

Making Everything Easier!™

Edição especial VMware

Micros-segmentação

PARA
LEIGOS®

Aprenda a:

- Desenvolver um data center seguro desde o início
- Impedir a propagação lateral de ataques ao data center
- Implantar uma plataforma para soluções de segurança avançadas

Produzido pela
vmware®

Lawrence Miller, CISSP
Joshua Soto



Sobre a VMware

A VMware é líder em infraestrutura em nuvem e mobilidade empresarial. Desenvolvidas na tecnologia de virtualização líder do setor da VMware, nossas soluções fornecem um novo modelo de TI proativo, fluido, instantâneo e mais seguro. Os clientes podem inovar com mais agilidade desenvolvendo rapidamente, fornecendo automaticamente e consumindo qualquer aplicativo com mais segurança. A empresa é sediada no Vale do Silício e conta com filiais pelo mundo todo. Visite o site **www.vmware.com**.

Micros- segmentação

PARA
LEIGOS[®]

Edição especial VMware

**por Lawrence Miller, CISSP,
e Joshua Soto**

WILEY

Microssegmentação Para Leigos®, Edição especial VMware

Publicado por

John Wiley & Sons, Inc.

111 River St.

Hoboken, NJ 07030-5774

www.wiley.com

Copyright © 2016 por John Wiley & Sons, Inc., Hoboken, New Jersey

Nenhuma parte desta publicação pode ser reproduzida, armazenada em um sistema de recuperação de dados ou transmitida de nenhuma forma ou por qualquer meio, eletrônico, mecânico, fotocópia, gravado, escaneado ou de outra forma, exceto conforme permitido nas Seções 107 ou 108 do Ato dos Direitos Autorais dos Estados Unidos de 1976, sem a permissão do autor ou da Editora. Solicitações à Editora para permissão devem ser endereçadas ao Departamento de Permissões, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, ou online em <http://www.wiley.com/go/permissions>.

Marcas comerciais: Wiley, For Dummies, o logotipo Dummies Man, The Dummies Way, Dummies.com, Making Everything Easier e outras identidades visuais relacionadas são marcas comerciais ou marcas comerciais registradas de John Wiley & Sons Inc. e/ou de suas afiliadas, nos Estados Unidos e outros países, e não podem ser utilizados sem autorização por escrito. IBM e o logotipo da IBM são marcas comerciais registradas na International Business Machines Corporation. Todas as outras marcas comerciais são propriedade de seus respectivos donos. John Wiley & Sons, Inc. não está associada com nenhum produto ou fornecedor mencionado neste livro.

LIMITE DE RESPONSABILIDADE/ISENÇÃO DE GARANTIA: A EDITORA E O AUTOR NÃO FAZEM REPRESENTAÇÕES OU GARANTIAS NO QUE DIZ RESPEITO À EXATIDÃO OU COMPLETITUDE DO CONTEÚDO DESTE TRABALHO E ESPECIFICAMENTE NEGA TODAS AS GARANTIAS, INCLUINDO GARANTIAS SEM LIMITAÇÃO PARA ADEQUAÇÃO A INTERESSE PERTINENTE. NENHUMA GARANTIA PODE SER CRIADA OU EXTENDIDA ATÉ RAVÉS DE VENDAS OU MATERIAIS PROMOCIONAIS. AS OPINIÕES E ESTRATÉGIAS AQUI CONTIDAS PODEM NÃO SE AJUSTAR A TODAS AS SITUAÇÕES. ESTE TRABALHO É COMERCIALIZADO COM O ENTENDIMENTO DE QUE A EDITORA NÃO ESTEJA COMPROMETIDA COM PRESTAÇÃO DE SERVIÇOS JURÍDICOS, CONTABILIDAD E OU OUTROS SERVIÇOS PROFISSIONAIS. SE FOR SOLICITADA ASSISTÊNCIA PROFISSIONAL, OS SERVIÇOS DE UM PROFISSIONAL COMPETENTE DEVEM SER BUSCADOS. NEM A EDITORA NEM O AUTOR DEVEM SER RESPONSABILIZADOS POR DANOS DECORRENTES DESTA PUBLICAÇÃO. O FATO DE UMA EMPRESA OU SITE TER SIDO MENCIONADO NESTE TRABALHO COMO CITACAO E/OU FONTE DE INFORMAÇÕES ADICIONAIS NÃO SIGNIFICA QUE O AUTOR OU A EDITORA APROVEM AS INFORMAÇÕES FORNECIDAS PELA EMPRESA OU PELO CONTEÚDO DO SITE, OU SUAS RECOMENDAÇÕES. ALÉM DISSO, OS LEITORES DEVEM ESTAR CIENTES DE QUE OS SITES RELACIONADOS NESTE TRABALHO PODEM TER SIDO MODIFICADOS OU DESAPARECIDOS ENTRE QUANDO ESTE TRABALHO FOI ESCRITO E QUANDO FOI LIDO.

ISBN 978-1-119-28482-6 (pbk); ISBN 978-1-119-28505-2 (ebk)

Fabricado nos Estados Unidos da América

10 9 8 7 6 5 4 3 2 1

Para maiores informações sobre outros produtos e serviços, ou como criar um livro *Para leigos* personalizado para o seu negócio ou organização, entre em contato com o nosso departamento de desenvolvimento de negócios nos EUA em 877-409-4177, entre em contato com info@dummies.biz, ou visite www.wiley.com/go/custompub. Para informações sobre concessão de licenças da marca *For Dummies* para produtos e serviços, entre em contato com BrandedRights&Licenses@Wiley.com.

