Guardicore

SEGMENTAÇÃO DE REDE E MICROSSEGMENTAÇÃO EM AMBIENTES EMPRESARIAIS MODERNOS

WHITE PAPER

VISÃO GERAL

A ideia de segmentação pela segurança não é novidade. Os firewalls perimetrais juntamente com as VLANs e ACLs são o que a maioria das empresas tem usado tradicionalmente para segmentar e proteger sua infraestrutura de TI. No entanto, os tempos estão mudando. O aumento da virtualização, SDNs (Software-Defined Networks), e o uso de infraestrutura pública e multi-nuvem tem criado um novo conjunto de questões de segurança a serem abordadas, que precisa de uma solução construída para um ambiente com seu conjunto único de requisitos. Ameaças Persistentes Avançadas atualmente são um risco para qualquer negócio, e os invasores estão se tornando mais sofisticados, ao mesmo tempo em que a visibilidade se torna mais difícil de ser compreendida. As tradicionais medidas de segurança perimetral, bem como os firewalls de próxima geração baseados em inspeção profunda de pacotes ou na detecção baseada em assinaturas, lutam para acompanhar a quantidade de tráfego que um data center empresarial apresenta hoje. Vejamos como as técnicas corretas de microssegmentação são a melhor tecnologia para resolver as deficiências de outras abordagens alternativas de segmentação de rede.

OS FIREWALLS LEGADOS SÃO INADEQUADOS PARA O TRÁFEGO LESTE-OESTE

Como os ambientes híbridos de nuvem se tornaram o padrão, eles exigem um conjunto específico de requisitos acima e além da segurança do perímetro tradicional.

Ao procurar segmentar ambientes híbridos de nuvem, uma empresa pode primeiro olhar para dispositivos de segurança perimetrais legados. Infelizmente, estes dispositivos são criados para monitorar o tráfego que se move de norte a sul, de cliente para servidor. Isto inclui qualquer tráfego que chegue ao 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 chamado de tráfego leste-oeste, tem aumentado exponencialmente. Isto se deve em grande parte ao crescimento da virtualização e da infraestrutura convergente, como o Hypervisor, o VPC e a computação baseada em containers.

Medidas de segurança perimetrais como firewalls tradicionais não fazem nada para proteger sua empresa de dispositivos infectados e para prevenir invasores à medida que eles expandem sua base utilizando o tráfego leste-oeste. Com o aumento da criptografia TLS e a fácil ocultação do tráfego malicioso através de portas de aplicação legítimas abertas, muitos ataques podem passar mesmo quando cruzam os firewalls. Isto deixa você incapaz de detectar as 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 o tempo de permanência, mais catastrófica é a brecha. A Pesquisa de Resposta a Incidentes SANS de

2017 descobriu que para 20% das empresas, o tempo de permanência foi superior a um mês, e para 50% ainda é superior a 24 horas[1]. Quanto mais tempo um invasor tem em sua rede antes de ser detectado, mais danos podem ser causados.

Simplesmente não é possível usar firewalls virtualizados suficientes para proteger milhares de aplicações ou workloads. Mesmo se uma solução virtualizada pudesse ser criada, seria impossível gerenciar ou controlar considerando os ambientes dinâmicos em constante mudança nos quais agora trabalhamos. Quando se trata de nuvem híbrida, por exemplo, os firewalls tradicionais são ainda mais difíceis de se usar, pois precisam funcionar em diferentes ambientes, rastrear workloads através de diferentes nuvens e ser controlados a partir de um único ponto. Devido a estas questões, surgiram diversas abordagens de segmentação de rede.

TRÊS ABORDAGENS DE SEGMENTAÇÃO A SEREM CONSIDERADAS

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

1. **Segmentação de Ambiente**
   Esta abordagem separa os diferentes ambientes uns dos outros. Desta forma, as empresas poderiam segmentar o setor de desenvolvimento de sua empresa em relação ao ambiente de produção, por exemplo. Esta é a primeira etapa crucial em qualquer estratégia de segmentação, e pode ser seguida por uma criação de políticas mais granulares.

