E-book

# Quatro razões pelas quais firewalls e VPNs estão expondo as organizações a violações



© 2024 Zscaler, Inc. Todos os direitos reservados.

# As soluções de ontem são os problemas de hoje

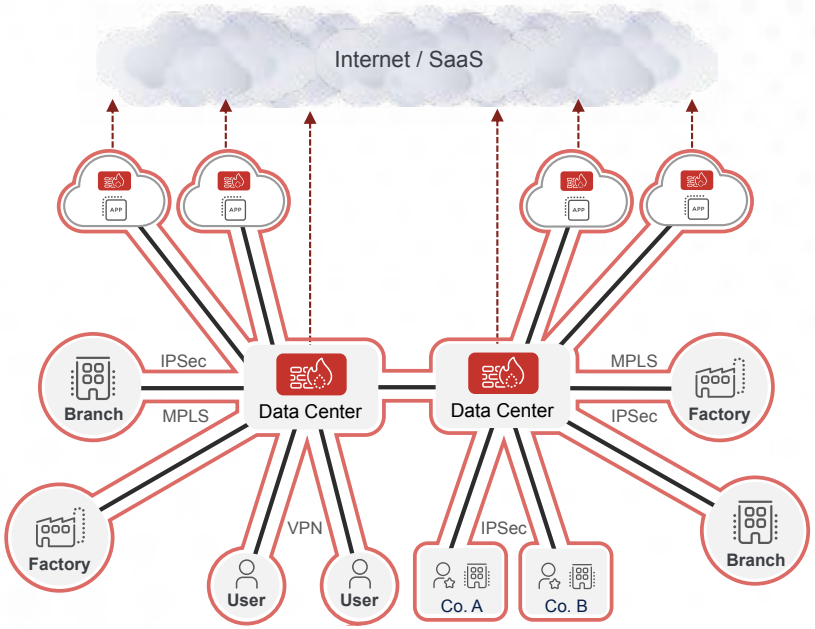
Os firewalls e as VPNs estão expondo as organizações a violações. Pode parecer contraintuitivo devido ao fato de que os dois têm sido ferramentas de segurança essenciais há décadas, mas é aí que reside o problema. Eles foram projetados para uma época em que o trabalho era feito de maneira muito diferente do que é hoje. Antigamente, os usuários e aplicativos eram locais (seja no escritório principal ou em uma filial) e os esforços de segurança se concentravam em estabelecer um perímetro ao redor da rede que os conectava. Em outras palavras, uma rede em estrela era defendida por um modelo de segurança de castelo e fosso.

Essa abordagem tem vários nomes, incluindo arquitetura baseada em perímetro, arquitetura centrada na rede e arquitetura tradicional ou legada. Independentemente do nome, ela envolve inerentemente o uso de ferramentas como firewalls e VPNs, que são implantados na tentativa de proteger a rede; mais especificamente, mantendo as coisas ruins fora e as coisas boas dentro.

As organizações evoluíram rapidamente nos últimos anos, em grande parte devido à pandemia da covid-19. Para permanecerem produtivas em 2020, elas tiveram que acelerar seus cronogramas de transformação digital, transformando os aplicativos na nuvem e o trabalho remoto no novo normal. No entanto, essa evolução era incompatível com firewalls, VPNs e as arquiteturas baseadas em perímetros que as ferramentas pressupunham. Isso porque é inviável construir um perímetro de segurança em torno de uma rede que seja infinitamente estendida a cada vez mais usuários, dispositivos, aplicativos e nuvens externos.

Para as organizações que avançam com a arquitetura legada em meio à transformação digital, isso cria inúmeros desafios em torno da complexidade, rigidez, custo e produtividade. Além disso, e mais importante, aumenta o risco cibernético e expõe as organizações a violações de quatro formas principais que são explicadas nas páginas seguintes.

**Arquitetura centrada em firewall e VPN**




**Uma rede confiável conecta usuários, sites e aplicativos. A proteção contra ameaças e dados concentra-se na segurança da rede.**

© 2024 Zscaler, Inc. Todos os direitos reservados.

