Akamai

WHITE PAPER

Microssegmentação e segmentação de rede em ambientes empresariais modernos

Visão geral

A ideia de segmentação por segurança não é novidade. Firewalls de perímetro, juntamente com VLANs e ACLs, são o que a maioria das empresas tradicionalmente usa para segmentar e proteger sua infraestrutura de TI. No entanto, os tempos estão mudando. O aumento da conteinerização, da rede definida por software, do uso de infraestrutura pública e de várias nuvens e a expansão de dispositivos conectados à Internet criaram um novo conjunto de problemas de segurança para resolver, um que precisa de uma solução criada para um ambiente de TI heterogêneo com conjuntos variados de requisitos de segurança. Além disso, ransomware e agentes de ameaça afiliados ao estado-nação agora são um risco para qualquer empresa, e os invasores estão se tornando mais sofisticados ao mesmo tempo em que está se tornando cada vez mais difícil de entender como ganhar visibilidade do seu ambiente de TI. As medidas tradicionais de segurança de perímetro, bem como os firewalls de última geração baseados em inspeção profunda de pacotes ou detecção baseada em assinaturas, têm dificuldades para acompanhar a quantidade de tráfego que um data center empresarial experimenta hoje. Vejamos como as técnicas de microssegmentação corretas são a melhor tecnologia para lidar com as deficiências de outras abordagens alternativas de segmentação de rede.

> À medida que os ambientes de nuvem híbrida se tornaram a norma, eles exigem um conjunto específico de requisitos que supere a segurança de perímetro tradicional

Os firewalls legados são inadequados para o tráfego leste-oeste

Ao segmentar ambientes de TI, uma empresa pode primeiro procurar dispositivos de segurança de perímetro legados. Infelizmente, esses dispositivos foram criados para monitorar o tráfego que se move de norte a sul, de cliente para servidor. Isso inclui qualquer tráfego que chegue no data center a partir de qualquer fonte externa. Mais recentemente, a quantidade de tráfego dentro do data center que se move de servidor para servidor, geralmente chamada de tráfego leste-oeste, aumentou exponencialmente. Isso se deve em grande parte ao crescimento da virtualização e da infraestrutura convergente, como hipervisor, VPC e computação baseada em contêiner.

Medidas de segurança de perímetro, como firewalls tradicionais, não protegem sua empresa contra dispositivos infectados ou impedem que invasores expandam sua posição usando o tráfego leste-oeste. Com o aumento da criptografia TLS e a fácil ocultação de tráfego mal-intencionado em portas de aplicações legítimas abertas, muitos ataques podem passar mesmo quando atravessam os firewalls. Isso deixa você incapaz de identificar violações existentes e resolvê-las ou desviá-las. Isso também significa que você não pode limitar facilmente o tempo de permanência que os invasores têm em sua rede. Quanto maior for o tempo de permanência, mais catastrófica será a violação. O Active Adversary Playbook 2022 da Sophos descobriu que, enquanto o tempo médio de permanência era de 15 dias, pequenas empresas e setores específicos perceberam tempos de permanência médios superiores de até 34 dias.[1] Quanto mais tempo um invasor não for detectado em sua rede, mais danos ele poderá causar.

Simplesmente não é possível usar firewalls virtualizados suficientes para proteger milhares de aplicações ou cargas de trabalho. Mesmo que uma solução virtualizada pudesse ser criada, seria impossível gerenciar ou controlar os ambientes dinâmicos em constante mudança nos quais trabalhamos agora. Quando se trata de nuvem híbrida, por exemplo, os firewalls tradicionais são ainda mais difíceis de usar, pois precisam trabalhar em vários ambientes, rastrear cargas de trabalho em diferentes nuvens e ser controlados a partir de um único ponto. Para tentar resolver esses problemas, surgiram várias abordagens de segmentação de rede.

Três abordagens de segmentação a serem consideradas

Com a compreensão de que os firewalls, mesmo quando virtualizados, são inadequados para proteger data centers de nuvem híbrida, as empresas procuram aplicar a segmentação dentro da infraestrutura leste-oeste de três maneiras básicas. Como discutimos, sem uma política de segmentação forte e medidas de segurança, qualquer porta ou servidor tem acesso para se comunicar com qualquer outra. Isso significa que, se um firewall de servidor for violado, o invasor pode se mover facilmente para qualquer outro na rede. A maneira mais eficaz de limitar a conectividade entre servidores é segmentando a rede. Há três tipos básicos de segmentação de rede, com a microssegmentação sendo a tecnologia que as empresas podem usar para aplicar políticas e controle cada vez mais granulares. Os usuários podem combinar os três tipos de política de segmentação listados abaixo, criando políticas mais granulares para aplicações críticas ou arriscadas.

