Zscaler Zero Trust SD-WAN

Conecte filiais, fábricas e data centers com segurança, sem sobreposições roteadas ou movimentação lateral de ameaças.

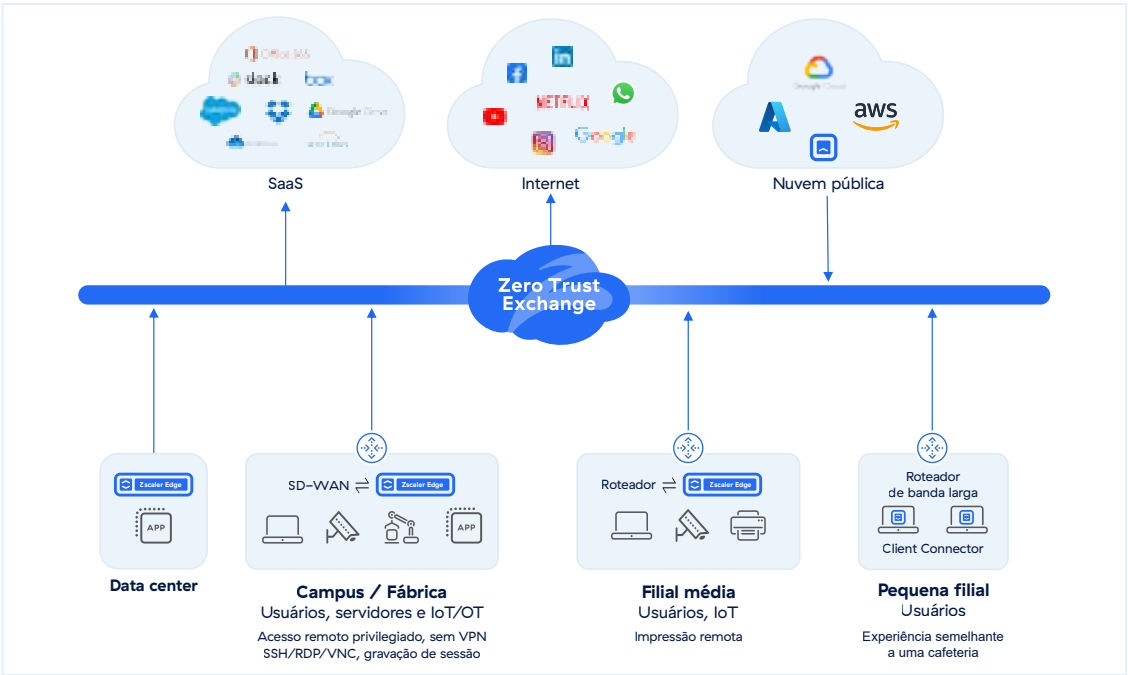
As SD-WANs tradicionais estendem sua rede para filiais remotas e para a nuvem. Isso expande sua superfície de ataque, permite a movimentação lateral de ameaças e facilita ataques de ransomware.

Proteger as redes tradicionais requer uma complexa rede de firewalls, proxies, gateways de NAC e agentes de terminal, o que leva a aumentos descontrolados de custos e complexidade. No final, você ainda fica vulnerável, pois os ataques de ransomware continuam aumentando em escopo e frequência.

Zscaler Zero Trust SD-WAN oferece um meio mais simples, seguro e econômico para usuários, dispositivos e cargas de trabalho se comunicarem, sem a complexidade e os desafios de segurança das redes sobrepostas roteadas.

Zscaler Zero Trust SD-WAN:

- Oferece filiais semelhantes a cafeterias, sem estender sua rede para todos os lugares
- Reduz o risco de ransomware eliminando a movimentação lateral de ameaças
- Reduz a superfície de ataque eliminando portas de VPN e firewalls expostos
- Reduz os custos de infraestrutura simplificando radicalmente sua arquitetura de rede
- Melhora o desempenho de aplicativos eliminando o tráfego de retorno para data centers
- Garante proteção contra ameaças cibernéticas e de dados inspecionando todo o tráfego



As SD-WANs tradicionais facilitam os ataques de ransomware

As organizações enfrentam vários desafios ao usar arquiteturas de rede e segurança legadas para conectar uma filial à internet ou a seus outros aplicativos em um ambiente de nuvem pública ou data center.

