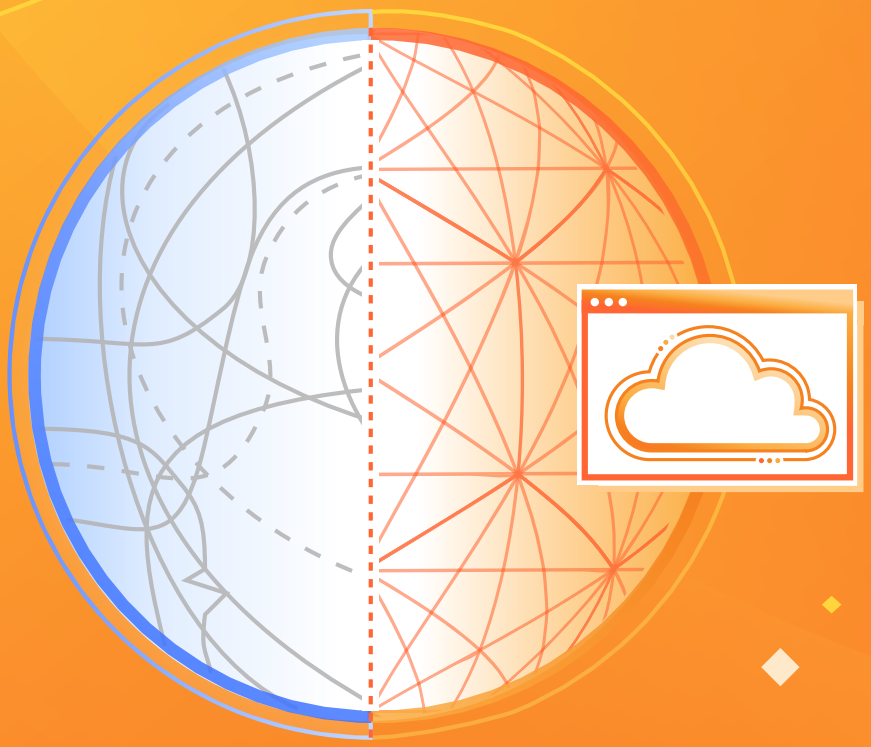
CLOUDFLARE

WHITE PAPER

Como desenvolver uma estratégia para a modernização da sua rede



Sumário

Redes obsoletas: um obstáculo para a modernização digital

A agilidade é essencial para se atingir a excelência em um mundo onde as condições de negócios podem mudar num piscar de olhos. Porém, a agilidade não é simplesmente uma questão de liderança e tomada de decisão: também depende da capacidade de uma organização para efetuar mudanças. Os sistemas devem ser estabelecidos de forma a serem flexíveis e a se adaptar sem entrar em pane. A empresa deve ser capaz de se realinhar para acomodar novos modelos de receita, ser compatível com novos aplicativos e conectar pessoas ao redor do mundo.

Agilidade é um dos principais resultados desejados para os projetos de modernização digital à medida que as organizações se reequipam para obter vantagem competitiva, o que é especialmente verdadeiro quando levamos em conta o estado da rede corporativa tradicional, que desempenha um papel essencial para produzir comunicações e capacitar a colaboração. A e por uma boa razão: foi projetada para resistir a choques no sistema, e a mudança cobra um alto custo e requer muito esforço.

Às vezes, as mudanças podem ser previstas porque acontecem ao longo do tempo, como, por exemplo, os efeitos da nuvem sobre o data center. Mas com o uso de redes, as forças exógenas do mercado estão impulsionando mudanças rápidas, às vezes da noite para o dia. A pandemia, por exemplo, nos deu lições dolorosas sobre a dificuldade enfrentada por algumas empresas para adicionar rapidamente uma capacidade para o trabalho remoto de forma a manter a produtividade dos funcionários e gerenciar custos dos funcionários e gerenciar custos, tendo em vista a parcela do orçamento que estava sendo consumida por redes ociosas em escritórios vazios.

