WHITE PAPER

Como projetar DNS para maior disponibilidade e resiliência contra ataques de DDoS

Introdução

O Edge DNS oferece às empresas um serviço de DNS autoritativo para conectar os usuários finais a websites e a outras aplicações. Embora as organizações se concentrem muito no desempenho, muitas vezes elas ignoram a importância da disponibilidade e da resiliência do DNS, especialmente contra ataques de DDoS que tentam interromper o serviço e impedir que os usuários finais se conectem. A Akamai projetou o Edge DNS para manter a disponibilidade perante os maiores ataques de DDoS, em uma escala global incomparável, com arquitetura IP Anycast segmentada e com vários controles contra DDoS, incluindo a possibilidade de aproveitar outros serviços da Akamai quando necessário. Oferecido como um serviço de DNS gerenciado, o Edge DNS oferece uma combinação ideal de desempenho e disponibilidade para conectar as organizações aos usuários finais.

Nota sobre as estatísticas

Originalmente, a Akamai desenvolveu o Edge DNS para fornecer serviços de DNS autoritativo que dão suporte às soluções de CDN (Rede de Entrega de Conteúdo) global. Ao longo dos anos, a Akamai agregou conhecimentos com relação à melhor forma de escalonar uma grande infraestrutura de DNS e manter a disponibilidade. As estatísticas de alto nível à direita fornecem uma visão geral da escala da plataforma. No entanto, as estatísticas por si só não são capazes de avaliar a disponibilidade e a resiliência e devem ser consideradas juntamente com a arquitetura da plataforma, os recursos específicos de atenuação de DDoS e a capacidade geral da Akamai de proteger a plataforma contra ataques.

Estatísticas da plataforma

- Milhares de nomes de servidores
- Mais de 1.000 pontos de presença
- Mais de 140 cidades
- Mais de 40 países

Observe que, por motivos de segurança, a Akamai não divulga detalhes específicos sobre o número de servidores de nomes, nem números, locais ou tamanhos dos nossos pontos de presença. Essa política protege a Akamai e nossos clientes contra invasores que podem tentar usar essas informações para planejar ataques.

Arquitetura

Como você pode notar nas estatísticas acima, o Edge DNS tem escalonamento maior que a maioria dos serviços de DNS autoritativo da concorrência disponíveis atualmente. No entanto, estatísticas de alto nível sobre o número de servidores e pontos de presença ou a capacidade total da rede não são suficientes para entender o grau de disponibilidade e de resiliência de uma plataforma global. Ao contrário de outras soluções de DNS que tradicionalmente se concentram no desempenho, a Akamai projetou o Edge DNS para proporcionar maior disponibilidade e resiliência contra ataques de DDoS e aumentar o desempenho com redundâncias de arquitetura em vários níveis, incluindo servidores de nomes, pontos de presença, redes e até mesmo nuvens IP Anycast segmentadas.

IP Anycast

O Edge DNS compreende milhares de servidores de nomes implantados em mais de 1.000 pontos de presença que empregam um modelo IP Anycast para responder a consultas de DNS. O IP Anycast direciona as consultas dos usuários finais para o ponto de presença mais próximo para que sejam resolvidas. Além de proporcionar maior desempenho, o IP Anycast oferece vários benefícios fundamentais quanto a disponibilidade e resiliência, e é por isso que a maioria dos serviços de DNS autoritativo usa esse recurso:

- **Disponibilidade**: o IP Anycast permite que servidores de nomes em diferentes locais de rede respondam a consultas feitas a um único endereço IP. Ao aproveitar o IP Anycast, o Edge DNS não só oferece às organizações a resolução de DNS em vários data centers, como também melhora a disponibilidade distribuindo a carga globalmente. Além disso, servidores físicos ou pontos de presença individuais podem ficar completamente off-line sem afetar a capacidade geral de resolução de um domínio.

- **Escalonamento**: englobando muitos servidores físicos em vários pontos de presença, a infraestrutura do Edge DNS oferece às organizações recursos de computação significativos nos quais elas podem confiar consistentemente ao responder a grandes volumes de solicitações de DNS. O Edge DNS também tem acesso a uma capacidade de rede adicional significativa em muitos dos seus pontos de presença, pois geralmente ela é compartilhada com outros serviços da Akamai. Isso proporciona ao Edge DNS um escalonamento muito maior para responder a inundações de DNS e a outras formas de ataques de DDoS do que um serviço de DNS autônomo.

