MICROSSEGMENTAÇÃO COM RECONHECIMENTO DE CONTEXTO NO VMWARE NSX DATA CENTER

Proteja a rede contra a propagação lateral de ameaças

Os aplicativos modernos são complexos, distribuídos e dinâmicos

Todas as organizações estão descobrindo como operar seus negócios no mundo hiperconectado, no qual aplicativos e dados são vitais. Os aplicativos modernos são distribuídos em vários data centers e nuvens e estendidos até o perímetro do ambiente.

A virtualização, juntamente com a chegada do DevOps, da conteinerização e dos microsserviços, permite que os aplicativos sejam criados e alterados com mais rapidez do que nunca. A natureza distribuída dos aplicativos modernos e a velocidade com a qual eles mudam tornam a manutenção da segurança um grande desafio.

As estratégias de segurança legadas não são mais eficazes

À medida que os aplicativos continuam se expandindo, as abordagens de segurança centralizadas no perímetro legado se mostram insuficientes para proteger os aplicativos e os dados. Os invasores provaram que podem penetrar ou contornar as medidas de segurança de perímetro com frequência. Depois de entrar, eles se movem lateralmente, de servidor para servidor, sem restrições, procurando informações para roubar ou sequestrar.

No mundo dos aplicativos distribuídos modernos, as equipes de segurança de TI e sistema de rede são frequentemente desafiadas a manter políticas de segurança distintas em diferentes partes do ambiente, o que resulta em falhas na postura geral de segurança.

Segurança consistente do data center à nuvem e ao perímetro

Com o VMware NSX® Data Center, as políticas de segurança podem ser definidas de forma consistente em todo o ambiente, independentemente do tipo de aplicativo ou de onde ele foi implantado. As políticas são aplicadas no nível da carga de trabalho individual, o que permite a segmentação das cargas de trabalho que residem no mesmo host físico, sem precisar redirecionar o tráfego por meio de um firewall externo físico ou virtual. Esse nível detalhado de segurança é chamado de microssegmentação.

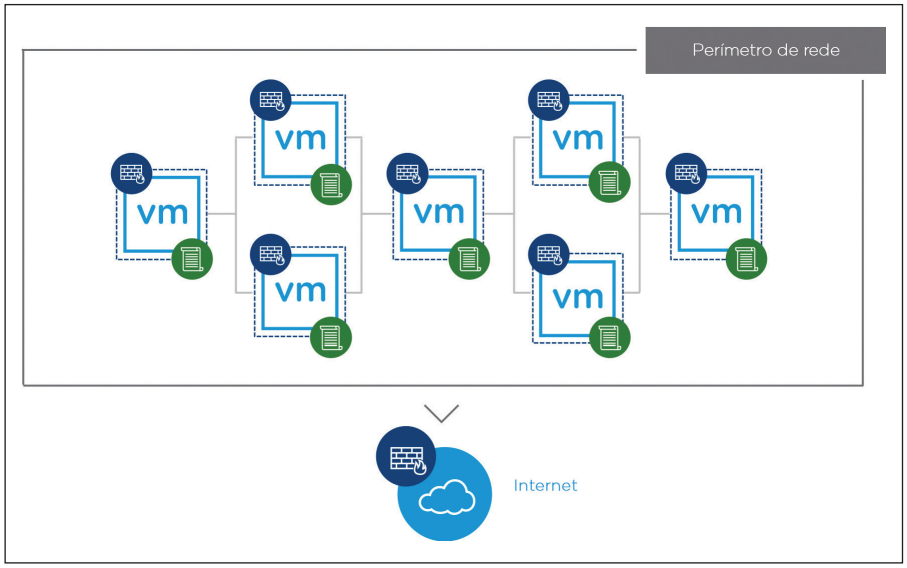

Figura 1. A microssegmentação se refere à aplicação da política de segurança de rede no nível da carga de trabalho individual.

"Com o crescente número de dispositivos de IoT, quanto mais segmentada for nossa rede, melhor estaremos... Assim, as ameaças não conseguem se mover lateralmente no data center."

CHRISTOPHER FRENZ
DIRETOR DE INFRAESTRUTURA
INTERFAITH MEDICAL CENTER

vmware®

PRINCIPAIS DESTAQUES

- A natureza dinâmica e distribuída dos aplicativos modernos torna a segurança legada e centrada no perímetro insuficiente.
- O VMware NSX Data Center permite a microssegmentação para proteger os aplicativos contra a propagação lateral de ameaças.
- A política de segurança é definida com base no contexto do aplicativo e aplicada à carga de trabalho.
- A segurança é fornecida de modo consistente do data center à nuvem e ao perímetro.

