PARTENAIRE LOGO

SASE : les dix principaux critères de sélection de votre fournisseur

Dans un monde idéal, il suffirait d'appuyer sur un bouton pour migrer la totalité de votre architecture réseau vers un environnement cloud parfaitement sécurisé. Seulement voilà, la réalité est hélas toute autre. Cela ne signifie pourtant pas que la migration SASE doit s'opérer dans la complexité et la douleur.

Elle peut au contraire s'effectuer en toute fluidité, à condition de trouver le bon fournisseur SASE pour vous accompagner. Celui-ci devra d'abord vous aider à capitaliser sur vos investissements existants, puis mettre toute son expérience dans la balance pour faciliter une transition sans risque et à votre rythme vers une sécurité en mode cloud.

1 GESTION UNIFIÉE DES POLITIQUES

Gérez la sécurité de tous vos environnements, sur site ou dans le cloud, depuis une plateforme cloud centralisée.

La gestion unifiée des politiques doit être au service de l'expérience utilisateur, avec des règles protégeant utilisateurs, appareils et applications où qu'ils aillent.

2 UNE PROTECTION RAPIDE ET EFFICACE CONTRE LES MENACES AVANCÉES

Défendez-vous contre les menaces invisibles et inconnues, même chiffrées.

Il vous faut pour cela un service cloud capable de détecter les malwares de façon statique et dynamique, afin d'identifier en temps réel les menaces même les plus sophistiquées et furtives, puis de les bloquer quasi immédiatement.

3 RÉSILIENCE ET ÉVOLUTIVITÉ

Optez pour une évolutivité efficace et transparente sur tous vos environnements de sécurité : physiques, virtuels et cloud.

Vous devez pour cela conjuguer sécurité et simplicité opérationnelle à grande échelle, sans aucun impact négatif sur l'expérience utilisateur.

4 ARCHITECTURE « SINGLE-STACK » DOTÉE D'UN CADRE DE POLITIQUES UNIQUE

Faites de vos investissements actuels votre rampe de lancement vers des services de sécurité cloud critiques.

Créez des politiques une seule fois, appliquez-les partout et gérez-les de façon unifiée (accès basés sur les utilisateurs et les applications, IPS, anti-malware, accès web sécurisé, etc. rassemblés au sein d'une seule et même politique).

5 UNE SÉCURITÉ HOMOGÈNE POUR VOS ÉQUIPES DISTRIBUÉES

Donnez à vos équipes distantes un accès sécurisé aux applications et ressources dont elles ont besoin pour accomplir leurs missions.

Des politiques de sécurité homogènes suivent les utilisateurs, les appareils et les applications dans tous leurs déplacements, sans avoir à copier ni recréer des ensembles de règles.

6 PRISE EN CHARGE DES ENVIRONNEMENTS HYBRIDES

Que votre infrastructure soit sur site, dans le cloud ou les deux à la fois, votre fournisseur SASE devrait la prendre en charge dans tous les cas.

Son rôle est de faciliter votre transition vers une architecture SASE, au rythme le mieux adapté à votre entreprise et sans compromettre sa sécurité.

7 UNE SOURCE UNIQUE POUR LES IDENTITÉS

Intégrez votre base d'identités en toute fluidité à n'importe quelle solution IAM disponible sur le marché.

Optez pour une solution SASE qui s'adapte au fournisseur IdP de votre choix, et non l'inverse.

8 SEGMENTATION DYNAMIQUE DES UTILISATEURS

Assurez la protection de vos utilisateurs, où qu'ils soient.

Optez pour des politiques qui suivent l'utilisateur dans tous ses déplacements, avec contrôle d'accès automatisé en fonction du risque représenté. Par précaution, tous les accès de tiers sont considérés comme des vecteurs d'attaque potentiels, ce qui réduit la surface d'attaque à la périphérie.

9 EFFICACITÉ VALIDÉE

Privilégiez un fournisseur SASE dont la sécurité a fait ses preuves.

Exploits côté client ou serveur, ransomware, botnets, tunnels DNS… sa solution doit avoir démontré son efficacité face aux menaces les plus diverses. En bref, vous avez besoin d'une sécurité à la hauteur des défis d'aujourd'hui, fournie sous forme de service et capable de déjouer les attaques dans vos environnements sur site et cloud.

10 MIGREZ EN TOUTE TRANSPARENCE ET À VOTRE RYTHME VERS UNE SÉCURITÉ PILOTÉE DEPUIS LE CLOUD

Personne ne devrait vous forcer à migrer vers une architecture SASE avant d'être prêt.

Avec les politiques unifiées et les assistants de déploiement intuitifs, votre transition vers une architecture de sécurité dans le cloud s'effectue à votre rythme et en toute fluidité, depuis une interface de gestion unique. Il devient alors plus facile et efficace d'orchestrer, de provisionner et de gérer les services de politiques, qu'importe leur environnement.

11 POINTS BONUS : GARANTIE DE SÉCURITÉ

Modifiez les règles de vos politiques en toute confiance, avec l'assurance que ces changements seront bien appliqués.

Qu'il s'agisse d'une règle pour une politique de pare-feu traditionnelle ou d'une politique fournie sous forme de service, son efficacité dépend de l'ordre de séquencement. Votre fournisseur SASE doit donc aider votre équipe IT à bien comprendre la mécanique des ensembles de règles et à signaler automatiquement les doublons et celles qui ne seront jamais déclenchées (« shadowed rules ») avant de les valider.

Naturellement, chaque transition SASE est différente. C'est donc à vous de déterminer comment concevoir, bâtir et gérer cette nouvelle architecture afin d'optimiser l'expérience utilisateur et les services, tout en garantissant l'accès aux données dès que vous en avez besoin. Quelle que soit la trajectoire que vous emprunterez, choisissez un fournisseur capable de s'adapter à votre situation de départ et de vous accompagner à chaque étape de votre migration SASE.

Siège social et commercial

Juniper Networks, Inc.

1133 Innovation Way

Sunnyvale, CA 94089, États-Unis

Téléphone : +1 888 586 4737

ou +1 408 745 2000

Fax : +1 408 745 2100

www.juniper.net/fr/fr

Siège EMEA et APAC

Juniper Networks International B.V.

Boeing Avenue 240

1119 PZ Schiphol-Rijk

Amsterdam, Pays-Bas

Téléphone : +31 0 207 125 700

Fax : +31 0 207 125 701

Juniper Networks | Driven by Experience™

RÉFÉRENCE : 3050168