Reconhecimentos da Editora

Algumas das pessoas que ajudaram a trazer esse livro para o mercado são:

Editor de desenvolvimento:

Elizabeth Kuball

Editor de cópia: Elizabeth Kuball

Editora de compras: Katie Mohr

Gerente de editorial: Rev Mengle

Representante de desenvolvimento do negócio: Karen Hattan

Coordenadora de produção: Kinson Raja

Ajuda especial: Geoff Huang, Catherine Fan, e Kausum Kumar

Índice

Introdução 1

Sobre este livro	2
Suposições inocentes	2
Ícones usados neste livro	3
Além do livro	3
Para onde vou agora.....	3

Capítulo 1: Defendendo o data center com uma abordagem ineficaz..... 5

Violações de dados continuam ocorrendo.....	5
O ciclo de vida de um ataque ao data center	6
Atirando pedras nas paredes (lógicas) de um data center	9

Capítulo 2: Microssegmentação explicada 15

Como limitar o movimento lateral no interior do data center	15
Crescimento do tráfego leste-oeste no interior	
do data center.....	17
Visibilidade e contexto.....	17
Isolamento	18
Segmentação	20
Automação.....	21
Elementos essenciais da microssegmentação	23
Persistência	23
Ubiquidade	24
Extensibilidade.....	24
Como equilibrar isolamento e contexto.....	25
Como implementar privilégio mínimo e confiança com	
microssegmentação	26
O que não é microssegmentação.....	27

Capítulo 3: Como migrar o data center para software..... 31

Principais motivadores para a transformação do data center	31
Transformando seu data center com a virtualização de redes ...	34
Como funciona a virtualização de redes	36
Elementos essenciais para virtualização de redes.....	39
Alguns planos...de dados, de controle	
e de gerenciamento	40
Encapsulamento	41

Capítulo 4: Como automatizar as tarefas de segurança 45

Como criar políticas de segurança para o data center definido por software.....	45
Políticas de segurança baseadas em rede.....	46
Políticas de segurança baseadas em infraestrutura	47
Políticas de segurança baseadas em aplicação	47
Aprovisionamento	48
Como se adaptar às mudanças dinamicamente.....	49
Como responder às ameaças dinamicamente	50
Como criar firewalls para dezenas de milhares de cargas de trabalho com um único firewall lógico	51

Capítulo 5: Microssegmentação: Como começar 53

Como obter a microssegmentação.....	53
Determine os fluxos de rede	55
Identifique padrões e relações.....	55
Crie e aplique o modelo de política	56
Casos de uso de segurança	56
Segurança de rede dentro do data center	57
DMZ em qualquer lugar	58
Ambientes seguros de usuários	58

Capítulo 6: Dez (ou mais) benefícios da microssegmentação 61

Minimize o risco e o impacto das violações de segurança do data center	61
Automatize o fornecimento de serviços da TI e acelere a entrega de seus produtos no mercado	62
Simplifique os fluxos de tráfego de rede	63
Ative funções avançadas de segurança através do Desvio de Tráfego e da Inserção e Encadeamento de Serviços	63
Aproveite a infraestrutura já existente	64
Reduza as despesas de capital (CapEx)	66
Reduza as despesas operacionais (OpEx)	66
Ative de modo seguro a agilidade comercial	67

Introdução

As abordagens tradicionais de segurança de data centers têm se concentrado em defesas fortes de perímetro para manter as ameaças do lado de fora da rede, assim como aquelas utilizadas por castelos na época medieval! Enquanto o perímetro (muralhas) do castelo era reforçado com parapeitos e bastiões, o seu acesso era controlado por uma ponte elevadiça (representada por um firewall no contexto de uma rede). Para uma força de ataque, romper o perímetro e entrada no castelo era a chave para a vitória. Uma vez dentro do castelo, as defesas eram praticamente inexistentes e os invasores estavam livres para queimar e pilhar!

No entanto, esse modelo é ineficaz para lidar com ameaças novas e atuais, incluindo as ameaças persistentes avançadas (conhecidas como APTs, acrônimo de Advanced Persistent Threats) e os ataques coordenados. É necessária uma abordagem mais moderna e sofisticada para a segurança do data center: uma que assuma que ameaças podem estar em qualquer lugar (principalmente dentro do perímetro de rede) e, em seguida, aja em conformidade. A microssegmentação não só adota essa abordagem, mas também fornece a agilidade operacional da virtualização de redes que é a base de um moderno data center definido por software.

Hoje em dia, as ameaças cibernéticas são ataques coordenados que normalmente incluem meses de reconhecimento, explorações de vulnerabilidade e agentes de malware “em repouso” que ficam suspensos até serem ativados por controle remoto. Apesar do aumento dos tipos de proteção na periferia das redes de data center, incluindo firewalls, sistemas de prevenção contra intrusões (conhecidos como IPSs, acrônimo de Intrusion Prevention Systems) e detecção de malware com base na rede, os ataques estão conseguindo penetrar no perímetro, e as violações continuam ocorrendo.

O principal problema é que, assim que um ataque passa pelo perímetro do data center, existem menos controles laterais para impedir que as ameaças afetem recursos internos. A melhor maneira de solucionar isso é adotar um modelo de segurança mais granular e rígido com a capacidade de associar

a segurança a cargas de trabalho individuais e aprovisionar políticas automaticamente. A Forrester Research chama isso de modelo de “confiança zero”, e a microssegmentação incorpora essa abordagem.

Com a microssegmentação, controles de rede individualizados ativam a segurança no nível de servidor, e políticas de segurança flexíveis podem ser aplicadas o mais próximo quanto possível da aplicação. Em uma rede física, isso exigiria a implantação de um firewall físico para cada carga de trabalho no data center, de modo que, até agora, a microssegmentação tem sido cara e operacionalmente inviável. Entretanto, com a tecnologia de virtualização de redes, agora a microssegmentação é uma realidade.

Sobre este livro

Este livro fornece uma visão geral ampliada de microssegmentação no data center. Após sua leitura, você terá um bom conhecimento básico sobre microssegmentação, assim como você teria em uma aula da faculdade para iniciantes, (mas com um tema muito mais fácil que microbiologia ou microeconomia básica).

Suposições inocentes

Já foi dito que a maioria das suposições deixou de ser útil; no entanto, ainda consideramos alguns pontos:

- ✓ Você tem um sólido conhecimento prático sobre os fundamentos de rede e segurança, conceitos e tecnologias e uma boa compreensão de virtualização.
- ✓ Você trabalha em uma grande organização ou empresa que opera um ou mais data centers em um ambiente de nuvem pública, privada ou híbrida para oferecer suporte às suas funções de negócios essenciais.
- ✓ Você é um executivo de segurança, como um diretor de segurança da informação (CISO) ou diretor de segurança (CSO), que avalia as estratégias de segurança de data center e as soluções para a organização. Se esse é o seu caso, este livro foi especialmente escrito para você.

