AS 7 ARMADILHAS QUE DEVEM SER EVITADAS AO ESCOLHER UMA SOLUÇÃO DE SSE

Construindo a borda do serviço de segurança (SSE - Security Service Edge) com base na Zero Trust

Por:

Sanjit Ganguli
VP de Estratégia de Transformação/CTO de Campo da Zscaler

Nathan Howe
VP de Tecnologias Emergentes e 5G da Zscaler

Patrocinado por:

zscaler™

As 7 armadilhas que devem ser evitadas ao escolher uma solução de SSE

ÍNDICE

SSE. O que é isso e por que devo me preocupar?

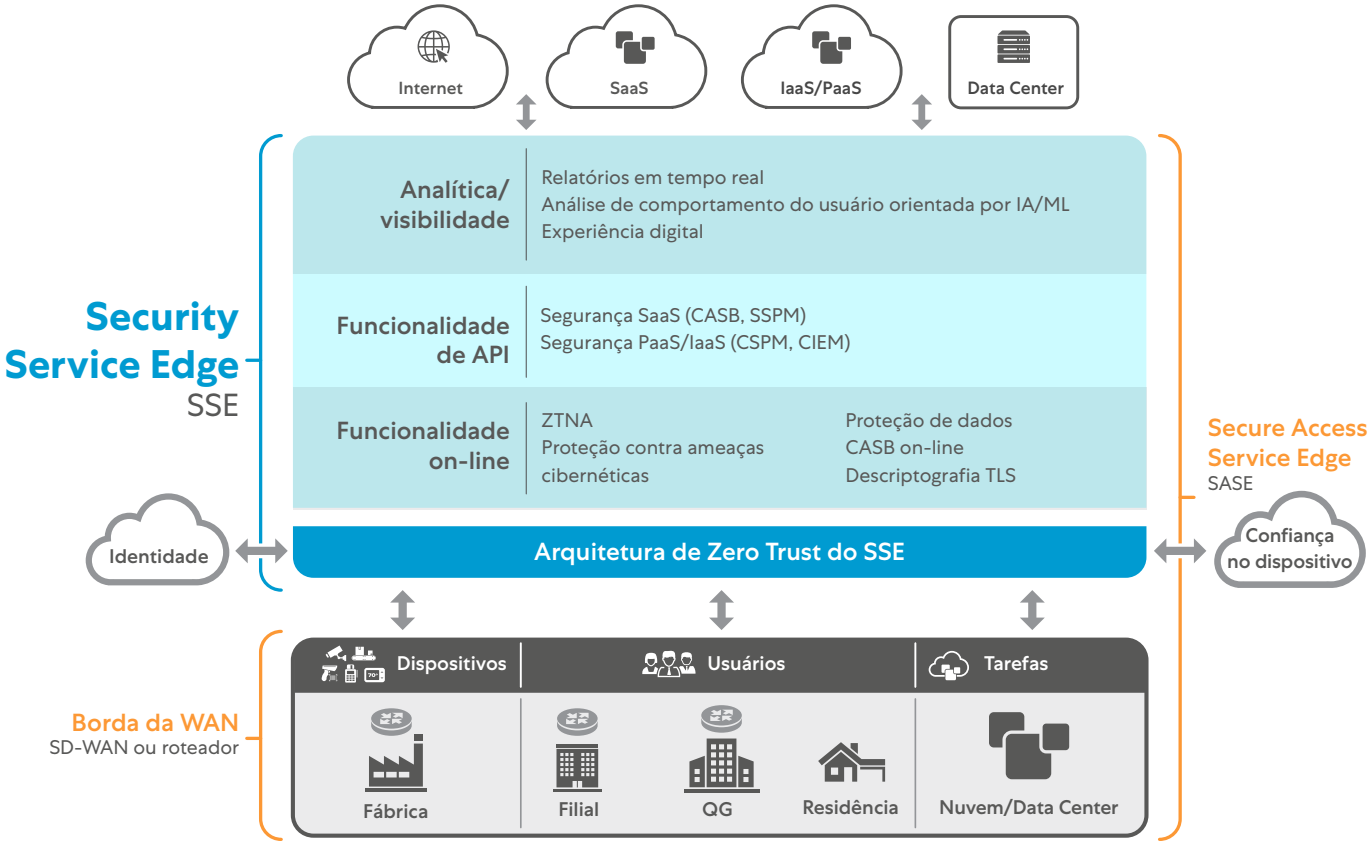


Figura 1: A estrutura do Secure Access Service Edge (SASE) inclui o SSE para fins de decisão e aplicação de políticas. O SASE requer o uso de soluções de conectividade dedicadas pela entidade solicitante e de um limite de segurança dento do qual a política é aplicada.

O Security Service Edge (SSE) é a especificação do Gartner para funções de decisão e aplicação de políticas como componentes da estrutura Secure Access Service Edge (SASE). O SSE promete funções de segurança e conectividade consolidadas, simplificadas e disponibilizadas através da nuvem.

A simplicidade da arquitetura é sempre um benefício para a empresa, especialmente quando essa simplicidade minimiza os esforços técnicos e acelera os negócios. Porém, em muitas organizações a segurança é vista como um incômodo, uma restrição que cria gargalos, um guardião que limita a agilidade ou cria obstáculos para o sucesso do negócio. O SSE se contrapõe a esses estereótipos. Dentro de um ambiente de SSE, a segurança garante proteção e controle, atuando como um facilitador do progresso da empresa.

Alguns antecedentes: Introduzida em 2019, a estrutura do SASE visa orientar as empresas em sua jornada de digitalização, uma jornada caracterizada principalmente pela adoção da nuvem e da mobilidade. O SASE unifica o acesso à rede e a segurança, disponibilizando ambos a partir de uma (altamente distribuída) borda da nuvem (consulte a Figura 1). Dessa forma, o SASE garante que a segurança não seja mais centralizada, e que conexões seguras possam ser feitas de e para qualquer lugar.

©2022 Zscaler, Inc. Todos os direitos reservados.

Vejamos como um telefone celular se conecta a várias redes celulares e sem fio. Não existe uma solução de roteamento de rede dedicada, mas o usuário exige controles de segurança para o tráfego entre a origem e o destino. Analogamente, a borda, a rede ou o local ao qual o usuário se conecta não deve ser relevante para a proteção do tráfego corporativo. O que o SSE oferece é isso

A arquitetura SASE foi rapidamente adotada pelas empresas de segurança digital. Alguns profissionais de marketing se apropriaram cinicamente do termo para obter ganhos de marca, sugerindo que o "Acesso" no SASE significasse sua conformidade com o SASE (ou a não conformidade dos seus concorrentes): "Eu tenho uma função de rede, portanto estou em conformidade com o SASE; você não está construindo roteamentos de rede, então você não está em conformidade com o SASE."

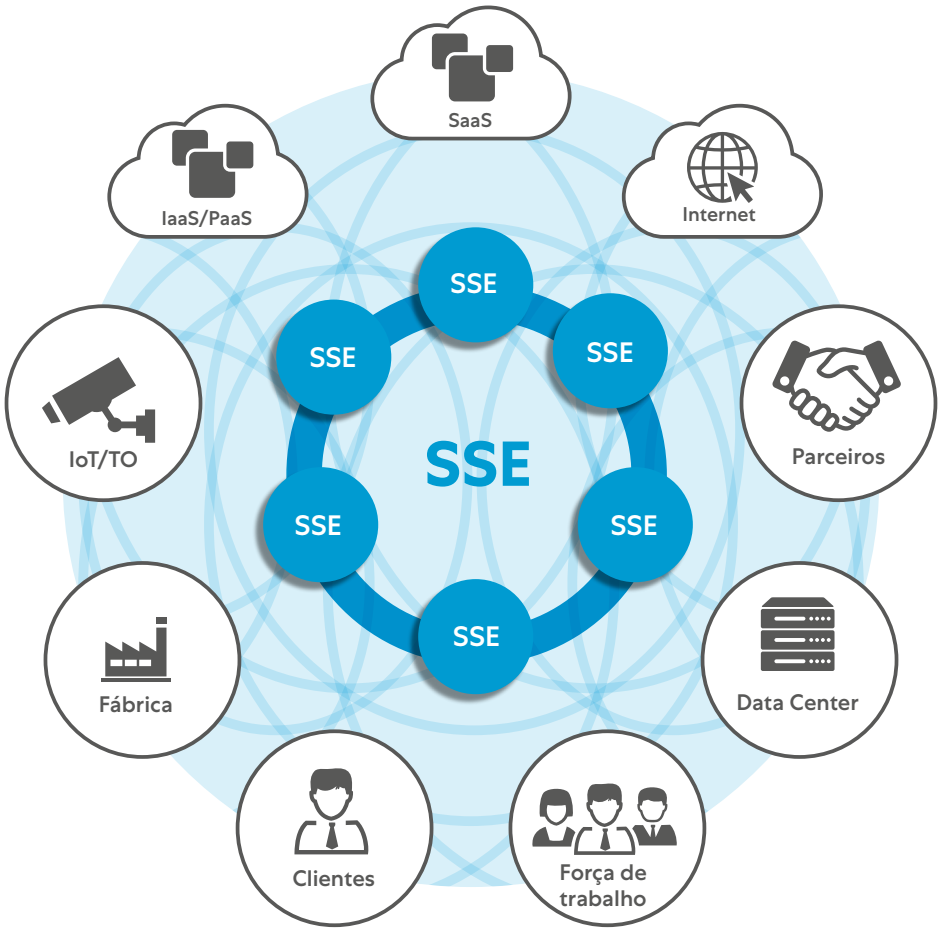


Figura 2: Disponibilize acesso de entidade a entidade na borda, validado e baseado em políticas, para o universo móvel da nuvem. O SSE garante a segurança do usuário na borda sem comprometer o desempenho, sobrepondo-se a todos os seus firewalls e VPNs ao mesmo tempo.

SSE refere-se ao conjunto de serviços SASE usados para proteger o tráfego corporativo. O SSE garante que o usuário (ou carga de trabalho) correto receba acesso, de forma segura e sob controle do TI da empresa, aos aplicativos e serviços corretos. Esses serviços podem ser tarefas de IaaS ou PaaS, aplicativos SaaS ou serviços via Internet como LinkedIn ou YouTube. O acesso ao serviço deve ser concedido conforme os controles do Zero Trust Access (ZTA), descritos com muito mais profundidade na **segunda armadilha a ser evitada**.

©2022 Zscaler, Inc. Todos os direitos reservados.

Para atingir esses objetivos de alto nível, o provedor de soluções de SSE deve fornecer uma solução de rede global, altamente disponível, escalável e generalizada, que ofereça políticas consistentes, acesso de confiança zero e uma experiência digital com total agilidade.

Sem esse tipo de funcionalidade e disponibilidade, as soluções SSE não podem oferecer proteção e disponibilidade onipresentes **(veja a Figura 2.)** Ao contrário do SASE, o SSE não prescreve nenhum método de conexão ou acesso. O SSE pressupõe seu funcionamento em qualquer rede e a disponibilização de controles para qualquer serviço autorizado, onde quer que esse serviço possa estar.

A meta do SASE é combinar conectividade e proteção, mas em um ambiente corporativo essa combinação só funciona se for transparente para os funcionários do usuário final. a conectividade é direta, seja de usuário para aplicativo, de aplicativo para aplicativo, de tarefa para tarefa e assim por diante. Os usuários nunca devem pensar: "Ah, preciso me conectar à rede para poder trabalhar". Em vez disso, sua atitude deve ser "Vou fazer meu trabalho agora".

Esse ideal de integração simplesmente não pode ser alcançado em ambientes corporativos dependentes de uma infraestrutura de rede e segurança legada. Nesse antigo modelo de arquitetura, a segurança era centralizada e o tráfego de dados – independentemente de sua localização (remoto ou ramificado), qualquer que fosse sua origem (usuário, aplicativo ou carga de trabalho) e destino (Internet, nuvem, data center) – primeiro precisava ser conectado e roteado pela rede corporativa até a (e através da) posição física dos controles de segurança localizados em dispositivos de hardware.

O verdadeiro valor comercial da transformação digital promovida pelo SSE

A adoção do SSE pode exigir uma significativa transformação digital da empresa. Mas essa mudança pode trazer resultados tangíveis:

Controle:

O SSE começa do zero. O SSE valida cada pessoa, máquina, carga de trabalho, rede e borda. Sem a identificação correta junto com o contexto fornecido pela análise comportamental, não há acesso – e isso dá à empresa controle total sobre o que ou quem pode acessar qualquer serviço dentro da empresa.

Conectividade direta:

A aplicação da política do SSE está em linha entre a entidade de origem e o serviço de destino. As decisões de acesso são tomadas relativamente a cada aplicativo individual, e não ao nível da rede.

Segurança como uma função de negócio:

As políticas que determinam quais entidades podem se conectar a quais serviços são definidas usando o critério de menor privilégio. Usuários, máquinas, tarefas etc. só podem se conectar àquilo que tiverem permissão para se conectar – e nada mais. Nenhuma outra conectividade é disponibilizada, e todos os demais acessos são bloqueados.

Aplicação global:

O SSE deve ter aplicação global para que os controles sejam aplicados no caminho de acesso de qualquer entidade, com base no contexto fornecido pela política, mecanismos cognitivos e aprendizagem externa (monitoração de ameaças, fraudes etc.). Essa aplicação global deve ser dimensionada de acordo com os requisitos de sua empresa.

Abrangência:

O SSE permite fazer uma análise on-line completa para inspecionar o tráfego em larga escala e em profundidade. O SSE oferece proteção contra ameaças avançadas para defender ativos corporativos (nuvem e além), evitar perdas de dados e garantir o controle em linha. Quando necessário, a solução deve permitir o controle do conteúdo armazenado em serviços na nuvem.

Ocultamento:

O SSE previne os indesejáveis acessos e exposições de ativos corporativos porque ele remove a superfície de ataque e não é possível atacar o que não é acessível.

Ubiquidade:

O SSE disponibiliza essa conectividade para todas as áreas da empresa, de qualquer lugar. O SSE protege e conecta uma base de usuários flexível, garantindo que tarefas, coisas e máquinas possam ser movimentadas, realocadas e transformadas sem perda de controle.

©2022 Zscaler, Inc. Todos os direitos reservados.

O SSE pode ser um catalisador das mudanças na organização porque protege a empresa de uma maneira inteiramente abrangente. Mas nem todas as soluções são criadas da mesma forma. Os executivos de TI que desejarem adotar o SSE devem avaliar e selecionar a solução certa, que permita à sua organização simplificar a segurança.

Há sete armadilhas a serem evitadas na jornada de transformação digital da empresa em direção ao SSE. Ao evitar esses erros, os executivos de TI poderão selecionar o conjunto certo de serviços, arquitetura e funções para realizar a proposição de valor do SSE. Essa jornada deve passar longe das "velhas formas de se trabalhar", como a dependência de redes ou a concessão de acesso generalizado aos serviços – o que limitaria a capacidade de transformar e atender às necessidades da empresa.

Armadilha nº 1:
Escolher uma solução de SSE sem histórico comprovado de operação de uma plataforma global de nuvem dimensionada para desempenho e disponibilidade

Armadilha nº 2:
Escolher uma solução de SSE que não tenha sido criada com base em uma arquitetura Zero Trust

Armadilha nº 3:
Escolher uma solução de SSE que prometa um sistema avançado de proteção contra ameaças e prevenção contra perda de dados, mas que não seja capaz de inspecionar o tráfego criptografado em larga escala

Armadilha nº 4:
Escolher uma solução de SSE de "tamanho único", não compatível com opções diversificadas, flexíveis e escalável de implementação e gerenciamento

Armadilha nº 5:
Escolher uma solução de SSE que ofereça uma experiência medíocre aos usuários, sem otimizar a conectividade de aplicativos nem diagnosticar degradações de UX

Armadilha nº 6:
Escolher uma solução de SSE cuja integração e orquestração com um ecossistema de fornecedores terceirizados sejam limitadas

Armadilha nº 7:
Escolher uma solução de SSE incapaz de mostrar valor facilmente em piloto de ambiente de produção

Quem deve ler isso?

A passagem para o SSE não é só uma questão de transformação da segurança, e requer muito mais do que apenas **arquitetos de segurança**. As melhores práticas descritas neste e-book são destinadas a **arquitetos de segurança**, **arquitetos de rede**, **arquitetos corporativos**, **arquitetos de nuvem** e **arquitetos de aplicativo**.

Nº 1 Armadilha

Escolher uma solução de SSE sem histórico comprovado de operação de uma plataforma global de nuvem dimensionada para desempenho e disponibilidade

Em vez disso, considere as soluções de SSE que:

- Ofereçam um conjunto diversificado e globalizado de limites de aplicação de políticas de serviço público cujo desempenho, disponibilidade, taxa de transferência e função sejam baseados em um SLA. Essas soluções devem aplicar políticas locais a todas as instalações do cliente.
- Tenham sido criadas para a nuvem com o que há de melhor em termos de resiliência, infraestrutura, diversidade geográfica, recursos funcionais e experiência do usuário. Disponibilizem serviços de SSE on-line em centros de dados de operadores neutros, e não como um serviço executado em uma nuvem gerenciada no destino ou em data centers terceirizados.
- Tenham um histórico comprovado e transparente de escalonamento, crescimento e disponibilidade validados por recomendações de clientes, relatórios históricos, certificações de terceiros e repositórios de dados externos de código aberto (https://www.peeringdb.com/org/12297).

Como os fornecedores certos de SSE fazem esse trabalho:

Criar e administrar uma plataforma de SSE com múltiplos usuários e que executa bilhões de transações significa muito mais do que o nível de computação, e não é nada simples. **A solução de SSE deve ser responsável pela proteção, conectividade e capacidade de sua empresa**, e portanto deve entregar o conjunto de serviços de SSE de maneira uniforme e em tempo hábil para todas as áreas da organização.

