FICHA DE DATOS

Zscaler Microsegmentation

Desafíos de la microsegmentación tradicional

Muchas empresas dependen de arquitecturas de seguridad heredadas para proteger sus cargas de trabajo. Estas arquitecturas son inadecuadas: son complejas de implementar, aumentan la superficie de ataque, amplifican el movimiento lateral y aumentan el costo operativo.

- Obtener un inventario de activos preciso es un desafío, especialmente en el caso de los recursos en la nube, donde se activan y desactivan de forma dinámica.
- Soluciones como los cortafuegos extienden la red a las cargas de trabajo y servidores, lo que amplifica los riesgos de movimiento lateral.
- Los mosaicos de dispositivos virtuales, herramientas operativas y políticas no estándar introducen brechas conocidas y desconocidas en la cobertura de seguridad, lo que aumenta el riesgo.
- Las herramientas de segmentación personalizadas de terceros son de difícil implementación y la aplicación de las políticas de seguridad corporativas es inconsistente.

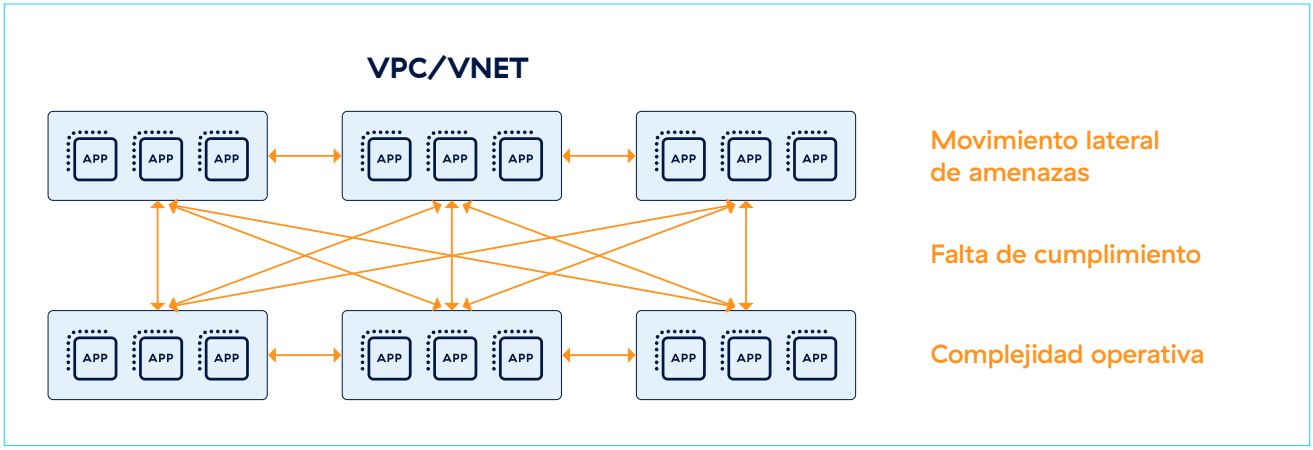

Figura 1: Las arquitecturas de protección de carga de trabajo tradicionales son inadecuadas para detener el movimiento lateral de amenazas

Amplíe la arquitectura zero trust a las nubes públicas y a los centros de datos locales

La microsegmentación basada en host aborda estos desafíos al dividir la red en segmentos más pequeños y más controlables. Aplica reglas de seguridad en cada segmento, otorgando exclusivamente acceso esencial. De esta manera, si se produce una infracción en un segmento, el resto de la red permanece segura. A medida que las ciberamenazas se vuelven más avanzadas, es evidente que las defensas perimetrales básicas ya no pueden detener estos ataques inteligentes.

La microsegmentación Zscaler proporciona:

Detección y visibilidad de activos en tiempo real: obtenga un inventario de activos en toda su infraestructura.

- Descubra activos en tiempo casi real. Obtenga un inventario de activos basado en etiquetas definidas por el usuario y atributos de la nube (VPC/VNET) u objetos de red (IP/subnet).
- Obtenga visibilidad de los recursos en múltiples nubes públicas, centros de datos y ubicaciones conjuntas en una sola consola.

Recomendación de políticas automatizada: garantice que todos los activos estén cubiertos por una política de seguridad.

- Obtenga recomendaciones de políticas para segmentar los flujos de trabajo según el análisis del flujo de tráfico.
- Reciba sugerencias de políticas proactivas para cubrir recursos que no están segmentados.

Aplicación de políticas granulares: detenga el movimiento lateral de amenazas.