Ícones usados neste livro

Ao longo deste livro, nós ocasionalmente usamos ícones especiais para chamar a atenção para informações importantes. Veja o que você pode encontrar:



Este ícone indica informações que podem muito bem valer a pena ocupar sua memória não volátil, a massa cinzenta ou a cachola, juntamente com datas de aniversários e comemorações.



Aqui você não vai encontrar um mapa do genoma humano, mas se deseja alcançar o nível de nerd mais alto, anime-se! Este ícone explica o que há além do jargão.



Obrigado pela leitura, espero que gostem do livro, por favor, cuidem de seus autores. Sério, este ícone indica sugestões úteis e informação preciosas.



Prossiga por sua conta e risco... Tudo bem. Na verdade, não há *nada* perigoso. Esses alertas úteis oferecem conselhos práticos que ajudam a evitar cometer erros potencialmente onerosos.

Além do livro

Embora este livro seja repleto de informações, há muito mais para saber do que nestas 72 páginas! Portanto, se você chegar ao final deste livro e pensar: “Puxa, este livro foi surpreendente. Onde posso aprender mais sobre microssegmentação?”, basta acessar <https://www.vmware.com/products/nsx>.

Para onde vou agora

Sem ofender Lewis Carroll, Alice e seu Gato que ri:

“Pode me dizer que caminho devo seguir?”

“Isso depende do lugar para onde você quer ir”, disse o Gato.

“Não tenho destino certo...”, disse Alice, aqui representando o leigo.

“Nesse caso, qualquer caminho serve!”

Isso certamente é uma verdade sobre *Microssegmentação Para Leigos*, que assim como *Alice no País das Maravilhas*, também está destinado a se tornar um clássico!

Se você não sabe para onde está indo, qualquer capítulo levará você até lá, mas o Capítulo 1 pode ser um bom lugar para começar!

No entanto, se você vir um tópico específico que desperte seu interesse, sinta-se à vontade para passar adiante para esse capítulo. Cada capítulo conclui-se de forma individual (mas não destina-se à venda individual) e está escrito de maneira independente; portanto, você pode começar a ler a partir de qualquer lugar e ir para onde achar melhor. Leia este livro na ordem que for mais conveniente para você (só não recomendamos de cabeça para baixo nem da direita para esquerda).

Prometemos que você não vai se perder caindo no buraco do coelho!

Capítulo 1

Defendendo o data center com uma abordagem ineficaz

Neste capítulo

- ▶ Como reconhecer o impacto de violações de data centers
- ▶ Saiba como os ataques exploram o interior desprotegido do data center
- ▶ Identificação do que está errado com a segurança tradicional de data center

Os data centers tornaram-se os cofres dos bancos virtuais do século 21. Informações confidenciais corporativas, financeiras e pessoais armazenadas em sistemas de data center valem provavelmente centenas de milhões de dólares para os cibercriminosos de hoje. Embora a dependência nesses sistemas tenha crescido consideravelmente ao longo das últimas décadas, a base subjacente para fornecer segurança avançada a esses sistemas permanece relativamente inalterada: um forte foco na segurança de perímetro externo com pouca (ou nenhuma) atenção voltada para neutralizar ameaças dentro do data center.

Neste capítulo, você vai explorar violações de data centers, como elas ocorrem e por que as abordagens tradicionais de segurança de data center que deixam seu interior relativamente indefeso são ineficazes.

Violações de dados continuam ocorrendo

Apesar de um foco maior sobre a segurança na empresa como evidenciado pelas leis de proteção de dados cada vez mais rigorosas, altos investimentos em tecnologia de segurança e equipes de segurança cada vez mais hábeis, as violações de data centers

continuam ocorrendo a um ritmo alarmante, onde nova violação supera a última em termos de milhões de registros e dólares roubados.

Embora os recentes ataques à Anthem, Home Depot, Sony e Target tenham sido diferentes entre si, eles têm uma característica em comum: Após o perímetro ter sido violado, os ataques conseguiram propagar lateralmente, de servidor a servidor, no interior do data center, praticamente sem controles de segurança no local para impedi-los de espalhar. Os dados sensíveis foram coletados, extraídos e explorados. Esses casos destacam um ponto fraco importante dos data centers modernos: Enorme esforço e tecnologia são aplicados para proteger o perímetro do data center, mas o mesmo nível de segurança não existe em seu interior. Para abordar eficazmente essa fraqueza, todas as tecnologias e controles de segurança que são aplicados à borda do data center precisam ser consideradas e implementadas também (se for o caso) *internamente* ao data center, a fim de parar ou isolar ataques após o perímetro ter sido violado.

De acordo com o *2015 Data Breach Investigation Report* (Relatório de investigação de violação de dados de 2015) da Verizon, em 2014, houve 79.790 incidentes de segurança confirmados em todo o mundo e 2.122 casos confirmados em que os dados sensíveis foram comprometidos. No *2014 Cost of Data Breach Study* (Estudo de custo da violação de dados de 2014), o Ponemon Institute calculou o total do custo médio de um incidente de violação de dados nas empresas dos EUA em US\$ 5,85 milhões.

É claro que os custos de uma violação de dados podem ser significativamente mais altos. Por exemplo, a Sony Pictures Entertainment foi vítima de duas violações de dados nos últimos anos. A violação ocorrida em junho de 2011 custou à Sony Pictures US\$ 171 milhões. Com base no que se soube sobre a violação ocorrida em novembro de 2014, os analistas acreditam que os custos provavelmente vão alcançar US\$ 100 milhões. O ataque de 2014 à Sony Pictures forçou um desligamento de toda a rede durante dias, o que também acarretou um evento de recuperação de desastres extremamente oneroso.

O ciclo de vida de um ataque ao data center

Os sofisticados ataques cibernéticos de hoje exploram uma vulnerabilidade fundamental que existe em projetos de data centers

modernos: a existência de pouco ou nenhum controle de segurança no interior do perímetro do data center. Os modelos de segurança mais populares, como o Lockheed Martin Cyber Kill Chain (consulte a Figura 1-1), fornecem um quadro simples para a compreensão do processo sistemático utilizado por cibercriminosos para violar um perímetro de data center. Uma vez em seu interior, um invasor depende muito da capacidade de mover-se lateralmente, de servidor a servidor, a fim de expandir a superfície de ataque e alcançar os objetivos do ataque.

