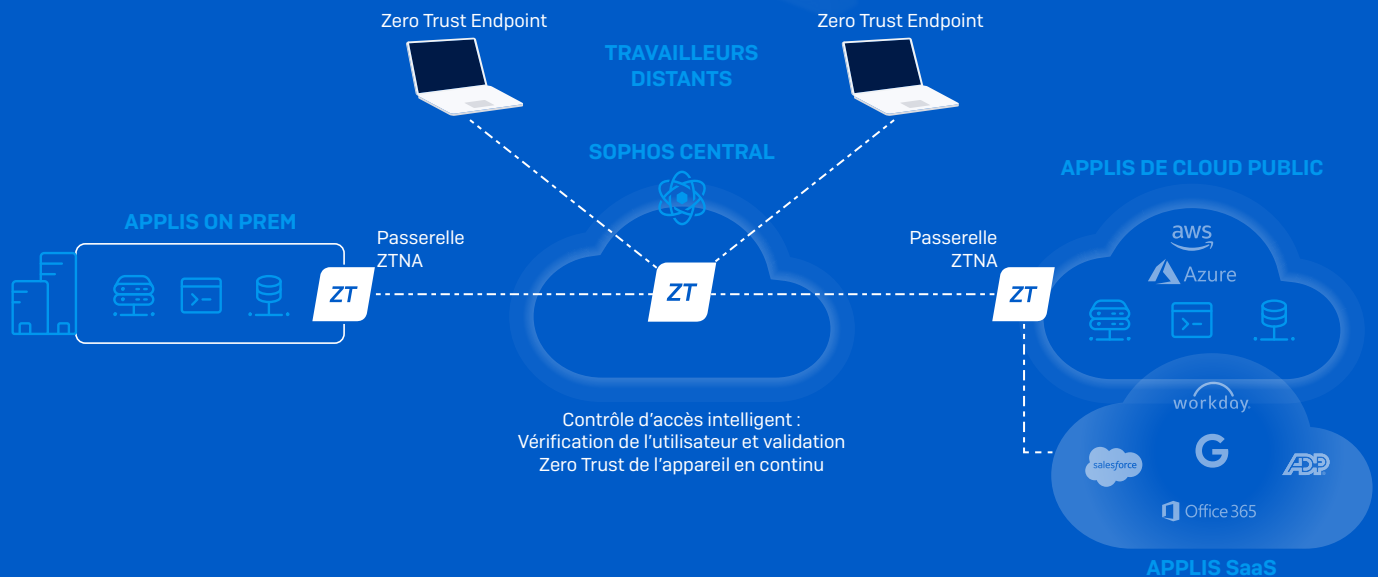




Checklist pour le déploiement de Sophos ZTNA

Le déploiement de Sophos ZTNA est simple et rapide grâce à sa mise en œuvre et sa gestion dans le Cloud depuis Sophos Central, la plateforme de gestion de la cybersécurité la plus fiable sur le marché. Utilisez cette checklist pour vous assurer que vous disposez des technologies nécessaires pour un déploiement en douceur.



Votre checklist pour un déploiement rapide :

- ✓ Vous souhaitez micro-segmenter les applications gérées à l'intérieur de votre réseau mais aussi celles hébergées dans AWS, en fournissant un accès sécurisé à vos utilisateurs distants.
- ✓ Vous disposez d'un hyperviseur ou d'un fournisseur de Cloud pris en charge pour les passerelles Sophos ZTNA.
- ✓ Vous disposez d'un fournisseur d'identité (IDP) moderne – Azure ou Okta. Azure peut être gratuit dans de nombreux cas pour des options IDP de base et s'intègre rapidement à Active Directory sur site.
- ✓ Vous disposez de Windows 10 ou macOS pour l'accès lourd aux applications ou souhaitez offrir un accès par navigateur sans client aux applications Web sur toutes les plateformes.
- ✓ En option, vous souhaitez intégrer l'état de sécurité des appareils dans les politiques d'accès en utilisant la Sécurité Synchronisée de Sophos avec Intercept X.

Ce qu'il faut prendre en considération :



Identifiez toutes vos applications gérées : Identifiez les applications que vous souhaitez micro-segmenter et auxquelles vous souhaitez fournir un accès distant sécurisé. Sophos ZTNA requiert que ces applications soient hébergées sur place, dans votre datacenter, chez un hébergeur ou dans le Cloud public Amazon Web Services (AWS). Sophos ZTNA peut également contrôler l'accès aux applications SaaS qui offrent des restrictions de contrôle des adresses IP.



Déterminez votre stratégie de passerelle : Les passerelles Sophos ZTNA facilitent la connexion sécurisée au niveau de l'application. Les passerelles Sophos ZTNA sont requises au niveau de la passerelle réseau de chaque site d'hébergement d'applications. Par exemple, si vous avez des applications hébergées dans deux datacenters différents et aussi dans AWS, vous aurez besoin de trois passerelles Sophos ZTNA.