1 Bromiley, Matt. 2017. "The Show Must Go On! The 2017 SANS Incident Response Survey." SANS. June 12. https://www.sans.org/reading-room/whitepapers/incident/paper/37815

2. **Segmentação de Aplicação**
Levando isto adiante, as aplicações "ring-fencing" de alto valor levam cada aplicação essencial específica e a mantêm separada do resto da rede. As melhores soluções de microssegmentação permitirão até mesmo que isto seja controlado em um nível de processo.

3. **Segmentação em Camadas**
A forma mais restrita de segmentação está dentro de uma aplicação propriamente dita. Aqui você poderia criar uma política de como as comunicações são gerenciadas entre camadas dentro do mesmo cluster de aplicação, controlando o tráfego entre servidores web, servidores de aplicação e servidores de banco de dados, por exemplo. Isto também pode ser controlado com a aplicação de processos, se você preferir.

MÉTODO DE SEGMENTAÇÃO DE REDE – SEGMENTAÇÃO DE REDE ATRAVÉS DE VLANS

A maioria das empresas começa empregando VLANs. Estas redes locais virtuais permitem às empresas alocar a cada segmento seu próprio caminho de comunicação, através de um firewall ou listas de controle de acesso (ACLs) no próprio roteador. Embora a VLAN seja uma escolha comum, existem inúmeros problemas escondidos. Vamos olhar mais a fundo, fazendo um balanço dos motivos pelos quais as VLANs são uma escolha não muito adequada para suas necessidades de segurança.

É fácil ver porque muitas empresas escolhem as VLANs como seu método de segmentação. Isso pode ser feito com a arquitetura existente, o que faz com que pareça de baixo custo e simples de ser implantado. Entretanto, é uma abordagem de segmentação muito rígida e complexa, pode ser de manutenção cara e oferece pouca garantia de segurança.

Para começar a usar VLANs, você precisará se familiarizar com os servidores e dependências em cada segmento, e então criar a configuração desejada para o switch ou switches de rede que você está segmentando. Como isto é feito por engenheiros de rede, e muitas vezes envolve múltiplos locais, este processo pode levar diversos dias e custar uma quantia desmedida 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 uma necessidade, custos elevados e velocidade lenta quando se trata de mudanças, significa um desastre para o seu resultado final. De acordo com a Forbes, a adaptabilidade é a chave para a sobrevivência: "A disrupção não é nova, mas a velocidade, a complexidade e a

natureza global da disrupção está em uma escala que nunca vimos antes. Não é a maior ou mais estável financeiramente que sobreviverá, mas as que conseguem se adaptar ao ritmo exponencialmente acelerado da mudança".[2]

É importante reconhecer que as VLANs não foram criadas com a segmentação em mente. Construídas para reduzir o congestionamento, usá-las para limitar as comunicações não é uma forma inteligente de alavancar a tecnologia existente – é, em muitos sentidos, um mau uso. Considerando isto, não é surpreendente que o uso de VLANs para segmentação venha com limitações.

- **Tecnologia de Nuvem:** As 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, você provavelmente precisará contar com o SDN (software-defined networking) para a nuvem. Isso geralmente é feito através de provedores de software de terceiros que utilizam firewalls ou sub-redes virtualizadas.
- **Containers:** A segurança tradicional continua sendo uma barreira para a adoção generalizada de containers em ambientes de TI. Como cada container é executado sobre o mesmo núcleo, um exploit poderia colocar todos os containers em risco. O isolamento tem sido uma luta contínua, e não pode ser resolvido com a segmentação de rede.
- **Restrições de Protocolo:** O limite para VLANs é de 4096 segmentos, o que limita a capacidade de fornecer uma segmentação adequada em grandes data centers. Abordagens de segmentação mais granulares não possuem esta limitação.

