FICHA TÉCNICA

Zscaler Microsegmentation

Desafios com a microssegmentação legada

Muitas empresas dependem de arquiteturas de segmentação legadas para proteger suas cargas de trabalho. Essas arquiteturas são inadequadas: elas são complexas de implantar, aumentam a superfície de ataque, amplificam a movimentação lateral e aumentam o custo operacional.

- Obter um inventário preciso de ativos é um desafio, especialmente para recursos na nuvem, onde eles são criados e encerrados dinamicamente.
- Soluções como firewalls estendem a rede para cargas de trabalho e servidores, ampliando os riscos de movimentação lateral.
- Os mosaicos de dispositivos virtuais, ferramentas operacionais e políticas não padronizadas introduzem brechas conhecidas e desconhecidas na cobertura de segurança, aumentando o risco.
- Ferramentas de segmentação personalizadas de terceiros são complexas de implantar, e a aplicação de políticas de segurança corporativa é inconsistente.

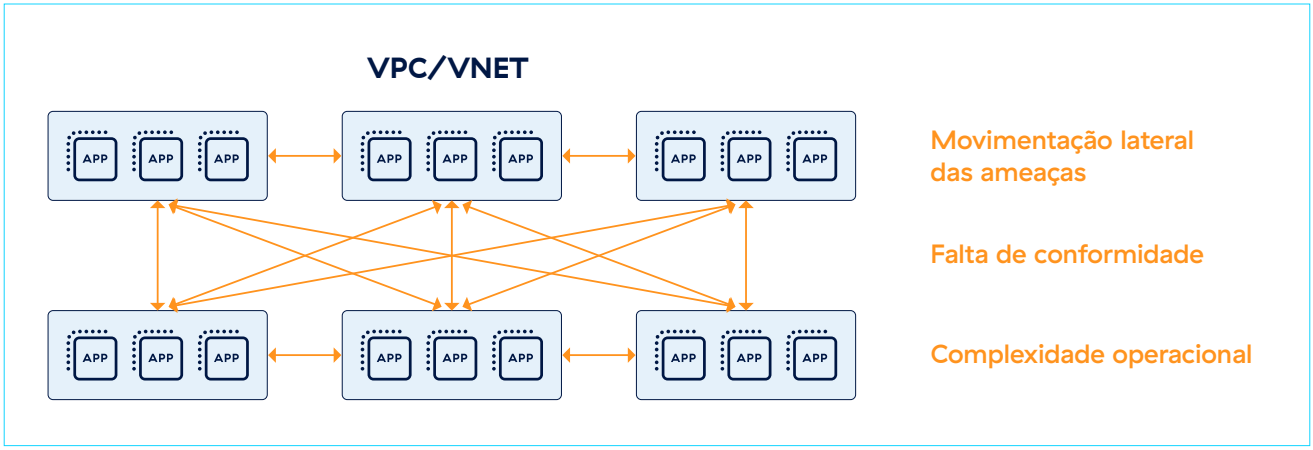

Figura 1: as arquiteturas legadas de proteção de cargas de trabalho são inadequadas para impedir a movimentação lateral de ameaças

Estenda a arquitetura zero trust para segmentar cargas de trabalho em nuvens públicas e data centers locais

A microssegmentação baseada em host aborda esses desafios dividindo a rede em segmentos menores e mais controláveis. Ela aplica regras de segurança em cada segmento, concedendo apenas acesso essencial. Dessa forma, se um segmento for violado, o restante da rede permanecerá seguro. Com as ameaças cibernéticas se tornando mais avançadas, é evidente que as defesas básicas de perímetro não conseguem mais impedir esses ataques inteligentes.

A Zscaler Microsegmentation fornece:

Descoberta e visibilidade de ativos em tempo real: obtenha um inventário dos ativos em sua infraestrutura.

- Descubra ativos quase em tempo real. Obtenha um inventário de ativos com base em tags definidas pelo usuário, atributos de nuvem (VPC/VNET), ou objetos de rede (IP/subnet).
- Obtenha visibilidade dos recursos em diversas nuvens públicas, data centers e colocalizações em um único console.

Recomendação de políticas automatizada: garanta que todos os ativos estejam cobertos por uma política de segurança.

- Obtenha recomendações de políticas para segmentar fluxos de trabalho com base na análise do fluxo de tráfego.
- Receba sugestões de políticas proativas para cobrir recursos que não são segmentados.

Aplicação granular de políticas: interrompa a movimentação lateral de ameaças.

- Aplique controles no nível do host para limitar o acesso.
- Obtenha uma política de segurança consistente em todos os recursos em data centers e nuvem pública.