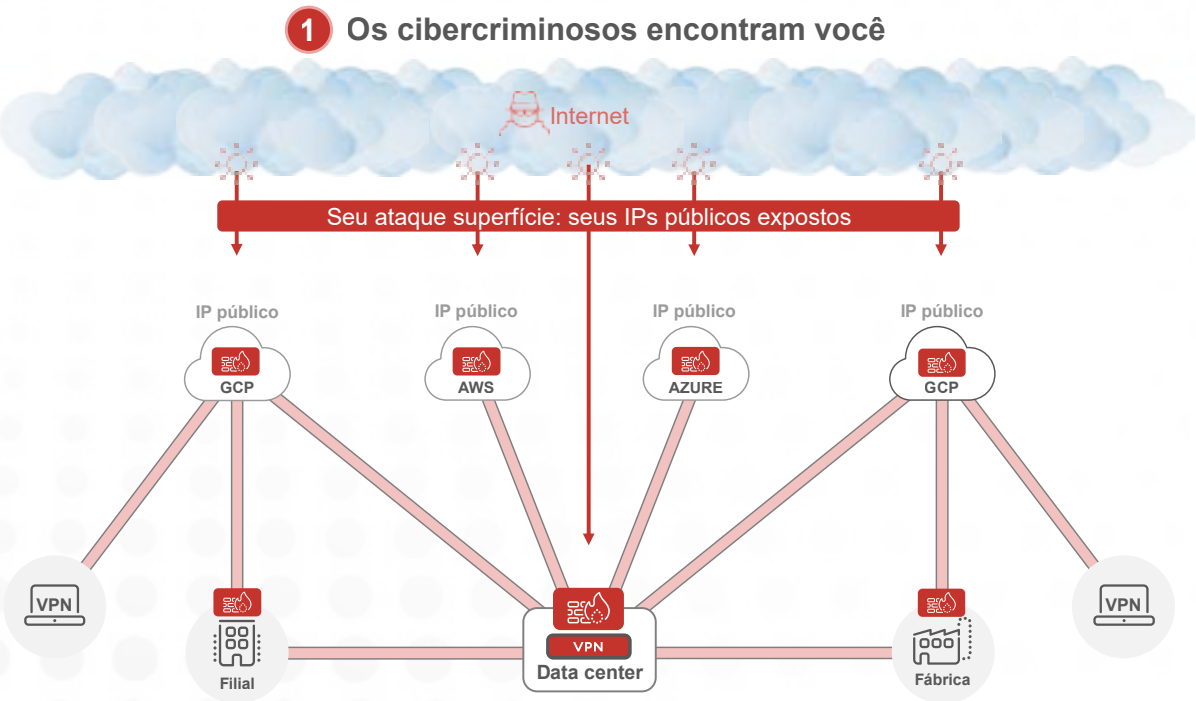
Nº 1

# Firewalls e VPNs expandem a superfície de ataque

Os cibercriminosos estão constantemente à procura de alvos que possam atacar, a fim de penetrar nas defesas das organizações e executar seus projetos mal intencionados. Infelizmente, com a forma como o trabalho é feito hoje, as arquiteturas baseadas em perímetro expandem a superfície de ataque e auxiliam inadvertidamente agentes mal-intencionados em seus esforços para identificar alvos atraentes.

Conforme mencionado anteriormente, continuar a usar uma rede em estrela no mundo moderno envolve estender continuamente essa rede para cada vez mais usuários remotos, dispositivos, recursos baseados na nuvem, filiais e mais. Isso significa efetivamente que uma rede plana e extensa é um tesouro crescente de recursos interconectados e que existem muitos caminhos (aplicativos na nuvem, usuários remotos, etc.) para os cibercriminosos explorarem como pontos de entrada nessa rede. Dito de forma simples, uma rede em constante expansão significa uma superfície de ataque em constante expansão.

**Como a arquitetura centrada em firewall e VPN aumenta o risco**




© 2024 Zscaler, Inc. Todos os direitos reservados.



Infelizmente, os problemas de superfície de ataque das arquiteturas baseadas em perímetro vão muito além do acima exposto, e isso se deve aos firewalls e VPNs. Estas ferramentas são os meios pelos quais os modelos de segurança de castelo e fosso supostamente defendem as redes em estrela, mas sua utilização traz consequências indesejadas.

Firewalls e VPNs possuem endereços IP públicos que podem ser encontrados na internet pública. Isso ocorre intencionalmente para que usuários legítimos e autorizados possam acessar a rede pela web, interagir com os recursos conectados nela e realizar seu trabalho. No entanto, esses endereços IP públicos também podem ser encontrados por agentes maliciosos que procuram alvos que possam atacar para obter acesso à rede.

