Akamai

WHITE PAPER

Um modelo para o Zero Trust Network Access

Quem deve ler este guia?

Arquitetos de rede, engenheiros de segurança, CTOs, CISOs e outros tomadores de decisão de TI e de segurança se beneficiarão com a leitura deste guia.

Para os responsáveis pela definição do escopo, configuração, implantação, implementação e gerenciamento de um projeto Zero Trust Network Access (ZTNA), este guia fornece uma revisão abrangente dos benefícios potenciais e das diferenças entre os diferentes sistemas. O guia inclui:

- As limitações e falhas de segurança nas antigas abordagens de acesso a aplicações e por que o ZTNA é necessário
- Os componentes do ZTNA e como ele funciona
- Como o Akamai Enterprise Application Access e o Akamai MFA podem entregar o ZTNA de forma rápida e fácil

À medida que o mundo dos negócios muda e as ciberameaças aumentam, as empresas estão encarando de uma nova forma suas defesas cibernéticas. Muitos perceberam que a arquitetura de rede tradicional, que dependia de um local centralizado onde todas as partes pudessem acessar aplicações, deixa-os vulneráveis. Essa abordagem de castelo e fosso em relação à segurança, protegendo o perímetro e assumindo que todos dentro dele sejam seguros, deixa as empresas em risco de ataques cibernéticos no cenário atual de conexões móveis e na nuvem. Em vez disso, empresas inovadoras estão recorrendo ao conceito de arquitetura Zero Trust para proteger ativos vitais. Um princípio fundamental de qualquer projeto Zero Trust é proteger a rede. Este white paper detalha como as abordagens tradicionais de hub-and-spoke para a segurança de rede não são mais suficientes e como a mudança para o ZTNA pode defender melhor os ativos críticos e servir como o principal ponto de partida para uma arquitetura Zero Trust abrangente.

O ritmo das mudanças para as empresas nunca foi tão rápido

A forma como as empresas operam e usam a tecnologia está evoluindo e a um ritmo cada vez mais rápido. A evolução da computação levou a uma rápida transição da hospedagem de aplicações de negócios em data centers locais para o uso de várias nuvens públicas, nuvens privadas ou uma abordagem híbrida (tanto no local quanto na nuvem pública/privada).

A evolução do modelo de negócios também estimulou o aumento da colaboração entre as entidades e a necessidade de fornecer aos parceiros e fornecedores acesso a aplicações e recursos.

Por fim, à medida que as empresas continuam a adotar o trabalho remoto ou híbrido, os usuários passaram a acessar aplicações e recursos de negócios de qualquer lugar, tanto em dispositivos gerenciados quanto não gerenciados.

Com essas mudanças, as antigas abordagens para gerenciar o acesso a aplicações não são mais suficientes, e as empresas agora devem adotar uma nova abordagem que permita o acesso seguro, independentemente de onde as aplicações estão hospedadas ou onde os usuários estão localizados.

Acesso a aplicações antigas

Há mais de 20 anos, as empresas confiam em firewalls para construir um perímetro de segurança forte e confiam nos usuários que estão dentro desse perímetro. Isso é o mesmo que tratar as redes como se fossem castelos com fossos: paredes espessas e portões fortemente protegidos formam o perímetro para proteger o castelo (ou, nesse caso, a rede) e somente usuários com as credenciais corretas têm acesso permitido. Uma vez lá dentro, os usuários podem acessar aplicações específicas com base em sua identidade, que é entregue por meio de soluções de provedor de identidade (IdP), como o Microsoft Active Directory.

No entanto, com redes planas, os usuários realmente têm acesso de IP a toda a rede, o que significa que podem descobrir outros servidores e aplicações. Por exemplo, se o IdP estiver configurado corretamente, um usuário poderá encontrar o servidor no qual a aplicação de folha de pagamento está hospedada, mas quando tentar fazer login na aplicação, o acesso será negado.

Para corrigir esse problema de movimento lateral irrestrito, as empresas particionaram as aplicações por meio de VLANs (redes de acesso local virtual) em segmentos separados atrás de um firewall e aplicaram regras agora arcaicas baseadas em intervalos de IP para usuários individuais ou grupos. Este processo é frágil e muito sujeito a erros. Considere um cenário em que alguém esteja fazendo manutenção e mova as máquinas para um novo rack ou precise gerar um novo IP para elas para um novo intervalo. De repente, os usuários são impedidos de entrar e as chamadas de suporte chegam. Ou talvez uma atualização de software exija alterações na arquitetura de uma aplicação e os usuários sejam redirecionados para outra máquina como parte do fluxo de trabalho. Essa máquina pode então ficar inacessível a determinados usuários ou grupos porque as regras de firewall não foram atualizadas.

