est cruciale dans le paysage actuel des menaces en constante évolution. Recherchez des solutions qui combinent plusieurs méthodes de détection avec des capacités de réponse automatisées afin de fournir une protection complète contre les attaques sophistiquées.

Exigence	Sous-exigence	O/N	Notes
Protection contre les menaces	Prévention des menaces de type "zero-day		
	Capacités avancées de sandboxing		
	Intégration des renseignements sur les menaces		
	Caractéristiques de l'analyse comportementale		
	Réponse automatisée aux menaces		

5.10 Gestion de l'identité et de l'accès

Conseil : le contrôle d'accès basé sur l'identité est fondamental pour la sécurité zéro confiance. Évaluez les solutions en fonction de leur capacité à s'intégrer aux systèmes d'identité existants tout en offrant de solides capacités d'authentification et d'autorisation.

Exigence	Sous-exigence	O/N	Notes
IAM	Prise en charge de l'authentification multifactorielle		

	Capacités d'authentification unique		
	Intégration des services d'annuaire		
	Gestion des accès privilégiés		
	Mécanismes de vérification de l'identité		

5.11 Surveillance et analyse en temps réel

Conseil : une surveillance et une analyse efficaces offrent une visibilité sur la sécurité et les performances. Privilégiez les solutions qui offrent des capacités complètes de surveillance en temps réel avec des informations exploitables et des rapports personnalisables.

Exigence	Sous-exigence	O/N	Notes
Surveillance et analyse	Contrôle des performances en temps réel		
	Analyse des événements de sécurité		
	Suivi de l'expérience utilisateur		
	Analyse des performances du réseau		
	Outils de reporting personnalisables		

5.12 Support multi-cloud

Conseil : la prise en charge multi-cloud est essentielle pour les architectures distribuées modernes. Évaluez les solutions en fonction de leur capacité à fournir une sécurité et une connectivité cohérentes entre les différents fournisseurs de cloud tout en maintenant une gestion unifiée.

Exigence	Sous-exigence	O/N	Notes
Multi-cloud	Connectivité inter-cloud		
	Sécurité d'un nuage à l'autre		
	Sécurité de l'accès au nuage		

	Protection de la charge de travail en nuage		
	Outils de gestion multi-cloud		

5.13 Soutien à l'informatique de pointe

Conseil : l'informatique en périphérie permet un traitement plus proche des sources de données. Recherchez des solutions capables d'étendre les capacités de sécurité et de mise en réseau aux sites périphériques tout en conservant un contrôle centralisé.

Exigence	Sous-exigence	O/N	Notes
Informatique de pointe	Déploiement de services en périphérie		
	Soutien au traitement local des données		
	Contrôles de sécurité en périphérie		
	Optimisation des performances des bords		
	Caractéristiques de l'informatique distribuée		

5.14 Réponse automatisée aux incidents

Conseil : Les capacités de réponse automatisée aux incidents réduisent le temps moyen de réponse et de récupération après un incident de sécurité. Privilégiez les solutions qui offrent une automatisation complète tout en maintenant une supervision humaine appropriée.

Exigence	Sous-exigence	O/N	Notes
Réponse aux incidents	Atténuation automatisée des menaces		
	Automatisation du flux de travail en cas d'incident		
	Orchestration des réponses		
	Procédures de récupération automatisées		
	Outils d'analyse post-incident		

5.15 Gestion de la conformité

Conseil : Les fonctionnalités de gestion de la conformité aident à maintenir l'adhésion aux réglementations. Évaluez les solutions en fonction de leur capacité à appliquer les politiques de conformité et à générer la documentation et les rapports requis.

Exigence	Sous-exigence	O/N	Notes
Conformité	Outils de contrôle de conformité		
	Fonctionnalités des rapports réglementaires		
	Maintenance de la piste d'audit		
	Vérification de la conformité de la politique		
	Fonctionnalité du tableau de bord de conformité		

B. Exigences en matière d'IA et d'apprentissage automatique

5.16 Sécurité alimentée par l'IA

Conseil : La sécurité alimentée par l'IA améliore les capacités de détection et de réponse aux menaces. Recherchez des solutions qui exploitent efficacement l'IA tout en assurant la transparence de leurs processus décisionnels.