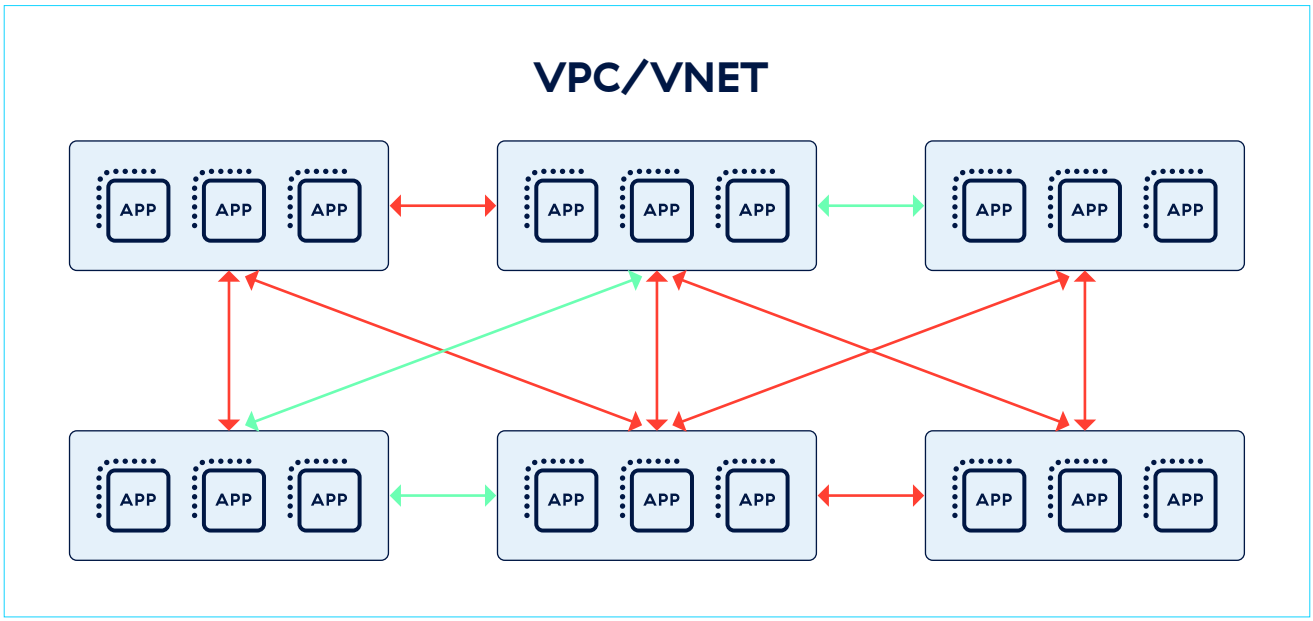

Figura 2: a Zscaler Microsegmentation oferece segmentação baseada em host e zero trust

Recursos da Zscaler Microsegmentation

CARACTERÍSTICAS	DETALHES
Cobertura de nuvem pública e local	Proteja cargas de trabalho da AWS e Microsoft Azure, com suporte adicional para servidores de data center locais.
Inventário do host	Obtenha visibilidade de suas cargas de trabalho na nuvem, incluindo detalhes do host, ambiente de nuvem e tags definidas pelo usuário.
Inventário de fluxo	Obtenha visibilidade granular dos fluxos, incluindo detalhes de 5 tuplas, nome do aplicativo e rota do aplicativo.
Mapa de aplicativo	Obtenha um mapa interativo de fluxos correspondentes entre recursos de aplicativos no ambiente.
Políticas de recursos	Crie e aplique políticas entre os recursos do seu aplicativo.
Zonas de aplicação	Alcance de controle das regras de política com base em zonas de aplicação ou ambientes.
Melhorias simplificadas de agentes	Melhore os agentes da Zscaler Microsegmentation por grupos usando perfis de versão.
Painel de análise	Painéis de análise, incluindo os N principais recursos como iniciadores, receptores e fluxos para a internet com base em registros de fluxo observados.
Amplo suporte de plataforma	Agentes leves podem ser instalados em sistemas operacionais comuns, incluindo Windows e Linux.
Transmissão de registros	Consolide logs de todas as cargas de trabalho e servidores, globalmente, em um repositório central determinado pela sua organização, com o Zscaler Log Streaming Service. Os administradores podem visualizar e extrair dados de log de tráfego de cargas de trabalho em tempo real.

zscaler™ | Experience your world, secured.™

Sobre a Zscaler
A Zscaler (NASDAQ: ZS) acelera a transformação digital para proporcionar aos seus clientes mais agilidade, eficiência, resiliência e segurança. A Zscaler Zero Trust Exchange protege milhares de clientes contra ataques cibernéticos e perda de dados ao conectar com segurança usuários, dispositivos e aplicativos em qualquer local. Distribuída em mais de 150 data centers no mundo inteiro, a Zero Trust Exchange baseada em SASE é a maior plataforma de segurança integrada na nuvem do mundo. Saiba mais em **zscaler.com/br** ou siga-nos no Twitter **@zscaler**.

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