SEGMENTAÇÃO DE REDE PARA SEGMENTAÇÃO DE APLICAÇÃO – INTRODUÇÃO DE CONTROLES DE CAMADA 4

Muitas destas questões foram melhoradas ao adotar a segmentação de aplicações usando grupos de segurança dentro de ambientes de nuvem e firewalls baseados em hypervisor para ambientes virtualizados no local. A segmentação tradicional de aplicações implementa controles de Camada 4, permitindo isolar as camadas de serviço umas das outras, de modo que uma aplicação tenha um limite seguro. Cada camada é limitada ao nível de acesso necessário para fornecer sua funcionalidade completa, mas não mais do que o necessário. Há uma clara separação entre as camadas de uma aplicação individual e a ameaça de um possível comprometimento é mantida a um mínimo.

2 Gonda, Rob. 2018. "Adaptability Is Key To Survival In The Age Of Digital Darwinism." Forbes. May 24. https://www.forbes.com/sites/forbestechcouncil/2018/05/24/adaptability-is-key-to-survival-in-the-age-of-digital-darwinism/#16c5c766408c

Pense nas camadas que você pode encontrar em um negócio padrão, desde balanceamento de carga e bancos de dados até servidores de aplicação ou dentro/fora de sua própria DMZ. Manter estas camadas separadas permite que cada uma tenha suas próprias regras e capacidades de segurança. A segmentação de aplicações pode ajudar as empresas a permitir os controles corretos para cada camada, limitando suas comunicações e informações sensíveis, ao mesmo tempo em que permite um amplo acesso do usuário quando necessário. Por exemplo, uma empresa pode impedir que certos bancos de dados se comuniquem completamente com a internet, ou garantir que, se um invasor violar um simples balanceador de carga, ele não possa se movimentar para acessar informações mais sensíveis no nível de banco de dados.

À medida que a solução se torna mais granular, a segmentação de aplicações permite a um negócio segmentar um cluster de aplicações inteiro a partir de outras áreas do negócio. Como discutido, isto reduz a área de superfície de ataque e a capacidade dos invasores de fazer movimentos laterais de um nível para outro.

OS LIMITES DA CAMADA 4

A segmentação das aplicações tradicionais pode faltar profundidade, o que tem um impacto direto em sua visibilidade. A camada de rede, onde o roteamento acontece, move os dados entre os sistemas, atribuindo endereços de IP e protocolos detalhando o caminho que os segmentos de dados levam ao seu destino. A segmentação de aplicações muitas vezes utiliza controles de Camada 4, observando a forma como os dados são entregues por si mesmos. Segmentos de dados maiores são divididos em segmentos ou blocos menores, prontos para serem colocados de volta em seu destino. O controle de fluxo permite que este processo seja acelerado ou retardado dinamicamente, onde os dispositivos que enviam ou recebem as informações necessitam.

No atual cenário de ameaças, os controles destas camadas são vitais, mas em certos casos você pode querer a liberdade de estabelecer políticas a um nível ainda mais granular. Os invasores têm demonstrado sua capacidade de falsificar endereços de IP e usar técnicas de piggybacking em portas permitidas para romper uma rede. Além disso, a proteção da Camada 4 não limita o movimento lateral dentro de uma aplicação ou de uma camada, o que poderia deixá-lo com uma área de ataque maior do que o necessário.

Um dos melhores exemplos da necessidade de mais do que a Camada 4 está na conformidade. As técnicas tradicionais de segmentação de aplicação permitiram, até certo ponto, que as empresas gerenciassem algumas regulamentações específicas de conformidade, tais como manter o CDE separado para PCI DSS, ou proteger o PHI para HIPAA. Entretanto, embora as técnicas de Camada 4 tenham sido aceitas no passado como um meio eficaz de mostrar conformidade, a realidade tem mostrado que pode

não fazer o suficiente. De acordo com o Relatório de Conformidade com a PCI da Verizon em 2018, apenas 52% das empresas estão em conformidade por completo.[3] Ainda pior, mesmo 100% em conformidade não equivale a 100% seguro. Embora os controles de C4 possam cobri-lo em termos de conformidade, isso não reduz suficientemente a área de ataque. Ponto final. Os invasores podem percorrer uma porta C4 aberta entre duas camadas com um processo separado (C7) e acessarem tudo o que quiserem.