Em outras palavras, firewalls e VPNs oferecem aos cibercriminosos mais vetores de ataque, expandindo a superfície de ataque da organização. Ironicamente, isso significa que a estratégia padrão de implantação de firewalls e VPNs adicionais para dimensionar e melhorar a segurança na verdade agrava ainda mais o problema da superfície de ataque.

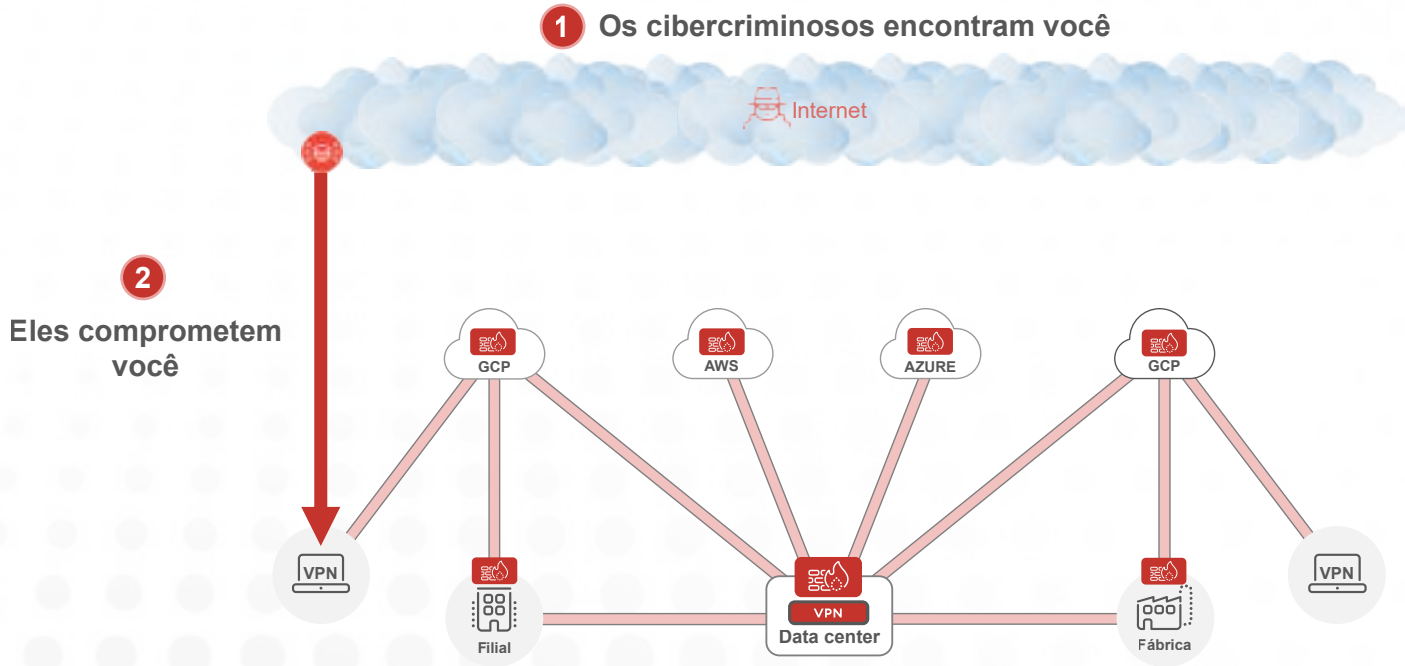
© 2024 Zscaler, Inc. Todos os direitos reservados.

# Nº 2 Firewalls e VPNs não conseguem evitar comprometimentos

Depois que os cibercriminosos identificam com sucesso um alvo atraente, eles lançam seus ataques cibernéticos na tentativa de penetrar nas defesas da organização. Infelizmente, mais uma vez, ferramentas tradicionais como firewalls e VPNs não são adequadas para proteger esta fase da cadeia de ataque.

Prevenir o comprometimento requer o uso de políticas de segurança integradas que interrompam as ameaças em tempo real, antes que elas consigam entrar no ambiente de uma organização e começar a causar danos. Isso, por sua vez, significa que as organizações devem ser capazes de inspecionar todo o tráfego em suas operações para que possam identificar quaisquer ameaças potenciais. Para conseguir isso, a capacidade de inspecionar o tráfego criptografado é extremamente importante, porque a grande maioria do tráfego da web hoje é criptografada, mais de 95%. Mas é aqui que outra fraqueza importante da arquitetura baseada em firewall e VPN se torna conhecida.

