WHITE PAPER – MARÇO DE 2021

Proteção do data center em apenas quatro etapas

vmware | intel

SOBRE A INTEL E O FIREWALL DEFINIDO POR SERVIÇO DA VMWARE NSX

Otimizado na arquitetura Intel®, o Firewall definido por serviço da VMware pode reduzir despesas de Capex e Opex em comparação com appliances de firewall personalizados que usam hardware proprietário e podem ter a manutenção muito cara.

Da posição que tem dentro do hypervisor, o Firewall definido por serviço da VMware oferece visibilidade do comportamento do aplicativo e do tráfego da rede para fornecer proteção à carga de trabalho, pois detecta e reduz ameaças no tráfego leste-oeste dentro do perímetro do datacenter. Com microssegmentação avançada e baseada em software.

Com os Serviços de detecção de intrusão/Serviços de prevenção contra intrusões (IDS/IPS), o Firewall definido por serviço minimiza as superfícies de ataque e reduz os falsos positivos ao atribuir assinaturas selecionadas a aplicativos que se movem enquanto os aplicativos migram com o vMotion pelas redes.

O suporte da Intel® QuickAssist Technology (Intel® QAT) para criptografia em massa de VPN agora é compatível com a estrutura VMware NSX-T a fim de descarregar a criptografia em massa de VPN na borda bare metal para a obtenção de maior proteção e melhor experiência do usuário.

Introdução

Na luta sem fim contra os ataques cibernéticos, as empresas dependem há muito tempo de firewalls perimetrais tradicionais para impedir que os criminosos atinjam seus alvos no data center. Devido às evidências de que o perímetro atual é permeável e suscetível de ser violado, as empresas começaram a tentar melhorar as posturas de segurança dentro das redes corporativas.

No entanto, no contexto dos aplicativos distribuídos modernos e das cargas de trabalho cada vez mais dinâmicas, a proteção de todo o tráfego, ou ao menos a maioria do tráfego leste-oeste (interno), tem sido vista como muito complexa, cara e demorada para os data centers existentes e até mesmo os novos. Essa percepção é certamente precisa para as empresas que tentam proteger o tráfego leste-oeste por meio de firewalls perimetrais tradicionais com base em appliances, como firewalls internos.

De fato, há uma alternativa simples, segura e econômica. Um *firewall interno distribuído e com dimensionamento horizontal* designado especificamente para monitorar e proteger o tráfego leste-oeste é a melhor solução para defender os data centers e as cargas de trabalho de hoje, pois elimina a complexidade, os gastos e as limitações de dimensionamento e flexibilidade dos firewalls perimetrais tradicionais.

Ao impedir o movimento lateral, um firewall interno distribuído como o *Firewall definido por serviço NSX da VMware* melhora a segurança das cargas de trabalho modernas. Como é distribuído, tem reconhecimento de aplicativo e é simples de operar, o firewall definido por serviço simplifica e automatiza muito do planejamento, implantação, configuração e gerenciamento dos firewalls internos e das políticas e recursos detalhados que fornecem suporte para ele.

Entretanto, cada nova solução implantada requer tempo e esforço por parte das equipes de segurança para aprender a usar a tecnologia de maneira eficaz e saber como melhor implementá-la no ambiente atual de uma organização. Neste white paper, apresentamos uma abordagem de quatro etapas que ajuda as organizações a aproveitar rapidamente os benefícios da implantação do firewall definido por serviço, além de expandir o uso com o tempo para proteger o data center completo.

Segurança que supera os desafios de hoje

Os CISOs e suas equipes de segurança encaram cada vez mais desafios na tentativa de proteger os negócios contra ataques cibernéticos:

- O novo campo de batalha das ameaças cibernéticas é o interior do data center
- As equipes têm pouca ou nenhuma visibilidade do tráfego leste-oeste
- As ameaças que ultrapassam o perímetro podem se mover lateralmente sobre o tráfego permitido no data center quase sem interrupções
- Os modelos de home office e a infraestrutura de desktop virtual (VDI, pela sigla em inglês) permitem que o tráfego chegue diretamente ao data center, expondo a ameaças as cargas de trabalho em execução.