Na tentativa de superar essas dificuldades, também se tornou evidente que algumas empresas não apenas foram capazes de se adaptar, mas também de prosperar. Não se tratou apenas de uma questão da capacidade da gerência no sentido de tomar as decisões de negócios corretas, mas também da capacidade de transformação e execução da empresa. No que se refere ao diretor de TI, é preciso desenvolver estratégias para lidar com a mudança, reequipar-se para facilitar as necessidades futuras e transformar a TI em um acelerador, não um retardador da mudança.

Com os enormes investimentos imobilizados em redes locais, modernizar não é uma decisão simples. Para concretizar plenamente os benefícios da modernização de redes, é necessário examinar o que precisa ser alcançado para definir o que precisa ser mudado.

Entendendo a jornada

Quando você reflete sobre as boas práticas de design de redes ao longo dos anos, a conclusão é de que há uma boa razão para tanta complexidade. Durante décadas, as organizações construíram e reforçaram suas redes acumulando camadas e mais camadas de novas tecnologias. A cada nova geração de design e com o advento de cada inovação, a rede se tornava mais complicada. A oportunidade de buscar simplicidade não estava disponível e, muitas vezes, o acréscimo de novas tecnologias tornava a velocidade, a resiliência e a segurança ainda mais complicadas.

Com os serviços de rede e segurança fornecidos na nuvem, estamos agora na vanguarda da próxima mudança geracional no design das redes corporativas. Ao utilizar os serviços fornecidos na nuvem como uma extensão da rede, as organizações são capazes de enfrentar novos casos de uso, ampliar sua cobertura e proteger aplicativos muito além do data center, o que representa a oportunidade de uma enorme simplificação da rede, já que a prestação de serviços se baseia na conexão existente entre a rede e o PoP do provedor de nuvem sem que a conexão seja interrompida para inserir outro dispositivo. A rede estabelecida entre a rede local e o serviço na nuvem permanece a mesma, enquanto os serviços incluídos no serviço na nuvem são inseridos e consumidos.

O problema é que nem todas as plataformas de rede e segurança fornecidas na nuvem são construídas da mesma forma, e nem sempre é fácil ver o que as diferencia uma da outra. Muitas têm uma vantagem limitada na jornada de modernização. Para entender as diferenças, é necessário mapear seus objetivos de modernização de rede de modo a evitar a substituição de uma fonte de complexidade por outra.

Quatro caminhos essenciais do tráfego de rede

Ao avaliar o escopo do seu projeto de modernização de rede, considere que sua rede cobre um grande número de pontos de contato, alguns dos quais atravessam a mesma infraestrutura (por exemplo, o tráfego de entrada, saída e leste-oeste passa através da sua rede principal), enquanto outros operam fora dela (como, por exemplo, sua rede de nuvem pública).

Tráfego de entrada: considerando-se que partes da rede estão expostas à internet, é necessário manter defesas de entrada para fornecer proteção contra tentativas de incapacitar ou explorar a empresa e, ao mesmo tempo, permitir o tráfego de usuários legítimos. As defesas de perímetro tradicionais podem ficar sobrecarregadas e exigir recursos para lidar com negações de serviço distribuídas.

Tráfego de saída: as conexões com a internet e aplicativos baseados em nuvem requerem políticas que fornecem proteções para o uso corporativo seguro, como a proteção contra ameaças e exfiltração de dados. Devido à variabilidade na localização de um usuário, as organizações implementaram uma combinação de tecnologias de proteção de saída que incluem dispositivos locais como firewalls (para quando o usuário está na rede) e resolvedores de DNS, além de proxies baseados em nuvem como SWG e CASB. (para quando o usuário estiver remoto).

Rede WAN: a rede WAN e seus respectivos limites, incluindo o campus e a filial, estão sendo reprojetados para favorecer iniciativas que colocam a nuvem em primeiro lugar e dispositivos habilitados para IoT. Desta forma, a topologia de rede tradicional está desfazendo o backhaul para o data center em favor de arquiteturas do tipo direto para a internet. Com os rápidos avanços das redes nessas áreas, a inserção da segurança, por outro lado, se tornou mais complexa. Em muitos casos, os caminhos de tráfego interno permanecem dependentes de dispositivos de segurança implementados na borda, impedindo o progresso transformacional da organização.