A solução de SSE correta deve proteger sua empresa por meio de um serviço distribuído globalmente. Arquitetonicamente, a forma mais eficaz é a utilização de um serviço baseado em proxy. Não ancorado ao estado da rede, o serviço de proxy se concentra em executar o SSE no acesso aos aplicativos, permitindo maior abrangência sem a necessidade de plataformas adicionais para tarefas como inspeção em larga escala **(Veja a Armadilha nº. 3)**.

Observe que uma verdadeira arquitetura de proxy exige um esforço significativo de P&D e muitos anos de refinamento para atender aos requisitos de escala das empresas modernas. a solução de SSE certa deve ter diversos exemplos de implementações de grandes porte, para as quais a arquitetura de proxy demonstrou ser dimensionada.

Esse serviço deve ser fornecido por meio de um conjunto uniforme de políticas de borda através das quais toda e qualquer função de transmissão de dados de sua empresa esteja protegida; e não deve consistir apenas no número de nós, mas sim no número de instalações – garantidas por SLA – que disponibilizam os serviços necessários ao cliente. O provedor de SSE não deve disponibilizar PoPs públicos se não for possível garantir o SLA naquela região devido a problemas no tráfego ponto a ponto ou a outros motivos.

A adoção do SSE significa que você vai consolidar, fortalecer e compartilhar as responsabilidades pela segurança, conectividade e controle de sua empresa com um fornecedor de segurança confiável. Esse modelo compartilhado simplifica os meios pelos quais você pode fornecer proteção e conectividade a seus usuários, tarefas, serviços e filiais, entre outros. O provedor de SSE deve fornecer um conjunto de SLAs definidos, testados e aprovados para garantir o funcionamento de sua empresa com total proteção.

©2022 Zscaler, Inc. Todos os direitos reservados.

Quando o serviço corporativo de sua empresa é conectado, ele precisa de um caminho eficaz para consumir a função de destino. Isso só pode ser alcançado por meio de uma solução de SSE com tráfego ponto a ponto altamente eficaz em centros de dados de operadores neutros. Portanto, os controles devem ser aplicados on-line entre a origem e o destino, independentemente da localização da origem e/ou do destino.

As soluções que hospedam o serviço de segurança em nuvens de computação centrais, geralmente dentro de estruturas de hiperescala e que têm gateways de entrada, como mostrado na Figura 3 (os assim chamados serviços on-ramp), dependem de bordas de entrada distribuídas, mas processam o controle de políticas e de aplicativos centralmente, introduzindo assim uma latência indesejada e resultando em uma experiência do usuário medíocre.

Os fornecedores de SSE devem demonstrar a capacidade de oferecer uma plataforma de nuvem completa, de grande porte e escaláveis. Além dos SLAs, a plataforma de SSE também deve fornecer evidências de escalabilidade, estabilidade, disponibilidade, implementação em diversas áreas geográficas etc. Para validar essa análise, consulte dados históricos disponibilizados publicamente e fale com clientes existentes para entender suas experiências.

Aplicação uniforme das políticas de borda

O conjunto de bordas de serviço do fornecedor de SSE deve permitir a aplicação de políticas. Estas não podem ser bordas de conectividade com uma rede maior baseada em nuvem com a mera função de rotear ou desviar seu tráfego para uma infraestrutura central de aplicação de políticas. Esses esquemas impedem a prestação de serviços altamente eficazes e de baixa latência.

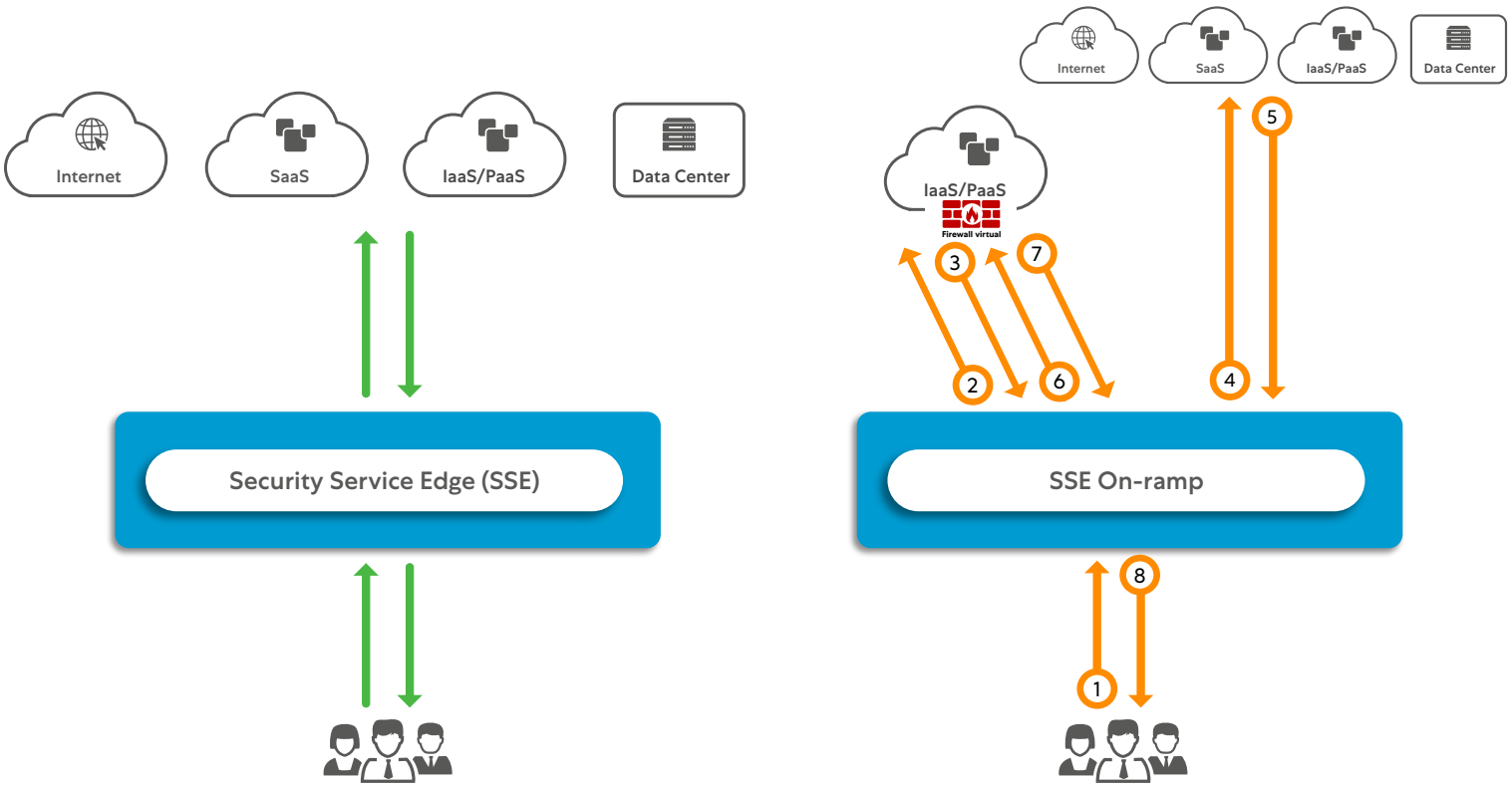


Figura 3: Os serviços de SSE em linha (à esquerda) aplicam controles de segurança ao tráfego em linha. Os controles de segurança on-ramp (à direita) fornecem gateways de entrada na borda só para encaminhar esse tráfego para um controle hospedado em uma nuvem de computação central – aumentando assim a latência, a ineficiência e proporcionando uma experiência de usuário medíocre.

©2022 Zscaler, Inc. Todos os direitos reservados.

O fornecedor precisa resolver as seguintes questões de projeto, garantindo que as bordas sejam:

- Hospedadas em instalações vitais com tráfego ponto a ponto dentro do data center de operadores neutros, garantindo assim uma latência mínima entre a origem e o destino. Ao avaliar um fornecedor de SSE, analise as estatísticas de consultas públicas, como PeeringDB e implementações de parceiros **(Veja a Armadilha nº. 6 para obter mais detalhes sobre a integração de parceiros)**.
- Baseadas em um SLA válido. Isso garante a estabilidade das funções de negócio e indica que o fornecedor de SSE está trabalhando em todas as regiões para assegurar os SLAs.
- Implementadas de forma particular para cada cliente em instalações cujas condições locais exijam implementações mais individualizadas, como as feitas no local ou dentro de um nó de computação de borda **(a Armadilha nº. 4 contém mais detalhes)**.
- Capazes de demonstrar um histórico de aumento progressivo das taxas de transferência.
- Capazes de oferecer tolerância a falhas implementada no modo ativo-ativo para garantir disponibilidade e redundância. (O fornecedor monitora e mantém suas bordas de serviço público para garantir uma disponibilidade contínua.)
- Capazes de promover a privacidade dos dados para garantir que o tráfego do cliente não seja repassado para nenhum outro componente dentro da infraestrutura, e que nenhum dado seja armazenado em disco.
- Capazes de disponibilizar controles uniformes para recursos corporativos em todas as bordas, sem rotear ou "desviar" o tráfego de bordas remotas para instalações centrais.
- Capazes de assegurar proteção em escala global para proteger todos os serviços corporativos assim que uma ameaça seja detectada

⚠ Com o que devo tomar cuidado?

- Bordas públicas que não permitem a aplicação de políticas. Em vez disso, o tráfego deveria ser encaminhado para data centers onde maiores recursos de aplicação de políticas estão disponíveis.
- Citações de centenas de bordas públicas sem compartilhar a função e a capacidade de cada uma
- Bordas sem SLAs sobre disponibilidade, taxa de transferência e resiliência.
- Serviços de borda sem multilocação, que forçam o tráfego via encaminhamento/roteamento para outros locais.
- Serviços de SSE sem evidências comprovadas de implementação em clientes de grande porte.
- Serviços sem informações publicamente disponíveis sobre sua estabilidade e disponibilidade

Resultados:

Uma solução de SSE que seja dimensionada para sua empresa hoje e, sobretudo, que permita atingir seus objetivos futuros é um investimento essencial. A escalabilidade não é simplesmente um mecanismo de expansão, mas sim – o que é mais importante – uma forma de atender às necessidades de sua empresa sem sacrificar a função, a estabilidade e a proteção de seus negócios. Assim, procure uma solução que:

- Forneça evidências transparentes de uma implementação global e diversificada.
- Tenha SLAs documentados e validados sobre a perda ou degradação dos serviços de SSE.
- Tenha sido implementada em um grande número de clientes de tamanho e complexidade semelhantes aos da sua empresa.
- Tenha disponibilizado informações públicas e passíveis de análise para cada PoP utilizando ferramentas públicas (como o PeeringDB, por exemplo).
- Permita a execução de todas as funções críticas em todas as instalações sem estrangular o tráfego.
- Forneça proteção alinhada entre a origem e o destino.
- Seja projetada para a resiliência operacional, funcional e da infraestrutura.
- Possa ser utilizada de várias formas em diversas instalações.

Nº 2
Armadilha

Escolher uma solução de SSE que não tenha sido criada com base em uma arquitetura Zero Trust

Em vez disso, considere as soluções de SSE que:

- Só concedam acesso a identidades validadas contextualmente, independentemente da localização/rede. Este caminho do menor privilégio é para todos os serviços, não apenas para usuários. As empresas que, por meio dos controles corretos de SSE, conectam origens autorizadas somente a destinos válidos e nada mais conseguem eliminar a movimentação lateral que muitas vezes é explorada pelos autores de ameaças.
- Concentram-se exclusivamente na conexão de acesso dinâmico por sessão. a confiança zero não é fornecida com firewalls, SD-WAN e outros serviços de rede. Ela deve ser uma sobreposição independente da rede.
- Nunca exponham ativos corporativos a uma origem não autorizada; isso reduz a superfície de ataque e garante que os controles corretos sejam aplicados a todos os serviços.

Como os fornecedores certos de SSE fazem esse trabalho:

Confiança zero para todas as comunicações corporativas significa que nenhum acesso é concedido de qualquer ponto de origem (incluindo usuários, terceirizados, redes e assim por diante) para qualquer ponto de destino sem a expressa permissão e aprovação para tanto.

Tradicionalmente, oferecer confiança zero em ambientes corporativos é desafiador devido ao contexto de rede compartilhada de conectar a origem ao destino, utilizando um caminho de rede físico ou lógico para interconectar essas duas entidades. A Figura 4 descreve essas questões de compartilhamento físico. Você não pode criar ou acrescentar confiança zero com SD-Wans ou firewalls.

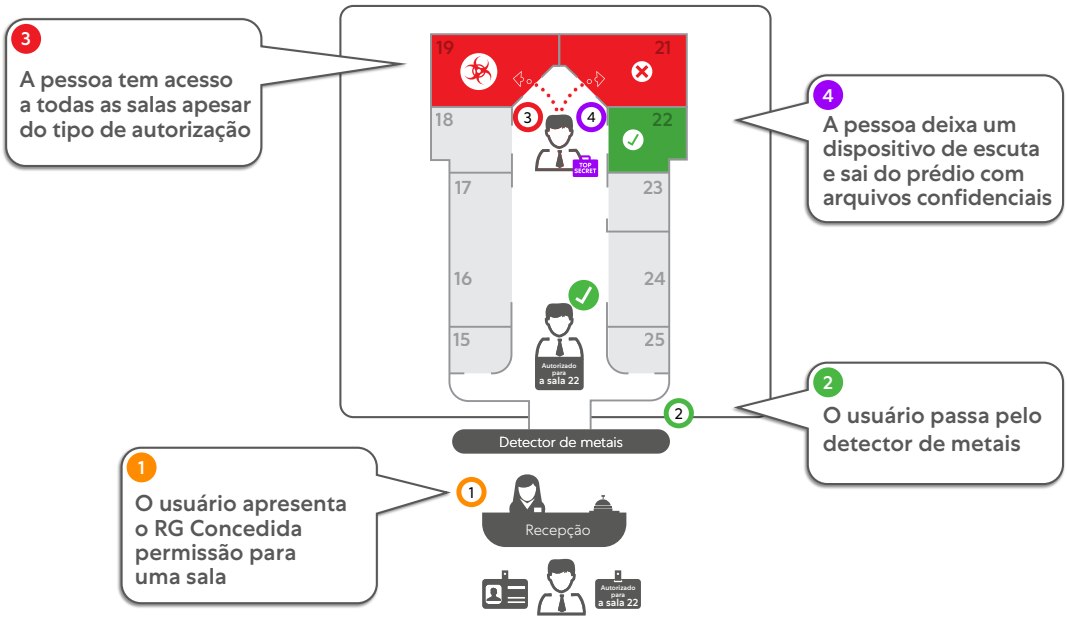


Figura 4: Como não habilitar o acesso – o velho mundo da analogia da segurança de rede. Conectar usuários à sua rede corporativa é como permitir que visitantes percorram suas sedes-centrais sem serem acompanhados, facilitando assim o roubo de dados confidenciais.

©2022 Zscaler, Inc. Todos os direitos reservados.

O SSE pode ajudar a aplicar restrições de acesso dos usuários às suas tarefas na empresa inteira. Ao estender esses controles para além dos funcionários, você protege sua empresa contra diversos riscos, como uma superfície exposta a ataques ou a movimentação lateral de ameaças dentro do ambiente.

Entre tantas outras coisas, a arquitetura Zero Trust aplica controles granulares, garantindo que cada solicitante se comunique com o destino correto em cada sessão, conforme mostrado na Figura 5. Essas regras exigem conhecimento das entidades de origem e destino, e são o motivo pelo qual a maioria das empresas começa sua jornada de confiança zero (e SSE) pela sua base de usuários. Normalmente, uma identidade é atribuída a cada usuário para diferenciá-lo dos vários serviços. No entanto, como as redes são planas, expostas e abertas, o risco de um usuário ter acesso a mais informações apenas porque compartilha uma rede é uma grande preocupação para a estabilidade das empresas.