Segmentação de ambiente

Essa abordagem separa ambientes diferentes uns dos outros. Dessa forma, as empresas podem segmentar o braço de desenvolvimento de sua empresa a partir do ambiente de produção, por exemplo. Este é o primeiro estágio crucial em qualquer estratégia de segmentação, que pode então ser seguido por uma criação de políticas mais granular.

Segmentação de aplicações

Levando a segmentação ainda mais longe, "delimitar" o acesso a aplicações de alto valor envolve pegar cada aplicação crítica específica e mantê-la separada do restante da rede. As melhores soluções de microssegmentação permitirão até mesmo que isso seja controlado em nível de processo.

Segmentação de nível

A forma mais rígida de segmentação está dentro da própria aplicação. Aqui, você pode criar uma política de como as comunicações são gerenciadas entre níveis dentro do mesmo cluster de aplicações, controlando o tráfego entre servidores da Web, servidores de aplicações e servidores de banco de dados, por exemplo. Isso também pode ser controlado com a aplicação no nível do processo, se você escolher.

Método de segmentação de rede – segmentação de rede por VLANs

A maioria das empresas começa empregando VLANs. Essas redes locais virtuais permitem que as empresas aloquem cada segmento com seu próprio caminho de comunicação, por meio de um firewall ou de listas de controle de acesso (ACLs) no próprio roteador. Embora a VLAN seja uma escolha comum para segmentação de rede, há muitos problemas sob a superfície. Vamos analisar mais detalhadamente o motivo pelo qual as VLANs são uma escolha inferior para atender às necessidades de segurança atuais.

É fácil ver por que muitas empresas escolhem VLANs como seu método de segmentação. Isso pode ser feito com a arquitetura existente, o que faz com que ela pareça de baixo custo e simples de implantar. No entanto, é uma abordagem de segmentação muito rígida e complexa, pode ser cara para manter e requer tempo de inatividade para implementar.

Para começar a usar VLANs, você precisará se familiarizar com os servidores e dependências em cada segmento e, em seguida, criar a configuração desejada para o switch ou switches de rede que está segmentando. Como isso é feito por engenheiros de rede e geralmente envolve vários locais, isso pode levar muitos dias e custar uma quantidade desproporcional de tempo e dinheiro. O tráfego pode ser interrompido ou ficar lento durante o tempo de configuração.

Em uma época em que a agilidade é uma grande vantagem competitiva e talvez até mesmo um item obrigatório, custos altos e velocidade lenta quando se trata de mudanças significam um desastre para seus resultados. De acordo com a Forbes, a adaptabilidade é fundamental para a sobrevivência: "Interrupções não são novidade, mas a velocidade, a complexidade e a natureza global das interrupções estão em uma escala que nunca vimos antes. ... Não são os maiores ou financeiramente mais estáveis que sobreviverão, mas os que conseguirem se adaptar ao ritmo exponencialmente acelerado da mudança."[2]

É importante reconhecer que as VLANs não foram criadas com a segmentação em mente. Inicialmente criada para reduzir o congestionamento, usá-las para controlar as comunicações não é uma maneira inteligente de aproveitar essa tecnologia existente - é, em muitos aspectos, um uso indevido. Considerando isso, não é surpreendente que a segmentação usando VLANs tenha limitações.

- **Tecnologia de nuvem** – VLANs e outras políticas tradicionais de segmentação de rede não podem ser estendidas para a nuvem. Se você usar firewalls segmentados internos (ISFW) ou ACLs para controlar quais usuários podem acessar segmentos de rede, provavelmente precisará contar com SDN (rede definida por software) para a nuvem. Isso geralmente é feito por meio de provedores de software de terceiros que usam firewalls ou sub-redes virtualizados.
- **Contêineres** – a segurança continua sendo uma grande preocupação, dada a ampla adoção de contêineres em ambientes de TI. Como cada contêiner é executado no mesmo kernel, uma exploração pode colocar todos os contêineres em risco. O isolamento tem sido uma luta contínua e não pode ser resolvido com os métodos usuais de segmentação de rede.
- **Restrições de protocolo** – o limite para VLANs é de 4.096 segmentos, o que restringe a capacidade de fornecer segmentação adequada em grandes data centers. Abordagens de segmentação mais granulares não têm essa limitação.