As soluções de segurança tradicionais com base em appliances não são eficazes para dar visibilidade do tráfego leste-oeste e impedir o movimento lateral das ameaças. É por isso que as empresas estão adotando o firewall definido por serviço da VMware, um firewall interno distribuído que protege todo o tráfego leste-oeste com segurança intrínseca à infraestrutura, o que simplifica radicalmente o modelo de implantação. (Para saber mais sobre os desafios dos controles de segurança de rede tradicionais para proteger as cargas de trabalho modernas, leia o white paper *Cinco requisitos essenciais para firewalls internos no data center.)*

Com o firewall definido por serviço, as equipes de segurança podem proteger a marca de ameaças internas e minimizar o dano de ataques cibernéticos que ultrapassam o perímetro de rede tradicional. A solução inclui um *firewall distribuído*, um *sistema de detecção e prevenção de intrusões (IDS/IPS, pela sigla em inglês)*, e técnicas de análise por meio do *NSX Intelligence* (veja a Figura 1).

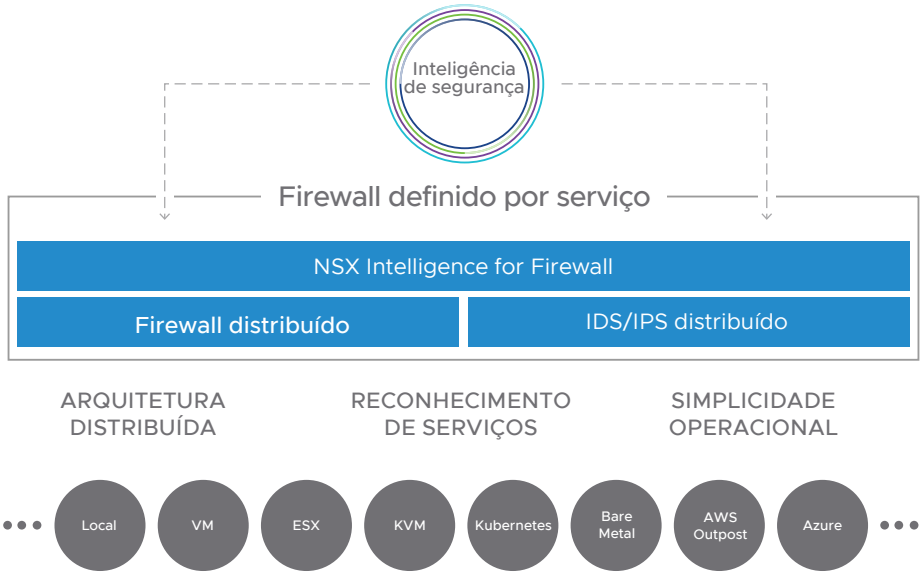

FIGURA 1: Arquitetura do firewall definido por serviço VMware NSX

As quatro etapas de modernização do data center

A implementação de qualquer nova abordagem ou solução de segurança requer tempo e compromisso de uma equipe de segurança que já está no limite. Por esse motivo, embora a implantação de segurança leste-oeste seja mais fácil e rápida com um firewall interno distribuído, muitas organizações ainda preferem uma abordagem iterativa por fases para melhorar a segurança do data center.

Além de não sobrecarregar a equipe com uma grande iniciativa, a divisão da implantação de um firewall interno em projetos menores traz benefícios adicionais: Permite que as equipes de segurança comprovem o êxito mais cedo e demonstrem o valor da abordagem para as partes interessadas internas. Depois, elas podem usar sua experiência para expandirem o uso dos firewalls internos distribuídos e obter maturidade, velocidade e confiança na organização conforme progridem.

Embora haja diferentes abordagens, as quatro etapas a seguir (Figura 2) têm sido usadas por clientes VMware para começar com pouco e fortalecer continuamente as defesas de seus data centers ao longo do tempo.