Essa arquitetura é extremamente complexa e requer um alto grau de comunicação entre proprietários de aplicação, administradores de rede e grupos de segurança durante quaisquer alterações para garantir tempo de inatividade zero.

Sabemos o que acontece frequentemente quando essa coordenação falha. Os administradores desejam seguir as práticas recomendadas, mas em momentos de desespero, adicionam a temida regra IP ANY/ANY ALLOW como uma solução rápida para permitir que os usuários afetados acessem tudo até que o problema subjacente possa ser diagnosticado e reparado. No entanto, muitas vezes não há tempo para voltar e reverter essas alterações, e essas correções rápidas diminuem a postura de segurança de uma empresa ao longo do tempo.

VPNs adicionam complexidade, desempenho e desafios de segurança

Para usuários remotos, uma VPN (rede virtual privada) geralmente fornece acesso a aplicações locais hospedadas dentro do perímetro, que, em seguida, fornecem acesso direto por túnel à rede da empresa.

Para gerenciar o acesso dos usuários a aplicações, as empresas geralmente adicionam controladores de entrega de aplicações dedicados ou usam os controles de acesso integrados às suas soluções de VPN. O objetivo é alinhar as permissões de acesso às aplicações, independentemente de onde o usuário esteja localizado. Se um usuário tiver acesso negado à aplicação CRM quando estiver dentro do perímetro, ele deverá ter acesso negado quando estiver conectado por meio da VPN. Embora esse seja o objetivo, as complexidades da sincronização de permissões de aplicações entre os dois casos de uso e as correções rápidas podem levar os usuários a adquirir acesso não intencional às aplicações.

Acesso a aplicações para prestadores de serviços, parceiros e fornecedores

As empresas também geralmente usam VPNs para permitir o acesso remoto a aplicações para prestadores de serviços, empresas parceiras ou fornecedores. Por exemplo, uma empresa pode permitir o acesso externo a seus sistemas financeiros para permitir que os fornecedores enviem faturas. Permitir o acesso de terceiros a aplicações por meio de uma VPN introduz riscos de segurança adicionais, pois a empresa não mantém mais a segurança completa. Se um dispositivo de terceiros com acesso VPN ficar comprometido, os invasores poderão obter acesso à rede da empresa.

VPNs e desempenho

A mesma compensação acontece com o desempenho. Na forma mais simples de uma VPN, todo o tráfego é redirecionado para a infraestrutura do data center. Isso pode resultar em acesso extremamente lento a propriedades da Internet e aplicações de software como serviço (SaaS) devido ao hairpinning, que efetivamente duplica o tráfego.

Para superar esse obstáculo de desempenho, muitas vezes, os administradores implantam túneis divididos, novamente marcando quais intervalos de IP devem viajar pela VPN e quais devem sair diretamente para a Internet. Isso pode ser simples e eficaz quando você possui apenas um perímetro interno. No entanto, isso começa a ficar muito mais complexo à medida que você adiciona vários data centers e provedores de nuvem privada virtual. Os administradores devem então determinar se instalarão agregadores VPN em cada data center e como gerenciarão efetivamente os túneis divididos multiponto.

Não é que as VPNs não agreguem valor. Longe disso, na verdade. O acesso website a website para múltiplas infraestruturas de data center é um caso em que elas se destacam. No entanto, o acesso em nível de rede não é o paradigma correto para os usuários que acessam aplicações, pois o acesso em nível de rede impõe um comprometimento não natural entre simplicidade e segurança/desempenho.

O acesso a aplicações baseadas em rede é uma boa notícia para os invasores

Até agora, focamos nos riscos e desafios associados à concessão de acesso em nível de rede a todos os funcionários. No entanto, essa abordagem também expõe as empresas a outro risco: os cibercriminosos que exploram credenciais de usuário roubadas ou uma vulnerabilidade de segurança também têm o potencial de obter acesso irrestrito em toda a rede. Por exemplo, se um invasor tiver acesso VPN usando credenciais de funcionários comprometidas, ele poderá mover-se lateralmente pela rede para encontrar, acessar e atacar alvos de alto valor.