Segmentação de rede para segmentação de aplicações – apresentando os controles da Camada 4

Muitos desses problemas foram aprimorados adotando a segmentação de aplicações usando grupos de segurança em ambientes de nuvem e firewalls baseados em hipervisor para ambientes virtualizados locais. A segmentação tradicional de aplicações implementa os controles da Camada 4, permitindo que você isole níveis de serviço uns dos outros, para que uma aplicação tenha um limite seguro. Cada nível é limitado ao nível de acesso necessário para fornecer sua funcionalidade completa, mas não mais. Há uma separação clara entre os níveis de uma aplicação individual, e a ameaça de um possível comprometimento é mantida ao mínimo.

Pense nos níveis que você pode encontrar em uma empresa padrão, de balanceadores de carga e bancos de dados a servidores de aplicações dentro/fora de sua própria DMZ. Manter esses níveis separados permite que cada um tenha suas próprias regras e recursos de segurança. A segmentação de aplicações pode dar suporte às empresas ao permitir os controles certos para cada nível, limitando suas informações confidenciais e comunicações, ao mesmo tempo em que permite amplo acesso do usuário quando necessário. Por exemplo, uma empresa pode impedir que determinados bancos de dados se comuniquem com a Internet ou garantir que, se um invasor violar um balanceador de carga simples, ele não possa se mover para acessar informações mais confidenciais no nível do banco de dados.

À medida que a solução se torna mais granular, a segmentação de aplicações permite que uma empresa segmente um cluster de aplicações inteiro de outras áreas da empresa. Conforme discutido, isso reduz a área de superfície de ataque e a capacidade dos invasores de fazer movimentos laterais de um nível para outro.

Os limites dos controles da Camada 4

A segmentação tradicional de aplicações pode não ter profundidade, o que tem um impacto direto na sua visibilidade. A camada de rede, onde ocorre o roteamento, move os dados entre os sistemas, atribuindo endereços IP e protocolos que detalham os segmentos de dados do caminho que levam ao seu destino. A segmentação de aplicações geralmente usa os controles de rede da Camada 4, concentrando-se na maneira como os próprios dados são fornecidos. Segmentos de dados maiores são divididos em segmentos ou blocos menores, prontos para serem reunidos novamente em seu destino. O controle de fluxo permite que esse processo seja acelerado ou desacelerado dinamicamente, onde os dispositivos que enviam ou recebem as informações precisam.

No cenário atual de ameaças, os controles para essas camadas são essenciais, mas em certos casos você pode querer definir a política em um nível ainda mais granular. Os invasores mostraram sua capacidade de falsificar endereços IP e usar técnicas de "piggybacking", ou seja, pegar carona para entrar em portas permitidas para violar uma rede. Além disso, a proteção da Camada 4 não limita o movimento lateral dentro de uma aplicação ou de um nível, o que ainda pode deixá-lo com uma superfície de ataque maior do que você gostaria.

Um dos melhores exemplos da necessidade de controles mais granulares do que apenas a Camada 4 está nas iniciativas de conformidade. As técnicas tradicionais de segmentação de aplicações têm, até certo ponto, permitido que as empresas satisfaçam algumas normas específicas de conformidade, como manter o CDE separado para o PCI-DSS ou proteger PHI para HIPAA. No entanto, embora as técnicas da Camada 4 tenham sido aceitas como meios eficazes de demonstrar conformidade, a realidade mostrou que isso pode não ser suficiente. De acordo com o Payment Security Report da Verizon de 2022, apenas 43% das empresas estão "em total conformidade".[3] Ainda pior, mesmo 100% de conformidade não significa que você está 100% seguro. Embora os controles da Camada 4 possam cobrir você em termos de conformidade, eles não reduzem a superfície de ataque o suficiente para fazer uma diferença significativa para a segurança. Ponto final. Os invasores podem usar uma porta aberta da Camada 4 entre dois níveis com um processo separado (Camada 7) e tomar tudo o que quiserem.