**Como a arquitetura centrada em firewall e VPN aumenta o risco**




© 2024 Zscaler, Inc. Todos os direitos reservados.

A inspeção do tráfego criptografado é um processo que consome muitos recursos, o que significa que é necessária uma grande quantidade de poder de computação para descriptografar, examinar e criptografar novamente o tráfego. Infelizmente, os dispositivos de segurança, como os firewalls, têm dificuldade para funcionar conforme necessário para conseguir isso, sejam eles implantados como dispositivos de hardware no local ou como dispositivos virtuais em uma instância de nuvem.

Isso ocorre porque os aparelhos possuem capacidades fixas para fornecer um determinado nível de serviço. Eles não podem ser ampliados indefinidamente para atender aos requisitos cada vez maiores de uma organização para inspeção de tráfego em tempo real, especialmente quando se trata de tráfego criptografado. Como resultado, as organizações que dependem de ferramentas e arquiteturas tradicionais ficam com uma inspeção incompleta do tráfego criptografado na melhor das hipóteses e, na pior, sem nenhuma inspeção do tráfego criptografado.

Deixar de inspecionar o tráfego criptografado em larga escala significa que as ameaças conseguem passar pelas defesas sem serem detectadas, permitindo que os invasores executem seus esquemas. Lamentavelmente, parece que os cibercriminosos tomaram consciência desse fato e começaram a utilizar o tráfego criptografado como meio preferido de execução dos seus ataques. Hoje, aproximadamente **86%** dos ataques cibernéticos ocorrem por meio do tráfego criptografado. Portanto, se uma organização não inspecionar seu tráfego criptografado, ela não conseguirá impedir a grande maioria das ameaças que tentam violar suas defesas. Simplificando, as arquiteturas de firewall e VPN não conseguem evitar comprometimentos.