Essas abordagens abrem a possibilidade de uma violação catastrófica

Teoricamente, é possível gerenciar o acesso a aplicações com segurança e com o mínimo de atrito usando essas abordagens. Talvez você já esteja usando alguma combinação delas. O problema é que implementá-las bem, mantê-las e fornecer segurança e desempenho adequados ao longo de sua vida útil é muitas vezes complexo demais do ponto de vista operacional para que tudo esteja sempre correto. Em muitos casos, as empresas se convencem de que, como os funcionários podem acessar suas aplicações, tudo deve estar funcionando perfeitamente. Eles então são pegos de surpresa quando uma dessas soluções rápidas resulta em uma violação catastrófica ou degrada o desempenho tão severamente que há uma interrupção ou a produtividade dos funcionários é significativamente limitada.

Uma abordagem Zero Trust para acesso a aplicações

Dadas as falhas inerentes às abordagens de segurança de perímetro e os desafios específicos que elas apresentam no gerenciamento de acesso a aplicações, o modelo de segurança virtual Zero Trust emergente oferece uma alternativa melhor. Apresentado pela Forrester Research em 2010, é uma estrutura que as empresas estão usando para transformar sua infraestrutura de TI, políticas de segurança e processos de negócios.

O princípio por trás dela é muito simples, mas muito poderoso: a confiança não é um atributo do local. Você não deve confiar em algo simplesmente porque está protegido por seu firewall. Em vez disso, qualquer ação, não importa onde ocorra, só deve ser confiável se tiver sido explicitamente permitida. Em última análise, apenas o que *deveria* acontecer *pode* acontecer. Remova toda a confiança implícita para ações que não são necessárias porque elas criam risco, mas não valor.

Isto requer autenticação e autorização fortes, e os sistemas não devem transferir dados até que a confiança seja estabelecida. Além disso, análises, filtros e registros devem ser empregados para verificar o comportamento e observar continuamente sinais de comprometimento.

Esta mudança fundamental anula uma grande parte das concessões à segurança que vimos na última década. Os invasores não podem mais explorar pontos fracos em seu perímetro e, em seguida, coletar seus dados e aplicações confidenciais porque conseguiram entrar no castelo. Agora não há fosso a ser atravessado para ter acesso. Existem apenas aplicações e usuários que devem autenticar e verificar mutuamente a autorização antes que o acesso possa ocorrer.

Zero Trust Network Access

ZTNA é uma arquitetura baseada nesses princípios que concede acesso seguro a aplicações e recursos com base em autenticação, autorização e contexto fortes. Uma arquitetura ZTNA fornece acesso apenas às aplicações de que os usuários precisam para realizar seu trabalho, e não a toda a rede. Com uma abordagem ZTNA, não importa mais onde os usuários estão localizados; não há mais o conceito de dentro ou fora do perímetro. Tornou-se irrelevante onde uma aplicação é hospedada, no local, na nuvem pública ou na nuvem privada, porque os usuários autenticados só têm acesso a aplicações que têm autorização para usar.

Por exemplo, um funcionário de vendas terá acesso somente a aplicações relacionadas à sua função de vendas, não a recursos humanos ou aplicações financeiras.

Como funciona o ZTNA da Akamai

O Akamai Enterprise Application Access e o Akamai MFA permitem que você mude para uma arquitetura ZTNA, que pode ser uma etapa importante e crítica em sua jornada rumo ao Zero Trust.

O Enterprise Application Access é um IAP (Identity-Aware Proxy) na nuvem. É um serviço flexível e adaptável com tomada de decisão granular baseada em sinais em tempo real, como inteligência de ameaças, postura do dispositivo e informações de identidade do usuário. Akamai MFA é um serviço de autenticação multifator que fornece os níveis mais fortes de autenticação para garantir que o usuário que solicita acesso é quem afirma ser.

Para começar, você executa uma pequena máquina virtual chamada Enterprise Application Access Connector atrás do firewall, mas com conectividade com suas aplicações. Não precisa nem *deveria* estar dentro da sua DMZ. O endereço dela deve estar em um espaço de IP privado e não deve ser diretamente acessível a partir da internet. Na verdade, ela deve ser exatamente como qualquer outra aplicação que você colocaria por trás do firewall.

Para dar suporte a ambientes multinuvem, um conector pode ser implementado dentro do data center local ou em uma nuvem privada ou pública.

O conector Enterprise Application Access estabelece imediatamente uma conexão criptografada de saída com o IAP no Akamai Connected Cloud. Uma vez conectado ao IAP, o conector baixa sua configuração e está pronto para atender conexões. A conexão entre o conector e o IAP é de saída, o que permite fechar todas as conexões de entrada do firewall, tornando as aplicações quase invisíveis na Internet pública.