1. Rastejamento: Macrossegmente a rede
2. Caminhada: Proteja aplicativos essenciais
3. Trote: Ganhe visibilidade e proteja aplicativos adicionais
4. Corrida: Proteja todos os aplicativos

FIGURA 2: Uma abordagem em quatro etapas para proteger o data center

Para saber mais sobre a proteção do ambiente VDI, leia a visão geral da solução *Firewall definido por serviço para desktops virtuais.*

Rastejamento: Macrossegmente a rede

Para muitas organizações, a primeira etapa na proteção do tráfego leste-oeste é a mais difícil. Isso acontece porque tentar macrossegmentar a rede por meio de firewalls tradicionais com base em appliances é, além de caro, demorado, complexo e inflexível.

No entanto, o uso de um *firewall interno distribuído* simplifica a arquitetura de segurança e acelera o time to value, o que facilita a implantação da macrossegmentação para melhorar a segurança do tráfego leste-oeste. Também é mais flexível e se adapta facilmente a mudanças nos requisitos de rede e segurança conforme a empresa evolui.

Com o firewall definido por serviço, sua equipe de segurança pode começar a usar *segmentação de rede* para isolar e proteger mutuamente ambientes específicos, como o de desenvolvimento e produção. Isso impede, de maneira instantânea, invasores e funcionários maliciosos de se mover lateralmente entre esses ambientes.

Objetivo

Implantar o firewall definido por serviço para proteger segmentos da rede criando zonas de segurança virtual. Ao macrossegmentar esses ambientes, a equipe de segurança pode melhorar a postura geral de segurança para o data center, impedindo o movimento lateral entre zonas.

Caso de uso comum

Dependendo da estrutura de negócios e dos casos de uso, uma equipe de segurança normalmente escolheria segmentar ambientes que não são capazes de se comunicar entre si. Os exemplos comuns incluem diferentes unidades de negócios, ambientes de parceiros e ambientes de desenvolvimento e produção.

Benefícios

- Mostrar prova de êxito a partes interessadas internas da empresa graças a uma abordagem apropriada de firewall interno
- Impedir que atacantes se movam entre zonas para limitar os danos causados por um ataque em uma zona específica
- Fornecer uma solução mais flexível em comparação com um firewall tradicional baseado em appliance para permitir que as organizações aumentem facilmente o número de zonas conforme necessário

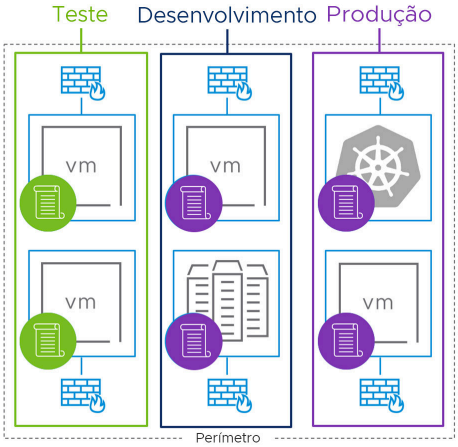

FIGURA 3: Segmentação de rede

Caminhada: Proteja aplicativos essenciais

Normalmente, a próxima etapa da proteção do data center é começar a passar da macrossegmentação para a *microssegmentação*, o que permite que a equipe de segurança defina e aplique controles mais detalhados, até o nível da carga de trabalho.

A equipe de segurança escolhe um pequeno número de aplicativos bem compreendidos que são essenciais para os negócios e devem ser isolados e protegidos com controles de segurança adicionais para impedir acessos não autorizados, violações de dados e outras formas de ataque.

Para esses aplicativos, os controles de segurança detalhados podem ser ainda mais aprimorados com recursos de *IDS/IPS* para detectar padrões de tráfego que sinalizem um ataque. Embora seja possível isolar aplicativos com algumas soluções expressamente projetadas para microssegmentação, elas não fornecem recursos de IDS/IPS, necessários para a conformidade com regulamentos como o Health Insurance Portability and Accountability Act (HIPAA) e o Payment Card Industry Data Security Standard (PCI DSS).