- **Distribuição**: além de permitir maior escalonamento, o IP Anycast possibilita que o Edge DNS distribua o tráfego em vários pontos de presença e em diversos locais de rede. Analisar cuidadosamente as localizações geográficas e implantações de rede para esses pontos de presença ajuda a deter o impacto de ataques menores a regiões geográficas ou redes específicas e preserva a disponibilidade dos sistemas de clientes em outras áreas.

O uso do IP Anycast não é exclusivo da Akamai. Ao permitir que vários servidores de nomes resolvam consultas de DNS dos usuários finais, o IP Anycast melhora a disponibilidade da resolução de nomes de qualquer serviço de DNS. Mas, mesmo com o IP Anycast, a resiliência permanece limitada pelo escalonamento total de uma plataforma, e grandes ataques de DDoS ainda podem sobrecarregar uma plataforma baseada em nuvem. Além disso, sem uma arquitetura diversificada, mesmo ataques menores podem derrubar serviços de DNS em regiões geográficas específicas, tornando-os indisponíveis para um grande número de usuários finais e afetando a disponibilidade dos websites aos quais esses usuários se conectam.

Nuvens do Edge DNS

Para melhorar ainda mais sua resiliência contra ataques, o Edge DNS segmenta os servidores de nomes e pontos de presença em várias nuvens IP Anycast. Uma nuvem do Edge DNS consiste em servidores de nomes e pontos de presença dedicados e engloba a capacidade e a conectividade associadas à rede. Cada nuvem opera de forma independente, e o Edge DNS pode ser equivalente a vários provedores de DNS autônomos em termos de disponibilidade, escalonamento e distribuição.

As nuvens IP Anycast do Edge DNS representam um conjunto diversificado de arquiteturas. Embora todas as nuvens sejam diferentes uma da outra, elas precisam atender a dois princípios de design: desempenho e disponibilidade:

- **Desempenho**: uma nuvem de desempenho pode ter mais de 100 pontos de presença distribuídos em todo o mundo, cada um consistindo em um conjunto de servidores de nomes. Como mostrado na Figura 1, uma nuvem de desempenho implanta pequenos clusters de servidores de nomes em vários locais próximos dos usuários finais e dos ISPs (Provedores de Serviços de Internet) locais para agilizar o tempo de pesquisa e melhorar o desempenho bruto. A desvantagem é que pontos de presença pequenos oferecem menos resiliência a ataques de DDoS por padrão, além de menos recursos de computação e menor capacidade de rede.
- **Disponibilidade**: o Edge DNS conta com muitas nuvens de disponibilidade. Como mostrado na Figura 1, as nuvens de disponibilidade têm menos pontos de presença, mas dispõem de regiões-base que podem incluir centenas de servidores de nomes em um data center centralizado com uma grande quantidade de capacidade de rede dedicada e conectividade por meio de várias redes. A região-base fornece a nuvem de disponibilidade com escalonamento para responder a grandes picos de solicitações de DNS e outros tráfegos de rede. As nuvens de disponibilidade aumentam as regiões-base com alguns pontos de presença menores para manter um nível aceitável de desempenho para os usuários no mundo todo.

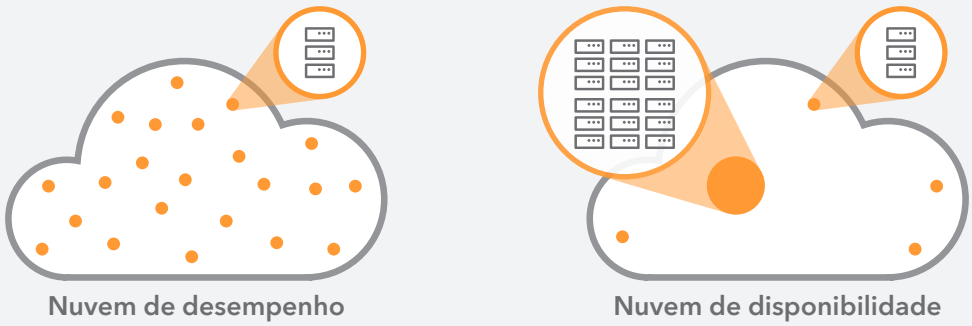

Figura 1: O Edge DNS combina várias nuvens de DNS e arquiteturas diferentes para oferecer o melhor desempenho, disponibilidade e resiliência contra ataques de DDoS.