O IAP executa todo o pré-processamento que acontece antes que um usuário seja conectado à aplicação, incluindo autenticação, autorização e verificações de segurança e postura do dispositivo. Quando um usuário tenta acessar uma aplicação, ele é direcionado para a Akamai por meio de um DNS CNAME e conectado ao IAP. Supondo que seu usuário final e seu dispositivo sejam aprovados em todas as verificações, eles serão roteados para autenticação, autenticação multifator e logon único, após o qual as funções de identidade do dispositivo serão executadas.

Depois que o usuário e a máquina forem autorizados, a conexão do usuário final será unida à conexão de saída do conector Enterprise Application Access. O tráfego da sessão do usuário flui através desse IAP costurado, que então se conecta à aplicação ou ao serviço solicitado. Nesse ponto, um caminho de dados completo é estabelecido e todas as decisões de acesso são então aplicadas de forma contínua e dinâmica com base na identidade, no dispositivo e no contexto do usuário.

Existem vantagens diferentes e significativas nesse método de acesso. As atividades mais sensíveis ao desempenho e à segurança ocorrem na edge, mais próximas do usuário final, onde a Akamai possui mais de 4.200 locais em 134 países.

Além disso, o caminho sensível de entrada na aplicação acontece por meio de um túnel de aplicação reversa, removendo efetivamente a visibilidade do IP do perímetro e reduzindo o risco de ataques volumétricos.

Como o Enterprise Application Access pode se integrar diretamente à infraestrutura de identidade de uma empresa, mesmo que use vários diretórios e provedores de serviços de identidade, o serviço ZTNA pode ser implantado rapidamente sem a necessidade de alterar a infraestrutura ou arquitetura de identidade existente.

Para aplicações obsoletas, que não suportam protocolos de autenticação modernos, o Enterprise Application Access tem um recurso de ponte IdP que fornece autenticação para IdPs baseados em SAML e converte o token de autenticação no protocolo de autenticação suportado pelas aplicações antigas.

O que torna as abordagens baseadas em IAP, como o Enterprise Application Access, tão atraentes é que elas fornecem acesso no nível da aplicação. Com acesso no nível da aplicação, o desempenho e a segurança são *dissociados* da complexidade.

Você simplesmente pega todas as aplicações que possuem localidade entre si (todas hospedadas no mesmo data center ou na mesma nuvem privada virtual, por exemplo), coloca-as em um espaço IP de rede privada ou em uma VLAN restrita e coloca um proxy de acesso nesse microperímetro. É isso: você terminou.

Os proprietários de aplicações definem suas próprias políticas de segurança no proxy de acesso, políticas sobre quem pode acessar o quê e por quê e, o que é ainda mais atraente, os usuários podem estar em qualquer lugar. Não há distinção entre local e externo porque não há perímetro de rede que inclua os usuários finais. Um funcionário que trabalha em uma cafeteria é igual a um funcionário que trabalha em seu escritório. Tudo o que importa é se o usuário está autorizado e se a máquina é segura.

Com acesso no nível da aplicação, você obtém o melhor desempenho da categoria, apesar da facilidade de implantação e uso. Os usuários simplesmente acessam a Internet para acessar as aplicações diretamente, não importa onde estejam hospedadas ou onde apareçam, permitindo que a Internet encaminhe os pacotes para o seu destino sem ter que passar por agregadores ou intermediários que não estejam em seu caminho.

De fato, com o acesso no nível da aplicação, as redes internas muitas vezes se dissolvem em um simples Wi-Fi para visitantes. Lembre-se, para que o Zero Trust seja realmente eficaz, você não pode tratar os usuários internos de maneira diferente dos usuários externos. Ninguém é confiável por padrão.

Estado final desejado do ZTNA

Todos os usuários, sejam eles locais ou externos, devem ser obrigados a acessar todas as aplicações por meio de proxies de acesso com reconhecimento de identidade, independentemente de onde as aplicações estejam hospedadas. Esses proxies devem executar não apenas a autenticação padrão, mas também usar a autenticação multifator à prova de phishing, como a MFA da Akamai. Além disso, deve haver capacidades robustas de postura de dispositivos que obtenham critérios de dispositivos para permitir acesso a aplicações específicas.

Acreditamos firmemente que o ZTNA não termina com autenticação e autorização. Para dar suporte aos princípios de Zero Trust, todos os parâmetros que são verificados no estágio inicial de autenticação e autorização devem ser monitorados continuamente durante a sessão de ativação. Qualquer alteração detectada deve acionar uma ação, por exemplo, autenticar novamente o usuário, remover o acesso à aplicação ou limitar o acesso à aplicação.