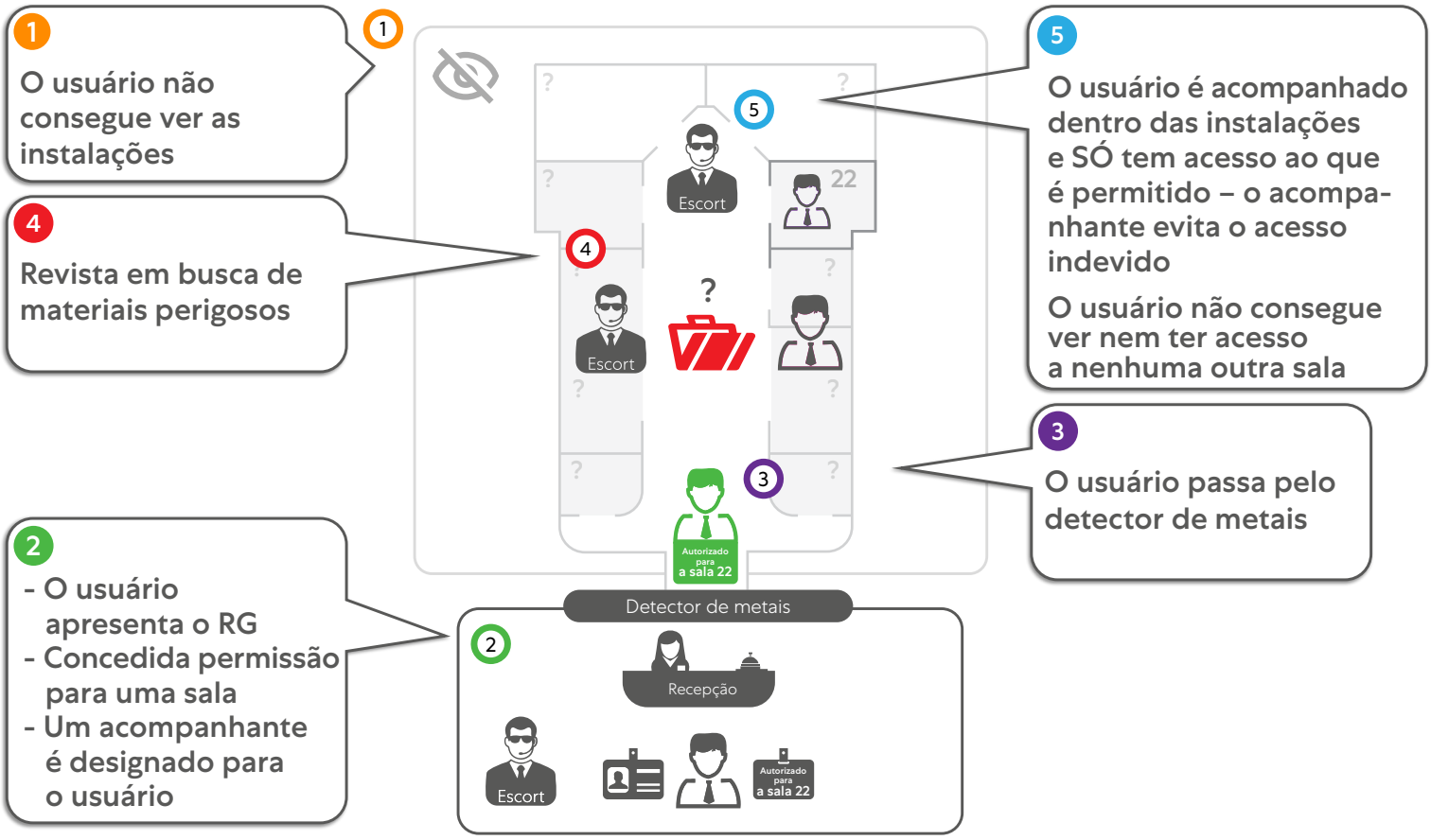


Figura 5: a maneira correta de fornecer acesso é por meio do controle ponta a ponta. o acesso de confiança zero é como acompanhar um visitante de olhos vendados para participar de uma reunião em seu escritório, e em seguida acompanhá-lo até a saída. O visitante nunca é deixado sozinho e não pode ficar bisbilhotando.

Considere todos os casos de uso da empresa, como a proteção aos usuários e ativos de negócio importantes, e aplique os controles de SSE ao tráfego como um todo. Estabeleça conexões depois de analisar dinâmica e contextualmente o risco dos quatro valores de conexão a seguir (Figura 6):

Iniciador da conexão

Qual é a identidade e a confiabilidade do usuário/dispositivo/rede? Como essa identidade diferencia o acesso concedido a esse ponto de origem e sob quais condições?

Exemplo: a Sara do RH precisa acessar o sistema de RH hospedado na nuvem, e também o sistema de contabilidade hospedado internamente. O acesso é concedido por meio da plataforma SSE desde que a identidade de Sara e a confiabilidade do dispositivo tenham direitos de acesso definidos.

Controle das políticas

Onde, como e quais controles são aplicados? Os critérios de controle incluem a eficácia do caminho, o risco e a confiabilidade do iniciador, a função do destino solicitado e as políticas da empresa.

Exemplo: Pierre tem uma identidade válida para acessar o Salesforce, mas sua empresa só quer conceder a ele direitos de visualização, sem fazer downloads nem manipular nenhum dado. Portanto, a solução de SSE só permite que Pierre visualize o conteúdo do aplicativo – e nada mais.

Destino da conexão

A quais serviços o solicitante tem acesso? É um SaaS público ou uma carga de trabalho interna? Quais controles devem ser aplicados? O acesso pode mudar conforme o contexto das políticas de identidade e controle.

Exemplo: Um iniciador válido pode ter autorização para acessar um serviço específico de PaaS na nuvem, e se for um serviço de nuvem, o SSE vai inspecionar a tarefa para garantir que ela não esteja vazando segredos corporativos. Esse mesmo iniciador pode então se conectar a um serviço interno com o mesmo nível de confiabilidade simplesmente estabelecendo um iniciador para a conexão ao serviço, sem nenhum controle adicional.

Estabelecimento da conexão

Finalmente, considerando os dados anteriores, as análises condicionais das tarefas, as capacidades de rede ou de borda, a política definida pela empresa etc., é possível conceder o acesso. A solução de SSE deve identificar variações, como por exemplo um local alterado, e orientar o acesso pelo melhor caminho aplicável.

Exemplo: Depois que a origem, o controle e os destinos são validados, a conexão é autorizada para aquela sessão – e nada mais. o fluxo de ponta a ponta da aplicação por sessão é descrito na Figura 6.

©2022 Zscaler, Inc. Todos os direitos reservados.

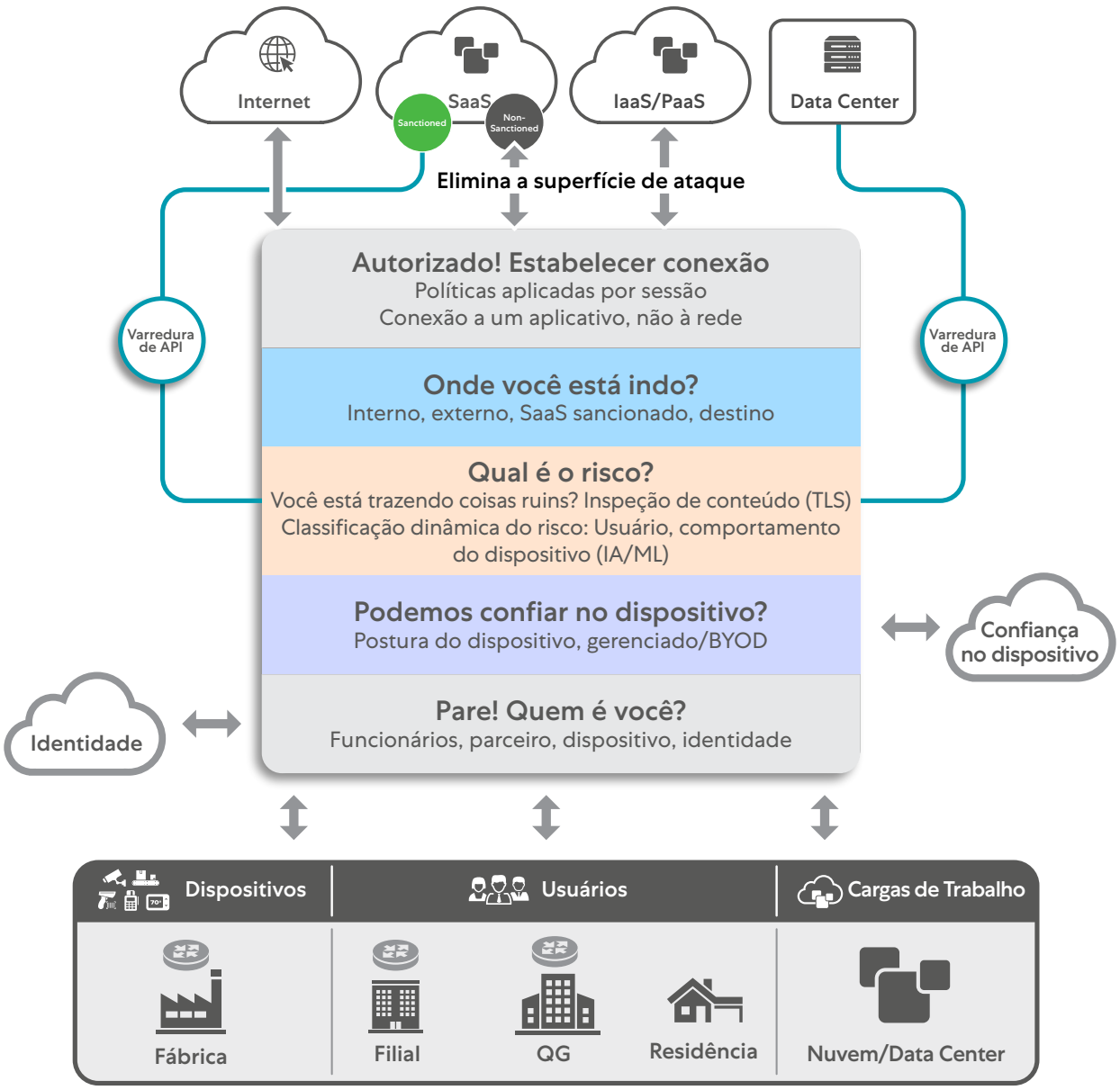


Figura 6: Etapas de uma arquitetura de confiança zero, mostrando o controle e a aplicação de políticas em cada etapa

A definição dos controles de conexão na solução de SSE **garante que somente a origem correta pode consumir o destino correto** através da solução de SSE correta. Esse uso do SSE conforme o menor privilégio oferece vários benefícios para a empresa, entre eles:

- A aplicação dos controles de SSE corretos à origem correta
- Os serviços protegidos pelo SSE não são expostos a origens não autorizadas, reduzindo assim os riscos de segurança cibernética
- Redução de resíduos, por exemplo, não permitir que um servidor Linux se conecte a um sistema de atualização do Windows.
- Visibilidade granular e aprendizado de fluxos – uma solicitação por acesso, não de IP de rede para IP de rede
- Acessos consolidados com base na identidade e não na rede, o que permite racionalizar o funcionamento das redes (e da infraestrutura)

©2022 Zscaler, Inc. Todos os direitos reservados.

Progressão do SSE em fases com confiança zero:

Ao selecionar uma solução de SSE que permita o controle em todos os casos de uso a seguir – e um controle baseado exclusivamente no usuário – é possível estender a proteção a todas as funções da empresa (Veja a Figura 7):

De usuário para cargas de trabalho

Permitir o acesso do usuário às cargas de trabalho significa que você pode remover o contexto de rede dos acessos do usuário, e, ao mesmo tempo, visualizar as cargas de trabalho que estão sendo acessadas pelos usuários. Essa ação resulta em um duplo benefício, cujo valor normalmente é recebido com maior rapidez.

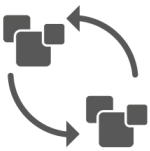
Considere o controle granular sobre os usuários no inteiro ambiente de aplicativos. Por exemplo, serviços via internet como o YouTube podem ser limitados ao depto. de relações públicas da organização.

Permitir um maior desenvolvimento do inventário de serviços corporativos e também regras mais granulares, como o acesso a plataformas de TO e P&D isoladas, sem nunca expor o ecossistema inteiro à base de usuários.

Acesso de terceirizados

A implementação do acesso de confiança zero para parceiros terceirizados elimina os riscos de conectividade de rede e exposição da superfície a ataques, riscos esses ainda presentes nos sistemas legados de acesso de terceiros. o controle de confiança zero pelo menor privilégio permite controlar e limitar o acesso de parceiros a partir de dispositivos não confiáveis ou pessoais apenas àqueles aplicativos especificamente designados – e nada mais – permitindo assim maior visibilidade daquilo que está sendo acessado.

Os controles da solução de SSE sobre terceiros devem oferecer vários mecanismos de controle de acesso. Estas opções vão desde o acesso autorizado do cliente a partir de diversos provedores de identidade até aplicativos específicos, além do acesso isolado exclusivamente via navegador, ou o isolamento completo do acesso a uma imagem renderizada exibida a terceiros (streaming de pixels para o dispositivo do usuário, como BYOD).



De carga de trabalho para carga de trabalho

Os controles entre cargas de trabalho são solicitações de acesso a aplicativos e serviços. Geralmente, máquinas Windows solicitam atualizações do Windows, não do Linux. Assim, é fundamental que a empresa categorize quais sistemas devem ter acesso a quê.

Assim como acontece com os usuários, os controles de cargas de trabalho devem fornecer uma identidade válida para consumir um serviço. Se a cargas de trabalho consome recursos públicos, como serviços de IoT/TO baseados em PaaS, a borda de segurança deve validar e entender seu contexto – e bloquear qualquer tentativa de uso indevido.

Por outro lado, se a cargas de trabalho acessar um serviço local privado, isso só pode ser feito através de controles de SSE em linha, após a aprovação da identidade, conforme uma validação de confiança zero.

De local para local

À medida que o acesso e o controle evoluem na empresa como um todo, deve-se considerar a extensão da confiança zero para a conectividade entre instalações. é preciso isolar e limitar o conjunto dos serviços a uma rede, instalação, VPC etc. a conexão entre o local e a instalação conhecida não deve ser feita através de uma rede compartilhada. A confiança zero permite que um local válido se conecte a um conjunto válido de cargas de trabalho existentes dentro de outro local. A confiança zero não utiliza o acesso pela camada de enlace da rede; ela exige uma conectividade de aplicativo para aplicativo e de maneira uniforme em qualquer instalação, VPC, VLAN etc.

©2022 Zscaler, Inc. Todos os direitos reservados.

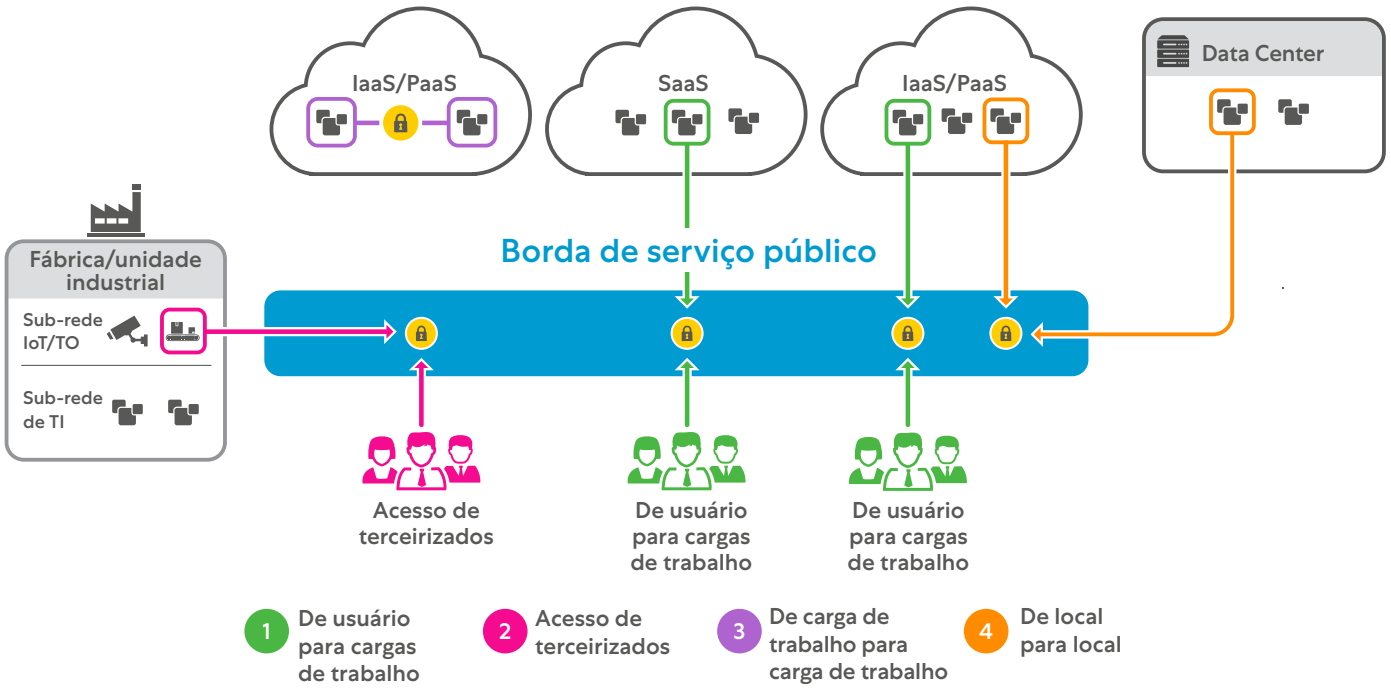


Figura 7: Uma sugestão de abordagem da segmentação empresarial. Possibilidade de uma abordagem em etapas do controle, da aprendizagem, e da segmentação e isolamento adicionais como parte de uma implementação de confiança zero

Um exemplo recente ocorreu quando pesquisadores de segurança descobriram a vulnerabilidade de dia zero do Log4j, pela qual todos os clientes que executavam o utilitário de registro vulnerável baseado em Java do Apache corriam o risco de uma completa execução remota do código. No entanto, os aplicativos internos de quem tivesse uma arquitetura de confiança zero estariam completamente invisíveis para a Internet, e isso significa que os invasores não conseguiriam encontrá-los e explorá-los; além disso, até mesmo versões suscetíveis do Apache Log4j estariam protegidas contra essa vulnerabilidade – e outras futuras. Isso seria impossível com serviços legados e expostos, como VPNs e firewalls. **A confiança zero garante que os aplicativos só possam ser acessados por usuários autorizados; ela evita a movimentação lateral com microssegmentação, tanto de usuário para aplicativo quanto de aplicativo para aplicativo, e é capaz de inspecionar o tráfego de entrada e de saída**.

Isso também aconteceu com o ataque Colonial Pipeline, no qual credenciais de VPN roubadas (que não tinham MFA habilitado) deram aos hackers acesso para se mover lateralmente pela rede e acessar dados confidenciais. Uma arquitetura de confiança zero que conecta usuários autorizados só a aplicativos, e não a redes, impede a movimentação lateral porque segmenta as comunicações de usuário para aplicativo e aplicativo para aplicativo

Com o que devo tomar cuidado?