- **Superfície de ataque expandida:** estender a rede para filiais remotas oferece mais oportunidades para invasores se infiltrarem em sua organização. Cada firewall ou gateway de VPN é um ponto de entrada, e vulnerabilidades de dia zero continuam a assolar o setor.
- **Movimentação lateral de ameaças:** um usuário infectado ou dispositivo de IoT em uma filial é capaz de verificar a rede e se mover lateralmente para outros locais, data centers e nuvens privadas virtuais. Ataques recentes de ransomware levaram apenas 45 minutos da invasão inicial até interrupções paralisantes, não deixando tempo para as equipes de operações reagirem.
- **Custo e complexidade:** a colcha de retalhos de firewalls, proxies, agentes de NAC e políticas baseadas em IP projetadas para proteger e segmentar SD-WANs adiciona enorme complexidade operacional e custo, além de prejudicar a agilidade da sua organização.
- **Desempenho e experiência de usuário insatisfatórios:** o tráfego de retorno para data centers e por meio de vários pontos de inspeção de segurança geralmente resulta em baixo desempenho do aplicativo e uma experiência inconsistente para os usuários.

Zero Trust SD-WAN elimina a movimentação lateral de ameaças

Zero Trust SD-WAN conecta com segurança suas filiais, fábricas e data centers sem a complexidade de VPNs ou roteamento de sobreposição. Ela garante acesso zero trust entre usuários, dispositivos de IoT/OT e aplicativos com base em políticas organizacionais. Combinando o poder da avançada plataforma Zero Trust Exchange da Zscaler com a conectividade contínua para locais, nuvens e usuários, as organizações podem adotar uma estrutura de Secure Access Service Edge (SASE) e oferecer uma experiência de filial semelhante ao de uma cafeteria.

- Zero Trust SD-WAN fornece às filiais, campi e fábricas acesso rápido e confiável à internet, aplicativos SaaS e aplicativos privados com uma arquitetura direta à nuvem que fornece alta segurança e simplicidade operacional
- Ela elimina a movimentação lateral de ameaças e reduz bastante o risco de ransomware para sua organização.
- Ela reduz os custos de infraestrutura e operação ao eliminar roteamentos complexos, VPNs e firewalls, ao mesmo tempo em que garante proteção total contra ameaças cibernéticas e proteção de dados.

Como funciona a Zero Trut SD-WAN

Zero Trust SD-WAN usa um dispositivo físico ou virtual na filial/campus/fábrica para gerenciar conexões de ISP e encaminhar tráfego para a Zero Trust Exchange com base em políticas organizacionais. O tráfego de filiais é encaminhado com segurança por conexões DTLS efêmeras para a Zero Trust Exchange, onde pode ser inspecionado quanto a ameaças cibernéticas e perda de dados com políticas de segurança sensíveis ao contexto.

A Zero Trust Exchange facilita a comunicação bidirecional entre dispositivos e aplicativos de internet ou aplicativos privados executados em outros locais, data centers ou na nuvem.

Por exemplo, um servidor de impressão em um data center pode enviar trabalhos de impressão para uma impressora em uma filial remota por meio da Zero Trust Exchange, sem a necessidade de redes roteadas, VPNs ou portas expostas. O tráfego de aplicativos confiáveis pode ser enviado diretamente pela internet com desvios diretos de internet.

Essa abordagem única oferece três vantagens principais:

- **Uma organização mais segura:** o ransomware não pode se mover lateralmente entre os locais; os dispositivos infectados não podem verificar nada além de suas redes locais
- **Uma filial mais simples e econômica:** chega de sobreposições roteadas, firewalls ou VPNs site a site
- **Experiência de usuário aprimorada:** os aplicativos são executados mais rapidamente sem retorno de tráfego e vários pontos de estrangulamento de segurança

Casos de uso de Zero Trust SD-WAN

- **Substituição da VPN:** elimine a complexidade de VPNs site a site e sobreposições roteadas com uma solução de zero trust mais simples e segura
- **Atualização da SD-WAN:** forneça filiais semelhantes a cafeterias e reduza o risco de ransomware
- **Fusões e aquisições:** integre usuários e aplicativos sem a complexidade e o custo de integrar redes
- **Fábricas seguras:** elimine a movimentação lateral entre fábricas e proteja ambientes de TI/OT

