INFORME SOBRE LA SOLUCIÓN DE AKAMAI

Gestión de acceso e identidades de usuario con la segmentación

Una capa de control crítica adicional para los centros de datos híbridos modernos

Reducir la superficie de ataque de los entornos de TI actuales no solo consiste en crear controles estrictos en torno a aplicaciones específicas, acordonándolas frente a cualquier daño. Sin duda es un buen primer paso y puede ser útil en ciertos casos, como en la contención de filtraciones o el cumplimiento de normativas. Sin embargo, sin una solución de segmentación que admita la gestión de acceso e identidades de usuario, su organización dispone de un punto ciego de seguridad que incluye a cada persona que utiliza la red o entra en ella.

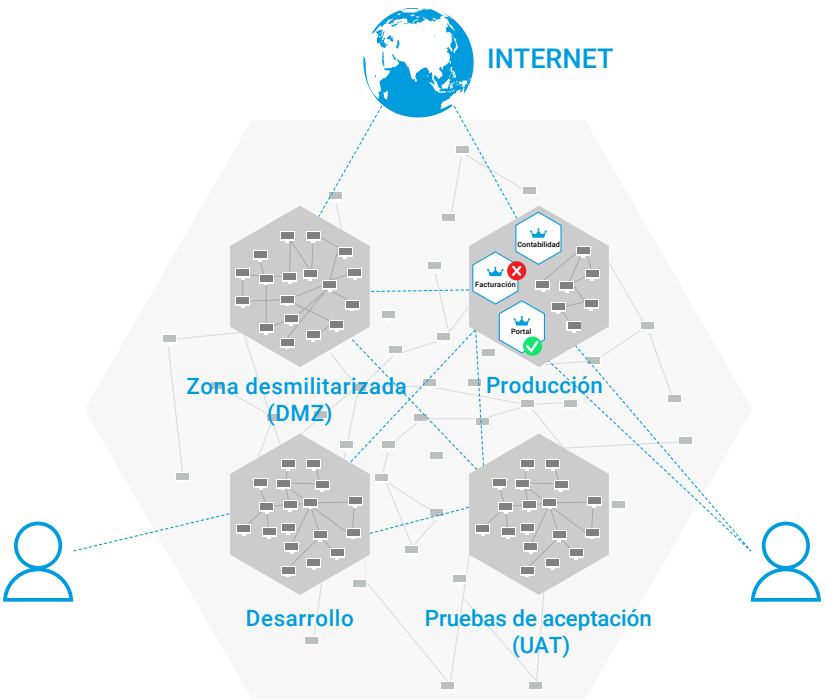
Una vez implementada la segmentación de aplicaciones, el siguiente paso esencial consiste en aprovechar la solución de segmentación para crear políticas en torno a quién puede acceder a estas aplicaciones; así se garantiza que sean igual de seguras en todas y cada una de las arquitecturas de la red.

Casos de uso: segmentación para acceso e identidades de usuario

Gestión de acceso de usuarios

Mediante un grupo de usuarios de Active Directory, Guardicore Segmentation de Akamai puede controlar el acceso de los usuarios a cualquier aplicación o carga de trabajo, y desde cualquier entorno. Los grupos de usuarios específicos tienen acceso a servidores específicos, a través de puertos o procesos específicos, mientras que otros no. Los grupos de usuarios tienen sus propios permisos, mientras que el resto de los accesos se pueden bloquear. Sin necesidad de un firewall centralizado, puede utilizar un control de acceso detallado entre cargas de trabajo en segmentos específicos de la red.

Control de acceso de usuarios



¿Por qué se recomienda la segmentación para el control de acceso de usuarios?

Control de acceso de usuarios en cualquier lugar
Las políticas funcionan en portátiles, equipos de escritorio, VDI, servidores virtuales o bare metal e infraestructura de nube.

Segmentación definida por software
Sin cambios en la red ni en la arquitectura, sin cables, sin tiempo de inactividad del servidor y sin necesidad de reiniciar los sistemas.

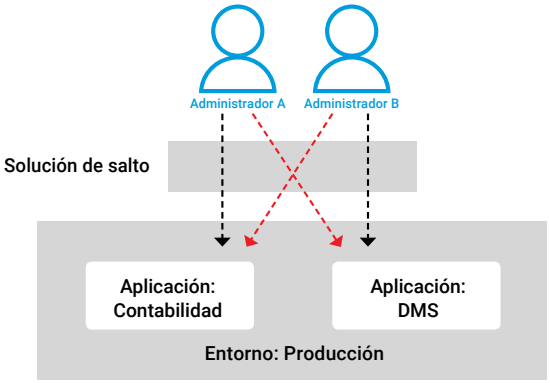
Rapidez y potencia
La creación de políticas es sencilla e intuitiva, y pueden aplicarse de inmediato tanto en las sesiones nuevas como en las activas.

Rentabilidad
En comparación con los casos de uso similares con la infraestructura de solución de salto tradicional, se ha demostrado que los costes son hasta un 60 % inferiores.

Akamai

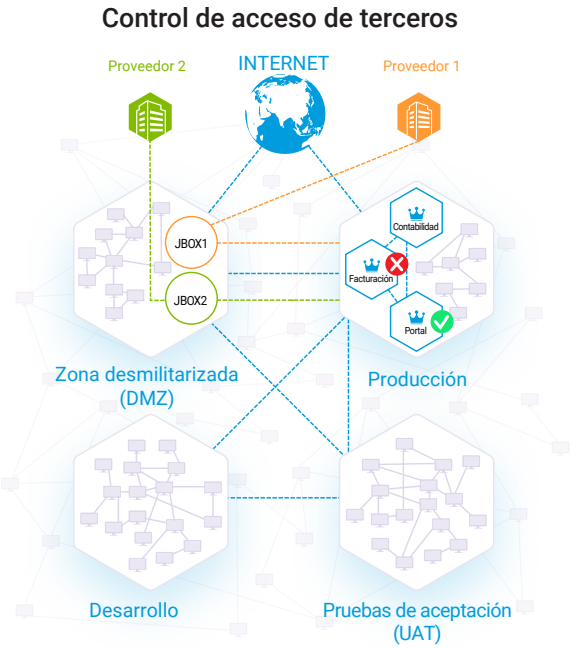
Gestión de acceso simultáneo de usuarios

Los administradores pueden acceder a diferentes aplicaciones a través de la misma solución de salto o servidor de terminales, incluso cuando están conectados a la vez. Mientras tanto, las políticas dispares funcionarán sin problemas, lo que permite a un usuario acceder a los recursos a los que está autorizado mientras que el otro usuario permanece bloqueado, sin interrumpir el servicio o el acceso de ninguno de los dos usuarios.



Control de acceso de terceros

En función de la identidad del usuario, Guardicore Segmentation de Akamai puede controlar el acceso de terceros, por ejemplo, de proveedores externos o de SaaS. Con la ayuda de grupos de usuarios, cada conexión de terceros puede tener sus propias políticas de acceso definidas tanto para el centro de datos como para aplicaciones específicas, lo que permite la asignación de permisos en relación con lo que el usuario necesita para su propia función, y nada más.



Juntas, la segmentación de aplicaciones y la gestión de acceso e identidades de usuario ofrecen el efecto dos en uno más sólido para proteger el centro de datos empresarial moderno.

¿Quiere saber cómo funcionan de forma conjunta? Póngase en contacto con uno de nuestros expertos.

Publicado en 06/23