Rede na nuvem pública: à medida que as organizações desenvolvem seus aplicativos em diversas nuvens, fica cada vez mais difícil estabelecer e manter configurações de rede e segurança ponto a ponto. Configurar e gerenciar a rede consome tempo e recursos — um tempo que é mais bem gasto no desenvolvimento de projetos.

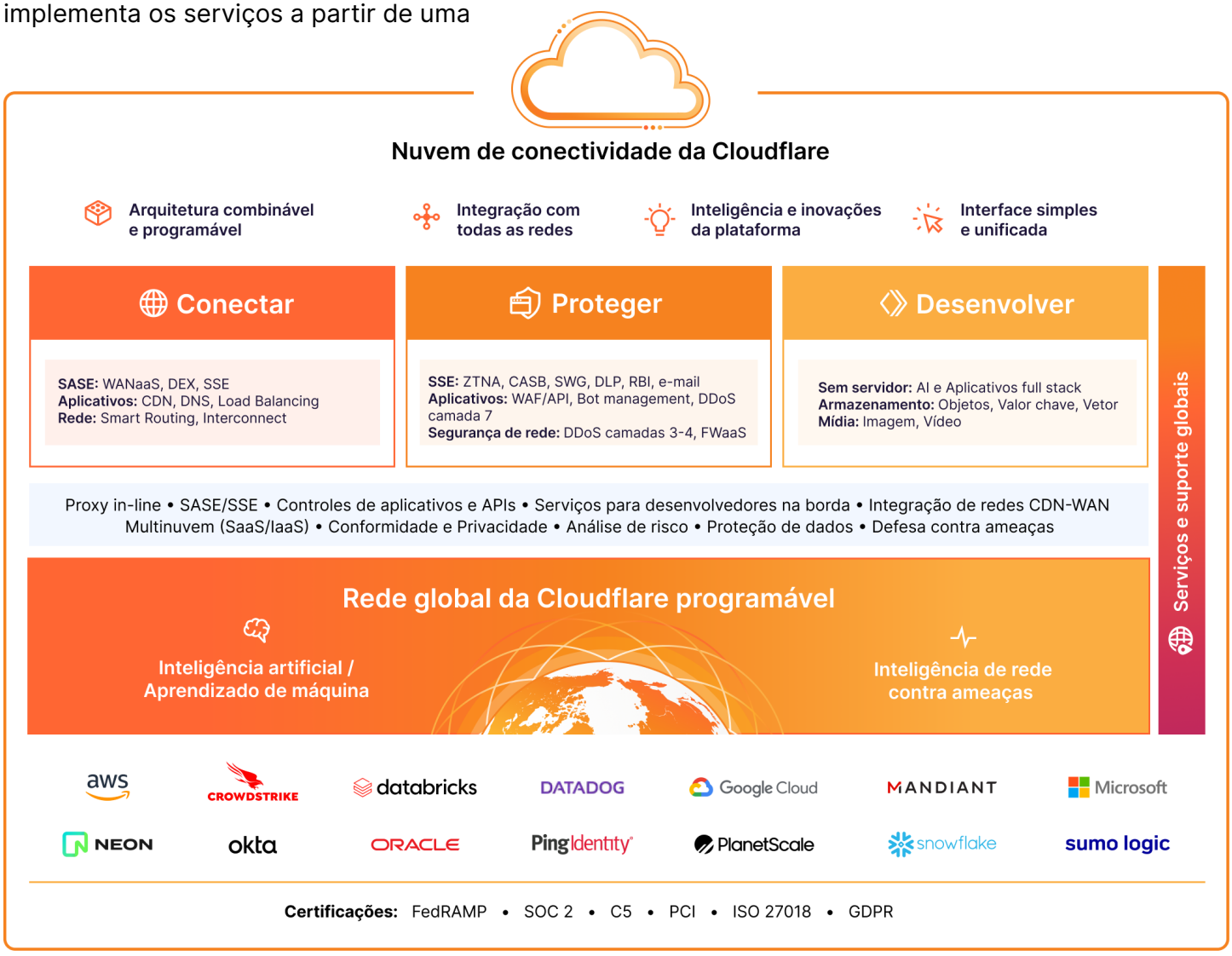
Cada um desses caminhos de tráfego conta com uma série de tecnologias que as organizações implementam em sua rede ou consomem a partir da nuvem. Considerando-se que os projetos de modernização envolvem os caminhos do tráfego em diversas direções, é preciso planejar a jornada completa de modernização da rede nas quatro direções para evitar um erro de arquitetura que limite os benefícios transformacionais alcançáveis ou requeira múltiplas tecnologias díspares para lidar com casos de uso não abordados.