- Aplique controles a nivel de host para limitar el acceso.
- Logre una política de seguridad uniforme en todos los recursos en los centros de datos y la nube pública.

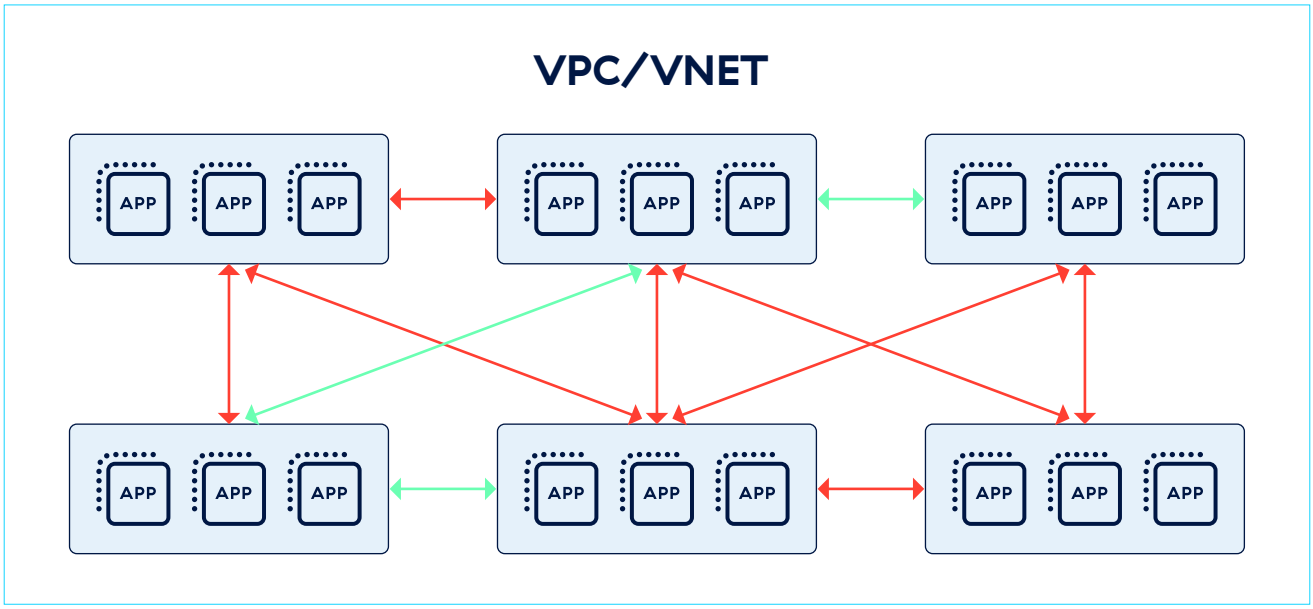

Figura 2: La microsegmentación de Zscaler ofrece una segmentación basada en zero trust y en el host

Capacidades de microsegmentación de Zscaler

Característica	Detalles
Cobertura local y en la nube pública	Cargas de trabajo seguras en AWS, Microsoft Azure, con soporte adicional para servidores de centros de datos locales.
Inventario de host	Obtenga visibilidad de sus cargas de trabajo en la nube, incluidos los detalles del host, el entorno de nube y las etiquetas definidas por el usuario.
Inventario de flujos	Obtenga visibilidad granular de los flujos, incluidos detalles de 5 tuplas, nombre de la aplicación y ruta de la aplicación.
Mapa de aplicación	Obtenga un mapa interactivo de flujos coincidentes entre los recursos de la aplicación en el entorno.
Políticas de recursos	Cree y aplique políticas entre los recursos de su aplicación.
Zonas de aplicación	Alcance de control de las reglas de política basadas en zonas o entornos de aplicación.
Actualizaciones de agente simplificadas	Actualice los agentes de microsegmentación de Zscaler por grupos utilizando perfiles de versión.
Panel de análisis	Paneles de análisis que incluyen los principales recursos iniciadores, receptores y flujos a Internet basados en registros de flujos observados.
Compatibilidad con una gran variedad de plataformas	Se pueden instalar agentes ligeros en sistemas operativos comunes, como Windows y Linux.
Transmisión de registros	Consolide registros de todas las cargas de trabajo y servidores, a nivel global, en un depósito central determinado por su organización, con Zscaler Nanolog Streaming Service. Los administradores pueden ver y extraer datos del registro de tráfico de las cargas de trabajo en tiempo real.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com/es