- Evite serviços de SSE que não seguem os princípios da arquitetura Zero Trust, como a Publicação Especial 800-207 do NIST.
- Certifique-se de que o serviço de SSE ofereça controles de confiança zero a todos os recursos corporativos, e não apenas aos usuários.
- A confiança zero não é uma função de firewall ou SD-WAN. Ela é independente da rede e capaz de operar em qualquer rede. O SSE de um provedor que seja dependente da rede pode expô-lo a uma deficiência da arquitetura de confiança zero.
- Certifique-se de que os controles de confiança zero comecem com o acesso zero; nenhum ativo corporativo deve ser acessado antes da validação.
- Aborde todos os aspectos de sua empresa. Não limite seus controles de confiança zero a apenas uma parte da empresa.

Resultados:

A proteção da empresa e de seus usuários deve ser abordada para que o acesso seja concedido conforme a necessidade e segundo o princípio do menor privilégio. **A confiança zero deve ser o controle básico ao escolher uma solução de SSE**, de forma que:

- O fornecedor de SSE proteja todos os serviços corporativos e valide a identidade das entidades antes de conceder o acesso; todo o resto deve ser bloqueado.
- Soluções que forçam a conectividade de rede devem ser evitadas e o acesso deve ser independente da rede, onde quer que seja.
- O serviço de SSE deve disponibilizar uma superfície de ataque zero para seus serviços corporativos privados.

Nº 3
Armadilha

Escolher uma solução de SSE que prometa um sistema avançado de proteção contra ameaças e prevenção contra perda de dados, mas que não seja capaz de inspecionar o tráfego criptografado em larga escala

Em vez disso, considere as soluções de SSE que:

- Permitam a inspeção SSL/TLS do tráfego em escala de produção com o mínimo de impacto sobre o desempenho. Isto requer uma arquitetura de proxy escalável.
- Capturem e analisem as informações aprofundadas obtidas com a inspeção para aplicar proteção avançada contra ameaças ao tráfego criptografado e aplicar políticas avançadas de classificação de dados para fins de prevenção de perda de dados.
- Inspecionem todo o tráfego, inclusive o criptografado, de usuários, dispositivos, cargas de trabalho etc.

Como os fornecedores certos de SSE fazem esse trabalho:

Nenhum fornecedor de SSE pode dizer que tem a melhor proteção avançada contra ameaças e prevenção contra perda de dados sem ter a capacidade de inspecionar todo o tráfego em escala de produção, incluindo o tráfego criptografado.

Desconfie das afirmações de fornecedores de SSE sobre esse ponto, porque isso depende muito da arquitetura da solução. Os fornecedores de SSE que criaram seu proxy de nuvem de forma nativa para a nuvem desde o início levam uma distinta vantagem nessa área.

Como a grande maioria (cerca de 85%) do tráfego de Internet é criptografado, os fornecedores de SSE devem inspecionar esse tráfego em escala e em profundidade para garantir uma proteção adequada contra ameaças e prevenção de perda de dados, algo cada vez mais necessário diante do crescimento exponencial dos riscos de segurança representados pelos canais criptografados. Por que a descriptografia SSL/TLS em escala é tão importante (Veja a Figura 8)?

- A criptografia SSL/TLS pode ocultar conteúdo prejudicial, como vírus, spyware e outros códigos maliciosos.
- Os invasores criam seus sites com criptografia TLS e SSL ou injetam conteúdo malicioso em sites conhecidos e confiáveis habilitados para SSL e TLS.
- O SSL/TLS pode ocultar vazamentos de dados, como a transmissão de documentos financeiros confidenciais de uma organização.
- O SSL/TLS pode ocultar a navegação em sites pertencentes a categorias de responsabilidade legal.
- A capacidade de controlar e inspecionar o tráfego de e para serviços on-line usando HTTPS se tornou uma parte importante da postura de segurança das organizações.

©2022 Zscaler, Inc. Todos os direitos reservados.

Figura 8: a arquitetura de passagem empregada por alguns fornecedores não permite a inspeção do tráfego criptografado em larga escala; isso equivale a um posto de controle de segurança básico que permite que um carro passe sem verificar se há cargas indevidas em seu porta-malas

Devido a esses riscos, a arquitetura do fornecedor de SSE deve ser dimensionada para atuar como um proxy de SSL/TLS intermediário, que faz uma análise completa do conteúdo de entrada e saída e bloqueia imediatamente qualquer ameaça detectada em qualquer lugar na nuvem.

Os atores de ameaças continuam a desenvolver suas ferramentas, técnicas e procedimentos para vitimar as organizações, incluindo o abuso de provedores de serviços de armazenamento legítimos, como Dropbox, Box, OneDrive e GDrive para hospedar conteúdo malicioso. Essas conexões usam certificados SSL/TLS de caracteres universais desses fornecedores renomados para enviar conteúdo malicioso, que se não for inspecionado resultará em um ataque bem-sucedido. Esses conteúdos maliciosos (executáveis, documentos etc.) também são de natureza polimórfica, pois o objetivo é evitar as detecções básicas de impressão digital. A arquitetura dos fornecedores de SSE deve permitir a extração completa do conteúdo dessas conexões SSL/TLS criptografadas e deve ser capaz de descompactar e abrir esses arquivos para realizar uma detecção precisa (Veja a Figura 9).

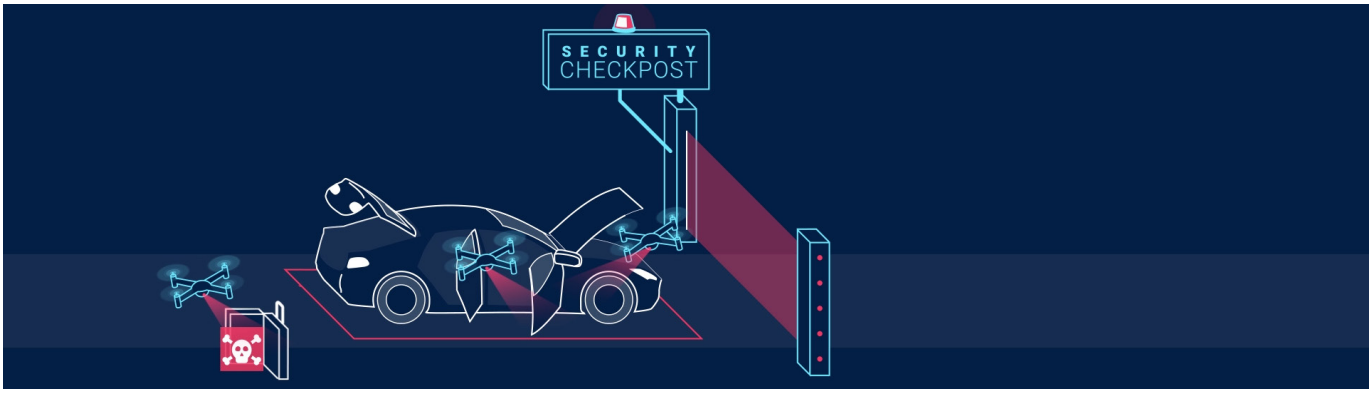


Figura 9: o fornecedor de SSE certo permite uma completa inspeção SSL/TLS do tráfego inteiro usando uma arquitetura de proxy, semelhante a um carro que é parado e totalmente inspecionado antes de ser autorizado a passar pelo ponto de verificação de segurança

Essa proteção contra ameaças deve utilizar diversos fluxos de ameaças provenientes de fontes comerciais, particulares e de código aberto, além de permitir atualizações de segurança frequentes.

©2022 Zscaler, Inc. Todos os direitos reservados.

Além de bloquear ameaças, a inspeção em larga escala permite a prevenção avançada da perda de dados. **Os fornecedores de SSE devem ser avaliados quanto aos seus recursos de classificação de dados**. Isso deve incluir expressões regulares (regex) como mecanismo básico, mas localizar e classificar rapidamente dados confidenciais em todos os canais de dados na nuvem é um requisito essencial para proteger dados pessoais, de saúde e confidenciais contra perdas. Essa classificação requer uma inspeção SSL/TLS e habilita recursos avançados, como:

- **Correspondência exata dos dados**. O SSE usa modelos de índice para identificar um registro de uma fonte de dados estruturada que corresponda a critérios predefinidos.
- **Impressão digital de documentos**. O SSE usa um repositório de documentos para identificar documentos total ou parcialmente correspondentes ao avaliar o tráfego de saída.
- **OCR (reconhecimento óptico de caracteres)**. O SSE detecta dados confidenciais em arquivos de imagem, imagens incorporadas, capturas de tela e textos manuscritos e fecha todos os canais de exfiltração de dados baseados em nuvem.
- **Aprendizagem automatizada.** Algoritmos especificamente configurados tomam decisões sobre a sensibilidade dos dados.

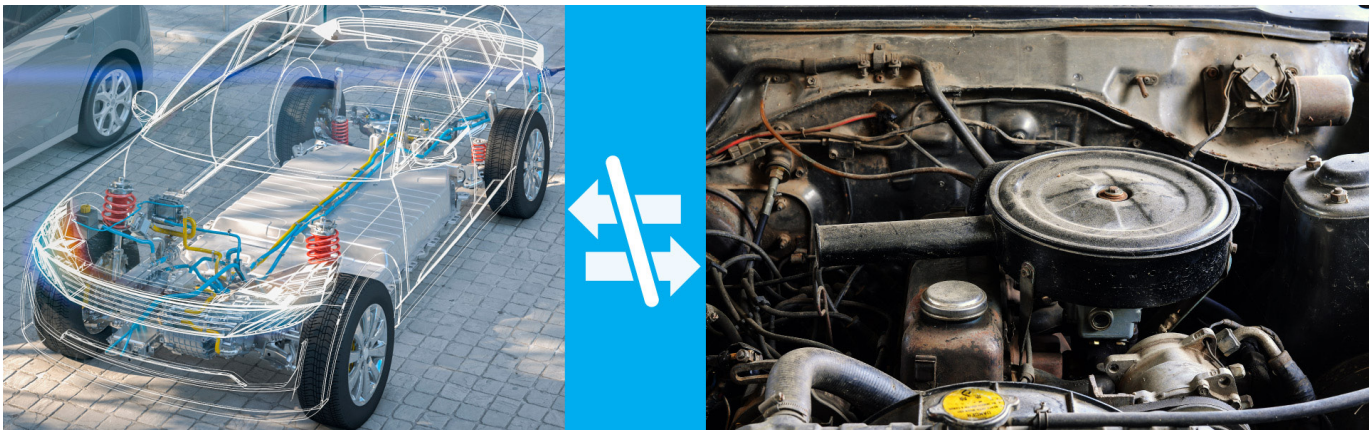


Figura 10: Assim como um motor de combustão interna não pode ser adaptado para funcionar como um veículo elétrico, tome cuidado com fornecedores que adotam recursos como inspeção SSL/TLS para arquiteturas legadas

O SSE inclui a funcionalidade do corretor de segurança de acesso à nuvem (CASB) para monitorar e aplicar políticas entre usuários de serviços de nuvem e aplicativos, e a capacidade de inspecionar o tráfego criptografado on-line tem diversas vantagens nesse contexto. A inspeção pode ser "fora da faixa", o que significa escanear as APIs dos provedores de SaaS para proteger os dados em repouso, ou "on-line", o escaneamento de dados em movimento. Preste atenção especial a este último item, pois a inspeção on-line impede que os dados sejam transferidos para aplicativos não autorizados, que eles sejam baixados para dispositivos não autorizados e que conteúdo malicioso seja baixado ou transferido. O fornecedor de SSE também deve permitir o controle de acesso granular com base em um conjunto avançado de definições de aplicativos da nuvem, controles por tipo de arquivo e atributos de risco.

Com a adoção de centenas e até milhares de aplicativos na nuvem, hoje os dados confidenciais das organizações são amplamente distribuídos. Os dois principais canais de exfiltração de dados são aplicativos de e-mail pessoal e de desktop na nuvem. Um bom fornecedor de SSE deve oferecer completa visibilidade contextual e aplicação de políticas quando usuários desonestos enviam dados confidenciais para seu Box ou Dropbox pessoal e outros desktops na nuvem. Eles também devem impedir a exfiltração de dados em serviços de webmail pessoais e não autorizados, como Gmail e Hotmail.

©2022 Zscaler, Inc. Todos os direitos reservados.

Onde a diferenciação entre os fornecedores de SSE se torna aparente é até que ponto sua capacidade de descriptografar e inspecionar o tráfego de SSL/TLS é elasticamente escalonada de acordo com as demandas de tráfego, e o fato de que esse nível de inspeção deve ser disponibilizado sem questões de desempenho – isso só pode ser realizado com uma solução de SSE baseada em proxy e criada desde o início com a escalonabilidade em mente (Veja a Figura 10).

É importante investigar como o fornecedor de SSE consegue realizar isso. Para manter a latência mínima para cada inspeção de pacotes, o fornecedor deve empregar uma arquitetura de passagem única na qual o pacote é colocado na memória uma vez e os serviços de inspeção, cada um com recursos de CPU dedicados, possam realizar suas varreduras simultaneamente. Fornecedores que realizam essas inspeções com aplicativos físicos e virtuais serializados incorrem em uma penalidade de processamento em cada etapa, e correm o risco de uma latência excessiva ser aplicada a cada pacote.

Essas vantagens arquitetônicas devem ser aplicadas a padrões mais recentes, como o TLS 1.3, porque uma verdadeira arquitetura de proxy tem a vantagem de estar alinhada com duas conexões separadas, com o cliente e o servidor. Como isso permite que o objeto inteiro seja remontado e verificado, é possível aplicar proteção avançada contra ameaças, DLP e área de segurança. Certifique-se de que as versões TLS e as atualizações de criptografia sejam tratadas sem problemas pelo fornecedor dentro de sua nuvem – certos fornecedores baseados em hardware podem forçar as atualizações do dispositivo a assumir uma carga adicional para suporte a novas criptografias.

O gerenciamento de certificados também deve ser considerado, dada a complexidade potencial que pode ser introduzida. Os fornecedores de SSE devem dar a possibilidade de usar os certificados deles ou de você trazer os seus próprios, e permitir a alternância entre ambos via API. Os certificados devem ser replicados automaticamente entre as várias bordas de serviço.

Tome cuidado com fornecedores de SSE que podem associar recursos de inspeção SSL/TLS em NGFWs existentes, que sofrem de problemas de escala inerentes. Isso afeta até mesmo os fornecedores que levantam e deslocam NGFWs com recursos de inspeção em instâncias virtuais nos nós de computação do CSP

⚠ Com o que devo tomar cuidado?

Ao avaliar a capacidade de um fornecedor de SSE de inspecionar SSL/TLS, certifique-se de validar se a latência incorrida é aceitável. Infelizmente, arquiteturas não nativas da nuvem podem induzir quedas significativas de desempenho, especialmente ao usar o TLS 1.2 ou versões anteriores. **A privacidade dos dados também pode ser uma preocupação, portanto, entenda as restrições regulatórias e como o fornecedor lida com elas**. Fornecedores de SSE devem permitir a fácil exclusão de certos tipos de dados para permanecer dentro das restrições de privacidade. Fornecedores de SSE nunca devem armazenar dados do usuário na nuvem.

Tome cuidado com fornecedores de SSE que podem associar recursos de inspeção SSL/TLS em NGFWs existentes, que sofrem de problemas de escala inerentes. Isso afeta até mesmo os fornecedores que levantam e deslocam NGFWs com recursos de inspeção em instâncias virtuais nos nós de computação do CSP. Além disso, tome cuidado com fornecedores que combinam recursos CASB fora da faixa com uma inspeção limitada do tráfego on-line. A proteção de dados em repouso e dados em movimento é fundamental.

Avalie como o fornecedor de SSE gerencia certificados e esteja ciente de que a validação de certificados pode ser um problema.

Historicamente, a implementação da inspeção SSL/TLS tem sido desafiadora para as empresas por diversos motivos. **O fornecedor de SSE deve ser o especialista mais confiável e deve dar orientações, facilitar a compreensão e a implementação ao habilitar a inspeção SSL/TLS. A inspeção SSL/TLS** não é negociável no mundo do SSE, pois não deve haver sacrifício da velocidade em favor da segurança.

Resultados:

A inspeção SSL/TLS em larga escala com latência mínima aumenta significativamente a capacidade de bloquear ameaças, utilizando a capacidade da nuvem para identificar e proteger dados confidenciais. Somente os fornecedores de SSE com a arquitetura certa, nativa da nuvem, vão poder oferecer:

- Inspeção SSL/TLS de todo o tráfego em escala de produção com impacto mínimo sobre o desempenho para garantir a mais profunda proteção de dados contra ameaças.
- Uma única arquitetura de varredura de memória para obter vantagens exclusivas de escalabilidade na descriptografia em larga escala.
- A experiência necessária para orientar os clientes ao longo das etapas e desafios da inspeção SSL/TLS.

Nº 4
Armadilha

Escolher uma solução de SSE de “tamanho único”, não compatível com opções diversificadas, flexíveis e escaláveis de implementação e gerenciamento

Em vez disso, considere as soluções de SSE que:

- Ofereçam modelos de implementação flexíveis para proteger usuários e aplicativos onde quer que o aplicativo esteja hospedado, incluindo data centers, nuvem pública, nuvem privada, nó de computação na borda e nas instalações do cliente.
- Ofereçam proteção aos usuários que acessam aplicativos em dispositivos ou objetos, gerenciados e não gerenciados, de usuários finais.
- Estendam essas mesmas proteções de dados e proteções contra ameaças cibernéticas para proteger todas as outras comunicações de tarefa para tarefa, seja na mesma nuvem ou em diversas nuvens diferentes.