Exigence	Sous-exigence	O/N	Notes
Sécurité de l'IA	Détection des menaces basée sur l'IA		
	Réponses automatisées en matière de sécurité		
	Évaluation des risques pilotée par l'IA		
	Analyse de l'apprentissage automatique		
	Analyse des comportements		

5.17 Intégration de l'IA générative

Conseil : les capacités d'IA générative améliorent les processus d'automatisation et de prise de décision. Concentrez-vous sur les solutions qui exploitent l'IA générative pour

améliorer la configuration, le dépannage et la gestion des politiques tout en maintenant la sécurité et la précision.

Exigence	Sous-exigence	O/N	Notes
IA générative	Génération de politiques alimentées par l'IA		
	Assistance à la configuration automatisée		
	Création intelligente de documents		
	Dépannage assisté par l'IA		
	Capacités de traitement du langage naturel		

5.18 Gestion des réseaux assistée par l'IA

Conseil : La gestion de réseau assistée par l'IA améliore l'efficacité opérationnelle et les performances du réseau. Évaluez les solutions en fonction de leur capacité à automatiser les tâches de routine et à fournir des recommandations d'optimisation intelligentes.

Exigence	Sous-exigence	O/N	Notes
Gestion du réseau d'IA	Optimisation automatisée du réseau		
	Dépannage intelligent		
	Prévision des performances		
	Gestion intelligente de la configuration		
	Capacités d'automatisation du réseau		

5.19 Gestion autonome de l'expérience numérique (ADEM)

Astuce : L'ADEM garantit une expérience utilisateur optimale grâce à une surveillance et une optimisation automatisées. Recherchez des solutions qui offrent une visibilité complète de l'expérience utilisateur et des capacités de remédiation automatisées.

Exigence	Sous-exigence	O/N	Notes

ADEM	Suivi de l'expérience en temps réel		
	Suivi des performances des applications		
	Evaluation de l'expérience utilisateur		
	Remédiation automatisée des problèmes		
	Outils d'optimisation de l'expérience		

5.20 Opérations d'IA (AIOps)

Conseil : Les capacités AIOps rationalisent les opérations informatiques grâce à l'automatisation intelligente. Concentrez-vous sur les solutions qui combinent efficacement les données opérationnelles avec l'IA pour améliorer l'efficacité et réduire les interventions manuelles.

Exigence	Sous-exigence	O/N	Notes
AIOps	Automatisation des tâches opérationnelles		
	Fonctions de maintenance prédictive		
	Optimisation des ressources		
	Système d'alerte intelligent		
	Optimisation des performances		

5.21 Amélioration de la détection des menaces grâce à l'IA

Conseil : La détection des menaces par l'IA permet une identification plus précise et plus rapide des menaces de sécurité. Évaluez les solutions en fonction de leur capacité à exploiter l'IA pour améliorer la détection des menaces tout en minimisant les faux positifs.

Exigence	Sous-exigence	O/N	Notes
Détection des menaces par l'IA	Analyse des menaces avancées		

	Capacités de reconnaissance des formes		
	Détection des anomalies		
	Identification prédictive des menaces		
	Analyse des menaces en temps réel		

5.22 Prise de décision basée sur l'IA

Conseil : Les décisions prises par l'IA améliorent les temps de réponse et la précision. Recherchez des solutions qui fournissent des décisions d'IA transparentes et explicables tout en maintenant une supervision humaine appropriée.

Exigence	Sous-exigence	O/N	Notes
Prise de décision par l'IA	Décisions politiques automatisées		
	Évaluation intelligente des risques		
	Optimisation de l'allocation des ressources		
	Décisions fondées sur les performances		
	Pistes d'audit des décisions		

5.23 Interfaces en langage naturel

Conseil : les interfaces en langage naturel améliorent l'interaction avec l'utilisateur et l'efficacité de la gestion. Privilégiez les solutions qui offrent un traitement intuitif et précis du langage naturel tout en maintenant les contrôles de sécurité.