Arquitetura segmentada

O Edge DNS oferece um grau de disponibilidade diferente em comparação com os outros provedores que operam serviços de DNS autoritativo em uma única nuvem IP Anycast. O IP Anycast oferece a todos os provedores o benefício de disponibilidade, permitindo que o serviço mantenha o tempo de atividade geral em caso de ataques menores que afetem regiões geográficas específicas em vez de toda a plataforma. No entanto, mesmo as interrupções localizadas afetarão os usuários finais nas regiões impactadas e as organizações que dependem desse serviço para se conectar aos usuários. Além disso, ataques de DDoS maiores com tráfego gerado por sistemas de ataque globais podem causar uma interrupção de toda a plataforma.

Como o Edge DNS têm várias nuvens IP Anycast, ele continua funcionando mesmo com a perda de uma ou mais nuvens. Isso proporciona maior disponibilidade e resiliência contra ataques de DDoS em comparação com uma arquitetura de nuvem única. Além disso, usar várias nuvens IP Anycast oferece a vantagem de segmentar o tráfego em subseções da plataforma para atenuar o impacto até mesmo

de ataques de DDoS massivos. Por exemplo, um ataque contra uma única nuvem IP Anycast do Edge DNS será direcionado para os servidores de nomes físicos e pontos de presença que compõem essa nuvem específica. A arquitetura segmentada evita que as outras nuvens IP Anycast sejam afetadas, permitindo que o Edge DNS mantenha a disponibilidade da plataforma em todas as regiões geográficas, mesmo que nuvens ou clientes individuais estejam sob ataque de DDoS.

Figura 2: Cada cliente do Edge DNS recebe servidores de nomes em uma combinação exclusiva de nuvens de desempenho e disponibilidade, o que minimiza os danos colaterais de um ataque contra outros clientes.

Além de aumentar a resiliência geral da plataforma, a arquitetura segmentada do Edge DNS também reduz o risco de danos colaterais para clientes individuais quando os servidores de nomes usados por outros clientes são atacados. O Edge DNS atribui a cada cliente várias nuvens usando uma combinação exclusiva de nuvens de desempenho e disponibilidade que nenhum outro cliente terá acesso. Conforme mostrado na Figura 2, essa distribuição minimiza a sobreposição em servidores de nomes e nuvens IP Anycast entre dois clientes. Ela também garante que todos os clientes tenham servidores de nomes disponíveis, mesmo quando as nuvens IP Anycast atribuídas a outro cliente estejam sendo afetadas por um grande ataque de DDoS.

Gerenciar delegações dos clientes

Alguns ataques de DDoS contra uma única organização duram períodos mais longos. A Akamai viu campanhas de ataque amplas e contínuas se estenderem por meses ou mais. Nessa situação, a arquitetura segmentada do Edge DNS oferece à Akamai maior flexibilidade para minimizar ainda mais o impacto sobre os clientes que não são alvo do ataque. Como mostrado na Figura 3, a Akamai pode reatribuir as nuvens de um cliente individual e isolar ainda mais o efeito de um ataque quando necessário.

Figura 3: A Akamai pode gerenciar delegações de servidores de nomes para minimizar ainda mais o impacto de um ataque (em comparação com a Figura 2 acima), como remover um cliente alvo de uma nuvem individual e restringir a sobreposição para aqueles que não são alvo do ataque.

Por exemplo, a Akamai pode:

- **Remover um cliente alvo de uma nuvem específica**: todos os clientes do Edge DNS compartilham nuvens IP Anycast com outros clientes. Como resultado, um ataque direcionado a todas as nuvens do Edge DNS de um cliente pode afetar a disponibilidade das nuvens também atribuídas a outros. Em circunstâncias normais, os resolvedores recursivos alternam automaticamente para nuvens de melhor desempenho, mas, no caso de campanhas persistentes, a Akamai pode reatribuir as nuvens IP Anycast do cliente para restaurar a disponibilidade de quem não é alvo do ataque.