Como os fornecedores certos de SSE fazem esse trabalho:

Ao avaliar soluções de SSE, é preciso considerar a preparação de seu ambiente para determinar a melhor forma de aplicar as proteções do SSE. Para apoiar a diversidade de cenários de implementação, os fornecedores de SSE devem permitir tanto bordas de serviço público quanto as de serviço privado.

Como os fornecedores certos de SSE fazem esse trabalho:

Ao avaliar soluções de SSE, é preciso considerar a preparação de seu ambiente para determinar a melhor forma de aplicar as proteções do SSE. Para apoiar a diversidade de cenários de implementação, os fornecedores de SSE devem permitir tanto bordas de serviço público quanto as de serviço privado.

A maioria dos usuários se conecta ao SSE por meio da borda de serviço público do provedor. Essas bordas são gateways de internet seguros, completos, e provedores de aplicativos privados que fornecem segurança integrada. Elas inspecionam todo o tráfego em ambos os sentidos à procura de malware aplicando políticas de segurança, de conformidade e firewall, e precisam processar centenas de milhares de usuários ao mesmo tempo com milhões de sessões simultâneas. Por isso, seus usuários podem obter acesso a partir de qualquer dispositivo, independentemente de onde eles estiverem:

- A internet com as bordas de serviço público protegendo o tráfego e aplicando suas políticas corporativas.
- Aplicativos internos com acesso forçado e políticas de reautenticação baseadas nas melhores práticas corporativas de sua empresa.

Figura 11: o fornecedor de SSE deve oferecer opções de borda de serviço públicas e privadas, que também devem funcionar em harmonia entre si por meio de um gerenciamento centralizado

©2022 Zscaler, Inc. Todos os direitos reservados.

É importante garantir que essas bordas de serviço público tenham recursos significativos de tolerância a falhas e sejam implementadas no modo ativo-ativo para assegurar disponibilidade e redundância. o fornecedor deve monitorar e manter suas bordas de serviço público para garantir uma disponibilidade contínua. Para garantir a privacidade dos dados, o tráfego do cliente não deve ser repassado para nenhum outro componente dentro da infraestrutura, e nenhum dado deve ser armazenado em disco.

No entanto, pode haver situações nas quais a borda de serviço público não consiga atender os requisitos e, nesses casos, o fornecedor de SSE deve oferecer opções de bordas de serviço privado (Veja a Figura 11). Essa opção estende a arquitetura e os recursos das bordas de serviço público às instalações ou locais privados da empresa, aproveitando a mesma política controlada centralmente das bordas de serviço público.

Para garantir o acesso seguro à internet, as bordas de serviço privado podem ser instaladas no data center da empresa e serem dedicadas ao seu tráfego, mas devem ser gerenciadas e mantidas pelo fornecedor de SSE, com quase nenhuma intervenção da empresa. Esse modelo de implementação normalmente beneficia organizações que têm determinados requisitos geopolíticos, ou que usam aplicativos que requerem o endereço IP da empresa como o endereço IP de origem.

Para o acesso a aplicativos internos, a borda de serviço privado permite um gerenciamento semelhante ao das conexões entre usuário e aplicativo e aplica as mesmas políticas que a borda de serviço público, sendo o serviço hospedado no local ou na nuvem pública, mas sempre gerenciado pelo fornecedor de SSE. Esse modelo de implementação permite a confiança zero dentro das instalações da empresa porque reduz a latência do aplicativo quando aplicativo e usuário estão no mesmo local (e ir para a borda de serviço público aumentaria ainda mais a latência). Essa opção também oferece uma camada de sobrevivência se a conexão com a internet for perdida. O fornecedor de SSE deve distribuir imagens para implementação em ambientes de centrais de dados corporativos e de nuvem privada local.

Para garantir proteção de confiança zero a aplicativos internos, os fornecedores de SSE devem oferecer uma maneira de criar uma interface segura e autenticada entre os servidores de aplicativo e as bordas de serviço público e privado, protegendo assim os aplicativos internos. **Esse mecanismo deve estar disponível em vários formatos**: uma imagem de máquina virtual (VM) padrão ou uma implementação conteinerizada em centrais de dados corporativos, ambientes de nuvem privada local, como VMware, ou ambientes de nuvem pública, como Amazon Web Services (AWS), EC2, e pacotes que podem ser instalados em distribuições Linux suportadas.

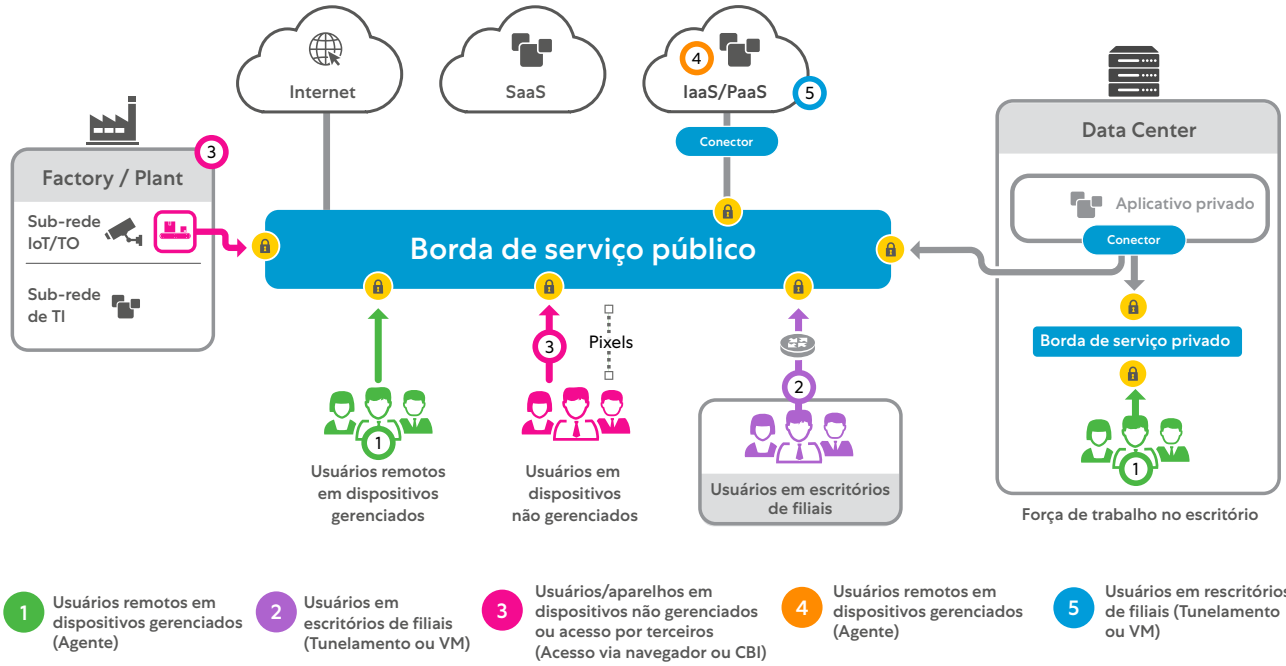


Figura 12: o fornecedor de SSE deve oferecer suporte a diversos modos de implementação e gerenciamento, abrangendo usuários remotos, usuários em filiais, usuários na sede da empresa, tarefas que se comunicam com outras tarefas etc., por meio de agentes e VMs.

©2022 Zscaler, Inc. Todos os direitos reservados.

Depois que for decidido de onde as políticas de SSE serão administradas e aplicadas, deve-se determinar como usuários e cargas de trabalho vão receber essa proteção. é importante considerar vários cenários (Veja a Figura 12):

Para usuários remotos em dispositivos gerenciados, o fornecedor de SSE deve oferecer um só agente unificado que encaminhe o tráfego para a borda de serviço, garantindo assim o acesso seguro à internet. O agente também deve permitir o acesso granular e baseado em políticas aos recursos internos. Tudo isso deve ser automatizado usando a inteligência incorporada ao agente. O tráfego móvel de seus usuários em redes Wi-Fi ou celulares também deve ser protegido. O agente encaminha o tráfego do usuário para o serviço de SSE, que aplica as políticas de segurança e acesso de sua organização onde quer que os usuários estejam acessando a internet e estabelece um transporte seguro para acessar aplicativos e serviços corporativos. Certifique-se de que esse agente seja capaz de detectar quando o usuário se conecta a uma rede confiável e, se uma rede confiável for detectada, se o agente deve desativar o seu serviço conforme determinado pela política. Certifique-se também de que esses agentes ofereçam suporte a uma ampla variedade de sistemas operacionais, incluindo Windows, MacOS, Linux, iOS e Android.

Para os usuários localizados nas filiais da empresa, um método comum de encaminhar o tráfego para a borda de serviço é através de um túnel GRE ou IPsec. No entanto, o fornecedor de SSE deve oferecer uma abordagem alternativa. Uma máquina virtual instalada na filial pode simplificar a complexidade e a administração contínua desses túneis e eliminar a movimentação lateral das ameaças ao remover a rede roteável gerenciada pelo cliente. a implementação deve ser automatizada e precisa incluir políticas flexíveis de direcionamento de tráfego para a borda de serviço com monitoramento de SLA e failover integrados. Essa opção funciona bem para filiais de médio e grande porte e para aquelas que oferecem serviços locais.

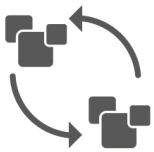
A opção anterior de tratar cada usuário como um usuário remoto deve ser considerada para filiais menores, onde nenhum serviço local é oferecido (como lojas e restaurantes de uma rede, por exemplo). Como eventos recentes alteraram a importância das filiais essa opção é desejável, pois não permite a presença de ninguém na rede corporativa e evita a possibilidade de movimentação lateral.

Para usuários/itens em dispositivos não gerenciados ou acesso de terceirizados a aplicativos internos via web, os fornecedores de SSE devem fornecer proteção de SSE equivalente, sem a necessidade de instalar agentes. Esses usuários devem poder usar o navegador para sua autenticação de usuário; em seguida, a proteção de confiança zero é garantida pela publicação de um CNAME específico do aplicativo em sua zona DNS para que o navegador possa redirecionar automaticamente essas solicitações. Como alternativa, o fornecedor de SSE também deve ter um recurso de isolamento do navegador (CBI) integrado para garantir segurança sem agente para qualquer dispositivo não gerenciado em qualquer lugar. Um benefício adicional é que isso evita inteiramente a necessidade de um frágil proxy reverso.

Com o CBI, os administradores podem configurar os recursos de SSO autorizados da nuvem para fazer o redirecionamento para o fornecedor do SSE. Assim, quando o usuário tentar acessar esse recurso da nuvem a partir de um terminal pessoal ou de terceiros, seu tráfego será enviado automaticamente para o CBI, sem nenhuma instalação de software. Ele renderiza o conteúdo em pixels que são então enviados para os dispositivos do usuário, impedindo downloads, copiar/colar e impressão. Dessa forma, o usuário pode realizar suas tarefas de trabalho a partir de terminais não gerenciados sem o risco de vazamento de dados, sem uploads de malware, e respeitando os requisitos de conformidade.

Para cargas de trabalho conectadas a cargas de trabalho dentro da mesma VPC ou central de dados, a segmentação de rede tradicional era a resposta. Embora isso fizesse sentido no papel, realizar a segmentação de rede na prática provou ser um desafio. Portanto, o fornecedor de SSE deve estender a proteção do tráfego usuário-aplicativo às comunicações entre cargas de trabalho. Com a instalação de um agente na própria tarefa, o provedor de SSE deve então determinar o risco e aplicar proteção baseada em identidade às cargas de trabalho sem nenhuma alteração na rede; além disso, as políticas devem se adaptar automaticamente às mudanças no ambiente.

©2022 Zscaler, Inc. Todos os direitos reservados.



Para cargas de trabalho conectadas a cargas de trabalho em VPCs ou CSPs ou via internet, o fornecedor de SSE também deve estender a essas tarefas a mesma proteção de SSE oferecida aos usuários. Para tanto, o fornecedor de SSE deve oferecer um mecanismo, normalmente via máquina virtual (disponível em nuvens públicas ou hipervisores locais), que simplifique o encaminhamento do tráfego para a borda de serviço. O resultado é que a proteção dos dados e cargas de trabalho contra ameaças cibernéticas não se limita à rede corporativa ou à nuvem privada, mas abrange a internet como um todo; isso também é válido para a proteção de confiança zero daquelas cargas de trabalho localizadas em uma nuvem que acessam cargas de trabalho em outra nuvem. Com essa abordagem, o fornecedor de SSE pode consolidar vários produtos (por exemplo, proxies web, firewalls, gateways NAT, filtragem de URL etc.) em uma única solução.

Para proteger dados em repouso em ambientes IaaS e SaaS, o fornecedor de SSE também deve oferecer soluções no espaço do CASB (corretor de segurança de acesso à nuvem), do CIEM (gerenciamento de direitos da infraestrutura de nuvem) e do CSPM (gerenciamento de postura de segurança na nuvem), para que a verificação baseada em API possa ocorrer com os aplicativos SaaS e IaaS mais comuns. Isso permite a identificação e correção de configurações incorretas e permissões indevidas em ambientes de nuvem, juntamente com auditorias e verificações de plataformas SaaS e IaaS, para garantir a proteção dos dados e evitar ameaças. o fornecedor de SSE deve oferecer esses recursos off-line em total sintonia com seus recursos on-line para aplicar políticas consistentes tanto a dados em repouso quanto aos dados em movimento.

O benefício de ter um único fornecedor de SSE que disponibilize essa ampla cobertura de proteção é que ela pode ser gerenciada a partir de um plano de controle central, com políticas corporativas aplicadas de maneira uniforme e dinâmica a todas as comunicações entre usuários/dispositivos e aplicativos, e de carga de trabalho para carga de trabalho

⚠ Com o que devo tomar cuidado?

A implementação da tecnologia SSE depende muito da complexidade do ambiente da organização. **Portanto, é muito importante entender a localização, o comportamento e os requisitos de acesso do usuário, assim como os requisitos dos aplicativos**. Além disso, alguns países (como a China) apresentam desafios únicos de desempenho devido aos controles sobre a internet que nem mesmo os modelos de implementação mais flexíveis conseguem superar. O fornecedor de SSE deve oferecer soluções inovadoras para enfrentar esses desafios.

Resultados:

Se implementadas corretamente, essas opções flexíveis, diversificadas e escaláveis trarão à sua organização todos os benefícios do Security Service Edge, independentemente de onde o usuário/dispositivo esteja e de onde o aplicativo esteja hospedado, podendo até mesmo estender essa proteção dentro do próprio aplicativo:

- O benefício de ter um único fornecedor de SSE que disponibilize essa ampla cobertura de proteção é que ela pode ser gerenciada a partir de um plano de controle central, com políticas corporativas aplicadas de maneira uniforme e dinâmica a todas as comunicações entre usuários/dispositivos e aplicativos, e também às comunicações entre cargas de trabalho.
- Se a mesma proteção dada a dispositivos gerenciados for oferecida a dispositivos pessoais (BYOD) não gerenciados e ao acesso por pessoal terceirizado, será possível aumentar a flexibilidade tanto para os terceirizados quanto para os funcionários.
- A segurança de carga de trabalho para carga de trabalho oferece aos engenheiros de DevOps e CloudOps as mesmas proteções de confiança zero para seus aplicativos que acessam outras tarefas, outras nuvens ou a internet.

Nº 5
Armadilha

Escolher uma solução de SSE que ofereça uma experiência medíocre aos usuários, sem otimizar a conectividade de aplicativos nem diagnosticar degradações de UX

Em vez disso, considere os fornecedores de SSE que:

- Sejam transparentes, fáceis de autenticar e que estejam sempre ativos, garantindo que os usuários finais localizados em sua plataforma de SSE tenham uma ótima experiência de usuário através de medidas objetivas.
- Correlacionem as más experiências do usuário final com suas causas subjacentes, estejam elas no ponto de acesso, na rede, no aplicativo ou nas ferramentas de segurança.
- Mantenham parcerias com os fornecedores de SaaS mais conhecidos, como Microsoft 365, para minimizar a latência entre a borda de serviço público e a rede do provedor de aplicativos

Como os fornecedores certos de SSE fazem esse trabalho:

Os pontos de presença do fornecedor de SSE em todo o mundo e as relações entre pontos de troca de tráfego de provedores e fornecedores de aplicativos são uma alternativa poderosa ao backhauling e ao estrangulamento do tráfego exigidos pelas ferramentas de segurança legadas.

Além destes benefícios da arquitetura, o fornecedor de SSE está bem posicionado para medir e diagnosticar a experiência do usuário final com base em sua presença nos terminais do usuário e no caminho de dados dos aplicativos. Estas vantagens permitem ao fornecedor de SSE entender a experiência do usuário do ponto de vista do terminal do usuário, e fornecer diagnósticos e escalonamentos mais aprofundados utilizando a infraestrutura da borda de serviço público.

Dê preferência aos fornecedores de SSE que ofereçam uma solução de monitoramento (comumente chamada de **Monitoramento da Experiência Digital**, ou DEM) integrada a seus agentes e infraestrutura de nuvem existentes. Aqueles que oferecem soluções que exigem agentes adicionais ou que sejam pacotes de aquisições com baixo nível de integração não serão capazes de oferecer o mesmo nível de visibilidade e de diagnóstico.

A solução DEM oferecida pelo fornecedor de SSE precisa ser ampla, com visibilidade de ponta a ponta e solução de problemas de desempenho do usuário final disponíveis para qualquer usuário ou aplicativo, independentemente de sua localização. Além disso, ela deve permitir o monitoramento contínuo das equipes de rede, segurança, desktop e central de atendimento com informações sobre problemas de desempenho do dispositivo, da rede e do aplicativo do usuário final. Por fim, ela também deve permitir os fluxos de trabalho reativos que ajudam a solucionar anomalias relatadas por funcionários, e os fluxos de trabalho proativos que ajudam a identificar macro anomalias (como interrupções regionais de ISP ou tempo de inatividade global de aplicativos) antes que os usuários percebam. **Isso precisa ser ativado por meio de algoritmos de classificação baseados em aprendizagem automática, rastreando a experiência normal/anormal do usuário para cada usuário, aplicativo, escritório ou geolocalização**.

