SOPHOS

Lista de comprobación para el despliegue de Sophos ZTNA

El despliegue de Sophos ZTNA es rápido y sencillo al distribuirse y gestionarse en la nube a través de Sophos Central, la plataforma de gestión de ciberseguridad en la que más confía el mundo. Utilice esta lista de comprobación para asegurarse de que dispone de las tecnologías de apoyo necesarias para llevar a cabo un despliegue sin problemas.

Lista de comprobación para un despliegue rápido:

- ✔ Desea microsegmentar las aplicaciones gestionadas dentro de su red y las alojadas en AWS y ofrecer un acceso seguro a sus usuarios remotos.
- ✔ Cuenta con una plataforma de hipervisor o un proveedor de la nube compatibles con las puertas de enlace ZTNA.
- ✔ Tiene un proveedor de identidad moderno: Azure u Okta. Azure puede ser gratuito en muchos casos para el soporte IDP básico y se integra rápidamente con una implementación local de Active Directory.
- ✔ Dispone de Windows 10 para acceder a aplicaciones de cliente pesado o desea ofrecer un acceso sin cliente basado en navegador a las aplicaciones web en todas las plataformas.
- ✔ Quizá también desea integrar el estado de seguridad de los dispositivos en las políticas de acceso usando la Seguridad Sincronizada de Sophos con Intercept X.

Consideraciones específicas:

Identifique todas sus aplicaciones gestionadas: identifique las aplicaciones que desea microsegmentar y a las que quiere proporcionar un acceso remoto seguro. Sophos ZTNA requiere que estas aplicaciones estén alojadas de forma local, en su centro de datos, en un proveedor de alojamiento o en la nube pública de Amazon Web Services (AWS). Sophos ZTNA no puede controlar el acceso a aplicaciones de terceros alojadas en Internet (SaaS) como SalesForce.com u O365, ya que estas aplicaciones son de cara al público por diseño.

Determine su estrategia de puertas de enlace: las puertas de enlace de Sophos ZTNA controlan el acceso a las aplicaciones permitiendo la validación continua de la identidad del usuario y la verificación del dispositivo. Las puertas de enlace ZTNA son necesarias en la puerta de enlace de la red de cada ubicación que aloje aplicaciones. Por ejemplo, si tiene aplicaciones alojadas en dos centros de datos diferentes y en AWS, necesitará tres puertas de enlace ZTNA. Se pueden desplegar gratuitamente tantas puertas de enlace de Sophos Zero Trust como necesite. Las plataformas que admiten las puertas de enlace ZTNA se detallan en la tabla que aparece más abajo. Asegúrese de que dispone de estas plataformas para desplegar su puerta o puertas de enlace.

Defina su estrategia de identidad: necesitará un proveedor de identidad (IDP) compatible con Sophos ZTNA para autenticar a sus usuarios. La lista de proveedores se incluye en la tabla que encontrará más abajo. Sophos ZTNA funcionará con la mayoría de soluciones de autenticación multifactor (MFA) que se integran con los IDP compatibles. Puede utilizar una implementación local de Active Directory para importar un árbol de directorios en Sophos Central para la creación de políticas basadas en usuarios, pero esto no es suficiente como solución de IDP de acceso remoto.

Determine el número de usuarios: la concesión de licencias de ZTNA es sumamente sencilla, ya que se basa en los usuarios, por lo que basta con contabilizar el número de usuarios que requieren acceso seguro a una aplicación. Para facilitar el despliegue del cliente, el cliente de Sophos ZTNA se despliega fácilmente desde Sophos Central junto con Intercept X Endpoint Agent, pero también puede desplegarse de forma independiente junto con cualquier otro producto antivirus de escritorio.

Considere su estrategia en cuanto al estado de seguridad de los dispositivos (opcional): se trata de una capa de seguridad complementaria opcional para controlar el acceso a las aplicaciones en función del estado del dispositivo o de su cumplimiento. En un principio, Sophos ZTNA es compatible con Sophos Security Heartbeat para conocer el estado y el cumplimiento de los dispositivos. Esto requiere Sophos Intercept X, que también se gestiona a través de Sophos Central, plataforma que ofrece un único panel de control intuitivo para administrar todas sus necesidades de ciberseguridad. Intercept X comparte el estado de seguridad de los dispositivos con Sophos ZTNA, información que puede utilizarse en las políticas de acceso a las aplicaciones.

Plataformas compatibles con Sophos ZTNA

Plataformas compatibles	Actuales	Previstas
Proveedores de identidad	Microsoft Azure y Okta	IDP adicionales en función de la demanda
Plataformas para puertas de enlace ZTNA	VMware ESXi 6.5+ y AWS	Azure, Hyper-V, Nutanix y GCP
Plataformas para el cliente ZTNA	Windows	macOS, iOS, Android
Estado de seguridad de dispositivos para ZTNA	Sophos Security Heartbeat (Intercept X)	Centro de seguridad de Windows: se han previsto atributos adicionales de evaluación de la postura

Licencias de Sophos ZTNA

- Las licencias de Sophos ZTNA se conceden simplemente en función del número de usuarios.
- Se pueden desplegar gratuitamente tantas puertas de enlace de Sophos ZTNA como necesite.
- La administración en Sophos Central está incluida sin costes adicionales.
- Sophos ZTNA funciona mejor junto con Sophos Intercept X y Sophos Firewall (pero también funciona perfectamente junto a cualquier firewall o producto para endpoints).

Recursos adicionales

Saque partido de los siguientes recursos para planificar mejor su despliegue de Sophos ZTNA.

- Documentación de Sophos ZTNA
- Recursos de ZTNA en Sophos Community

Pruebe Sophos ZTNA gratis durante 30 días en
sophos.com/ztna

Ventas en España:
Tel.: (+34) 91 375 67 56
Email: comercialES@sophos.com

Ventas en América Latina:
Email: Latamsales@sophos.com

21-08-18 ES (DD)