Segmentação no escuro – a falta de visibilidade na segmentação de rede e aplicações

Como as empresas estão descobrindo, embora não haja dúvidas de que a segmentação de aplicações é um passo na direção certa, ela não vai suficientemente longe para resolver todos os problemas inerentes a uma abordagem de segmentação comum. Outro desafio que ainda precisa ser abordado é a visibilidade. Ser capaz de ter uma visão geral precisa e em tempo real da sua rede é essencial em cada estágio do seu processo de segmentação, o que é uma limitação de muitas abordagens de segmentação.

Antes de começar, você desejará visualizar as dependências da aplicação para poder elaborar regras de política precisas. Depois que a segmentação for implementada, você precisará de evidências de que sua segmentação está funcionando conforme o esperado, não apenas para confirmar que sua postura de segurança é forte, mas também para fornecer evidências de conformidade regulatória quando necessário.

Sem visibilidade histórica e em tempo real, não há evidências para você ou para terceiros interessados e órgãos reguladores. A coleta manual dessa evidência é demorada e cara para gerenciar, e há sempre a possibilidade de erros de configuração. Uma solução de segmentação que não pode fornecer esse tipo de visibilidade simplesmente não é suficiente.

Microssegmentação até a Camada 7 – a camada de aplicação

Por outro lado, a segmentação na camada de aplicação (Camada 7) é altamente eficaz na limitação do movimento lateral, mesmo dentro de um cluster de aplicações. A Camada 7 é onde os serviços de rede se integram ao sistema operacional. Protocolos como HTTP, FTP, TFTP e SMTP são protocolos da Camada 7. Os mais recentes avanços na tecnologia de microssegmentação são capazes de segmentar nessa camada com muito mais profundidade do que outras soluções, permitindo que sua empresa visualize e controle a atividade na Camada 7, bem como na Camada 4 tradicional. Isso significa que, em vez de depender de endereços IP e portas, processos e fluxos específicos podem ser usados quando as empresas configuram suas políticas. Isso leva os benefícios da segmentação muito além de um nível específico ou até mesmo de um cluster de aplicações. Ela também permite que você identifique ameaças em potencial com algo tão pequeno quanto o hash errado, mesmo quando o invasor está espelhando um processo ou caminho autorizado.

Quando se trata da criação de políticas, a segmentação para a Camada 7 permite regras ou exceções de lista de permissões muito específicas, em que apenas processos ou fluxos exatos são permitidos e todas as outras comunicações são bloqueadas por padrão. Isso pode impor o isolamento de dados entre sistemas, mas ainda permitir a comunicação para fluxos de dados necessários ou críticos para os negócios.

As melhores soluções de microssegmentação fornecem a visibilidade de que as empresas precisam para ganhar agilidade

Com agentes em todas as cargas de trabalho – baseadas em hipervisor ou VPC, contêineres, servidores bare-metal ou até mesmo sistemas IoT/OT – uma solução holística de microssegmentação pode fornecer à sua empresa um mapa visual completo de toda a sua infraestrutura de TI. Com as soluções realmente inteligentes, isso inclui ambientes de data center, nuvem, multinuvem e nuvem híbrida, além de dispositivos remotos. As soluções tradicionais de segmentação de aplicações lutam para obter essa visão multifuncional, geralmente porque usam uma combinação de tecnologias centradas em rede.

Um mapa visual abrangente de seu ambiente também deve mostrar quais políticas de segurança estão em vigor e que estão sendo aplicadas em tempo real. Rapidamente, seus engenheiros e profissionais de segurança devem ser capazes de ver possíveis lacunas a serem solucionadas em sua cobertura de política ou quais políticas adicionais eles precisam implementar ou criar desde o início.

Ter essa visibilidade também permite que sua empresa se prepare antecipadamente para novos softwares ou atualizações de sistemas existentes, criando as regras para segmentação de aplicações atualizadas ou novas com antecedência, antes que elas estejam prontas para implantação. Quando as atualizações estiverem ativas, suas equipes de segurança terão as informações em tempo real necessárias para detectar e resolver atividades de aplicações fora do padrão, garantindo que nenhum risco de segurança seja despercebido ou se torne ativo. Após isso, sua empresa tem as ferramentas contextuais para comparar um incidente com dados históricos e entender o ambiente exato que permitiu que a anomalia ocorresse. As políticas podem ser ajustadas, a segmentação pode ser adaptada e você pode detalhar o incidente para regulamentos de conformidade ou estudos adicionais.