Esse monitoramento deve ser feito em vários níveis, incluindo a camada 7 para obter informações sobre os tempos de resposta de aplicativos web, e a camada 3 para entender o comportamento da rede, incluindo informações salto a salto sobre caminho, latência e perda de pacotes. Essa análise também deve incluir o autodiagnóstico da nuvem do fornecedor de SSE para identificar se e quando o salto de SSE está induzindo atrasos anômalos. Por fim, a solução deve fornecer informações sobre a integridade do dispositivo/terminal do usuário e identificar quaisquer eventos do dispositivo que estejam contribuindo para quedas de classificação **(Veja a Figura 13)**.

Os fornecedores de SSE estão bem posicionados para medir e diagnosticar a experiência do usuário final com base em sua presença nos terminais do usuário e no caminho de dados dos aplicativos.

©2022 Zscaler, Inc. Todos os direitos reservados.

Monitoramento e solução de problemas de desempenho e qualidade do Microsoft Teams e Zoom

Como o Teams e o Zoom se tornaram as principais plataformas de colaboração e comunicação para muitas empresas, a medição e o diagnóstico de problemas de qualidade de áudio/vídeo tornam-se ainda mais urgentes. As soluções DEM oferecidas pelo fornecedor de SSE devem ser capazes de interagir com os aplicativos UCaaS mais comuns, como Zoom e Microsoft Teams, para obter métricas de qualidade de áudio e vídeo e compará-las com as análises aprofundadas de rede salto a salto e de dispositivos terminais. Ao combinar esses conjuntos de dados, a solução DEM deve identificar aqueles que têm problemas de qualidade, além de indicar a causa raiz do problema.

Além disso, o DEM deve aproveitar a escala da nuvem do fornecedor de SSE e utilizá-la para fazer testes de telemetria por proxy e cache para coletar dados granulares de cada usuário final, a intervalos de poucos minutos e com impacto mínimo sobre os aplicativos.

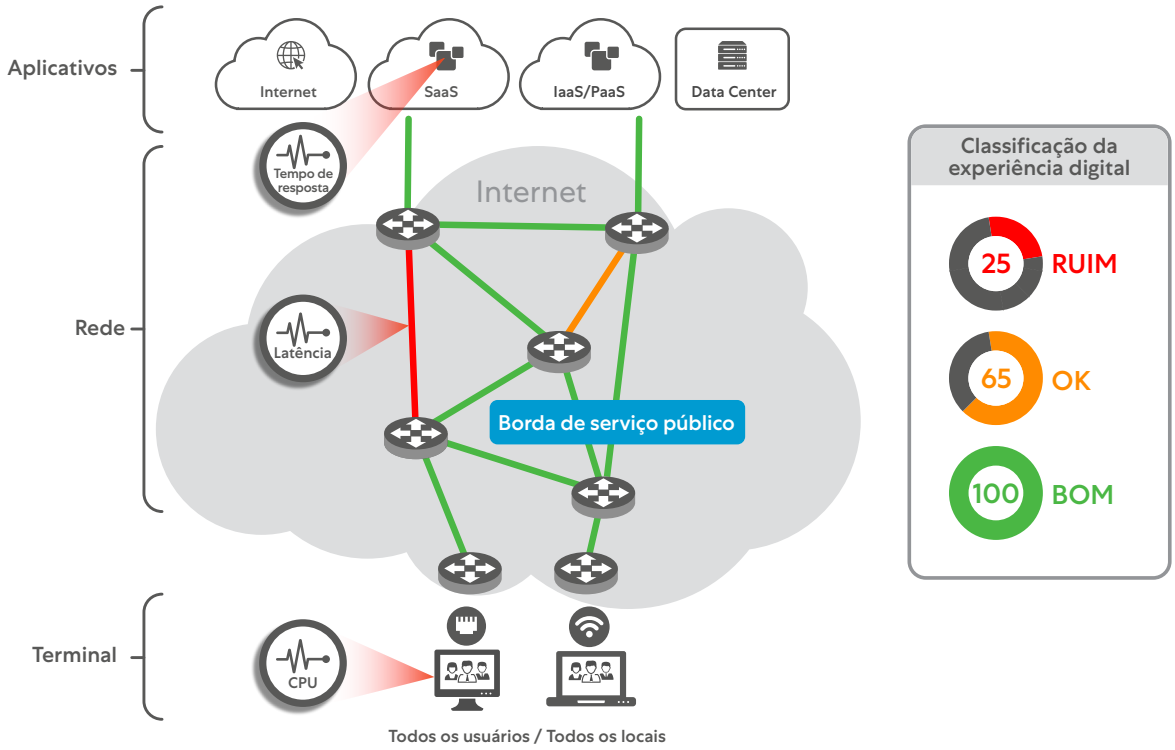


Figura 13: a solução DEM incorporada como parte da plataforma SSE deve fornecer visibilidade única da qualidade da experiência do usuário do ponto de vista do usuário final, esclarecendo problemas de terminal, rede e aplicativos

Desconfie das ferramentas de monitoramento legadas que adotam uma abordagem concentrada no data center para monitorar e coletar métricas de locais fixos, ao invés de obtê-las diretamente dos dispositivos do usuário. Essa abordagem não oferece uma visão unificada do desempenho com base no dispositivo do usuário, no caminho da rede ou no aplicativo, e resulta em baixa visibilidade quando os usuários e aplicativos não estão localizados na central de dados ou na rede corporativa. Ferramentas como essas criam silos de informações e não compartilham nenhum contexto, levando a uma visibilidade fragmentada da experiência do usuário e a um prolongamento do tempo gasto na solução de problemas. As ferramentas de monitoramento de pontos otimizadas para data center deixam lacunas de visibilidade ao detectar, diagnosticar e solucionar problemas de desempenho do usuário final na internet, ao passo que uma solução DEM moderna, integrada a uma plataforma de SSE, disponibiliza uma gama bem mais ampla de dados para análises de causa raiz (Veja a Figura 14).

A solução DEM deve identificar aqueles que têm problemas de qualidade, além de indicar a causa raiz do problema

©2022 Zscaler, Inc. Todos os direitos reservados.

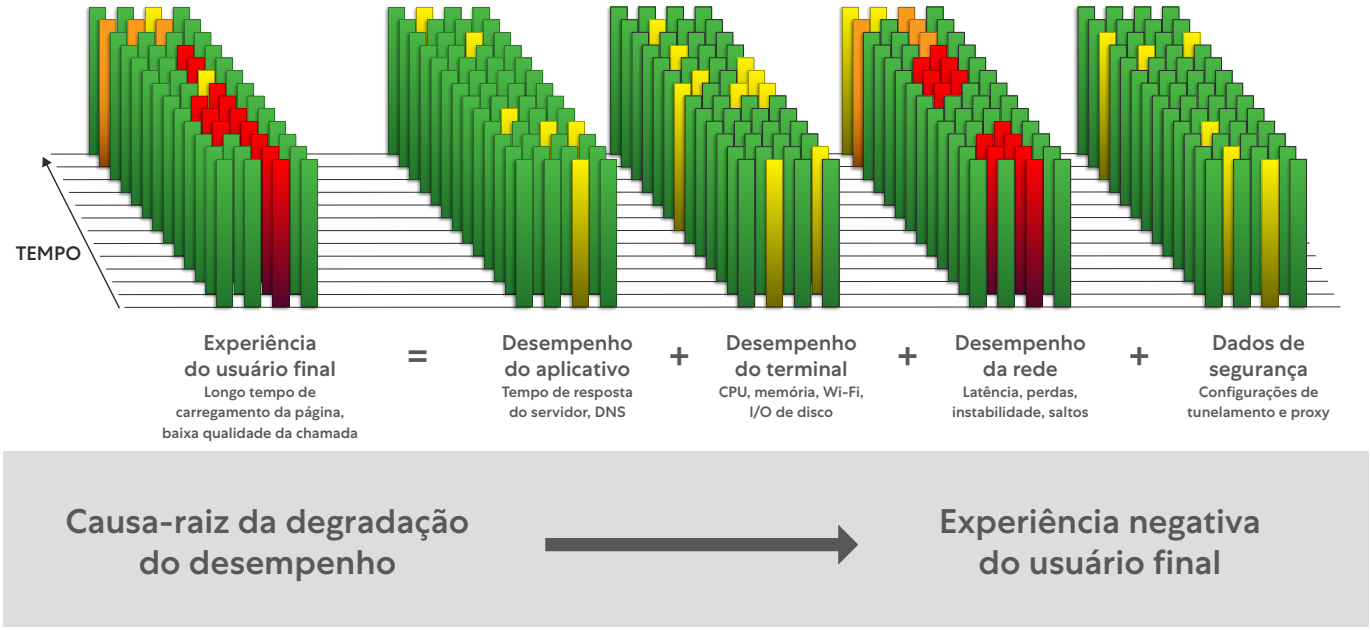


Figura 14: a solução DEM incorporada como parte da plataforma SSE deve fornecer visibilidade única da qualidade da experiência do usuário do ponto de vista do usuário final, esclarecendo problemas de terminal, rede e aplicativos

Otimização da experiência dos usuários do M365

Uma plataforma Security Service Edge abrangente é capaz de fazer mais do que medir e diagnosticar a experiência do usuário final, podendo também ser usada para otimizar o desempenho dos aplicativos SaaS mais comuns, como o Microsoft 365. O desafio é que muitas empresas direcionam seu tráfego centralmente, através de redes em estrela e do ExpressRoute. Além disso, o tráfego dos usuários do M365 aumenta a utilização da rede em 40%, e como a maioria das infraestruturas de empresas originadas na internet simplesmente não está à altura da tarefa, a experiência do usuário é prejudicada. A Microsoft recomenda conexões diretas com a internet e uma arquitetura de fornecedor de SSE que permita que as reuniões locais via internet ofereçam desempenho e custo ideais.

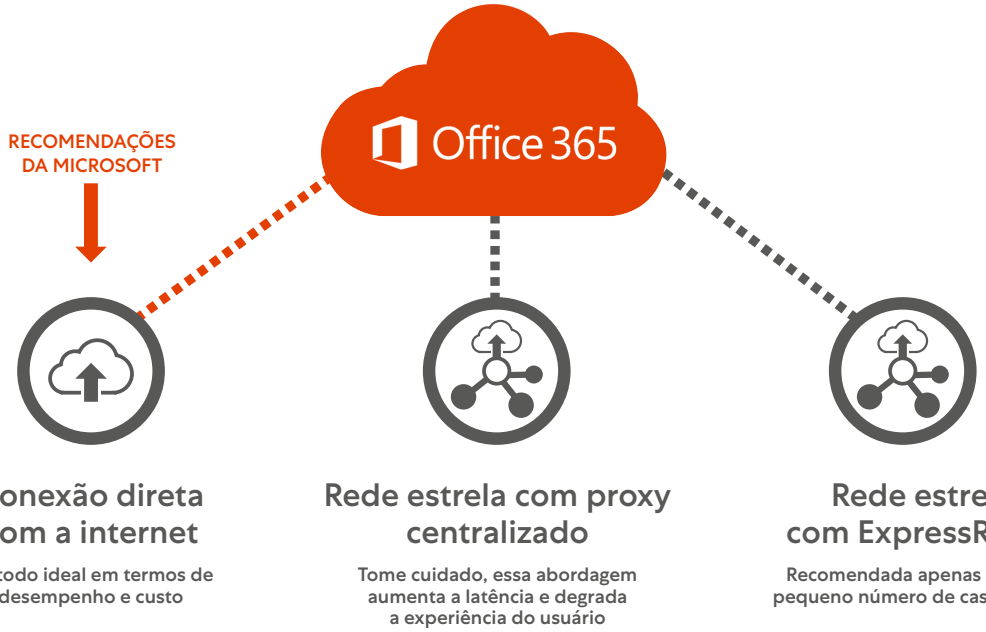


Figura 15: a Microsoft recomenda uma conexão direta com a internet como o método ideal para desempenho e custo, em linha com os princípios do SSE (fonte: microsoft.com).

©2022 Zscaler, Inc. Todos os direitos reservados.

Mas a arquitetura é importante. Os pontos de presença do fornecedor de SSE no mundo inteiro e suas relações com provedores e fornecedores de aplicativos precisam aproximar a borda dos usuários, proporcionando um acesso de alta conectividade e baixa latência. Procure fornecedores de SSE que utilizem a fibra direta com o Microsoft 365 na maioria dos principais pontos de conexão para reduzir a latência a aproximadamente 1-2 ms (tempo de ida e volta), e sejam capazes de escalar para lidar com o alto número de conexões de longa duração, acelerar o download de arquivos e permitir uma rápida resolução de DNS com menos saltos. (Veja a Figura 15).

É especialmente importante proteger as conexões M365 com a solução de SSE, pois a inspeção de aplicativos como OneDrive e SharePoint é vantajosa para prevenir a perda de dados confidenciais. Isso também fornece uma trilha de auditoria completa de todas as comunicações de e para os aplicativos M365. No entanto, esteja ciente de que certos aplicativos M365, como o Teams, podem não precisar ser inspecionados, já que grande parte desse tráfego de voz/vídeo é feito via UDP.

⚠ Com o que devo tomar cuidado?

Hoje o trabalho é feito de qualquer lugar (WFA), e existem muitos elos fracos ao longo do conjunto de aplicativos de bom desempenho em toda a malha global de redes com e sem fio. Otimizar a experiência do usuário é difícil, mesmo com uma arquitetura superior e conjuntos de ferramentas dedicadas para medir e diagnosticar problemas de UX. É essencial estabelecer expectativas razoáveis junto aos usuários finais sobre o que constitui uma experiência de usuário aceitável com relação a aplicativos críticos. Em seguida, é vital usar essas expectativas para criar linhas de base para fins de monitoração e gerenciamento.

Diagnosticar problemas com a experiência do usuário é mais uma arte do que uma ciência. Isso requer ferramentas e arquiteturas excelentes, mas também depende de ter os conjuntos certos de capacitação para interpretar e atuar sobre os dados. Embora as ferramentas DEM oferecidas pelos fornecedores de SSE destaquem a maioria das causas dos problemas (Wi-Fi, ISP, backbone, terminal ou DNS), um subconjunto exige escalonamento e conjuntos de dados adicionais. Por exemplo, pode ser necessário fazer o registro e o rastreamento de pacotes para chegar à causa raiz. Há também um subconjunto de problemas que nunca serão resolvidos, o que é absolutamente normal.

Cuidado com fornecedores que estrangulam o tráfego. Os data centers do fornecedor de SSE devem ter capacidade de computação e inspeção, permitindo uma experiência de usuário melhor e mais rápida. Sua arquitetura nativa da nuvem não deve concentrar o tráfego em alguns locais centralizados para fins de inspeção. Por exemplo, se um usuário aparecer em Melbourne, a inspeção de seu tráfego com serviços de prevenção de ameaças e proteção de dados deve ocorrer localmente, e não ser desviada para outras regiões, como Sydney ou Singapura. Fornecedores de SSE que executam sua nuvem em estruturas de hiperescala geralmente acabam estrangulando o tráfego do usuário. Uma estrutura de hiperescala pode ter 120 pontos de borda, mas é provável que 80% deles sejam rampas que conduzem o tráfego para um número menor de de data centers, onde o controle das políticas de SSE pode ser aplicado. É importante entender quantos data centers são rampas e quantos são realmente capazes de aplicar políticas.

Resultados:

O sucesso de qualquer transformação, seja digital, de rede ou de segurança, é determinado pela forma pela qual o usuário final a experimenta. O objetivo final de qualquer projeto de SSE é melhorar a experiência do usuário final, reduzindo a exposição a ameaças e protegendo dados confidenciais. Portanto, o resultado ideal é que a capacidade do fornecedor de SSE de melhorar a experiência do usuário pode ser medida por sua capacidade DEM – essa deve ser uma tarefa fácil, pois evitar o estrangulamento do tráfego desviando-o para um data center ou para fora de VPNs são maneiras bem aceitas de melhorar a experiência do usuário:

- A solução de SSE deve modernizar a experiência do usuário e atualizar a experiência da central de atendimento. Ao utilizar uma abordagem proativa da experiência do usuário, a central de atendimento pode reagir antes que os usuários reclamem.
- A solução de SSE deve fornecer informações em tempo real sobre o desempenho de áudio e vídeo de plataformas de colaboração como Teams e Zoom.
- A solução de SSE deve coletar métricas das camadas de aplicativo, terminal e rede para encontrar anomalias e determinar a causa raiz.
- O fornecedor de SSE deve indicar saltos mínimos entre a nuvem e os destinos mais comuns, como Microsoft 365.

Nº 6
Armadilha

Escolher uma solução de SSE cuja integração e orquestração com um ecossistema de fornecedores terceirizados sejam limitadas

Em vez disso, considere os fornecedores de SSE que:

- Tenham integração por meio de APIs robustas com outros ecossistemas líderes de mercado (como CSPs, SD-WAN, IAM, SOAR/SIEM, EDR, etc.) para garantir a proteção e experiência de usuário ideais.
- Utilizem essas integrações para permitir a automação e a orquestração, reduzindo a complexidade operacional e as despesas indiretas.
- Não aumente os custos de sua área técnica adotando um conjunto de soluções cuja integração seja limitada, tanto dentro desse conjunto quanto fora dele (terceiros)

Como os fornecedores certos de SSE fazem esse trabalho:

A maioria das empresas com custos técnicos elevados percebe que a maior parte deles se deve à aquisição, feita ao longo dos anos, de tecnologias de fornecedores que não conseguem interoperar.