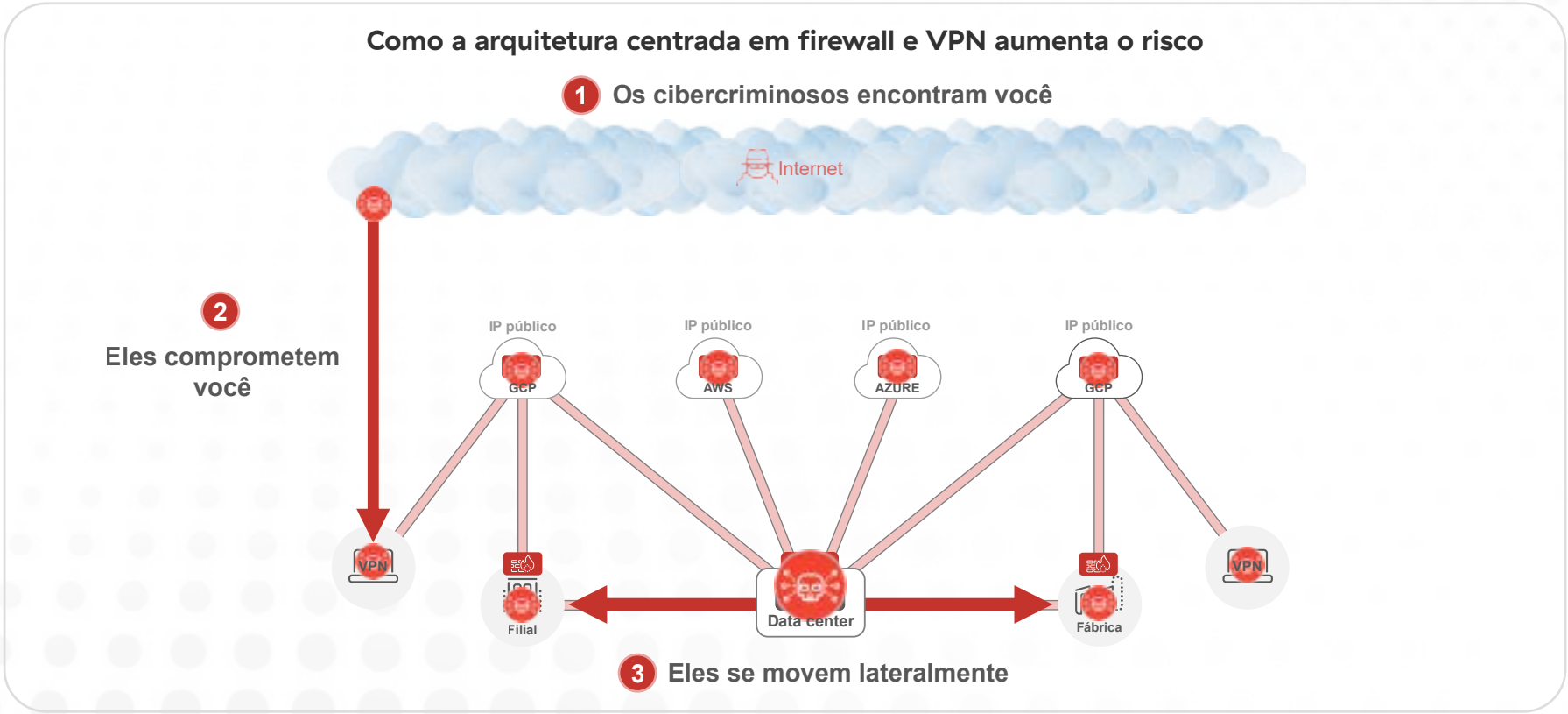


© 2024 Zscaler, Inc. Todos os direitos reservados.

# Nº 3 Firewalls e VPNs permitem a movimentação lateral de ameaças

Depois que o comprometimento ocorre e uma ameaça cibernética ultrapassa as defesas de uma organização, as fraquezas dos firewalls e das VPNs ficam totalmente expostas. A movimentação lateral de ameaças, também conhecida como propagação lateral, refere-se à maneira como as ameaças na rede podem acessar os vários recursos da organização, sejam eles aplicativos locais, cargas de trabalho em nuvens privadas ou instâncias de aplicativos SaaS. Raramente apenas um aplicativo é comprometido quando uma ameaça viola o perímetro de uma organização. Para compreender como a movimentação lateral de ameaças pode ocorrer, basta considerar a analogia contida na frase "segurança de castelo e fosso".

Um fosso é usado para defender um castelo; mais especificamente, para impedir que invasores tenham acesso ao castelo. Isso é feito para proteger as joias da coroa e as pessoas dentro da fortaleza. No entanto, se os atacantes conseguissem passar pelo fosso, o principal mecanismo de defesa do castelo seria inutilizado.




© 2024 Zscaler, Inc. Todos os direitos reservados.



Nesse caso, haveria pouca proteção restante para impedir que os inimigos saqueassem todo o castelo.

A fraqueza acima dos castelos e fossos também está presente ao usar firewalls e VPNs. Isso se deve à natureza altamente interconectada das redes em estrela nas quais algumas organizações ainda optam por confiar, bem como à forma como os modelos de segurança de castelo e fosso concentram os esforços de proteção contra ameaças na defesa do acesso à rede como um todo.

Basta imaginar os firewalls como o “fosso”, as VPNs como a “ponte levadiça” e a própria rede como o “castelo”. Assim que uma ameaça cibernética prevalece sobre o “fosso” e entra no “castelo”, o criminoso pode facilmente mover-se de um recurso conectado para outro, acessando os vários “cômodos” do “castelo”.

Para declarar tudo isso explicitamente, os firewalls e as VPNs permitem a movimentação lateral de ameaças e possibilitam que os cibercriminosos expandam o alcance de suas violações em toda a rede, causando enormes danos, interrupções e custos. Comprometimento em qualquer local significa efetivamente comprometimento em todos os locais. Embora a segmentação da rede seja frequentemente apresentada como a solução para esse problema, a tática inevitavelmente equivale à compra de cada vez mais firewalls, o que não consegue resolver os problemas arquitetônicos subjacentes inerentes às ferramentas baseadas em perímetro do passado.

© 2024 Zscaler, Inc. Todos os direitos reservados.