Adotar o modelo Zero Trust

Outro benefício adicional da microssegmentação é sua capacidade de adotar o modelo de segurança Zero Trust. Embora a ideia do Zero Trust tenha sido inventada pela Forrester em 2010, tecnologias como a microssegmentação estão ajudando a tornar o conceito uma realidade, e pesquisadores e especialistas em segurança continuam a anunciar seus benefícios por toda parte.[4]

A ideia é simples: Nenhum tráfego ou usuário é confiável até que seja comprovado e aprovado, seja vindo de uma fonte externa ou interna, sempre que houver uma tentativa de conexão. Os três princípios principais do Zero Trust [5], da Forrester, são todos suportados por políticas de microssegmentação fortes e granulares:

- Não confiar em nenhuma entidade por padrão
- Implementar monitoramento de segurança abrangente
- Impor acesso de privilégio mínimo

Zero Trust está na extremidade oposta do espectro da segurança somente perimetral, onde você protege as entradas para o seu castelo com um fosso profundo e assume que qualquer coisa dentro está livre para entrada. Como a maioria das empresas não tem mais uma rede ou data center contido, a ideia de um "castelo" é obsoleta, e uma estratégia de menos privilégios como Zero Trust é a única maneira de garantir que você saiba e controle quem está dentro em um determinado momento.

Prepare sua empresa para o futuro com microssegmentação

A segmentação de rede pode certamente ir além da segurança do perímetro, e a segmentação do ambiente e de aplicações até a Camada 4 são etapas importantes na criação de sua estratégia de segmentação. Porém, à medida que os ambientes de TI se tornam cada vez mais complexos, você pode achar que precisa de uma solução de segmentação que ofereça ainda mais granularidade com segmentação de nível e aplicação no nível do processo para a Camada 7 nos estágios de aplicação e nível.

As empresas modernas foram além de uma infraestrutura independente. Geralmente, elas dependem de tecnologia como SDN na nuvem, contêineres ou hipervisores bare-metal. Elas trabalham em várias regiões geográficas e data centers físicos.

A única maneira de se proteger contra ameaças externas e internas é empregar uma solução que inspeciona e controla todo o tráfego, leste-oeste e norte-sul, e, para aplicações cruciais ou arriscadas, oferece mais visibilidade do que pode ser obtida somente da Camada 4. A microssegmentação até a Camada 7 no nível da aplicação ou do nível permite que você obtenha uma visão precisa de todo o seu ambiente de TI e permite que você crie e aplique facilmente políticas de segurança granulares que seguem o modelo Zero Trust. Uma boa solução de microssegmentação não pedirá que você escolha entre segurança e agilidade, portanto, faça a escolha que lhe dá a postura de segurança geral mais forte em toda a sua organização.

Acesse akamai.com/guardicore para obter mais informações.

1 Shier, John. 2022. "The Active Adversary Playbook 2022." Sophos. 7 de junho.

2 Gonda, Rob. 2018. "Adaptability Is Key To Survival In The Age Of Digital Darwinism (a adaptabilidade é fundamental para a sobrevivência na era do Darwinismo digital)." Forbes. 24 de maio.

3 https://www.verizon.com/business/reports/payment-security-report/

4 Holmes, David. Junho de 2022. "Best Practices For Zero Trust Microsegmentation (práticas recomendadas para microssegmentação Zero Trust)". Forrester. Abril.

5 Holmes, David e Jess Burn. Janeiro de 2022. "The Definition Of Modern Zero Trust (a definição do zero trust moderno)." Forrester. Abril.

A Akamai protege sua experiência do cliente, sua força de trabalho, seus sistemas e seus dados ajudando a incorporar a segurança em tudo o que você criar, em qualquer lugar que você criar e entregar. A visibilidade da nossa plataforma em relação às ameaças globais nos ajuda a adaptar e desenvolver sua postura de segurança para permitir Zero Trust, interromper ransomware, proteger aplicações e APIs ou combater ataques DDoS, dando a você a confiança para inovar, expandir e transformar continuamente o que é possível. Saiba mais sobre as soluções de segurança, computação e entrega da Akamai em akamai.com e akamai.com/blog ou Akamai Technologies no Twitter e LinkedIn. Publicado em 05/23.