Reconhecimento	Coleta de informações específicas do alvo para violar o perímetro do data center
Armamento	Acoplamento de exploits e backdoor em uma carga útil para entrega
Entrega	Entrega de pacote com armamento para violação das defesas do perímetro do data center
Exploração	Movimentação lateral para aproveitar as vulnerabilidades nos sistemas de data center
Instalação	Instalação de malwares nos sistemas pelo data center
Comando e Controle (C2)	Definição de comunicação remota e canais de controle no interior do data center
Ações visadas	Prosseguimento das intenções de ataque com acesso completo pelo teclado

Figura 1-1: O Lockheed Martin Cyber Kill Chain.

Infelizmente, esses modelos refletem uma realidade sombria: Uma enorme e desproporcionada quantidade de esforços e de recursos tem sido aplicada para evitar uma violação no primeiro lugar, protegendo o perímetro do data center (que corresponde às três primeiras etapas na Figura 1-1). Após atacar um recurso interno, um invasor pode explorar as vulnerabilidades, instalar malware, estabelecer uma infraestrutura de comando e controle (C2) e mover-se lateralmente pelos sistemas em todo o data center com relativa facilidade (consulte a Figura 1-2).

A comunicação de C2 é fundamental para um ataque bem-sucedido e, portanto, deve ser sigilosa, a fim de evitar a detecção. O tráfego de C2 é muitas vezes do tipo SSL (Secure Sockets Layer) criptografado e usa proxies ou túneis em aplicativos ou protocolos legítimos.



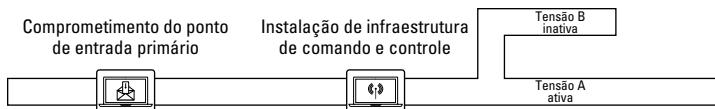


Figura 1-2: C2 ativa ainda mais reconhecimento no data center.

Em seguida, um invasor instala infraestrutura de C2 adicional em outros dispositivos e sistemas, encobre todos os vestígios de ataque e encaminha privilégios do sistema em um ataque de múltiplas frentes que se aproveita da segurança relativamente fraca ou inexistente no interior do data center (consulte a Figura 1-3).

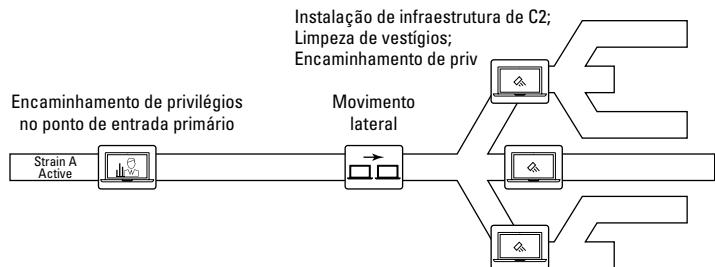


Figura 1-3: A infraestrutura de C2 adicional é instalada para garantir a persistência à medida que o invasor se move lateralmente pelo data center.



Os ataques cibernéticos modernos aproveitam a segurança relativamente fraca ou inexistente no interior do data center para se mover livremente entre os diferentes sistemas e roubar informações. O Capítulo 2 explica como a microssegmentação bloqueia o movimento lateral do invasor e ajuda a evitar a instalação bem-sucedida de uma infraestrutura de C2 no data center.

Ataques modernos e avançados são planejados para serem persistentes e resilientes. Dessa forma, se uma ameaça ativa é descoberta, o invasor pode simplesmente “acordar” uma instância de malware latente em outro sistema infectado no data center e continuar o ataque (consulte a Figura 1-4). A falta de controles de segmentação e de segurança adequados e a explosão do tráfego leste-oeste no interior do data center torna difícil, se não impossível, que as equipes de resposta a incidentes isolem efetivamente um ataque.

O invasor pode então realizar qualquer ação desejada contra o alvo (consulte a Figura 1-5).

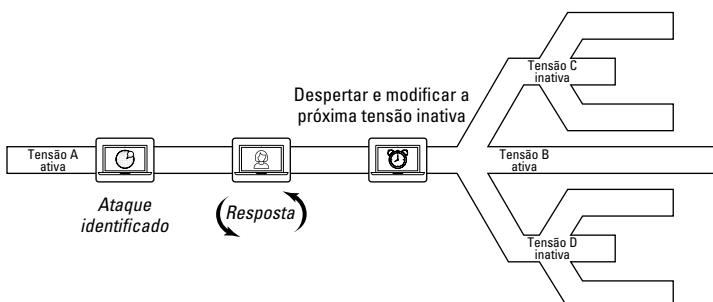


Figura 1-4: Se um ataque é descoberto, o invasor simplesmente ativa um elemento antes “em repouso” e continua o ataque.

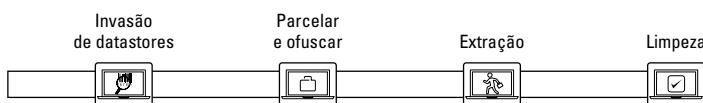


Figura 1-5: O invasor está livre para realizar quaisquer ações desejadas sobre o objetivo do data center.

Se a intenção é roubar informações confidenciais, o invasor divide os dados em pequenas cargas criptografadas para evitar a detecção durante a extração da rede de destino.



No Capítulo 2, você aprenderá como a microssegmentação evita um ataque bem-sucedido bloqueando o movimento lateral de um invasor no data center e com capacidades, tais como inserção de serviço de segurança que permite a inspeção detalhada do pacote DPI (Deep Packet Inspection), e bloqueando (se for o caso) cargas de saída criptografadas do data center.



Ao usar uma estratégia de ataque paciente, resiliente, sigilosa e de múltiplas frentes, um invasor no interior do data center pode mover-se entre sistemas relativamente livres e roubar dados sensíveis por meses (ou até anos) antes de ser detectado.

Atirando pedras nas paredes (lógicas) de um data center

A segmentação é um princípio fundamental de segurança de informações que tem sido aplicada ao projeto de data center durante décadas. Em seu nível mais básico, a segmentação

ocorre entre duas ou mais redes, tal como uma rede interna (o data center) e uma rede externa (a Internet) com um firewall implantado no perímetro entre as diferentes redes (consulte a Figura 1-6).