SEGMENTAÇÃO NO ESCURO — A FALTA DE VISIBILIDADE EM SEGMENTAÇÃO DE REDE E DE APLICAÇÕES

Como as empresas descobriram, embora não haja dúvida de que a segmentação de aplicações é um passo na direção certa, ela não vai suficientemente longe para resolver todas as questões de uma abordagem bruta de segmentação. Outro desafio que ainda precisa ser enfrentado é a visibilidade. Ser capaz de ver uma visão geral precisa e em tempo real de sua rede é essencial em cada etapa de seu processo de segmentação, uma limitação de muitas abordagens de segmentação.

Antes de começar, você vai querer visualizar as dependências da aplicação para que você possa elaborar políticas precisas. Após a segmentação ter sido colocada em prática, você precisará de provas de que sua segmentação está funcionando como planejado, não apenas para ter certeza de que sua postura de segurança é forte, mas também para fornecer provas de conformidade regulamentar, quando necessário.

Sem visibilidade histórica e em tempo real, não há provas para você ou para terceiros interessados e órgãos reguladores. Além disso, seu sistema ainda será demorado e caro de gerenciar e abri-lo a erros e falhas de configuração. Usar a segmentação de aplicações não é garantia suficiente por si só de que você tem a visibilidade necessária para corrigir estes problemas.

MICROSSEGMENTAÇÃO ATÉ A CAMADA 7 — A CAMADA DE APLICAÇÃO

Em contraste, a camada de aplicação (Camada 7) é altamente eficaz na limitação do movimento lateral, ainda que dentro de um cluster de aplicação. A Camada 7 é onde os serviços de rede se integram com o sistema operacional. Pense em protocolos como HTTP, FTP, TFTP e SMTP. Todos estes são protocolos da Camada 7. Os últimos avanços na microssegmentação são capazes de segmentar aqui, com muito mais

3 2018. "2018 Payment Security Report." Verizon. September. https://enterprise.verizon.com/resources/reports/2018_payment_security_report_executive_summary_en_xg.pdf

profundidade, permitindo que sua empresa visualize e controle a atividade na Camada 7, bem como na tradicional Camada 4. Isto significa que, ao invés de depender de endereços de IP e portas, processos e fluxos específicos podem ser usados quando as empresas configuram suas políticas. Isto leva os benefícios da segmentação muito além de uma camada específica ou até mesmo de um cluster de aplicações. Também permite detectar ameaças potenciais tão pequenas quanto um hash errado, mesmo quando o invasor está espelhando um processo ou caminho autorizado.

Quando se trata de criação de políticas, a segmentação para a Camada 7 permite exceções e regras de whitelisting muito específicas, onde apenas processos ou fluxos exatos são permitidos, e todas as outras comunicações são bloqueadas por padrão. Isto pode impor dois sistemas separados tendo seus dados isolados um do outro, mas ainda permitindo a comunicação para suporte ao cliente ou fluxos de dados necessários, por exemplo.

AS MELHORES SOLUÇÕES DE MICROSSEGMENTAÇÃO FORNECEM VISÃO QUE OS NEGÓCIOS PRECISAM PARA GANHAR AGILIDADE

Com agentes em cada VM — seja baseado em hypervisor ou VPC, cada container, e até mesmo servidores bare metal — uma solução integral de microssegmentação pode fornecer ao seu negócio um mapa visual completo de toda a sua infraestrutura de TI. Com as soluções verdadeiramente inteligentes, isto inclui ambientes de data center, nuvens e ambientes multi-nuvem e híbridos de nuvem. Isto tende a ser perdido com a segmentação de aplicações, porque você está usando uma combinação de tecnologias centradas em rede.

Esta representação visual pode lhe mostrar quais políticas estão em vigor e sendo aplicadas em tempo real. Com um olhar, seus engenheiros e profissionais de segurança podem ver onde há brechas a serem corrigidas na cobertura de suas políticas, ou que políticas adicionais eles precisam implementar ou criar do zero.