Pior ainda é a assim chamada "plataforma" oferecida por um só fornecedor que na realidade não é integrada, mas sim uma coleção de produtos adquiridos individualmente que não têm nenhuma integração real além de um painel. Muitas vezes, essas tecnologias adquiridas de fornecedores diversos exigem capacitações especializadas para operar e manter uma coexistência frágil com as tecnologias associadas. O SSE pode eliminar grande parte desses custos da área técnica com uma plataforma de segurança na nuvem, unificada e oferecida por um único fornecedor. Com essa visão, o SSE é capaz de coexistir com um ecossistema de tecnologias complementares, e os fornecedores devem considerar a interoperabilidade com esse ecossistema como um objetivo principal (**Veja a Figura 16**). Esse ecossistema de modo geral consiste em outras soluções de segurança, rede e nuvem.

Figura 16: Não fique no deserto com um fornecedor que não ofereça um rico ecossistema de integrações com terceiros, pois isso aumenta os custos da área técnica, limita a interoperabilidade e resulta em fragilidade (não agilidade) das ferramentas de segurança.

©2022 Zscaler, Inc. Todos os direitos reservados.

Para garantir a agilidade, rapidez e segurança da implementação e da integração, o fornecedor de SSE deve oferecer integrações com as empresas líder no setor de:

- Provedores de serviços de nuvem (CSPs), IaaS/PaaS e SaaS
- Detecção e resposta de terminal (EDR)
- SD-WAN
- Gerenciamento de identidade e acesso (IAM)
- Gerenciamento de eventos e informações de segurança (SIEM)/orquestração, automação e resposta de segurança (SOAR)
- Ferramentas de orquestração

Essas integrações devem permitir a orquestração do fornecedor de SSE com os demais fornecedores para reduzir a complexidade, o TCO e melhorar a postura de segurança (Veja a Figura 17).

Provedores de serviços em nuvem (IaaS/PaaS e SaaS)

No caso de aplicativos internos sendo migrados para a nuvem ou sendo criados nativamente na nuvem, o fornecedor de SSE deve integrar os principais provedores de IaaS/PaaS, como AWS, GCP e Azure, para que a conectividade de acesso remoto seguro com confiança zero seja estendida a esses aplicativos. Isso garante que esses aplicativos nunca sejam expostos à internet, tornando-os completamente invisíveis para usuários não autorizados, com fluxo de tráfego de dentro para fora por meio de conectividade baseada em políticas, sem nunca expor a rede a eles.

Essa abordagem garante o acesso direto à nuvem sem conexão via VPN de acesso remoto, com a possibilidade de aproveitar as vantagens de larga escala do provedor de nuvem sem nenhum aumento de complexidade da segmentação de rede. Ela não depende de nenhum dispositivo virtual ou físico e aproveita as vantagens da confiança zero para eliminar a superfície de ataque.

Para os aplicativos SaaS mais comuns, os fornecedores de SSE devem fornecer integrações com um clique. No caso do Microsoft 365, a integração do fornecedor de SSE deve mapear todos os intervalos e domínios de IP da Microsoft para os aplicativos M365 listados, permitindo o encaminhamento transparente do tráfego do usuário final para a sua nuvem. Além disso, o intercâmbio de tráfego com o Microsoft 365 reduz o tempo de ida e volta, melhora a escalonabilidade e permite downloads de arquivos e resolução de DNS mais rápidos.

A integração do SSE com outros fornecedores de SaaS, como o ServiceNow, pode melhorar a proteção dos dados. Ao escanear dados do ServiceNow novos e existentes, o fornecedor de SSE deve identificar os dados confidenciais com base em políticas de DLP e bloquear a saída/transferência de arquivos contendo dados confidenciais. A integração com o ServiceNow Security Incident Response pode orquestrar ações de resposta, incluindo a atualização de listas de bloqueio personalizadas. IPs, domínios e URLs arriscados podem ser bloqueados sem intervenção manual e configurações incorretas da nuvem podem ser fechadas para ajudar a reduzir o risco de falhas de segurança.

Detecção e resposta de terminal

O fornecedor de SSE deve garantir a integração com diversos parceiros de segurança de terminal para compartilhar telemetria, melhorar a visibilidade mútua e orquestrar respostas. Essa integração permite a defesa em profundidade e a implementação da confiança zero de forma eficaz e eficiente.

Essa integração deve oferecer a capacidade de avaliar a identidade, a localização e a postura do dispositivo do usuário para implementar automaticamente as políticas de acesso condicional apropriadas. Além disso, a correlação e o fluxo de trabalho entre plataformas podem acelerar a investigação e a resposta. Isso significa:

- Avaliar a integridade do dispositivo e implementar automaticamente as políticas de acesso apropriadas.
- Identificar ameaças de dia zero e correlacionar com a telemetria de terminal para identificar os dispositivos afetados e implementar respostas rápidas com um fluxo de trabalho de quarentena entre plataformas.
- Investigar ameaças com contexto de terminal e rede para garantir a eficácia da detecção e da tomada de decisão.

©2022 Zscaler, Inc. Todos os direitos reservados.

SD-WAN

O fornecedor de SSE deve garantir a integração com fornecedores de SD-WAN para simplificar o roteamento do tráfego das filiais e facilitar o estabelecimento de sessões locais seguras via internet.

Uma solução de SSE/SD-WAN conjunta pode permitir um acesso seguro e baseado em políticas tanto à internet quanto aos aplicativos críticos para a empresa, garantindo proteção idêntica para todos os usuários – não importando onde ou quando eles venham a se conectar a aplicativos na nuvem e à internet aberta. Soluções SD-WAN podem ser integradas ao SSE por meio da integração de APIs. Com essa solução combinada, as filiais corporativas podem gerenciar o aumento do tráfego com a nuvem e a internet sem desvios para a DMZ centralizada na central de dados, usando uma arquitetura de WAN híbrida para a transformação de rede em conjunto com uma segurança robusta.

Deve-se observar que o fornecedor de SSE não deve ser dependente de uma rede qualquer, e não deve estar vinculado exclusivamente a nenhuma solução de rede particular. Na verdade, muitos dos benefícios da SD-WAN advêm de seus recursos "definidos por software", mas não necessariamente da WAN, que inerentemente amplia a rede corporativa e permite a movimentação lateral de ameaças. Os responsáveis pela tomada de decisões de SSE devem avaliar cuidadosamente as razões para continuar a estender a rede corporativa às filiais, e considerar abordagens alternativas (como somente internet) que sejam mais seguras.

Figura 17: Os fornecedores de SSE devem garantir a integração com os melhores parceiros nas mais diversas funções.

Gerenciamento de identidade e acesso

O fornecedor de SSE deve oferecer integração com soluções de IAM para aplicar acesso de confiança zero orientado pela postura do dispositivo, garantindo assim uma proteção contra ameaças mais eficaz em todo o âmbito da empresa.

A utilização de padrões como SAML (Security Assertion Markup Language) facilita a implementação da integração. Os usuários devem poder se autenticar e ter acesso seguro à internet e aos aplicativos internos. O IAM gerencia o acesso do usuário final aos aplicativos por meio de uma combinação de SSO e MFA, enquanto o fornecedor de SSE garante a segurança da conexão. O suporte ao protocolo System for Cross-domain Identity Management (SCIM) permite que todas as informações do usuário sejam mantidas em sincronia entre os dois sistemas, incluindo alterações no grupo de usuários ou seus cargos, e exclusões de contas no caso de usuários que não trabalham mais na empresa.

©2022 Zscaler, Inc. Todos os direitos reservados.

SIEM e SOAR

O fornecedor de SSE deve incluir integrações com provedores de SIEM e SOAR para garantir um gerenciamento eficiente e eficaz tanto dos riscos quanto da conformidade, com enriquecimento e automação das informações.

O fornecedor de SSE deve poder enviar dados de log em tempo quase real para soluções SIEM/SOAR, tanto instaladas no local quanto as baseadas na nuvem, para facilitar a correlação de logs de fontes diversificadas – isso permite às empresas analisar os padrões de tráfego em sua rede como um todo. Além disso, as empresas devem ser capazes de utilizar os dados de log do SIEM para realizar análises históricas abrangentes (> 6 meses). Isso garante conformidade com as instruções normativas por meio do arquivamento local dos registros de log.

Ferramentas de orquestração

Quando a infraestrutura como código (IaC) e a DevSecOps forçam as equipes de segurança a antecipar sua ação, o provedor de SSE deve fornecer as APIs para orquestração. Aqui o foco está nos aplicativos internos quando a instanciação do acesso de confiança zero faz parte do ciclo de vida de entrega do aplicativo; ela é habilitada por scripts de orquestração (como Ansible ou Terraform), especialmente para configurações de segmentação – tanto de usuário para aplicativo quanto de carga de trabalho para carga de trabalho. Essa orquestração permite que os recursos de confiança zero sejam alinhados com os métodos mais ágeis usados pelos desenvolvedores de software.

Quando a infraestrutura como código (IaC) e a DevSecOps forçam as equipes de segurança a antecipar sua ação, o provedor de SSE deve fornecer as APIs para orquestração

⚠ Com o que devo tomar cuidado?

Os responsáveis pela tomada de decisões de SSE devem avaliar a profundidade das integrações de API e a frequência das atualizações, bem como monitorar as mudanças no mercado que possam impedir integrações futuras (por exemplo, um fornecedor que se torna concorrente devido a uma aquisição). Esteja ciente da escassez de talentos em sua empresa, pois a implementação dessas integrações – especialmente com ferramentas legadas – vai exigir profissionais especializados.

Resultados:

Os fornecedores de SSE que disponibilizam integrações avançadas com terceiros baseadas em API conseguem oferecer eficiências operacionais decorrentes de sua capacidade de orquestrar as melhores soluções, e com menor probabilidade de aprisionamento tecnológico por dependência de um fornecedor:

- O fornecedor de SSE integrado aos principais parceiros do ecossistema (como CSPs, SD-WAN, IAM, SOAR/SIEM, EDR, etc.) protege suas tecnologias contra a obsolescência e reduz os custos da área técnica.
- Um ecossistema orquestrado de fornecedores integrados reduz a complexidade operacional e as despesas indiretas, e pode limitar os erros do operador.
- Os fornecedores de SSE que montam um pacote de soluções por meio de aquisições tendem a ficar para trás em termos de inovação do produto, e muitas vezes não têm interoperabilidade com terceiros.

Nº 7
Armadilha

Escolher uma solução de SSE incapaz de mostrar valor facilmente em piloto de ambiente de produção

Em vez disso, considere os fornecedores de SSE que:

- Executem o piloto de sua solução com um único agente unificado, com acesso a um conjunto global de bordas de serviço (próximas do usuário), e com uma interface de usuário centralizada e fácil de usar.
- Orientem os diversos aspectos da plataforma SSE com o menor número possível de implementações adicionais.
- Inspirem total confiança de que sua solução vai funcionar como previsto após a implementação completa, com o mínimo esforço de pós-vendas.

Figura 18: Certifique-se de que o teste do fornecedor de SSE seja feito com a solução real, e não com uma réplica de recursos limitados. Somente um piloto executado no ambiente de produção pode comprovar o valor da solução do fornecedor de SSE.

Como os fornecedores certos de SSE fazem esse trabalho:

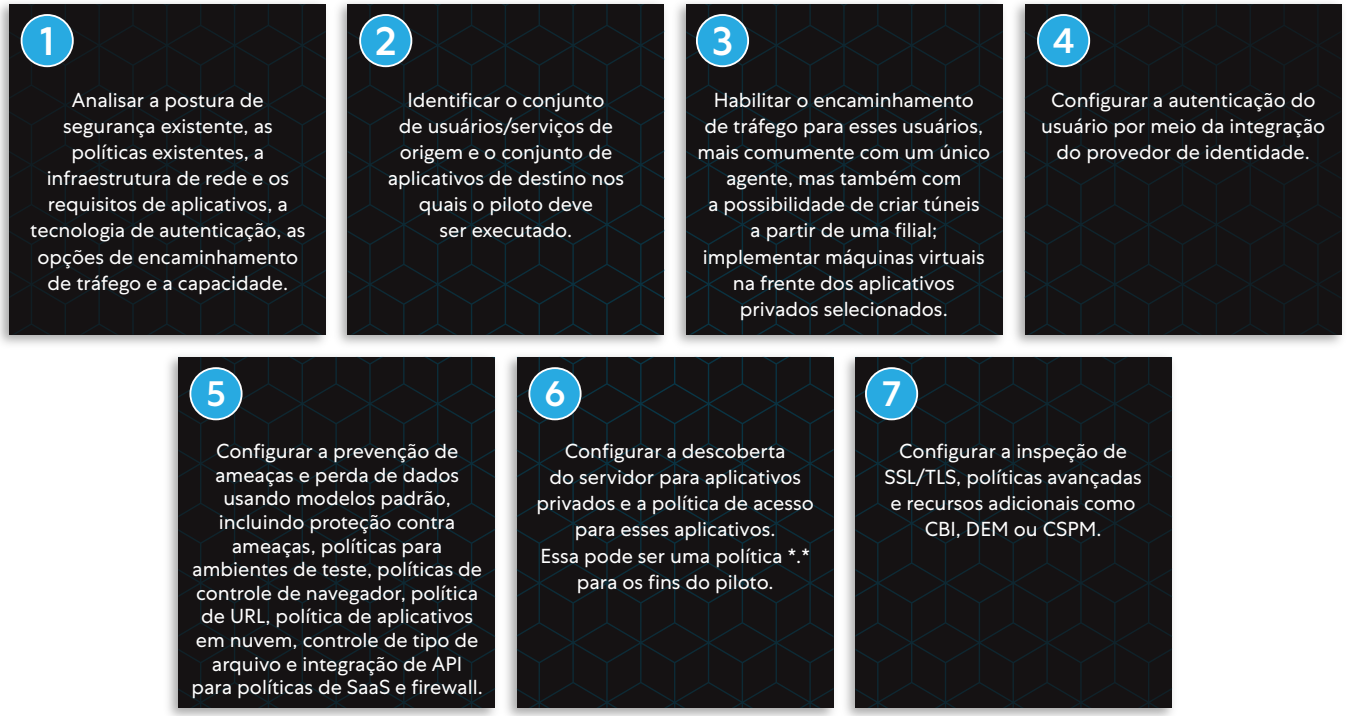
A adoção de uma plataforma de SSE exige que sua arquitetura de segurança seja inteiramente repensada; portanto, a escolha do fornecedor de SSE não deve ser uma decisão superficial. Dessa forma, é fundamental compreender a verdadeira capacidade do fornecedor de SSE de trabalhar em seu ambiente de produção. A facilidade com que isso é feito é um indicador da arquitetura da plataforma.

Ao considerar um fornecedor de SSE, deve-se entender as etapas necessárias para executar um piloto. Para o fornecedor de SSE certo, o processo deve ser o de encontrar uma maneira de encaminhar o tráfego para a borda de serviço do SSE; a partir dali o controle é assumido pela própria nuvem do fornecedor de SSE. Deve haver etapas mínimas a serem executadas pelo administrador do SSE, além de estabelecer um mecanismo de encaminhamento e configurar as políticas básicas, a autenticação e os relatórios. Obviamente, a configuração avançada das políticas vai exigir mais tempo.

©2022 Zscaler, Inc. Todos os direitos reservados.

O piloto deve abordar um conjunto predeterminado de resultados de negócios e envolver membros de diversas equipes, incluindo segurança, rede e desktop (para a instalação dos agentes nos terminais, por exemplo). No entanto, o envolvimento ativo dessas equipes deve ser mínimo – afinal, elas estão procurando adquirir uma solução de SaaS. Se o fornecedor de SSE exigir um envolvimento mais profundo, especialmente das equipes de rede, para lidar com os cenários complexos de roteamento no piloto, isso deve ser visto como um sinal vermelho.

Adote uma abordagem sequencial que reflita seus objetivos de negócio ao planejar o piloto de uma solução de SSE abrangente:



Todas as etapas acima devem ser diretas e passíveis de realização pelo fornecedor de SSE em um curto período de tempo (normalmente alguns dias), e sem grandes alterações de roteamento ou configuração. Embora a implementação completa e real exija etapas adicionais, configurações avançadas de políticas, diversos tipos de aplicativos e terminais, além de integrações e coexistência com outros agentes/tecnologias, o fornecedor de SSE deve ser capaz de demonstrar o valor da plataforma por meio de um piloto simples, mas bem executado.

Durante o piloto, o fornecedor de SSE deve ser capaz de comprovar o seguinte, alinhando-se com as seis práticas anteriores detalhadas neste documento:

- **Uma infraestrutura de nuvem global com latência mínima para o usuário final, e que opere com alta disponibilidade e desempenho.** O fornecedor deve demonstrar sua capacidade de operar essa nuvem em larga escala e de demonstrar os efeitos do failover.
- **Confiança zero para cada sessão de usuário**, incluindo a proteção de aplicativos privados, aplicativos públicos e até mesmo das comunicações entre cargas de trabalho (se o piloto solicitar isso).
- **Proteção avançada contra ameaças e DLP avançado por meio do intercâmbio de tráfego criptografado**. O gerenciamento de certificados pode exigir algumas etapas adicionais no piloto, mas a comprovação da capacidade do fornecedor de fazer inspeção de SSL/TLS com o mínimo de latência adicional é uma excelente maneira de diferenciar um fornecedor de SSE dos demais.
- **Opções flexíveis de implementação**. Embora isso possa não fazer parte do piloto, o fornecedor de SSE deve ter um plano para proteger todos os usuários, independentemente de localização ou do aplicativo. Isso pode exigir uma compreensão da implementação de bordas de serviço privado ou CBI para terceirizados. O ponto principal a ser verificado é se o modelo de implementação do fornecedor de SSE é capaz de atender aos requisitos de uma força de trabalho distribuída e aplicativos com seus modelos de implementação.