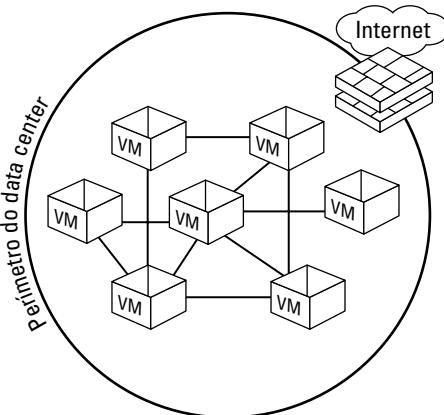


Figura 1-6: A segurança baseada em perímetro é insuficiente em um data center em que a segurança é necessária em todos os lugares.

Apesar de a segmentação *realmente* existir em data centers atualmente, os segmentos de rede são muito grandes para serem efetivos e foram tipicamente criados para limitar o tráfego “norte-sul” entre a Internet e o data center ou entre as estações de trabalho e o data center. Por exemplo, uma rede pode ser segmentada em vários níveis de confiabilidade que usam firewalls adicionais para criar uma DMZ (zona desmilitarizada) ou redes de departamentos separados (como finanças, recursos humanos e P&D). Para ser totalmente eficaz, a segmentação (e o uso de firewall) precisa alcançar granularidade da carga de trabalho (servidor). Mas um data center típico pode ter milhares de cargas de trabalho, cada uma com condições de segurança exclusivas. Novamente, o foco primário está no controle de *entrada e saída* do tráfego do data center, e não no tráfego “leste-oeste” *no interior* do data center no qual se baseiam os ataques modernos.

Para proteger eficazmente os data centers de ataques modernos, é necessário que a segmentação consiga distinguir cargas de trabalho individuais. Mas a implantação de centenas (ou até milhares) de firewalls baseados em hardware no interior do data center para proteger cada carga de trabalho individual é financeira e operacionalmente inviável. Além disso, os firewalls

virtuais, embora um pouco mais baratos do que firewalls de hardware, ainda não resolvem a necessidade dessa microssegmentação por servidor. O resultado: A manutenção de políticas de segurança exclusivas e eficazes para milhares de cargas de trabalho individuais como parte de uma estratégia de segurança corporativa abrangente e coesa usando processos, controles e tecnologias de segurança de data center já existentes tem sido impraticável. Até o momento. A virtualização de redes (explicada no Capítulo 3) torna a microsssegmentação uma realidade no data center, com total aproveitamento da infraestrutura de rede já existente.



No Capítulo 5, você aprenderá como implantar a microssegmentação, aproveitando e melhorando o desempenho das tecnologias de segurança e a infraestrutura do data center já existentes.

Muitas organizações criam logicamente partições de suas redes de data center em diferentes segmentos de segurança, que, em seguida, precisam ser convertidos em elementos de redes físicas, como sub-redes e LANs virtuais (VLANs). Essas técnicas fornecem apenas controle de acesso simples e resultam em estruturas de segurança que são demasiadamente rígidas e muito complexas porque as políticas de segurança são em grande parte definidas pelo local em que uma carga de trabalho está fisicamente implantada na topologia de rede (consulte a Figura 1-7). A segmentação de data center com essas grandes zonas cria uma superfície de ataque significativa e permite que as ameaças se movam ao longo de grande parte do data center sem restrições, uma vez que o invasor tenha superado as defesas de perímetro. Essas técnicas de segmentação também resultam em atrasos significativos na implantação de novas cargas de trabalho ou na mudança de cargas de trabalho existentes porque elas devem ser configuradas manualmente em uma topologia de rede rígida e estática.

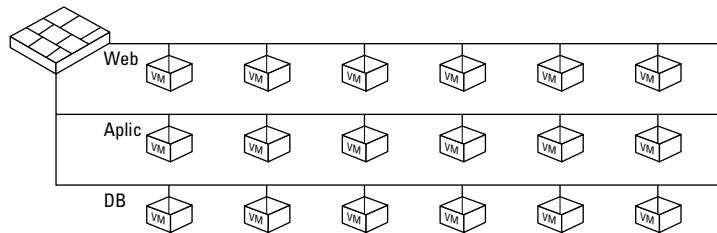


Figura 1-7: Atualmente, a segurança está relacionada a uma topologia de rede rígida e complexa que é ainda mais complicada por uma infraestrutura consolidada e de aplicações multicamadas.



Alterações de VLANs e sub-redes também podem ser uma fonte frequente de falhas de rede, comprometimento da segurança, erros de configuração e atrasos na implantação de aplicações. Além disso, nem sempre é possível testar exaustivamente as alterações propostas em um ambiente de teste que replica com precisão o data center de produção.



Diferentes segmentos devem ser criados no interior do perímetro para limitar a propagação lateral de ameaças no data center. Idealmente, a segmentação e a aplicação de políticas devem estar disponíveis até o nível da carga de trabalho individual.

Além da segmentação lógica inadequada, outra consequência infeliz do design tradicional de data center que aumenta a complexidade e degrada o desempenho da rede é o tráfego de redirecionamento (“hair-pinning”) leste-oeste do servidor por meio de um firewall: as comunicações entre servidores que, de outra forma, não atravessam o dispositivo (consulte a Figura 1-8).