- **Minimizar a sobreposição para clientes que não são alvos do ataque**: às vezes, vários clientes do Edge DNS compartilham um número de nuvens maior que o normal. Nessa situação, é possível que um ataque massivo contra um único cliente possa afetar significativamente o desempenho de outros, apesar de o serviço geral permanecer disponível. Quando necessário, a Akamai pode reatribuir as nuvens para os clientes que não são alvos do ataque a fim de reduzir ou eliminar a sobreposição com o alvo e restaurar o desempenho dos usuários finais.

Diversas implantações de servidor

A Akamai implanta em cada nuvem Anycast servidores de nomes físicos em diferentes locais projetados para aumentar a resiliência geral dessa nuvem. Implementar vários locais de nuvem do Edge DNS cria outra camada de segmentação de tráfego entre diferentes redes para maximizar a disponibilidade em circunstâncias diversas. Por exemplo:

- **Em data centers com várias redes**: a diversidade da conectividade de rede pode ser tão importante quanto a capacidade ao considerar a resiliência contra ataques de DDoS. Grandes ataques de DDoS podem sobrecarregar os ISPs upstream e outras redes antes de atingir um data center, causando congestionamento de rede e interrupções de serviço, mesmo que o data center em si não seja afetado. Para preservar a disponibilidade e sua capacidade de responder às consultas de DNS dos usuários finais durante ataques, o Edge DNS implanta servidores de nomes em grandes data centers com vasta capacidade e conectividade em várias redes.

- **Isolamento de ISP**: em muitos casos, o Edge DNS implanta clusters de servidores de nomes diretamente nas redes de ISPs individuais. Os servidores de nomes geralmente transmitem o tráfego IP Anycast somente dentro dessas redes e resolvem consultas de DNS apenas para os usuários finais do ISP em questão. Embora essa abordagem limite o número de usuários finais que são atendidos por um cluster específico de servidores de nomes, ela também preserva a disponibilidade para esses usuários quando uma nuvem IP Anycast é alvo de um ataque externo a esse ISP. Um invasor precisaria ter sistemas na rede desse provedor específico para ver os servidores de nomes, e, mesmo assim, a capacidade disponível é muitas vezes suficiente para proteger a nuvem.

- **Diversidade de redes**: são atribuídas aos clientes nuvens diversas intencionalmente. Algumas têm locais de servidor exclusivos para ISPs específicos, e outras dispõem de uma gama mais ampla de máquinas conectadas. Essa arquitetura garante que os servidores de nomes recursivos de um determinado cliente sempre possam se conectar a uma nuvem disponível do Edge DNS.

- **Em data centers compartilhados com outros serviços da Akamai**: ao operar muitos serviços diferentes além do DNS autoritativo, a Akamai pode implantar servidores de nomes do Edge DNS em data centers que oferecem suporte a vários serviços. Conforme discutido em mais detalhes abaixo, isso possibilita que o Edge DNS tenha acesso a uma capacidade de rede maior ao responder a grandes ataques de DDoS. Isso vale tanto para capacidade de rede dedicada quanto para arranjos de peering público que a Akamai já usa para outros serviços.

Controles contra DDoS

Além da forma como a arquitetura é projetada, o Edge DNS inclui vários controles para ajudar a atenuar o impacto de uma categoria de ataques de DDoS conhecida como inundações de DNS. Embora muitos ataques de DDoS usem uma grande quantidade de tráfego para sobrecarregar os links de rede, as inundações de DNS geram grandes volumes de solicitações de DNS legítimas para consumir recursos computacionais e memória nos servidores de nomes físicos e impedi-los de responder às consultas dos usuários finais reais. A Akamai protege a plataforma Edge DNS contra inundações de DNS de várias maneiras:

- **Escalonamento**: o escalonamento do serviço de DNS autoritativo da Akamai pode ser bem maior do que a de outras soluções de DNS concorrentes. O Edge DNS utiliza milhares de servidores de nomes implantados em mais de 1.000 pontos de presença no mundo todo. Embora não seja especificamente um controle contra DDoS, o IP Anycast distribui o tráfego do ataque entre regiões geográficas e redes, enquanto os servidores de nomes físicos existentes fornecem ao Edge DNS recursos de computação e memória suficientes para absorver grandes picos de solicitações de DNS.
- **Limitação de taxa**: o Edge DNS inclui recursos de limitação de taxa e pode eliminar automaticamente as solicitações de endereços IP individuais depois que o volume de solicitações excede um limite definido. A limitação de taxa impede que grandes picos de solicitações de DNS consumam recursos de computação e memória nos servidores de nomes físicos e pode ser útil ao responder a ataques que geram um alto volume de solicitações, mas consomem uma largura de banda relativamente baixa. Observe que esses recursos não são configuráveis pelos clientes, mas aplicados por algoritmos exclusivos da plataforma Edge DNS.
- **Lista de permissões de DNS**: devido à sua posição na Internet, a Akamai tem visibilidade exclusiva do comportamento dos resolvedores recursivos responsáveis por aproximadamente 95% das pesquisas legítimas de DNS na Internet. Quando o Edge DNS precisa lidar com uma alta carga de trabalho, ele pode empregar um modelo de segurança positivo e restringir as solicitações de DNS a uma lista de resolvedores de DNS confiáveis.

Capacidade

Embora os controles contra DDoS possam ser úteis para atenuar o impacto das inundações de DNS, outros tipos de ataques de DDoS na camada de rede exigem capacidade de rede suficiente para absorver o alto volume de tráfego. O risco de ataques massivos aumentou drasticamente nos últimos anos, e os maiores já vistos excederam 1 Tbps de largura de banda de pico.

A Akamai não divulga o volume da capacidade da plataforma Edge DNS para não fornecer um alvo quantificável para os invasores. No entanto, ela investe continuamente em todos os aspectos de escalonamento da plataforma, aumentando a infraestrutura do Edge DNS para acompanhar o ritmo dos novos clientes e a expansão do tráfego na Internet. Como um provedor de serviços de nuvem, a Akamai pode readaptar rapidamente os servidores e implantar a capacidade de DNS em novas regiões. Ela mantém um volume significativo de capacidade disponível para absorver grandes picos de tráfego, considerando que o tráfego normal na plataforma Edge DNS consome menos de 1% da capacidade geral. Se necessário, o Edge DNS também pode aproveitar recursos de outras plataformas da Akamai para atenuar ataques de DDoS.

Aproveitamento de outras plataformas da Akamai

O método tradicional de usar a capacidade de rede para verificar se a plataforma pode suportar um ataque de DDoS de alta largura de banda não funciona com o Edge DNS, principalmente porque ele consegue aproveitar recursos de outras plataformas da Akamai. Mais do que apenas uma empresa de DNS, a Akamai opera muitos outros serviços além do Edge DNS. Entre todos os serviços operados pela Akamai, o DNS autoritativo é essencial para a operação de outros serviços, mas consome pouco tráfego no geral. Isso possibilita aumentar a capacidade disponível para o Edge DNS quando necessário:

- **Capacidade fornecida pela CDN**: em muitos casos, o Edge DNS implanta servidores de nomes nos mesmos pontos de presença que os servidores de outros serviços da Akamai em execução na CDN própria. Esses pontos de presença geralmente são bem maiores, pois são projetados para oferecer suporte a serviços que consomem mais largura de banda. Isso também proporciona à Akamai a flexibilidade operacional para usar a capacidade da CDN quando necessário, desviando serviços de outros pontos de presença e disponibilizando a capacidade de rede compartilhada para o Edge DNS de modo que ele possa absorver grandes ataques de DDoS.

- **Implantação de capacidade de atenuação dedicada**: além de DNS autoritativo e CDN, a Akamai opera um serviço de proteção contra DDoS separado com capacidade e recursos de atenuação dedicados. Se for necessário atenuar grandes ataques de DDoS, a Akamai poderá atribuir delegações de servidores de nomes individuais por meio dos centros de depuração da Prolexic para aproveitar essa capacidade e as ferramentas de atenuação de DDoS dedicadas. Isso implanta os recursos de atenuação de DDoS da plataforma Prolexic no Edge DNS de forma eficiente, preservando os recursos do Edge DNS para responder às consultas legítimas dos usuários finais.