Nuvem de conectividade da Cloudflare

Recomendamos que, na sua modernização de rede, você pense em adotar a nuvem de conectividade da Cloudflare, concebida com uma filosofia que utiliza uma arquitetura combinável e programável para fornecer serviços de rede e segurança aos seus usuários e também em toda a infraestrutura e aplicativos da empresa habilitados para nuvem. Como resultado, tanto as necessidades atuais quanto futuras da sua jornada de modernização serão abordadas.

Com a Cloudflare, você pode acrescentar funcionalidades e dar suporte a novos casos de uso habilitando serviços em vez de inserir dispositivos. A conexão com um data center Anycast da Cloudflare continua a mesma, enquanto você configura e implementa os serviços a partir de uma interface de gerenciamento unificada para processar tráfego. Você pode satisfazer suas necessidades atuais e, ao mesmo tempo, implementar uma plataforma que dê suporte a casos de uso futuros e apoio a toda a sua jornada de modernização.

Em vez de construir sua própria infraestrutura global, use a nossa. Sua organização irá se beneficiar da velocidade fornecida por meio da rede global da Cloudflare, com a rapidez de um raio. Por meio de conexões diretas com praticamente todos os provedores de serviços e de nuvem, a rede da Cloudflare é capaz de alcançar 95% da população mundial conectada à internet a uma distância de aproximadamente 50 ms.



Principais casos de uso para a modernização de rede

Para começar, aborde casos de uso que proporcionem maior impacto sobre os negócios e o benefício mais significativo para a sua organização. Esses casos de uso não são prescritos em uma ordem específica, já que suas prioridades são exclusivas da sua empresa. O importante é atender às necessidades no curto prazo e, ao mesmo tempo, desenvolver uma arquitetura que irá facilitar sua jornada de arquitetura que irá facilitar sua jornada de modernização de rede, independentemente do caminho que você escolher.

	Projetos de modernização
Conectividade de filiais Reduza seus custos, aprimore a experiência do usuário	• Transição de MPLS para a nuvem de conectividade • Transição de SD-WAN para a nuvem de conectividade
Proteção da sua infraestrutura voltada para o público Prolongue a vida útil dos seus investimentos em FW e DMZ	• Redução da carga nos firewalls de rede • Transferência da segurança da DMZ para a nuvem de conectividade
Simplificação da sua rede corporativa Implemente o Zero Trust para aumentar a segurança e reduzir as despesas de capital	• Redução/eliminação da DMZ • Substituição da VPN pelo ZTNA • Eliminação da confiança elevada na LAN • Aceleração da sua conectividade para F&A
Conexão e proteção das suas nuvens Use o melhor de cada nuvem nos seus aplicativos	• Criação e proteção de aplicativos • Aproveitamento dos serviços para desenvolvedores de modo a centralizar as funções principais

Conectividade de filiais

Um componente importante da rede WAN é conectar locais menores, como filiais ou lojas, que dependem da conexão de usuários e dispositivos a aplicativos. As arquiteturas hub and spoke tradicionais vinculavam sites ao data center usando circuitos MPLS caros, mas com a crescente necessidade crescente de oferecer suporte aos aplicativos em nuvem, mais organizações estão usando arquiteturas de acesso direto à internet com banda larga.