O redirecionamento é incrivelmente ineficiente e aumenta consideravelmente a complexidade no data center:

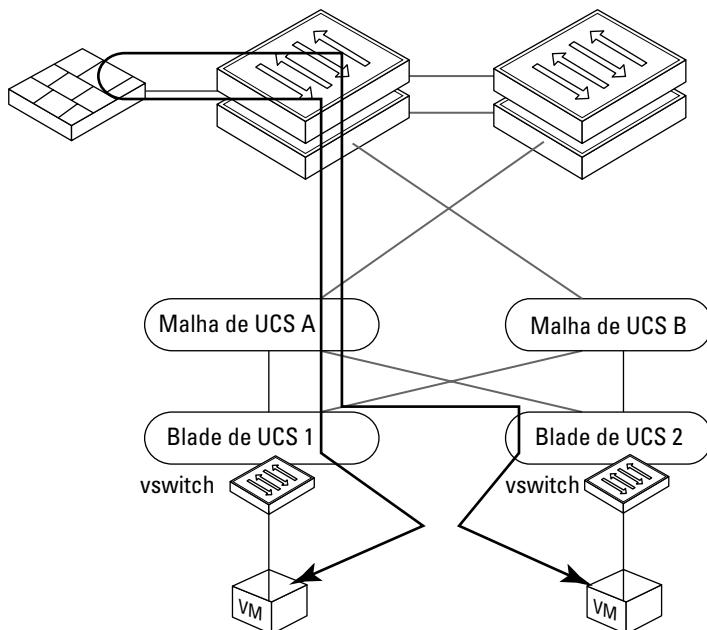


Figura 1-8: Tráfego de redirecionamento (“hair-pinning”) ou firewall host a host leste-oeste.

- ✓ Criando pontos de obstrução de desempenho desnecessários na rede e prováveis pontos de falhas
- ✓ Tráfego de retorno de até 60% de todo o tráfego de rede por meio de firewalls, acrescentando congestionamento e latência na rede
- ✓ Contribuindo para a proliferação de regras de firewall e galhos de desempenho à medida que administradores de segurança estão cada vez mais relutantes em modificar ou remover conjuntos de regras complexas quando cargas de trabalho são desativadas, com medo de causar uma interrupção ou falha de segurança

O redirecionamento é particularmente frustrante para o tráfego leste-oeste entre cargas de trabalho virtualizadas que, de outra forma, poderiam se comunicar quase à velocidade máxima (especialmente no tráfego de cargas de trabalho virtuais residindo em um mesmo host).

Finalmente, muitas soluções avançadas de segurança foram implantadas no perímetro, incluindo firewalls de última geração, antimalwares, sistemas de prevenção contra intrusões (IPS, Intrusion Prevention Systems), prevenção contra negação de serviço distribuído (DDoS, Distributed Denial-of-Service), gerenciamento de ameaças unificado (UTM, Unified Threat Management), filtragem de spam entre muitas outras tecnologias. Embora essas soluções reforcem as defesas de perímetro, elas muitas vezes são projetadas para lidar com ameaças específicas com contexto limitado e correlação entre diferentes tecnologias de segurança, e o problema fundamental com a segurança do data center permanece: quando um invasor consegue transpor o perímetro e entrar no data center, os controles de segurança são relativamente fracos ou inexistentes, e o invasor pode mover-se livremente (por assim dizer). A fim de parar ameaças em todos os lugares em que elas ocorrem, essas soluções precisam ser implantadas no perímetro e no *interior* do data center, em uma plataforma comum que forneça contexto e coordenação entre as cargas de trabalho individuais e as diversas tecnologias.



As metodologias ultrapassadas de segurança de data center não estão alinhadas às modernas exigências de negócios para acesso, em qualquer lugar e a qualquer momento, aos aplicativos do data center e aos dados provenientes de qualquer dispositivo e são insuficientes para lidar com os ataques sofisticados atuais. Essas metodologias e desafios incluem o seguinte:

- ✓ **Foco no perímetro:** O perímetro forte é importante, mas controles de segurança *no interior* do data center são fracos ou inexistentes. A combinação de soluções de segurança avançadas, como firewalls de última geração, prevenção IPS e DDoS e outras tecnologias fortalecem o perímetro, mas não é suficiente para tratar das ameaças *no interior* do data center.
- ✓ **Falta de controles internos:** Os invasores aproveitam os controles de segurança fracos ou inexistentes no interior do data center para se mover lateralmente entre as cargas de trabalho e expandir rapidamente a superfície de ataque.
- ✓ **Incapacidade de dimensionamento:** A implantação de centenas, possivelmente até mesmo milhares, de firewalls para proteger cada carga de trabalho no data center é inviável e impraticável.
- ✓ **Segurança mapeada na topologia de rede:** As políticas de segurança determinadas pela localização física de uma carga de trabalho do servidor no data center não atendem aos requisitos de negócios e de conformidade e são muito rígidas e complexas. Essa abordagem legada de segurança muitas vezes leva a atrasos significativos na implantação de aplicativos.
- ✓ **A ineficiência de redirecionamento (“hair-pinning”):** Ao forçar o tráfego leste-oeste por meio de firewalls, criam-se pontos de obstrução e tráfego de servidor de retorno desnecessário, além de colaborar para a proliferação de conjuntos de regras de firewall e complexidade.
- ✓ **Grandes zonas de segurança:** O uso de pontos de obstrução de firewall no interior do data center, em uma tentativa de segmentá-lo, cria zonas de segurança complexas que ainda permitem às ameaças mover-se relativamente livres ao longo desses grandes segmentos.

Embora a segurança baseada em perímetro seja um elemento importante da segurança, ela não define toda a sua arquitetura; tal como as paredes de um edifício formam um limite estrutural essencial, mas não são a base. Em vez disso, a base fornece uma plataforma sobre a qual o edifício é construído.

No Capítulo 2, você aprenderá tudo sobre a microsegmentação e como ela evita que ataques ao data center sejam bem-sucedidos.

Capítulo 2

Microssegmentação explicada

Neste capítulo

- ▶ Como reforçar a defesa do data center no interior de seu perímetro
 - ▶ Como usar o data center definido por software como uma ferramenta contra ataques
 - ▶ Como tornar a confiança zero uma realidade no data center
 - ▶ Como obter persistência, ubiquidade e extensibilidade com microssegmentação
 - ▶ Como reconhecer o que a microssegmentação não é
-

A microssegmentação permite que as organizações dividam logicamente o data center em segmentos de segurança distintos até o nível de carga de trabalho individual, definam os controles de segurança e forneçam serviços para cada segmento único. Isso restringe a capacidade de um invasor se mover lateralmente no data center, mesmo depois de o perímetro ter sido violado ter sido violado, parecido com os cofres bancários que protegem os objetos de valor dos clientes do banco. Neste capítulo, você aprenderá o que é microssegmentação e o que não é.