Os migrossegmentos criados com o NSX Data Center são definidos e gerenciados no software, tornando-os ágeis e automatizáveis. À medida que novas cargas de trabalho são implantadas, elas herdam automaticamente as políticas de segurança que permanecem com a carga de trabalho durante todo o seu ciclo de vida, independentemente de onde tenham sido aprovisionadas ou para onde possam migrar.

Microssegmentação com reconhecimento de contexto, segurança alinhada a aplicativos e dados

A capacidade de definir políticas de segurança de acordo com prioridades é tão importante quanto o fornecimento consistente das políticas. O NSX Data Center dissocia a política de segurança dos atributos de rede estáticos, como endereço IP, porta e protocolo, e permite a definição de políticas com base em uma compreensão contextual do aplicativo e da infraestrutura. Esses contextos incluem atributos de usuário e identidade, atributos de carga de trabalho (como o sistema operacional) ou até mesmo escopos de conformidade normativa.

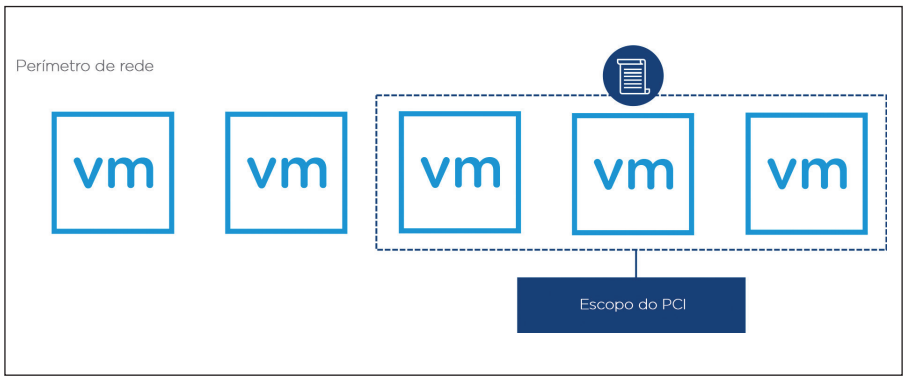

Figura 2. Os microssegmentos no NSX Data Center podem ser definidos com base em vários contextos diferentes, incluindo os escopos de conformidade normativa.

A microssegmentação com reconhecimento de contexto no NSX Data Center oferece às equipes de segurança de rede a flexibilidade necessária para proteger seus aplicativos e dados com base nos fatores mais importantes. Por exemplo, o NSX Data Center pode ser usado para proteger a implantação da infraestrutura de desktop virtual (VDI) por meio da aplicação da política de rede com base no contexto do usuário até o nível da sessão individual do RDSH. As políticas de segurança também podem ser aplicadas a todas as cargas de trabalho que se enquadram nos padrões da indústria de cartões de pagamento (PCI), independentemente de onde elas estejam fisicamente no ambiente.

Serviços avançados de segurança: onde e quando são necessários

O NSX Data Center permite a inclusão de serviços avançados de segurança de terceiros em um microssegmento específico. Em vez de rotear todo o tráfego de rede por meio de um appliance físico ou appliance virtual, como um firewall de próxima geração (NGFW) ou um sistema de detecção de intrusões (IDS)/sistema de prevenção contra intrusões (IPS), o NSX Data Center pode direcionar dinamicamente um tráfego específico para esses serviços na camada de rede virtual. Ao fazer isso, os serviços avançados de segurança podem ser inseridos nos lugares certos, no momento certo, maximizando a eficiência do tráfego de rede e aumentando a eficácia dos próprios serviços de segurança.

Visualize o tráfego de rede de todo o ambiente

O primeiro passo para a microssegmentação é entender como o tráfego de rede está fluindo. O VMware Network Insight™ fornece uma visão abrangente de todo o tráfego de rede no data center, incluindo tráfego de rede física e virtual. Após analisar o tráfego de rede, o VMware Network Insight recomendará automaticamente políticas de microssegmentação que podem ser utilizadas pelo NSX Data Center para implementação.

Comece hoje mesmo com uma avaliação de rede virtual gratuita para analisar seu tráfego de rede atual e começar a planejar seu projeto de microssegmentação. Para saber mais, acesse www.vmware.com/br/products/nsx/security.

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

Nº do item: 147939wf-vmw-q2fy19-sddc-launch-so-nsbu-context-aware-micro-seg-a4
5/18