A SD-WAN procurou tornar a conectividade de rede mais confiável, mas tem uma relação imperfeita com a inserção de segurança. A maioria das arquiteturas de SD-WAN dependem de dispositivos pesados na borda e firewalls locais para implementar políticas de segurança na malha SD-WAN e usam apenas a integração SSE/SASE para o tráfego de saída.

Use a nuvem de conectividade da Cloudflare para a conectividade de filiais e para apoiar você ao longo de todo o seu caminho de migração, seja aumentando ou substituindo os serviços obsoletos. A Cloudflare usa uma arquitetura baseada na filosofia “borda leve/nuvem pesada” para fornecer serviços de rede e segurança. Facilite a conectividade entre sites nos locais de rede — escritório de filiais, lojas ou fábricas — com a Magic WAN da Cloudflare. A solução fornece uma conectividade e roteamento seguros e de alto desempenho para toda a sua rede corporativa, reduzindo os custos e a complexidade operacional. Para fins de segurança, o Magic Firewall da Cloudflare é implementado de forma integrada junto com a Magic WAN, permitindo que você implemente políticas de controle de rede, seja no sentido Norte/Sul ou Leste/Oeste, à medida que o tráfego transita pela rede da Cloudflare.

Proteção da sua infraestrutura voltada para o público

A rede empresarial e a DMZ são endereçáveis e expostas à internet e exigem medidas para impedir que os invasores causem danos. Em um mundo perfeito, os firewalls de rede tradicionais poderiam inspecionar e eliminar todo o tráfego indesejado, mas cada firewall tem capacidades finitas (largura de banda disponível, utilização/computação, contagem de sessões etc.). A probabilidade de sucesso do invasor é simplesmente uma questão de escala, ou seja, se o invasor consegue ou não gerar ruído suficiente para sobrecarregar a capacidade da empresa de operar em diferentes camadas de protocolo de rede.

Não se trata apenas do volume do tráfego. Aceitar o tráfego de entrada abre a superfície de ataque para tráfego não autenticado/pré-autenticado. Falhas em aplicativos e sistemas operacionais podem ser exploradas por um invasor que nem possui conta no sistema. O preenchimento de credenciais e o uso da inserção de nomes de usuário/senhas obtidos em outras violações também representa uma importante fonte de risco. Ao aplicar os princípios de Zero Trust a aplicativos na DMZ, as organizações podem reduzir a exposição à internet e eliminá-la sempre que for possível.

As organizações podem aprimorar a proteção da rede aplicando princípios de defesa profunda para absorver o tráfego mal-intencionado a montante da infraestrutura pública da organização. O Magic Transit da Cloudflare com o Magic Firewall integrado, implantado por meio da rede Anycast da Cloudflare, atua como uma porta de entrada para a organização, filtrando o tráfego mal-intencionado e desnecessário e distribuindo apenas um tráfego de entrada limpo.

Após a mitigação de DDoS realizada pelos firewalls de rede, um dispositivo ainda precisa processar a conexão antes de poder descartá-la. Com a Cloudflare, nossa rede transmite o prefixo do cliente, atraindo, assim, o tráfego que de outra forma seria destinado ao firewall do perímetro. Graças à Anycast, estamos absorvendo com eficácia os ataques de DDoS ao distribuirmos a carga por todos os nossos data centers. Os membros da botnet enxergam o PoP da Anycast mais próximo, que processa o tráfego de acordo com as políticas do Magic Transit e do Magic Firewall.

Simplificação da sua rede corporativa

A simplificação gera uma série de benefícios de modernização. As equipes de TI podem tornar a rede mais confiável se o projeto tiver menos componentes sujeitos a falhas, além de torná-la mais segura adotando uma abordagem Zero Trust de negar tudo para os privilégios de acesso.

Para simplificar sua rede, pense em uma...

Migração da DMZ

As DMZs de rede representam uma dor de cabeça operacional por serem particularmente sensíveis à exploração de dia zero: um invasor não requer acesso à rede interna para se comunicar com os servidores na DMZ e, portanto, as organizações precisam permanecer vigilantes para evitar exploração e abuso.