Como limitar o movimento lateral no interior do data center

Os ataques modernos exploram as fraquezas inerentes às estratégias tradicionais de segurança de rede focada no perímetro (discutido no Capítulo 1) para se infiltrar nos data centers corporativos. Após escapar com sucesso das defesas de perímetro do data center, um ataque pode se mover lateralmente no seu interior, de

uma carga de trabalho para outra, com pouco ou nenhum controle para bloquear sua propagação.

A microsegmentação da rede do data center restringe o movimento lateral não autorizado, mas até o momento, esse controle não foi operacionalmente viável em redes de data center.

Os firewalls tradicionais de filtro em pacote e os mais avançados (de última geração) implementam controles como “pontos de obstrução” físicos ou virtuais na rede. À medida que o tráfego de uma aplicação passa por esses pontos de controle, seus pacotes são bloqueados ou permitidos com base nas regras de firewall que estão configurados naquele ponto de controle.

Há duas barreiras operacionais para a microsegmentação usando firewalls tradicionais: capacidade de throughput e gerenciamento de segurança.

As limitações à capacidade de throughput podem ser superadas, mas a um custo significativo. É possível comprar firewalls físicos ou virtuais suficientes para oferecer a capacidade necessária para alcançar a microsegmentação, mas na maioria (se não em todas) das organizações, o número de firewalls necessário para uma microsegmentação eficaz não é financeiramente viável.

A sobrecarga do gerenciamento de segurança aumenta exponencialmente com o número de cargas de trabalho e a natureza cada vez mais dinâmica dos data centers atuais. Se as regras do firewall precisarem ser adicionadas, excluídas ou modificadas manualmente sempre que uma nova máquina virtual (VM, Virtual Machine) for adicionada, movida ou desativada, a taxa de alterações dominará rapidamente as operações de TI. É essa barreira que representa o fim dos planos dos melhores esquemas da maioria das equipes de segurança no momento de criar uma estratégia confiável no nível de componente de aplicação (discutido posteriormente neste capítulo), com privilégio mínimo ou microsegmentação abrangente no data center.

O data center definido por software (SDDC, Software-Defined Data Center) aproveita uma plataforma de virtualização de redes para oferecer diversas vantagens significativas em relação às abordagens tradicionais de segurança de rede: aprovisionamento automatizado, mudanças automatizadas para cargas de trabalho, aplicação distribuída em cada interface virtual e em kernel, desempenho de firewall com dimensionamento horizontal, distribuição para cada hypervisor e incorporação à plataforma.

Crescimento do tráfego leste-oeste no interior do data center

Durante a última década, cada vez mais aplicativos têm sido implantados em infraestruturas de servidor multicamadas e as comunicações leste-oeste de servidor a servidor representam agora significativamente mais tráfego de data center do que as comunicações norte-sul (client-servidor). Na verdade, o tráfego *no interior* do data center agora é responsável por até 80% de todo o tráfego de rede. Estas infraestruturas de aplicações multicamadas são normalmente planejadas com pouco ou nenhum controle de segurança que restrinja as comunicações entre camadas e, cada vez mais, aproveitam a conectividade de Ethernet de 10 Gbps para obter throughput e desempenho ideais.

Os invasores modificaram sua estratégia de ataque para aproveitar essa mudança de paradigma no tráfego de data center, bem como o fato de que as estratégias de defesa centradas em perímetro dominantes oferecem pouco ou nenhum controle sobre as comunicações de rede no interior do data center. As equipes de segurança da mesma forma devem estender a estratégia de defesa *para o interior* do data center, local em que a grande maioria do tráfego de rede realmente existe e está desprotegido, em vez de focar quase exclusivamente nas defesas de perímetro.

Visibilidade e contexto

O crescimento do tráfego leste-oeste no interior do data center e o aumento da virtualização de servidores são duas tendências que contribuíram para uma alarmante falta de visibilidade e contexto no data center.

Para a maior parte, as comunicações de servidor leste-oeste no data center não passam por um firewall e, portanto, não são inspecionadas. Para todos os efeitos, esse tráfego é invisível para as equipes de segurança de rede. Quando um tráfego leste-oeste é forçado por meio de um firewall usando técnicas como redirecionamento (“hair-pinning”) para retornar ao tráfego através de um ponto de obstrução, o resultado é um caminho de comunicação complexo e ineficiente, que afeta negativamente o desempenho da rede em todo o data center.

A inovação em virtualização de servidores ultrapassou de longe as estruturas subjacentes de rede e segurança nos data centers tradicionais, o que contribui para o problema da visibilidade limitada e o contexto no data center. A implantação de várias cargas de

trabalho virtuais em um único host físico configurado com várias placas de interface de rede (NICs, Network Interface Controllers) é comum em ambientes de servidores virtuais. Sem switches virtuais inteligentes, o tráfego que vai e volta das VMs individuais não pode ser facilmente identificado. Isso pode causar problemas significativos para as equipes de rede que tentam identificar e solucionar problemas e é um terreno fértil para um invasor.

Um “hypervisor de rede” está posicionado exclusivamente para ver *todo* o tráfego no data center (consulte a Figura 2-1), até o nível de cargas de trabalho individuais (VMs). Esse nível de visibilidade e de contexto permite a microsegmentação baseada em atributos exclusivos para cada carga de trabalho, tais como o sistema operacional, nível de patch, serviços em execução e muitas outras propriedades. Essa capacidade, por sua vez, permite que decisões mais inteligentes sobre políticas de rede e segurança possam ser definidas com uma compreensão da finalidade específica de cada carga de trabalho individual no data center. Por exemplo, as políticas exclusivas podem ser especificamente definidas para a camada da Web de um aplicativo de recebimento de pedidos ou para um sistema corporativo de gerenciamento de recursos humanos, com base nas necessidades de carga de trabalho individual, em vez de serem definidas exclusivamente pela topologia de rede subjacente.

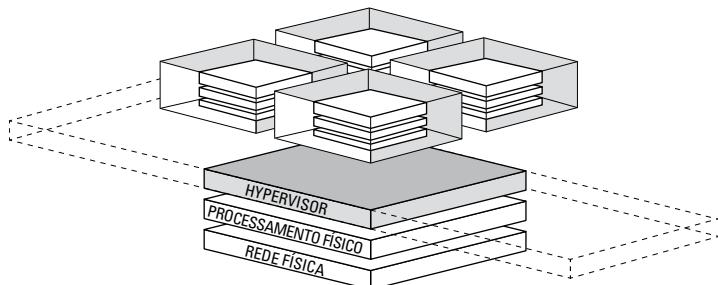


Figura 2-1: O hypervisor de rede está exclusivamente posicionado para ver todo o tráfego no data center.