Saiba mais sobre visibilidade no white paper *Operacionalize a microssegmentação facilmente com o NSX Intelligence.*

Objetivo

Usar microssegmentação para isolar e proteger um ou mais aplicativos críticos, aplicando controles de segurança em camadas específicos para o aplicativo e impedindo o movimento lateral de invasores dentro ou fora do segmento em que o aplicativo é executado.

Caso de uso comum

Ao considerar um aplicativo crítico para começar a microssegmentação, as organizações costumam iniciar pelo ambiente de infraestrutura de desktop virtual (VDI) ou outros aplicativos críticos como serviços compartilhados (como o Active Directory) ou servidores DNS. O ambiente VDI, além de melhorar a capacidade de gerenciamento, custos e proteção de dados para desktops de usuários, expõe a infraestrutura do data center a ameaças decorrentes de violações à segurança do usuário final. No entanto, com o firewall definido por serviço, a equipe de segurança pode isolar zonas de desktops dos recursos confidenciais do data center. A funcionalidade VMware NSX Distributed IDS/IPS adiciona recursos de inspeção de tráfego ao firewall definido por serviço para fornecer controle de ameaças, além do controle de acesso, em uma abordagem de segurança em camadas.

Benefícios

- Reduzir a superfície de ataque isolando aplicativos essenciais de outros recursos do data center.
- Mitigar o movimento lateral de fora do segmento
- Possibilitar controles de acesso específicos de usuários e aplicativos para aplicativos sensíveis
- Detectar ameaças avançadas usando recursos IDS/IPS

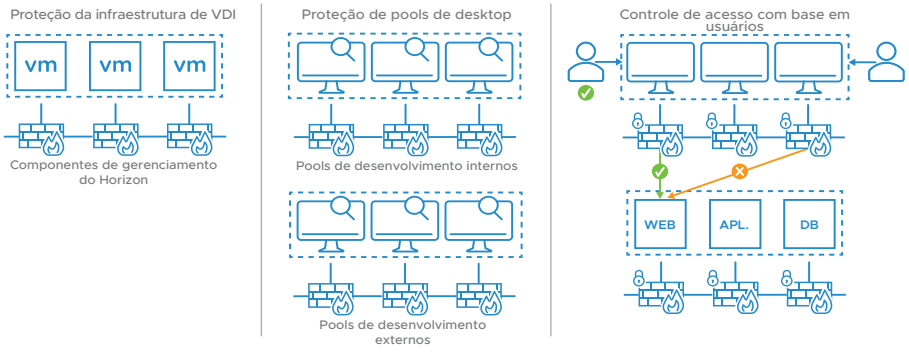

FIGURA 4: Proteção de ambientes de VDI

Trote: Ganhe visibilidade e proteja aplicativos adicionais

Conforme a equipe de segurança ganha mais experiência na operação de um firewall interno distribuído, pode continuar expandindo o monitoramento e a proteção do tráfego leste-oeste para outras cargas de trabalho essenciais ou importantes dentro do data center.

Para aplicativos que não são bem entendidos, o firewall definido por serviço dá à equipe de segurança visibilidade do data center completo e aplica o aprendizado de máquina incorporado para ajudar a equipe a entender aplicativos e fluxos de tráfego. A descoberta automatizada de aplicativos dá à equipe de segurança um mapa detalhado da topografia dos aplicativos, assim como recomendações geradas automaticamente para políticas de segurança com base nos fluxos de tráfego observados.

Objetivo

Aproveitar os conhecimentos e habilidades que sua equipe adquiriu nas duas primeiras etapas e usar a visibilidade e a automação incorporadas no firewall definido por serviço para isolar e proteger mais cargas de trabalho, o que reduz mais a superfície de ataque e fortalece a segurança do data center.