Um sistema de segurança crucial que deve ser colocado na camada superior dos seus proxies de acesso é a proteção de aplicações da Web e API (WAAP), que garantirá que os usuários finais não lancem ataques no nível de aplicação (intencional ou inadvertidamente) contra suas aplicações internas. Você pode aproveitar outros sistemas avançados, como detecção de humanos/bots para websites que não sejam API, para ajudar a garantir que o malware não se disfarce atrás de pontos de extremidade válidos. É no IAP que a Akamai pode aplicar WAAP, detecção de bots, análise comportamental e armazenamento em cache. Isso foi projetado para fornecer o melhor desempenho da categoria, bem como a capacidade de manter possíveis agentes de ameaças o mais longe possível de seus locais físicos, aplicações e dados.

À medida que você coloca suas aplicações online e as torna acessíveis por meio de proxies de acesso, a prevenção de negação de serviço distribuída (DDoS) se torna ainda mais importante. Você deve se alinhar com provedores que possam absorver ataques contra seus microperímetros e proxies de acesso, permitindo a operação contínua sob cargas intensas.

E, finalmente, para garantir que o desempenho seja o melhor para suas aplicações e que os usuários não apenas aceitem essa mudança no acesso, mas também a defendam, seus proxies de acesso devem ser liderados por redes que possam fornecer benefícios de desempenho. Especificamente, as redes de entrega de conteúdo e as sobreposições de roteamento da Internet devem fazer parte do seu arsenal não apenas para disponibilizar o acesso, mas também para torná-lo mais eficiente do que as metodologias anteriores jamais permitiram.

Proteção contra ameaças

Soluções como o Akamai Enterprise Application Access podem proteger suas aplicações contra agentes mal-intencionados. Mas e quanto a proteger os usuários de se tornarem inadvertidamente esses mesmos agentes por meio de comprometimento, como por meio de um dispositivo infectado por malware ou credenciais roubadas por meio de um link de phishing e de uma página de destino? É nesse ponto que a prevenção e detecção tornam-se cruciais para o tráfego da Web.

Uma abordagem é implantar uma solução de firewall DNS baseada em nuvem, como o Akamai Secure Internet Access. Esse produto inspeciona todas as solicitações de DNS feitas pelos usuários e aplica inteligência sobre ameaças em tempo real para que as solicitações benignas sejam resolvidas normalmente, mas quaisquer solicitações para domínios maliciosos sejam bloqueadas proativamente. Isso reduz os riscos de os dispositivos dos funcionários serem comprometidos com malware ou ransomware ou serem de vítimas de um ataque de phishing.

Resumo

As tradicionais arquiteturas de rede de hub e spoke, juntamente com o perímetro de segurança de "castelo e fosso" que utilizam, simplesmente não podem oferecer desempenho ou segurança efetivamente no mundo atual cada vez mais orientado à nuvem e a dispositivos móveis. Este é um problema que todas as empresas devem começar a resolver ou ficarão vulneráveis. A não transição para arquiteturas de segurança empresarial mais seguras é a causa número um de violações corporativas atualmente, e o número de violações só vai aumentar. Em termos simples: você não está seguro por trás do perímetro, porque o perímetro em si não existe mais.

Próximas etapas

Como você inicia a transição para uma arquitetura Zero Trust Network Access?

Os serviços de segurança em nuvem da Akamai podem ser combinados para construir uma arquitetura ZTNA abrangente, não apenas permitindo o acesso seguro a aplicações em um mundo multinuvem, mas também aproveitando a nuvem para eliminar quase completamente a necessidade de redes corporativas internas.

Ao utilizar nosso IAP distribuído avançado e nossa autenticação multifatorial à prova de phishing, juntamente com o poder do Akamai Connected Cloud, você pode finalmente migrar para um mundo sem perímetro de uma maneira extremamente fácil, implementando aplicações gradualmente, reduzindo seu perfil de risco de migração para quase zero e aproveitando o extenso histórico de soluções comprovadas de desempenho e segurança da Akamai.

Ao continuar sua jornada de Zero Trust, você pode ter certeza de que a Akamai estará com você em cada etapa, ajudando você a transformar sua rede em uma arquitetura que não apenas fornece acesso às suas aplicações e dados, mas também o faz de maneira fácil de gerenciar, mantendo os mais altos níveis de segurança e desempenho.

Saiba mais sobre como atender às necessidades do seu negócio com o portfólio Zero Trust da Akamai.