Resumo da solução

Os três principais benefícios da SASE e como alcançá-los

Por que usar Secure Access Service Edge (SASE)?

Os modelos de negócios digitais modernos estão permitindo novos níveis de envolvimento de clientes e funcionários, oferecendo acesso consistente disponível globalmente a aplicativos e serviços, independentemente de onde funcionários e clientes se conectam ou quais dispositivos usam.

A noção de segurança de rede quando seus usuários e aplicativos são distribuídos não é mais viável no mundo digital. A Gartner desenvolveu um novo modelo de rede e segurança que atende aos requisitos da empresa digital. Eles o estão chamando de Secure Access Service Edge (SASE).

> “A arquitetura SASE é importante. Idealmente, o produto é nativo da nuvem, baseado em microsserviços com capacidade de expansão conforme necessário. Para minimizar a latência, os pacotes devem ser copiados para a memória, tratados e encaminhados/bloqueados, não passados de máquina virtual (VM) para VM ou de nuvem para nuvem. A pilha de software não deve ter dependência específica de hardware e ser instanciada quando e onde necessário para fornecer recursos otimizados para riscos e baseados em políticas para a identidade do terminal.” **— Gartner**[1]

Nº 1

Reduz o custo e a complexidade da TI

Com os dados espalhados por aplicativos na nuvem e serviços SaaS, e os usuários muitas vezes trabalhando de qualquer lugar, o modelo tradicional de segurança baseado em rede atingiu seu limite. Para compensar, as organizações foram forçadas a implantar serviços adicionais para corrigir as falhas de segurança, ao mesmo tempo que aumentaram enormemente os custos de implantação, gestão e operação com uma equipe que não cresce na velocidade necessária. Mesmo com este aumento de custo e complexidade, o modelo de segurança de rede ainda não pode ser dimensionado, não é ágil e simplesmente não é eficaz em um mundo digital.

Em vez de tentar usar um conceito legado para resolver um problema moderno, a SASE inverte o modelo de segurança. Enquanto as abordagens legadas se concentram na criação de perímetros em torno dos aplicativos, a SASE se concentra nas entidades, como os usuários que acessam os aplicativos, e leva a segurança o mais próximo possível da entidade. Como um serviço na nuvem, a SASE autoriza ou nega dinamicamente as conexões com o serviço com base em regras de negócio ou ação definidas por uma organização. Tudo isso é feito por meio de um único serviço que unifica diversas funções anteriormente separadas, como SWG, ZTNA e assim por diante.

O QUE PROCURAR

O componente mais importante de um excelente produto SASE é a arquitetura sobre a qual ela é desenvolvida. A Gartner foi específica sobre o tipo de arquitetura necessária para cumprir a promessa da SASE. Mais importante ainda, ela deve ser desenvolvida desde o início para atender a escala necessária para um serviço de segurança totalmente fornecido na nuvem.

Isso significa que deve ser um produto distribuído compatível com vários usuários, com capacidade de dimensionamento global e dinâmico com base na demanda. Ela deve afastar-se dos conceitos tradicionais de redes de políticas e camadas de políticas e, em vez disso, basear-se em políticas organizacionais. Por último, esta arquitetura deve oferecer uma plataforma verdadeiramente integrada com gerenciamento unificado disponibilizado na nuvem.

O QUE EVITAR

A Gartner adverte especificamente contra abordagens tradicionais de segurança de rede que usam produtos baseados em VM executados em infraestruturas de provedores de nuvem. O uso dessas abordagens baseadas em VM em um ambiente de computação IaaS terá dificuldade de dimensionamento e fornecerá uma experiência de usuário inconsistente devido à limitação necessária entre os fornecedores de nuvem e os aplicativos que os usuários estão acessando.