Deux types de passerelles sont disponibles et peuvent être combinées en mode hybride :

- Cloud Gateway : passerelle légère déployée sur site qui se connecte automatiquement à Sophos Cloud via les points de présence Cloud régionaux de Sophos. Cette solution offre le meilleur déploiement rationalisé possible sans nécessiter de configurer les pare-feux et rend ainsi les applications plus invisibles et sécurisées.
- On-Premise Gateway : passerelle fournissant une connexion privée au niveau du plan de données directement entre vos terminaux et vos applications. Cette solution sera la meilleure option pour les clients qui ont des inquiétudes concernant la latence via les points de présence (PoP : Points of Presence) Cloud.

Quelle que soit l'option choisie, les passerelles Sophos ZTNA sont gratuites et vous pouvez en déployer autant que vous le souhaitez. La liste des plateformes prises en charge est présentée dans le tableau ci-dessous. Assurez-vous que vous disposez de ces plateformes pour le déploiement de votre passerelle.



Définissez votre stratégie d'identité : Pour authentifier vos utilisateurs, vous aurez besoin d'un fournisseur d'identité (IDP) qui est pris en charge par Sophos ZTNA. La liste des fournisseurs est présentée dans le tableau ci-dessous. Sophos ZTNA fonctionne avec la plupart des solutions d'authentification multifactor (MFA) qui s'intègrent aux IDP pris en charge. Vous pouvez utiliser Active Directory en local pour importer une arborescence d'annuaire dans Sophos Central pour la création de politiques basées sur les utilisateurs, mais cela n'est pas suffisant comme solution IDP d'accès à distance.



Déterminez votre nombre d'utilisateurs : La licence ZTNA est basée sur le nombre d'utilisateurs ; il suffit donc de compter le nombre d'utilisateurs qui ont besoin d'un accès sécurisé aux applications. Le déploiement du client Sophos est très facile depuis Sophos Central en parallèle de l'agent Intercept X, mais il peut également être déployé indépendamment en parallèle de tout autre produit antivirus.



Pensez à votre stratégie de sécurité des appareils (facultatif) : Il s'agit d'une couche de sécurité supplémentaire facultative qui permet de contrôler l'accès aux applications en fonction de l'état de sécurité ou de conformité de l'appareil. Sophos ZTNA prend en charge la fonction Sophos Security Heartbeat pour l'état de sécurité et la conformité des appareils. Pour cela, il faut également disposer de Sophos Intercept X dans Sophos Central, offrant ainsi un guichet unique pour la gestion de tous vos besoins en cybersécurité. Intercept X partage l'état de sécurité des appareils avec Sophos ZTNA, et ces données peuvent être utilisées dans les politiques d'accès aux applications.

Plateformes prises en charge par Sophos ZTNA

Plateformes prises en charge	Actuellement	Prévues
Fournisseurs d'identité	Microsoft Azure et Okta	Autres IDP selon la demande
Plateformes de passerelle Sophos ZTNA	VMware ESXi 6.5+, Hyper-V et AWS	Azure, Nutanix et GCP
Plateformes du client Sophos ZTNA	Windows 10 1803 ou supérieur, macOS 11 (Big Sur) ou supérieur	iOS et Android
État de sécurité de l'appareil Sophos ZTNA	Sophos Security Heartbeat (Intercept X)	Centre de sécurité Windows, des attributs supplémentaires d'évaluation de la posture sont prévus

Points de présence (PoP) Sophos ZTNA Cloud Gateway

Si vous déployez des passerelles Sophos Cloud Gateway, des points de présence sont disponibles dans les régions suivantes :

- Europe (Irlande et Francfort)
- Amérique du Nord (Ohio et Oregon)
- Asie-Pacifique (Mumbai et Sydney)

Licences Sophos ZTNA

- La licence Sophos ZTNA est simplement basée sur le nombre d'utilisateurs.
- Les passerelles Sophos ZTNA sont gratuites et vous pouvez en déployer autant que vous le souhaitez.
- La gestion dans Sophos Central est incluse sans frais supplémentaires.
- Sophos ZTNA fonctionne mieux avec Sophos Intercept X et Sophos Firewall (mais fonctionne aussi parfaitement avec n'importe quel produit endpoint ou pare-feu).

Ressources complémentaires

Tirez profit des ressources suivantes pour mieux planifier votre déploiement de Sophos ZTNA.

- [Documentation Sophos ZTNA](#)
- [Ressources de la communauté Sophos ZTNA](#)

Essayez gratuitement Sophos
ZTNA pendant 30 jours
sophos.fr/ztna

Sophos France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

© Copyright 2023. Sophos Ltd. Tous droits réservés.
Immatriculée en Angleterre et au Pays de Galles N° 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Royaume-Uni.

Sophos est la marque déposée de Sophos Ltd. Tous les autres noms de produits et de sociétés mentionnés sont des marques ou des marques déposées appartenant à leurs propriétaires respectifs.

23-01-10 FR (DD)

SOPHOS