No entanto, embora tenham desempenhado um papel importante no passado, as DMZs ainda são necessárias hoje? A importância da DMZ como uma construção de rede está diminuindo porque existem formas alternativas de construir e hospedar aplicativos.

- No caso dos aplicativos voltados para o público, a migração das cargas de trabalho para a nuvem pública traz benefícios técnicos e econômicos.
- Com o SaaS, muitos tipos de aplicativos públicos e privados não precisam ser executados na infraestrutura gerenciada pelo cliente.

Assim sendo, torna-se pragmático, do ponto de vista da segurança e do design de rede, começar a pensar em como reduzir ou eliminar a necessidade de uma DMZ, o que não apenas faz sentido do ponto de vista operacional, mas também simplifica bastante a arquitetura ao eliminar a infraestrutura de rede, como, por exemplo, o firewall, o WAF e os balanceadores de carga que lhe dão apoio.

E o que dizer dos aplicativos privados colocados na DMZ para conceder acesso aos funcionários, parceiros e prestadores de serviços? Seria mais seguro isolá-los em uma rede privada e conceder o acesso a funcionários e parceiros utilizando o Acesso à Rede Zero Trust (ZTNA).

Com o ZTNA, você reduz a superfície de ataque com eficácia ao eliminar o tráfego de rede de entrada no aplicativo. O ZTNA usa um acesso contextual e intermediado aos recursos por meio da nuvem de conectividade da Cloudflare, eliminando a necessidade de abrir portas no firewall da rede e, ao mesmo tempo, fornecendo à equipe de segurança uma visibilidade total sobre quem tem acesso a qual recurso.

Substituição da VPN pelo ZTNA

Os dias de uso das VPNs para acessar aplicativos estão contados. Do ponto de vista do design de rede, é impraticável restringir os usuários dentro de um túnel muito longo para acessar a internet e a nuvem. Além disso, colocar os usuários (e endpoints possivelmente comprometidos) na rede com uma VPN representa um enorme risco de segurança.

O acesso a aplicativos tampouco é a única função de uma VPN. Existem situações em que as organizações precisam de uma conectividade de rede mais ampla com um endpoint, como no caso da administração de endpoints e de comunicações iniciadas pelo servidor. Esses casos de uso, tradicionalmente, aproveitam a conectividade de rede da VPN em ambas as direções, um desafio que emperrou os primeiros produtos ZTNA lançados no mercado. Sem outra alternativa, as organizações passaram a executar o ZTNA e a VPN paralelamente.

Para modernizar sua infraestrutura de rede, as organizações podem consolidar suas funções com o ZTNA da Cloudflare porque, com a Cloudflare, as organizações podem ser compatíveis tanto com os casos de uso clássicos do ZTNA quanto com o tráfego bidirecional e iniciado pelo servidor. Essas funções ajudam as organizações a reduzir suas necessidades de acesso a aplicativos eliminando a VPN, além de aumentar ainda mais a segurança e a simplicidade.

Eliminação da confiança elevada na LAN

Com o trabalho híbrido, as diferenças entre a forma de trabalhar no escritório ou em qualquer outro local estão diminuindo. Na verdade, isso é especialmente verdadeiro quando os usuários trabalham com frequência em redes públicas não confiáveis, como as de cafeterias e espaços de trabalho compartilhados.

De certa forma, a rede pública aberta é a personificação do Zero Trust: ninguém tem acesso privilegiado e nada nem ninguém são considerados confiáveis. Se, em princípio, isso pode funcionar em um espaço de trabalho compartilhado, no home office e em uma cafeteria, por que a confiança não poderia também ser eliminada da rede corporativa?

A eliminação da confiança não requer uma sofisticação do design da rede, mas sim uma simplificação. Em vez de criar um acesso elevado para usuários autenticados e usar políticas de rede para abrir conexões com os recursos, é muito mais seguro pressupor que a rede inteira é não confiável. Com a expressão da segurança por meio do SASE, as organizações podem obter acesso aos aplicativos de que necessitam, com a segurança adequada para torná-los seguros, sem requerer qualquer suposição de confiança na rede propriamente dita. O Zero Trust não consiste em adicionar confiança à rede, mas em removê-la até que alcancemos um estado melhor e mais seguro sem as permissões explícitas e excessivas do passado.