©2022 Zscaler, Inc. Todos os direitos reservados.

- **Otimização da experiência do usuário**. Essa métrica abrange desde a facilidade de uso (como o usuário final interage com seu agente, por exemplo) até a experiência geral do usuário ao acessar aplicativos públicos e privados em sua plataforma de SSE. O fornecedor deve ser capaz de medir e diagnosticar um amplo conjunto de problemas de desempenho do usuário final (Wi-Fi, ISP, CPU etc.). Essa capacidade de medição/diagnóstico deve ser incorporada diretamente à plataforma SSE, sem a necessidade de implementar novos agentes.
- **Integração com fornecedores terceirizados**. Embora isso também possa não fazer parte do piloto, o fornecedor deve indicar métodos para integrar dados de log em uma ferramenta de SIEM externa ou em uma ferramenta de EDR existente. o fornecedor de SSE deve analisar o ecossistema de ferramentas existentes na empresa e fazer recomendações de integração assim que a implementação real começar.

Dê preferência aos fornecedores de SSE com os menores custos indiretos, devido à falta de pessoal qualificado existente no setor.

O benefício de recorrer a um fornecedor de segurança SaaS é que as tarefas normalmente feitas pela equipe interna são assumidas pelo fornecedor de SSE – o piloto deve dar uma indicação clara de quanto esforço será necessário para implementar, administrar e atualizar a solução de SSE.

⚠ Com o que devo tomar cuidado?

- Um projeto piloto não é capaz de testar todas as possibilidades, e podem surgir problemas imprevistos durante a implementação real.
- Procure confirmar que o fornecedor de SSE seja voltado ao cliente e demonstre disposição para solucionar quaisquer problemas de implantação que possam surgir.
- Lembre-se de que provavelmente o piloto não será implementado em larga escala e que seus resultados imediatos não serão evidentes. o fornecedor de SSE pode contornar problemas de rede ou de roteamento mais complicados durante o piloto, problemas esses que serão revelados só durante a implementação da solução completa. o fornecedor de SSE certo não deve depender de nenhum roteamento de rede para fazer as coisas funcionarem.
- Considere os custos e despesas indiretas de administração – quais serão as suas responsabilidades, e quais serão as responsabilidades do fornecedor de SSE? Calcule o esforço necessário para uma implementação em produção, além da manutenção contínua da solução.
- Alguns fornecedores de SSE podem não ser verdadeiros provedores de SaaS. Certifique-se de que a administração da solução de SSE tenha o menor custo total de propriedade; isso é especialmente importante devido à escassez de mão de obra especializada enfrentada pela maioria das empresas de TI.

Resultados:

Um piloto válido é a prova de que a solução de SSE é de fácil implementação, funciona em seu ambiente de produção e, sobretudo, é capaz de atingir seus objetivos

- A capacidade do fornecedor de SSE de construir um piloto exemplar de sua solução é um bom indício de seu potencial para concluir a implementação com sucesso. As metas de baixo TCO, um único agente unificado, acesso a um conjunto global de bordas de serviço e uma interface de usuário centralizada e fácil de usar simplificam muito a manutenção contínua da solução. Qualquer implementação em larga escala exige tempo e esforço, mas seu objetivo deve ser o de trabalhar junto com um fornecedor que seja capaz de minimizá-los.
- A arquitetura e o projeto do SSE devem facilitar a inclusão de recursos com o mínimo de requisitos adicionais de implementação (como agentes ou VMs adicionais). Dessa forma, o comprador pode adotar uma abordagem do SSE em fases, sabendo que a passagem de uma fase para outra não vai exigir grandes esforços.
- Em última análise, o objetivo é ter confiança de que o fornecedor de SSE seja capaz de fazer a implementação no ambiente de produção sem maiores problemas, e que ele estará disponível para solucionar os problemas inevitáveis. Fornecedores focados no cliente e que dispõem de uma arquitetura testada e aprovada são os melhores indícios de que seu investimento em segurança e transformação de rede será bem-sucedido.

Não confie apenas em nossas palavras

Aqueles momentos de "big bang" que permitem às empresas fazer investimentos drásticos em um caminho totalmente novo são muito raros. Assim, as empresas devem considerar uma abordagem comedida do SSE. O escopo do SSE corporativo (compartilhado publicamente em https://trust.zscaler.com) abordando todos os possíveis usuários, servidores, dispositivos etc., é descrito na Armadilha No. 2. Veja abaixo alguns exemplos de abordagem da adoção do SSE:

Exemplo A:

O cliente implementou a plataforma Zscaler SSE para ter um controle de confiança zero dos seguintes itens:

- Acesso granular do usuário final a serviços privados
- Segurança do usuário final na internet, incluindo inspeção e proteção de dados on-line
- Transformação da rede com os usuários completamente removidos da rede
- Proteção de cargas de trabalho, internet e acesso privado
- Acesso de terceirizados limitado e controlado

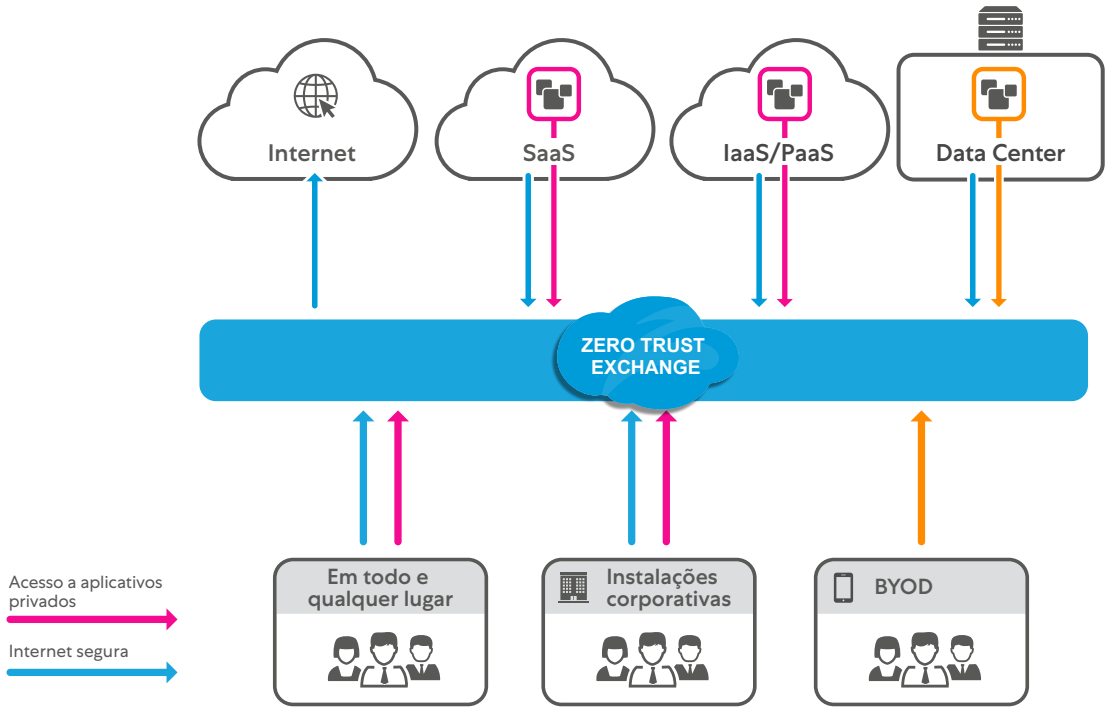


Figura 19: Representação de alto nível da conectividade implementada na empresa com a solução Zscaler

©2022 Zscaler, Inc. Todos os direitos reservados.

SANDVIK

"Em menos de cinco dias fizemos uma transição suave, segura e econômica de 20.000 funcionários para o WFA, substituindo as VPNs pela solução Zero Trust Network Access (ZTNA) da Zscaler."

Michael Alvmarken, gerente de serviços de segurança cibernética e tecnologia do Sandvik Group

reckitt

"A infraestrutura de nuvem da Zscaler e suas integrações nativas com ZIA e ZPA nos deram uma percepção muito melhor dos dados de nossos usuários finais"

John Dawes, diretor de arquitetura corporativa, Reckitt Benckiser

SIEMENS

"Sem desviar nosso tráfego, mas usando diretamente a internet, esperamos reduzir os custos em 70%."

Frederik Janssen, vice-presidente global de infraestrutura de TI da Siemens

Exemplo B:

O cliente implementou a plataforma Zscaler SSE para:

- Ter visibilidade total do acesso a todos os serviços via internet (nuvem etc.)
- Ter total controle on-line para restringir as perdas de propriedade intelectual da empresa
- Fazer o monitoramento digital da experiência de acesso do usuário durante o trabalho em casa

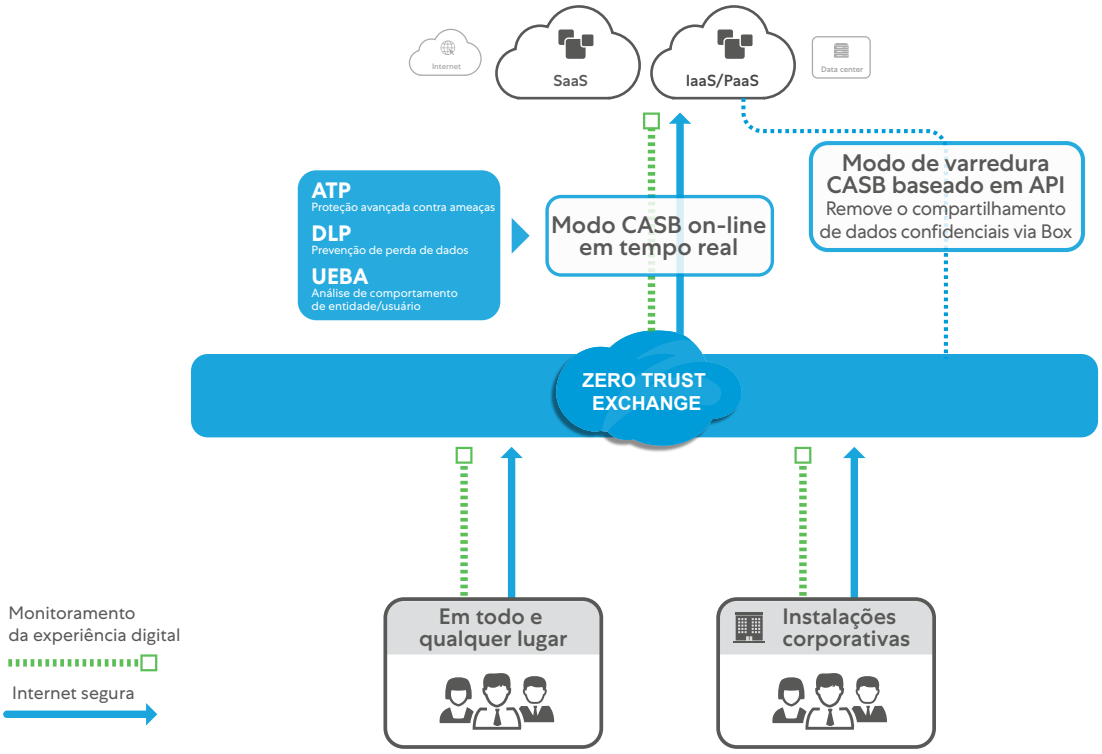


Figura 20: Exemplo de inspeção e monitoramento on-line da experiência com a plataforma Zscaler.

©2022 Zscaler, Inc. Todos os direitos reservados.

ciena

"Vemos o Zscaler Digital Experience como um serviço essencial, porque permite uma experiência de trabalho produtiva onde quer que seja. Tivemos a sorte de resolver 25% dos problemas dos usuários no passado. Agora o ZDX é o ponto de partida para resolver todos os nossos problemas de experiência do usuário, e conseguimos identificar a causa raiz 95% das vezes."

Ed DeGrange, arquiteto e chefe de segurança, Ciena

SIEMENS

"Seja um problema comercial ou de fraude, algum defeito no site ou fraude interna, tudo tem um impacto financeiro – e é por isso que a segurança tem que fazer parte disso."

Frederik Janssen, vice-presidente global de infraestrutura de TI da Siemens

BOMBARDIER

"Com o Zscaler Advanced Cloud Sandbox o pessoal de TI não precisa mais fazer o trabalho pesado – o que é fundamental, pois no mercado atual os talentos são tão escassos que qualquer contratação é um desafio extremo."

Mark Ferguson, CISO, Bombardier

Exemplo C:

O cliente disponibiliza proteção granular dos serviços que não são de TI usando a plataforma Zscaler:

- Confiança zero para tecnologias operacionais (OT), funcionários e terceirizados
- De TO para carga de trabalho
- De nuvem para carga de trabalho

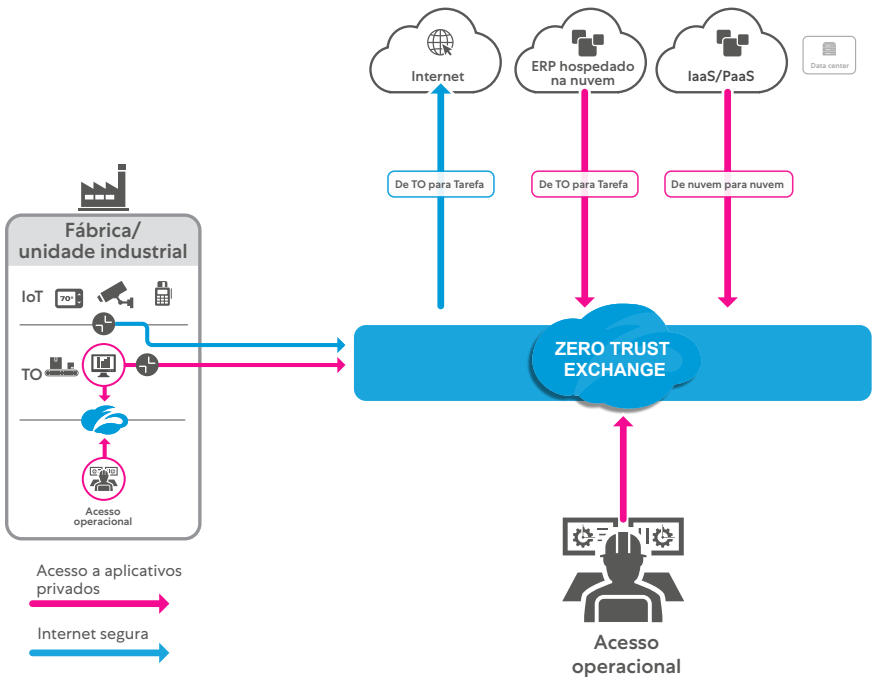


Figura 20: Exemplo de inspeção e monitoramento da experiência on-line com a plataforma Zscaler

©2022 Zscaler, Inc. Todos os direitos reservados.

Principais conclusões

O fornecedor de SSE deve oferecer um SLA documentado com base na perda ou degradação do serviço.

A solução de SSE deve oferecer a aplicação de políticas independentemente da localização – on-line, em escala global e dentro dos pontos de intercâmbio de tráfego com neutralidade relativamente ao operador, garantindo assim o caminho mais eficaz para os clientes.

O fornecedor de SSE deve oferecer controles de confiança zero a todos os usuários corporativos, tarefas e dispositivos autorizados por meio de qualquer protocolo.

A solução de SSE deve prestar o serviço de forma independente em qualquer rede.

O fornecedor de SSE deve viabilizar sua inspeção on-line por meio de uma arquitetura de proxy na nuvem, garantindo latência mínima e permitindo total visibilidade de todo o tráfego na web (até e incluindo o TLS 1.3).

A solução de SSE deve fornecer vários controles de segurança por meio de uma única arquitetura de varredura de memória, obtendo assim vantagens exclusivas de escalonabilidade para a descriptografia em larga escala.

O fornecedor de SSE deve oferecer uma solução gerenciada centralmente e implementada de várias formas para abranger a personalização em termos de localização, região, localidade e função do cliente.

A solução de SSE deve ser estendida para garantir a proteção do acesso não gerenciado de terceirizados, BYOD e de parceiros com o mesmo nível de controle granular exercido sobre os funcionários da empresa.

O fornecedor de SSE deve otimizar a experiência do usuário monitorando e diagnosticando problemas de desempenho dos serviços da empresa (Teams, Zoom etc.).

A solução de SSE deve coletar métricas das camadas de caminho de aplicativo, terminal e rede para identificar anomalias e fornecer informações às equipes de suporte.

O fornecedor de SSE precisa estar integrado aos melhores parceiros do ecossistema (como CSPs, SD-WAN, IAM, SOAR/SIEM, EDR, etc.) para oferecer controle e segurança completos e detalhados ao ambiente da empresa como um todo.

A solução de SSE deve ser integrada a esses provedores para permitir a orquestração e minimizar os custos operacionais indiretos.

O fornecedor de SSE deve ser capaz de implementar uma solução piloto abrangendo as funções e os locais necessários da empresa em produção.

A solução de SSE deve ser simples e extensível, sem a necessidade de hardware ou agentes adicionais, permitindo que as empresas ampliem sua utilização do SSE por meio de uma abordagem em fases.

Para obter mais informações sobre o SSE, visite Zscaler SSE 2022

Sobre os autores

Sanjit Ganguli (VP, Estratégia de Transformação/CTO de Campo) e Nathan Howe (VP, Tecnologia Emergente & 5G) com carreiras globais em empresas como Gartner, Nestlé, Riverbed e Verizon, trazem uma liderança e uma visão inovadoras de temas como nuvem, segurança, transformação e tecnologias emergentes.

©2022 Zscaler, Inc. Todos os direitos reservados.