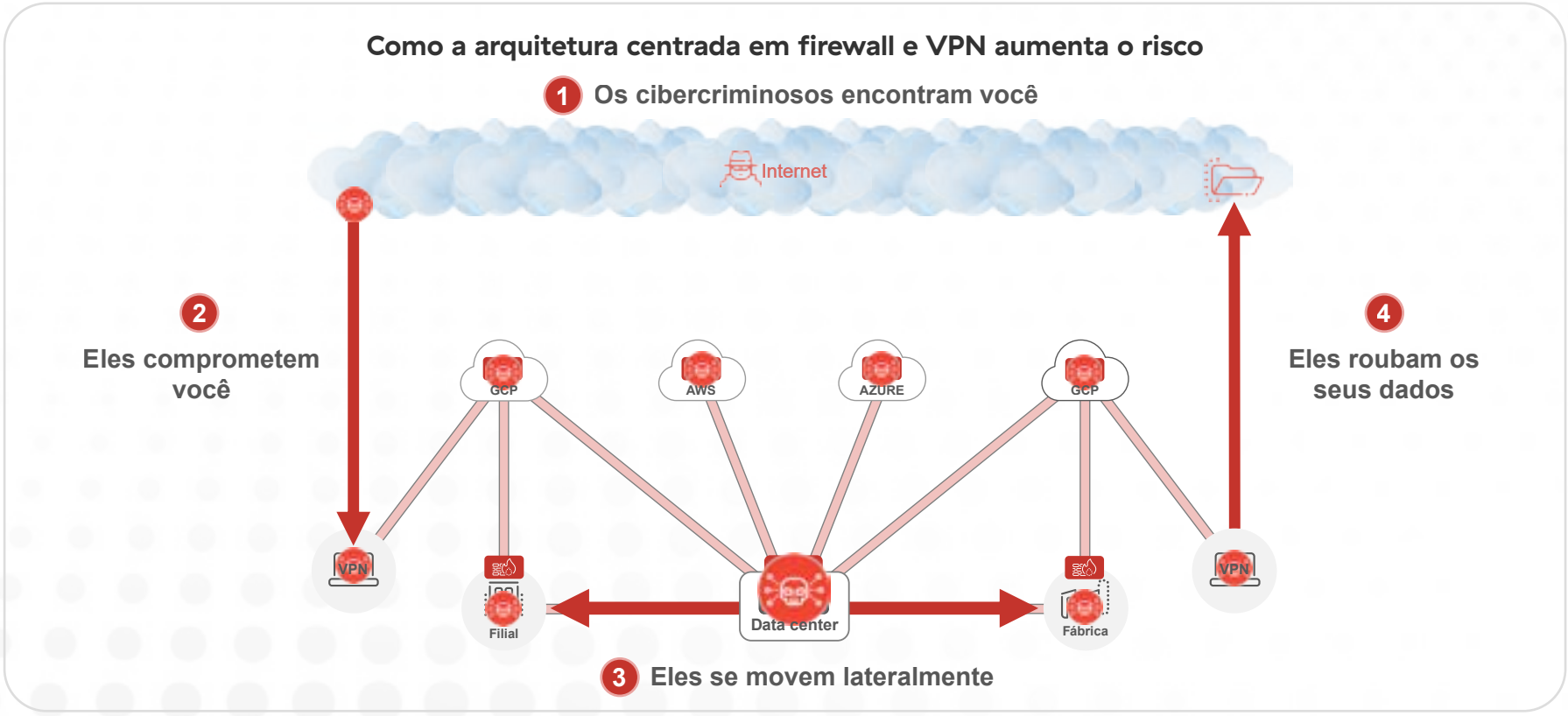
Nº 4

# Firewalls e VPNs permitem a perda de dados

Na grande maioria dos ataques cibernéticos, os criminosos não procuram violar as organizações apenas pela emoção. Em vez disso, eles têm um objetivo específico em mente, e esse objetivo é roubar informações sigilosas. Isso ocorre porque os dados roubados podem ser vendidos na dark web com um lucro significativo ou usados como alavancagem em um esquema de ransomware de dupla extorsão para pressionar uma organização a pagar um resgate. De qualquer forma, as repercussões podem ser catastróficas para qualquer organização.

Então, assim que os cibercriminosos encontrarem uma superfície de ataque, comprometerem as defesas e iniciarem a movimentação lateral (todos os três facilitados por firewalls e VPNs), eles procurarão o máximo de dados possível na rede, priorizando informações particularmente sigilosas ou regulamentadas. Naturalmente, isso é seguido pela exfiltração de dados.

Confiar em ferramentas tradicionais para interromper esse elo final da cadeia de ataque gera resultados arriscados mais uma vez e permite a perda de dados.




© 2024 Zscaler, Inc. Todos os direitos reservados.