Aceleração da conectividade para F&A

As organizações utilizam as fusões e aquisições como uma ferramenta para adquirir acesso a recursos e capacidades de negócios que, de outra forma, não estariam imediatamente disponíveis. Para capitalizar a oportunidade, as organizações precisam executar o processo rapidamente para tornar a empresa combinada melhor do que a soma de suas partes. No entanto, muitas vezes a TI não é capaz de se movimentar rapidamente porque os aplicativos e a infraestrutura de rede subjacente de duas organizações raramente se integram com facilidade.

Para acelerar a conectividade F&As, as organizações podem abordar o acesso a aplicativos como uma tarefa separada da integração de redes. O cronograma para projetar uma arquitetura de rede convergente pode se estender por vários anos, mas o acesso aos aplicativos não precisa depender de um marco de referência tão distante.

Isso ocorre porque a situação no primeiro dia é, na verdade, um caso de uso de Zero Trust, em que usuários confiáveis em redes não confiáveis ainda precisam de acesso aos aplicativos. Conceda o acesso usando o Cloudflare One, que fornece os meios para permitir conectividade em F&As sem se condicionar ao acesso à rede convergente.

Conexão e proteção das suas nuvens

À medida que o desenvolvimento da nuvem evolui, os componentes de uma nuvem se tornarão benéficos por serem reaproveitados em outra. Da mesma forma como irão se tornar multinuvem ao longo do tempo, todas as organizações precisarão gerenciar redes de nuvem pública ao longo do tempo. O desenvolvimento de aplicativos tende a ser tribal por natureza, com o DevOps em diferentes partes da organização preferindo as ferramentas com as quais está mais familiarizado. No entanto, o desenvolvimento dos recursos organizacionais para gerenciar a conectividade entre nuvens é complexo, já que o trabalho abrange conjuntos de ferramentas criados em estruturas totalmente diferentes.

Outro aspecto da complexidade multinuvem é a situação da nuvem híbrida. Uma nuvem híbrida combina a nuvem privada local com nuvens privadas virtuais. Às vezes, essas redes são criadas com redes dedicadas, como o Direct Connect da AWS, que podem ser caras e limitadas a apenas uma nuvem. À medida que criam aplicativos multinuvem, as organizações não vão querer necessariamente incorrer nos custos de uma rede dedicada para cada nuvem.

Em vez de criar redes e segurança diretamente de um aplicativo para outro, use a Cloudflare para orquestrar e conectar serviços de rede em nuvem pública. Acreditamos que a nuvem de conectividade da Cloudflare desempenha um papel ideal em uma arquitetura como essa, estando situada de forma ideal como um trânsito para o tráfego que passa entre nuvens ao longo da extensa rede da Cloudflare. Com a adição de recursos de gerenciamento de rede em nuvem pública, agora os clientes também podem orquestrar a configuração da conectividade da carga de trabalho por meio da Cloudflare.

Nossa rede na nuvem pública abrange mais do que a simples orquestração da infraestrutura subjacente. A plataforma para desenvolvedores fornece um rico ecossistema de tecnologia básico desenvolvido com software livre e padrões abertos. Nossa arquitetura vai mais além, ao fornecer serviços para desenvolvedores disponíveis para compilação e integração com aplicativos multinuvem. Você pode optar por usar todos os elementos da plataforma para desenvolvedores ou apenas aqueles que você escolher, sem ficar restrito a serviços específicos em uma determinada nuvem.

Próximas etapas

Para dar os próximos passos em sua jornada de modernização de rede, entre em contato com a Cloudflare e deixe-nos ajudar você a desenvolver uma estratégia. Trabalhamos em estreita colaboração com milhares de clientes durante a transição de sua arquitetura para a nuvem de conectividade da Cloudflare.

Para obter mais informações, acesse: http://www.cloudflare.com/pt-br

+55 (11) 3230.4523 | enterprise@cloudflare.com | www.cloudflare.com/pt-br/

REV:BDES-5483.2024JAN30