Esse modelo depende de uma arquitetura de usuário único que tenta usar políticas de acesso baseadas em rede em um modelo SASE baseado no acesso do usuário, o que cria implantações muito mais complexas que não se traduzem em um modelo SASE. Além disso, essas abordagens baseiam-se frequentemente em vários produtos que não estão verdadeiramente integrados, mas que são interligados através de uma interface sobreposta de serviços independentes, muitas vezes comprados através de aquisições.

> “A Secure Access Service Edge é um produto emergente que combina recursos abrangentes de WAN com funções completas de segurança de rede (como SWG, CASB, FWaaS e ZTNA) para oferecer suporte às necessidades dinâmicas de acesso seguro das empresas digitais.” **— Gartner**[1]

Nº 2 Oferece uma ótima experiência ao usuário

Há um bom motivo para o foco principal da SASE ser a experiência do usuário. Quando os usuários estavam na rede local, os aplicativos ficavam no data center e os servidores e a infraestrutura pertenciam e eram gerenciados pela TI, era fácil controlar e prever a experiência do usuário. Agora que os aplicativos estão distribuídos em várias nuvens, seu método de acesso a esses aplicativos ainda se baseia no antigo modelo de VPN que conecta-se a uma rede para segurança. Esse modelo leva o usuário à segurança, e não a segurança ao usuário, o que é necessário para uma ótima experiência de usuário. A SASE zero trust exige que a segurança seja aplicada próxima aos usuários, gerenciando de forma inteligente as conexões dos usuários nos pontos de troca de tráfego e otimizando as conexões diretas (emparelhamento) com aplicativos e serviços na nuvem para garantir largura de banda ideal e baixa latência.

O QUE PROCURAR

A chave para proporcionar uma ótima experiência ao usuário se resume a fornecer largura de banda ideal com a menor latência. A única maneira de fazer isso de forma eficaz é reduzir os saltos para chegar aos aplicativos e garantir que a largura de banda correta seja alocada por meio de controles de largura de banda.

A abordagem correta coloca a pilha de segurança o mais próximo possível do usuário nos pontos de troca de tráfego em uma implantação geográfica amplamente distribuída. O acesso a aplicativos a partir desses pontos requer a capacidade de encaminhar de forma inteligente o tráfego para a localização geográfica mais próxima do aplicativo através do emparelhamento direto.

O QUE EVITAR

Produtos baseados em VMs executadas em provedores de nuvem ou IaaS exigirão controle de tráfego. Tais ofertas são especificamente mencionadas no documento da SASE como não qualificadas para serem definidas como uma solução SASE, e devem ser evitadas.

Isso ocorre principalmente porque as arquiteturas baseadas em VM não são dimensionável e não controlam a conexão do usuário, fazendo isso a partir do ambiente de computação do aplicativo e, portanto, não podem garantir uma boa experiência do usuário. Além disso, esses produtos não podem ser dimensionados dinamicamente e exigem um planejamento de uso que não permite alterações posteriores sem tempo de inatividade programado.

> “Os recursos de decisão e aplicação de políticas da SASE precisam estar em todos os lugares onde as identidades de terminal estarão localizadas... Produtos SASE que usam apenas a capacidade de backbone da internet da IaaS, mas sem recursos locais de POPs/edge, correm o risco de sofrer com latência, problemas de desempenho e a resultante insatisfação do usuário final.” — **Gartner**[1]

Nº 3 Reduz os riscos

Segurança tem tudo a ver com identificação e prevenção de riscos. A SASE zero trust como um serviço na nuvem foi projetada para enfrentar os desafios únicos de riscos na nova realidade de usuários e aplicativos tão dispersos. Definir a segurança como uma função incorporada na própria estrutura do modelo, e não como uma função separada da conectividade dos serviços, garante que todas as conexões sejam inspecionadas e protegidas, independentemente de onde os usuários estão se conectando, quais aplicativos estão acessando ou qualquer criptografia que possa ser usada.