Modelos de hardware e software do Branch Connector

CARACTERÍSTICAS	ZT 400	ZT 600	ZT 800	ZT VM
				Zscaler Edge
Tipo	Filiais pequenas/médias	Filial pequena/média	Filial média/grande	Filial e data center
Taxa de transferência criptografada	200 Mbps	500 Mbps	1 Gbps	Varia
Portas físicas	4x RJ45 GbE	6x RJ45 GbE	6x RJ45 GbE, 2x SFP	N/A
Provisionamento zero touch	✓	✓	✓	N/A
Modo de gateway com seleção de rota sensível ao aplicativo	✓	✓	✓	N/A
Políticas de encaminhamento granulares	✓	✓	✓	✓
Políticas de proteção de dados e ameaças cibernéticas para tráfego de internet	✓	✓	✓	✓
Acesso privado seguro para dispositivos de IoT/OT	✓	✓	✓	✓

TABELA 1: RECURSOS DA ZSCALER ZERO TRUST SD-WAN	
CARACTERÍSTICAS	DETALHES
Recursos	
Provisionamento zero touch e implantação automatizada	• Provisionamento zero touch com modelos predefinidos • Implantação totalmente automatizada • Descoberta dinâmica da localização geográfica de filiais
Política de encaminhamento granular para tráfego de internet e aplicativos privados	• Opções para enviar o tráfego para ZIA, ZPA ou Direct (contornando os serviços da Zscaler) • Critérios flexíveis de seleção de tráfego: localização, sublocalização, grupo de localizações, tupla de 5 ou FQDN
Políticas zero trust unificadas	• Política unificada de usuário para aplicativo, dispositivo IoT para aplicativo e servidor para servidor por meio da política aprimorada do ZPA para incluir novos tipos de clientes • Localização e políticas baseadas em localização geográfica • Ativação de política de segurança que inclui IPS, proxy SSL, filtragem de URL e proteção de dados • Pilha de segurança completa com postura configurada para IoT/OT e servidores
Alta disponibilidade	• O failover automático com redundância N+2 garante a continuidade do serviço • Duas instâncias do Branch Connector fornecem suporte adicional para picos de tráfego e redundância em caso de falha de hardware • Um balanceador de carga é configurado para tolerância a falhas ativa-passiva usando um endereço IP virtual (VIP) usando o protocolo de redundância de endereço comum (CARP)
Visibilidade centralizada e registro granular	• Painel centralizado para monitoramento de tráfego e integridade do dispositivo • Filtragem disponível para implantações na nuvem, em data centers e filiais • Registro detalhado de cada sessão e transação para todas as portas e protocolos, incluindo todas as transações de DNS públicas e privadas • Integração total com a infraestrutura de NSS: a VM de firewall NSS existente pode ser usada para transmitir os logs para o SIEM
Encerramento da interface WAN	• Conectividade dupla do ISP (Ethernet) • Multihoming com um único dispositivo
Gerenciamento da interface LAN	• Múltiplas redes LAN L3 • Suporte para marcação 802.1q/VLAN • Servidor DHCP • Gateway DNS
Políticas de firewall no dispositivo	• Controle de acesso granular para tráfego local de LAN para LAN (leste-oeste) • Listas de controle de acesso (ACLs) L3/L4
Seleção de caminho com reconhecimento de aplicativo	• Seleção de rota dinâmica para SaaS ou aplicativos privados essenciais • Conectividade inteligente de POPs da Zscaler • Monitoramento e failover integrados de SLA
Roteamento	• Roteamento estático
Data centers/POPs da Zscaler	• A Zscaler desenvolveu sua plataforma de segurança na nuvem em mais de 150 data centers em todo o mundo, estrategicamente posicionados onde os clientes estão localizados • Disponibilidade integrada com failover contínuo para o próximo PoP de serviço disponível

zscaler™ | Experience your world, secured.™

Sobre a Zscaler
A Zscaler (NASDAQ: ZS) acelera a transformação digital para que seus clientes possam ter mais agilidade, eficiência, resiliência e segurança. A Zscaler Zero Trust Exchange protege milhares de clientes contra ataques cibernéticos e perda de dados, conectando com segurança usuários, dispositivos e aplicativos em qualquer local. Distribuída em mais de 150 data centers globalmente, a Zero Trust Exchange baseada em SSE é a maior plataforma integrada de segurança 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