Vários provedores de DNS

O Edge DNS oferece um serviço de DNS autoritativo da Akamai com escalonamento bem maior que a de outras soluções de DNS concorrentes, uma arquitetura resiliente com várias nuvens IP Anycast segmentadas e a possibilidade de aproveitar a capacidade e os recursos adicionais de outros serviços da Akamai para proteção contra ataques de DDoS. Com essas vantagens, o Edge DNS fornece a disponibilidade e a resiliência necessárias para operar como o único provedor de DNS autoritativo de uma organização. No entanto, algumas empresas podem optar por implantar o Edge DNS em paralelo a uma solução existente. Uma implantação multiprovedor permite que as organizações mantenham suas práticas de gestão de registros de DNS existentes e complementem a solução de DNS principal com a disponibilidade e a redundância adicionais do Edge DNS.

Opções de implantação

O Edge DNS oferece suporte a várias opções de implantação em um ambiente multiprovedor:

- **Serviço secundário tradicional**: as organizações com um provedor de DNS existente podem implantar o Edge DNS como um serviço secundário para aprimorar a solução principal. Assim, elas podem continuar gerenciando seus registros de DNS com o provedor principal e usar transferências de zona ou as APIs do Edge DNS para atualizá-lo automaticamente. As soluções principais e secundárias podem responder às consultas dos usuários finais, oferecendo disponibilidade adicional.
- **Arranjo primário oculto**: a Akamai recomenda essa opção de implantação para organizações que desejam continuar gerenciando os registros de DNS em uma solução interna de DNS. O arranjo primário oculto permite que o Edge DNS (como o provedor de DNS secundário único ou um de vários provedores) responda às consultas dos usuários finais sem expor a solução interna a ataques de DDoS. Assim, elas podem continuar gerenciando seus registros de DNS com o provedor principal e usar transferências de zona ou as APIs do Edge DNS para atualizá-lo automaticamente.
- **Arranjo primário duplo**: é uma variante do conceito de arranjo primário oculto. Alguns provedores de serviços de nuvem não adotam mais a funcionalidade tradicional de transferência de zona e exigem que os clientes usem APIs ou outras interfaces de usuário para fazer alterações no registro de zona. Também é possível implantar o Edge DNS de acordo com essa abordagem. Basta configurá-lo no modo primário e adicionar as nuvens dele como autoritativas.

Como manter a disponibilidade em um arranjo de solução secundária

Quando implantado como uma solução secundária, o Edge DNS conta com as atualizações de zona da solução principal para responder corretamente às consultas dos usuários finais. Normalmente, os arquivos de zona permanecem válidos em uma solução secundária de DNS durante o período de TTL (Vida Útil), e isso é definido pelo campo de expiração no registro de Início de Autoridade. Um ataque de DDoS que causa uma interrupção da solução principal também pode fazer com que a solução secundária pare de responder a consultas quando a duração da interrupção excede o valor da TTL. O Edge DNS protege contra esse cenário ao (1) manter o arquivo de zona mesmo após a expiração da TTL e (2) continuar respondendo a consultas de DNS enquanto o registro de DNS apontar para o Edge DNS. Isso ajuda a fornecer disponibilidade adicional como uma solução secundária de DNS, mesmo que a principal esteja indisponível.

Conclusão

O maior ataque de DDoS já visto excedeu 1 Tbps de largura de banda de pico. Nessa escala, calcular a largura de banda total disponível para um serviço baseado em nuvem não serve mais como uma avaliação precisa da sua resiliência a tais ataques, e até mesmo ataques menores podem causar interrupções em níveis regionais. O Edge DNS emprega uma abordagem multicamadas para propiciar 100% de disponibilidade aos clientes, combinando:

- Enorme escala com uma presença global, incluindo servidores de nomes e pontos de presença bem maiores que os de muitos serviços concorrentes
- Uma arquitetura resiliente com várias nuvens IP Anycast segmentadas para isolar o impacto dos ataques e evitar danos colaterais a outros clientes, bem como à plataforma geral
- Uma resposta gerenciada a ataques de DDoS, incluindo a possibilidade de implantar controles contra DDoS ou reatribuir delegações de clientes, conforme necessário
- A possibilidade de aproveitar outros serviços da Akamai, incluindo a CDN e a proteção Prolexic DDoS, para aumentar a capacidade e suportar ataques de DDoS grandes e pequenos

O DNS autoritativo é um serviço essencial que conecta usuários finais em todo o mundo à presença on-line das organizações. Seja implantado como o único provedor de DNS autoritativo ou combinado com uma solução existente, o Edge DNS oferece às organizações a disponibilidade de que precisam para manter o acesso global ao seu website e a outras aplicações na Internet.