Para um exemplo de uma organização que implantou o firewall definido por serviço para dar suporte à conformidade, leia o white paper *Firewall interno: a melhor maneira de proteger o tráfego leste-oeste.*

SOBRE AS SOLUÇÕES INTEL E VMWARE PARA A REDE DE NUVEM VIRTUAL

A VMware e a Intel transformaram a rede e segurança com o Virtual Cloud Network, uma visão de rede voltada à era digital. A Virtual Cloud Network, criada com base na tecnologia do VMware NSX e executada na arquitetura Intel® com a Intel® QuickAssist Technology (Intel® QAT), fornece uma camada de software onipresente em todo o data center, na nuvem, na borda e em outras infraestruturas de hardware, oferecendo conectividade e segurança abrangentes para aplicativos e dados, independentemente de onde eles residam. A Intel QAT acelera a Open SSL e aplicativos de borda de rede para a obtenção de resultados de alto desempenho durante a implantação de Firewalls definidos por serviço da VMware.

Caso de uso comum

As equipes de segurança costumam focar esse caso na proteção de aplicativos importantes para os quais uma interrupção ou roubo afetaria os resultados de negócios. Isso inclui aplicativos como os que geram receita, lidam com informações sensíveis de clientes ou empresas e fornecem experiências do cliente digital importantes, além de outros aplicativos essenciais para os negócios centrais.

Benefícios

- Fornecer visibilidade da topologia dos aplicativos com um mapa visual gerado automaticamente que mostra os aplicativos e fluxos de tráfego, eliminando a dependência de suposições
- Automatizar o processo de descoberta e aplicação de políticas de segurança e acelerar a criação de políticas com recomendações geradas automaticamente
- Reduzir os pontos cegos de segurança inspecionando mais tráfego leste-oeste para detectar e bloquear rapidamente o movimento lateral e limitar possíveis danos

Corrida: Proteja todos os aplicativos

Neste ponto da jornada, as equipes de segurança estão prontas para proteger todos os aplicativos no data center com o firewall definido por serviço e mitigar o risco de segurança enquanto o dimensionam sem complicações para proteger novas cargas de trabalho e aumentos no tráfego. Eles também podem ativar a conformidade com requisitos normativos por meio dos recursos de IDS/IPS do firewall definido por serviço. Organizações que antes usavam firewalls perimetrais com base em appliances como firewalls internos reduzirão custos ao substitui-los pelo firewall definido por serviço.

Objetivo

Estender a implantação do firewall definido por serviço para inspecionar e proteger todo o tráfego leste-oeste no data center e fornecer camadas de proteção adicionais para cargas de trabalho sensíveis com os recursos de IDS/IPS do firewall.

Caso de uso comum

Embora todo o tráfego leste-oeste agora seja monitorado pelo firewall definido por serviço, as equipes de segurança podem implantar detecção e prevenção avançadas de ameaças por meio de IDS/IPS para atingir conformidade normativa em aplicativos sensíveis, como aqueles em que se aplicam HIPAA, PCI DSS e outros mandatos.

Benefícios

- Melhorar a proteção de todas as cargas de trabalho no data center contra ataques cibernéticos
- Reduzir o custo e a complexidade ao eliminar a necessidade de firewalls físicos e appliances IDS/IPS
- Simplificar a implantação e o gerenciamento da funcionalidade IDS/IPS em cada carga de trabalho
- Atingir a conformidade normativa ativando a inspeção IDS/IPS para aplicativos sensíveis

Conclusão

Conforme as empresas tomam medidas para proteger o tráfego e as cargas de trabalho do data center contra ataques cibernéticos, elas precisam de uma abordagem apropriada de firewall interno que proteja a marca contra ameaças internas e minimize os danos de ataques cibernéticos que ultrapassem a segurança de perímetro tradicional.

Por meio de uma abordagem em várias etapas, as equipes de segurança podem usar o firewall definido por serviço da VMware para melhorar continuamente a segurança ao longo do tempo, começando por zonas de segurança virtual e expandindo-se para todas as cargas de trabalho no data center. O firewall definido por serviço protege todo o tráfego leste-oeste com segurança intrínseca à infraestrutura, simplificando radicalmente o modelo de implantação e permitindo que as equipes de segurança acelerem as operações de segurança.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 EUA Tel.: 1-877-486-9273 Fax: 1-650-427- 5001 www.vmware.com
Rua Surubim, 504 4º andar CEP 04571-050 Cidade Monções – São Paulo – SP Tel.: (11) 5509-7200 www.vmware.com/br