Conforme mencionado anteriormente, mais de 95% do tráfego da web hoje é criptografado, a inspeção do tráfego criptografado requer grande capacidade de computação e os dispositivos estáticos não conseguem expandir conforme necessário para processar os enormes volumes de tráfego criptografado gerados por organizações em crescimento. Esse desafio (tanto para hardware quanto para dispositivos virtuais) é relevante não apenas para comprometimentos, mas também para perda de dados. Os cibercriminosos estão cientes de que as organizações são mais propensas a ter pontos cegos onde o tráfego é criptografado e estão usando esse tráfego como uma via preferencial para a exfiltração de dados.

Mas não é apenas por causa dos desafios de dimensionamento que ferramentas como firewalls são incapazes de impedir a exfiltração de dados. As tecnologias de ontem foram projetadas para o mundo de ontem, antes dos aplicativos na nuvem e dos trabalhadores remotos. Como resultado, elas não conseguem proteger os caminhos modernos de fuga de dados; por exemplo, a funcionalidade de compartilhamento integrada em aplicativos SaaS como Google Drive, Box, Microsoft OneDrive e outros. Da mesma forma, recursos na nuvem mal configurados, como buckets S3 da AWS definidos erroneamente como “públicos”, expõem dados, mas não podem ser corrigidos com firewalls, VPNs ou mesmo ferramentas convencionais de prevenção contra perda de dados (DLP).

Os invasores externos estão ansiosos para usar esses e outros meios modernos para roubar informações sigilosas; no entanto, é fundamental observar que não são a única ameaça aos dados. As organizações devem lidar com a realidade de que pessoas internas mal-intencionadas e descuidadas também podem vazar informações sigilosas das formas descritas acima. Independentemente do perpetrador, a segurança deve evoluir para que os dados sejam mantidos seguros.



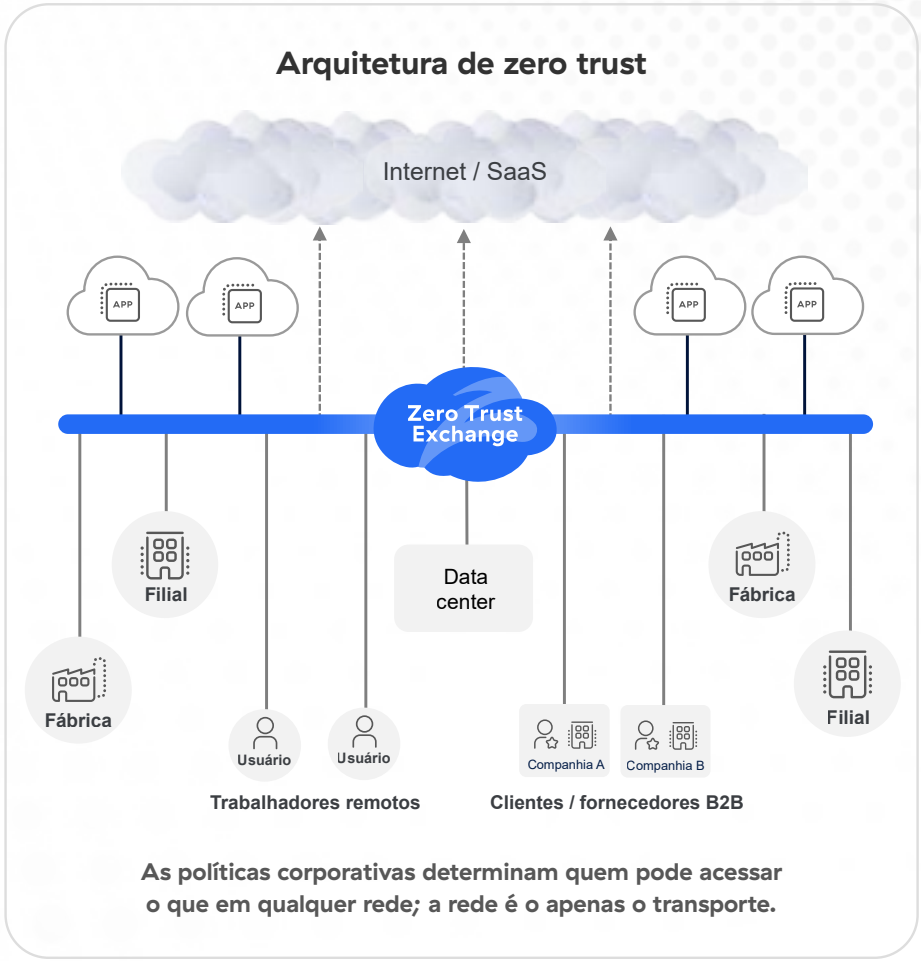
© 2024 Zscaler, Inc. Todos os direitos reservados.