Exigence	Sous-exigence	O/N	Notes
Langage naturel	Interprétation des commandes		
	Requêtes en langage naturel		
	Interface conversationnelle		
	Prise en charge multilingue		

	Prise en compte du contexte		

5.24 Capacités d'IA prédictive

Conseil : L'IA prédictive permet une gestion et une optimisation proactives. Évaluez les solutions en fonction de leur capacité à prévoir avec précision les tendances et les problèmes potentiels tout en fournissant des informations exploitables.

Exigence	Sous-exigence	O/N	Notes
L'IA prédictive	Prévision de capacité		
	Prévision des performances		
	Prévision des menaces		
	Prévision de l'utilisation des ressources		
	Analyse des tendances		

5.25 Cartographie des relations pour l'UEBA

Conseil : la cartographie des relations UEBA permet de mieux comprendre les modèles de comportement des utilisateurs. Recherchez des solutions qui cartographient et analysent efficacement les relations tout en respectant les exigences en matière de confidentialité et de conformité.

Exigence	Sous-exigence	O/N	Notes
Cartographie de l'UEBA	Analyse du comportement des utilisateurs		
	Cartographie des relations entre les entités		
	Reconnaissance des formes		
	Corrélation des anomalies		
	Analyse comportementale		

5.26 L'IA explicable pour la détection des anomalies

Conseil : l'IA explicable garantit la transparence des processus de détection des anomalies. Concentrez-vous sur des solutions qui fournissent des explications claires sur les anomalies détectées par l'IA tout en maintenant la précision de la détection.

Exigence	Sous-exigence	O/N	Notes
L'IA explicable	Une logique de décision transparente		
	Caractéristiques de l'explication des anomalies		
	Raisonnement de détection		
	Création d'une piste d'audit		
	Aide à l'enquête		

6. Qualifications des fournisseurs

Qualifications requises

1. Présentation de l'entreprise
    - Années sur le marché des SASE
    - Position sur le marché
    - Stabilité financière
    - Base de clientèle
2. Expertise technique
    - Expérience en matière d'architecture SASE
    - Certifications de sécurité
    - Capacités de mise en œuvre
    - Infrastructure de soutien
3. Couverture des services
    - Une présence mondiale
    - Mesures de la disponibilité des services

- Couverture géographique
- Points de présence

4. Certifications et normes
    - Certifications de sécurité
    - Certifications de conformité
    - Alignement sur les normes industrielles
    - Cadres de bonnes pratiques
5. Développement futur
    - Feuille de route du produit
    - Stratégie d'innovation
    - Améliorations prévues
    - Partenariats technologiques

7. Critères d'évaluation

Les propositions seront évaluées sur la base des éléments suivants

1. Capacité technique (30%)
    - Complétude des caractéristiques
    - Conception de l'architecture
    - Mesures de performance
    - Capacités de sécurité
2. Approche de la mise en œuvre (20 %)
    - Méthodologie de déploiement
    - Stratégie de migration
    - Gestion des risques
    - Faisabilité du calendrier

3. Qualifications des fournisseurs (20%)
    - Expérience
    - Références
    - Capacités de soutien
    - Stabilité financière
4. Structure des coûts (30%)
    - Coût total de possession
    - Modèle de tarification
    - Coûts supplémentaires
    - Rapport qualité-prix

8. Lignes directrices pour la soumission

Les propositions doivent comprendre

1. Résumé
2. Description de la solution technique
3. Approche de la mise en œuvre
4. Calendrier du projet
5. Détails des prix
6. Qualifications de l'entreprise
7. Références clients
8. Modèle de soutien
9. Exemples d'accords de niveau de service
10. Documentation complémentaire
11. Études de cas et références
    - Exemples de mise en œuvre similaires

- Déploiements spécifiques à l'industrie
- Mesures de réussite
- Témoignages de clients

9. Calendrier

- Date de publication de l'appel d'offres : [Date]
- Date limite pour les questions : [Date]
- Date d'échéance de la proposition : [Date]
- Présentations des fournisseurs : [Fourchette de dates]
- Décision de sélection : [Date]
- Début du projet : [Date]
- Objectif d'achèvement : [Date]

Soumettre les propositions à : [Coordonnées]