Este benefício também permite que sua empresa se prepare com antecedência para novos softwares ou atualizações de sistemas existentes, criando as regras para segmentar aplicativos atualizados ou novos antes que estejam prontos para a implantação com antecedência. Uma vez que as atualizações estejam ativadas, suas equipes de segurança têm as informações em tempo real que necessitam para detectar e resolver atividades de aplicações que estejam fora do normal, garantindo que nenhum risco de segurança passe despercebido ou se torne um exploit ativo.

Após o fato, sua empresa dispõe das ferramentas contextuais para comparar um incidente com dados históricos e entender o ambiente exato que permitiu que a anomalia ocorresse. As políticas podem ser mais rígidas, a segmentação pode ser adaptada e você pode detalhar o incidente para regulamentos de conformidade ou estudo adicional.

UTILIZANDO O MODELO CONFIANÇA ZERO

Outro benefício adicional da microssegmentação é sua capacidade de incorporar o modelo de segurança "confiança zero". Embora a ideia de confiança zero tenha sido criada pela Forrester em 2010, tecnologias como a microssegmentação estão ajudando-a finalmente a se tornar o padrão, e pesquisadores e especialistas em segurança continuam a clamar seus benefícios em toda parte.[4]

A ideia é simples: nenhum tráfego ou usuário é confiável até que seja comprovado e aprovado pela instância, seja de uma fonte externa ou interna. Os três princípios fundamentais da confiança zero da Forrester são todos cobertos sem esforço com uma forte política de microssegmentação.

- Garanta todos os recursos, independentemente do local
- O controle de acesso segue o modelo menos privilegiado
- Todo o tráfego é registrado e inspecionado

A confiança zero é a extremidade oposta do espectro da segurança de perímetro, onde você protege as entradas de seu castelo com um fosso profundo e assume que qualquer coisa dentro é autorizada para entrar. Como a maioria das empresas não tem mais um data center, a ideia de um "castelo" é ultrapassada, e o privilégio mínimo ou confiança zero é a única maneira de garantir que você saiba quem está lá dentro em um determinado momento.

ANTECIPE O FUTURO DE SUA EMPRESA COM A MICROSSEGMENTAÇÃO

A segmentação da rede pode certamente ir além da segurança de perímetro, e a segmentação do ambiente e da aplicação até a Camada 4 são passos importantes na construção de sua estratégia de segmentação. À medida que os ambientes de TI se tornam cada vez mais complexos, você pode achar que precisa de sua solução de segurança para oferecer ainda mais granularidade com a segmentação de camadas, e a aplicação do nível de processo para a Camada 7 nas etapas de aplicação e de camada.

4 Cunningham, Chase. 2018. "Next- Generation Access and Zero Trust." Forrester. Mar 27. https://go.forrester.com/blogs/next-generation-access-and-zero-trust/

Os negócios foram além de uma infraestrutura independente. Muitas vezes eles confiam em tecnologia como SDN na nuvem, containers, ou bare-metal hypervisors. Eles trabalham em diferentes geografias e data centers físicos.

A única maneira de se proteger de ameaças externas e internas é empregar uma solução que inspecione e controle todo o tráfego, tanto leste-oeste quanto norte-sul, e — para aplicações críticas ou de risco — lhe proporciona mais visibilidade do que pode ser obtida apenas a partir da Camada 4. A microssegmentação até a Camada 7, tanto no nível da aplicação como no nível de camada, lhe dá a capacidade de obter uma visão precisa em tempo real de todo o seu ambiente de TI, seguindo o verdadeiro modelo confiança zero.

Além disso, a tecnologia de microssegmentação não pede que você escolha entre segurança e agilidade, o que o ajuda a quebrar silos para uma forte postura geral de segurança em toda a sua organização.

Sobre a Guardicore

A Guardicore é a empresa de segmentação com soluções disruptivas para substituir o legado de firewalls tradicionais. Nossa abordagem, baseada unicamente em software, é independente da rede física, representando uma alternativa mais rápida ao firewall. Feita para empresas ágeis, a plataforma Guardicore oferece mais visibilidade e segurança na nuvem, datacenter e endpoints. Para mais informações acesse www.guardicore.com, nosso Twitter ou LinkedIn.

Guardicore