O QUE PROCURAR

A chave para a reduzir os riscos é ter a capacidade de abandonar os conceitos da conectividade baseada em rede e, em vez disso, conectar os usuários a aplicativos com base no verdadeiro acesso à rede zero trust (ZTNA). O ZTNA garante que apenas usuários autorizados a acessar um aplicativo possam fazê-lo, e essa autorização é definida por meio de políticas organizacionais e não por definições de políticas complexas em várias camadas.

Outra forma de uma plataforma SASE reduzir os riscos é removendo a superfície de ataque. Ao ocultar a rede corporativa e as identidades de origem da internet, a SASE evita que adversários atinjam você com ataques como DDoS.

O modelo SASE é fornecido por meio de uma arquitetura baseada em proxy que gerencia todas as comunicações entre usuários e aplicativos. Essa arquitetura garante que todo o tráfego possa ser descriptografado e inspecionado, além de fornecer visibilidade total. Por último, a arquitetura SASE é construída com contexto de dados completo sendo trocado entre entidades e aplicativos para garantir que todas as conexões atendam aos requisitos de conformidade e governança de dados.

O QUE EVITAR

As abordagens tradicionais de segurança de perímetro usavam um modelo baseado em firewall que analisava os fluxos de pacotes e determinava o risco com base na inspeção desses fluxos. Embora esse modelo tenha funcionado para a segurança baseada em perímetro, ele não é adequado aos novos desafios de uma implantação baseada em SASE.

O maior problema é que uma arquitetura de firewall executada como um serviço determina as ameaças após o fato, permitindo que elas cheguem ao destino antes da descoberta. A razão é simples: elas são incapazes de armazenar os dados e determinar seus resultados antes de enviá-los. Essa limitação torna a descriptografia da sessão e a proteção de dados excepcionalmente difíceis, porque são funções que exigem que o fluxo de dados seja mantido e remontado, semelhante a um proxy.

Com um serviço de firewall, as funções de descriptografia, inspeção e remontagem exigem um processo separado que é dissociado do serviço, complicando as políticas, introduzindo latência e resultando em baixo desempenho — e muitas vezes oferece funcionalidade limitada quando implementada. Além disso, a SASE requer uma arquitetura de passagem única para processar todo o conteúdo de uma só vez. Os produtos de firewall baseados no fluxo também expõem o endereço IP de origem da rede host a possíveis adversários, expondo efetivamente sua superfície de ataque, o que pode levar a ataques direcionados.

A abordagem da Zscaler para SASE

A plataforma de segurança na nuvem baseada em IA da Zscaler é um serviço SASE desenvolvido desde o início para oferecer desempenho e capacidade de dimensionamento. Como uma plataforma distribuída globalmente, os usuários estão sempre a poucos passos de seus aplicativos e, por meio do emparelhamento com centenas de parceiros nos principais pontos de troca em todo o mundo, a Zscaler garante desempenho e confiabilidade ideais para seus usuários, cargas de trabalho, parceiros de negócios e locais.

A SASE zero trust da Zscaler baseia-se na plataforma de SSE mais aprovada do setor com uma nova abordagem para SD-WAN. Atualmente, mais de 30% das organizações da Forbes Global 2000 confiam na Zscaler para liderá-las na era digital, de forma segura.

Devido ao seu tempo de mercado, a Zscaler provou que sua arquitetura foi construída para ser dimensionada, processando atualmente mais de 360 bilhões de transações por dia e mais de 500 trilhões de sinais diários para efeito de nuvem de IA/ML.

A arquitetura da SASE zero trust da Zscaler é oferecida de mais de 150 data centers em todo o mundo, garantindo que os usuários obtenham conexões seguras, rápidas e locais, independentemente de onde se conectem.

Para saber mais sobre a abordagem da Zscaler para SASE, acesse
zscaler.com.br/capabilities/secure-access-service-edge

[1] Gartner, O futuro da segurança de rede está na nuvem; Lawrence Orans, Joe Skorupa, Neil MacDonald

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 solução 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