# Como a arquitetura zero trust resolve esses problemas

O zero trust não é apenas mais uma ferramenta a ser adicionada ao status quo existente e centrado na rede. Não é algo que apenas diminui as dificuldades das arquiteturas baseadas em perímetro sem realmente resolver suas causas subjacentes. Em vez disso, o zero trust é uma arquitetura distinta que se baseia no princípio do acesso de privilégio mínimo; é inerentemente diferente de uma arquitetura padrão baseada em firewall e VPN.

Quando a arquitetura zero trust está em vigor, as organizações se beneficiam de uma nuvem de segurança global que atua como um painel de controle inteligente, conectando com segurança usuários, cargas de trabalho, dispositivos de IoT/TO e parceiros B2B, sem estender a rede a ninguém ou a nada. Ao mesmo tempo, a nuvem zero trust deve oferecer conjuntos abrangentes de soluções (como ameaças cibernéticas e proteção de dados) que são entregues como um serviço na borda, o mais próximo possível do usuário final.

**Com zero trust, a segurança e a conectividade são dissociadas da rede com sucesso, e as arquiteturas baseadas em perímetro tornam-se coisas do passado.**




© 2024 Zscaler, Inc. Todos os direitos reservados.



Com essa arquitetura moderna, as organizações podem acabar com as quatro formas pelas quais firewalls e VPNs as expõem a violações:

- **Minimizar a superfície de ataque:** aproveite o zero trust para impedir a expansão infinita da rede, elimine firewalls, VPNs e seus IPs públicos, evite conexões de entrada e oculte aplicativos atrás de uma nuvem zero trust.
- **Impedir o comprometimento:** inspecione todo o tráfego, incluindo o tráfego criptografado em larga escala, por meio de uma nuvem zero trust de alto desempenho que identifica ameaças e aplica políticas de segurança em tempo real.
- **Evitar a movimentação lateral de ameaças:** conecte usuários, cargas de trabalho e dispositivos diretamente aos aplicativos, em vez de conectá-los à rede como um todo, mantendo o princípio do acesso de privilégio mínimos.
- **Bloquear a perda de dados:** interrompa a perda de dados no tráfego criptografado e em todos os outros caminhos de vazamento de dados, incluindo dados em repouso na nuvem e dados em uso nos dispositivos dos funcionários.

Além de reduzir o risco de violações, uma arquitetura zero trust reduz a complexidade, aumenta a produtividade do usuário, economiza dinheiro e melhora o dinamismo organizacional, resolvendo uma variedade de problemas que afetam as arquiteturas baseadas em firewall e VPN.

© 2024 Zscaler, Inc. Todos os direitos reservados.

# Conclusão

Para aqueles que precisam de uma arquitetura zero trust, a Zscaler Zero Trust Exchange com tecnologia de IA é a plataforma certa. Sendo a maior e mais amplamente implantada nuvem de segurança integrada do mundo, sua escala e sucesso falam por si:

**Mais de 150**
Data centers globais

**Mais de 360 bilhões**
Transações protegidas diariamente

**500T+**
Sinais diários de telemetria

**Mais de 70**
Net Promoter Score

**40%**
Da Fortune 500 são clientes

**Líder**
No Gartner MQ para SSE

Para saber mais, inscreva-se em nosso webinar mensal, "Comece aqui: uma introdução ao zero trust." No webinar, discutimos a arquitetura zero trust a partir de uma perspectiva básica (bem como compartilhamos mais informações sobre a Zscaler) para que qualquer pessoa possa iniciar uma jornada zero trust com confiança.

© 2024 Zscaler, Inc. Todos os direitos reservados.

zscaler™ | Experience your world, secured.™

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

©2024 Zscaler, Inc. Todos os direitos reservados. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™, Zscaler Digital Experience, ZDX™ e outras marcas registradas listadas em **zscaler.com.br/legal/trademarks** são (i) marcas registradas ou marcas de serviço ou (ii) marcas comerciais ou marcas de serviço da Zscaler, Inc. nos Estados Unidos e/ou em outros países. Quaisquer outras marcas registradas são de propriedade de seus respectivos detentores.

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