Isolamento

O isolamento é um princípio importante na segurança de rede, seja por questão de conformidade, contenção ou simplesmente para manter os ambientes de desenvolvimento, de teste e de produção separados. O roteamento configurado e mantido

manualmente, as listas de controle de acesso (ACLs, Access Control Lists) e/ou as regras de firewalls em dispositivos físicos têm sido usados tradicionalmente para estabelecer e aplicar o isolamento nas redes de data center.



A Forrester Research descreve seu modelo de “confiança zero” de segurança da informação e isolamento, em que os controles de segurança são estendidos por todo o data center. Ele exige que as organizações protejam os recursos de dados internos e externos e aplique controles de acesso rigorosos. A “confiança zero” incorpora o princípio de “privilegio mínimo”: um dos pilares da segurança da informação que limita o acesso e as permissões para o mínimo necessário para executar uma função autorizada. Finalmente, o “confie, mas verifique” tão falado na década de 80 (com respeito e desculpas devidas ao presidente Reagan): “Nunca confie, sempre verifique” é o novo paradigma para um mundo seguro e protegido.

No modelo proposto pelo VMware NSX, as redes virtuais são isoladas inherentemente de outras redes virtuais e da rede física subjacente por design. Esse conceito é distintamente diferente da abordagem legada de assumir algum nível padrão de confiança no interior do data center. Nesse contexto, não são necessárias sub-redes físicas, LANs virtuais (VLANs), ACLs ou regras de firewall para ativar esse isolamento. As redes virtuais são criadas em isolamento e permanecem isoladas, a menos que deliberada e explicitamente conectadas entre si.

Qualquer rede virtual isolada pode ser composta por cargas de trabalho distribuídas em qualquer lugar no data center e as cargas de trabalho na mesma rede virtual podem residir em hosts virtualizados ou nos mesmos. Além disso, as cargas de trabalho em várias redes virtuais isoladas podem residir no mesmo hypervisor.

O isolamento entre redes também permite o uso de endereços IP sobrepostos. Dessa forma, é possível, por exemplo, ter redes virtuais isoladas para desenvolvimento, teste e produção, cada uma com versão diferente do aplicativo, mas com os mesmos endereços IP, todas operando ao mesmo tempo e na mesma infraestrutura física.

Finalmente, as redes virtuais também são isoladas da infraestrutura física subjacente. Como o tráfego entre diferentes hosts é encapsulado, os dispositivos de rede física funcionam em espaços de endereço completamente diferentes das cargas de trabalho conectadas às redes virtuais. Por exemplo, uma rede virtual pode oferecer suporte a cargas de trabalho de aplicativos IPv6 em uma rede física IPv4. Esse isolamento protege a infraestrutura física

subjacente de qualquer ataque possível iniciado pelas cargas de trabalho em qualquer rede virtual. Novamente, tudo isso independe de quaisquer VLANs, ACLs ou regras de firewall que seriam tradicionalmente exigidas para criar esse isolamento.

Segmentação

A segmentação está relacionada ao isolamento, geralmente decorrente da comunicação entre camadas de uma mesma aplicação. Tradicionalmente, a segmentação de rede é realizada com um firewall físico ou roteador que permite ou nega o tráfego entre camadas ou segmentos de rede; por exemplo, entre uma camada Web, camada lógica de negócio (aplicação) e camada de banco de dados. A segmentação é um princípio importante no design de segurança, pois permite que as organizações definam diferentes níveis de confiança para diferentes segmentos de rede e reduz a superfície de ataque, impedindo que o invasor viole as defesas de perímetro. Infelizmente, os segmentos de rede do data center são muitas vezes muito grandes para serem eficazes e os processos tradicionais para definir e configurar a segmentação são demorados e propensos a erros humanos, muitas vezes resultando em falhas de segurança.

Uma segmentação de rede mais granular é o recurso fundamental de uma plataforma de virtualização de redes. Uma rede virtual pode oferecer suporte a um ambiente de rede multicamadas: vários segmentos de camada 2 com segmentação de camada 3 (ou microssegmentação) em um único segmento de camada 2, usando firewall distribuído definido por políticas de segurança de carga de trabalho. Isso poderia, por exemplo, representar as três camadas supracitadas (web, aplicação e banco de dados).

Em uma rede virtual, os serviços de rede e segurança, como camada 2, camada 3, ACLs, firewall, qualidade de serviço (QoS, Quality of Service) entre outros, aprovisionados com uma carga de trabalho são criados e distribuídos de modo programático para o switch virtual do hypervisor e aplicados à interface virtual. A comunicação em uma rede virtual nunca sai do ambiente virtual, eliminando a necessidade de configuração e manutenção da segmentação de rede na rede física ou no firewall.

Automação

A automação permite que as políticas corretas de firewall sejam aprovisionadas quando uma carga de trabalho é criada de modo programático, e essas políticas seguem a carga de trabalho à medida que ela é movida para qualquer lugar no data center ou entre data centers.

Igualmente importante, se o aplicativo for descontinuado, as políticas de segurança serão automaticamente removidas do sistema. Esse recurso elimina outro ponto problemático significativo: a proliferação de regras de firewall, o que potencialmente deixa milhares de definições de políticas de segurança obsoletas e ultrapassadas no lugar, muitas vezes resultando em degradação do desempenho e questões de segurança.

As empresas também podem aplicar uma combinação de diferentes recursos de parceiros, encadeando serviços avançados de segurança e aplicando serviços distintos com base em situações de segurança diferentes. Isso permite que as organizações integrem as tecnologias de segurança já existentes para construir uma capacidade de segurança mais abrangente e correlacionada no interior do data center. As tecnologias de segurança já existentes realmente funcionam melhor com microssegmentação porque têm uma maior visibilidade e contexto do tráfego da VM, e as ações de segurança podem ser personalizadas para cargas de trabalho individuais como parte de uma solução de segurança completa. Por exemplo, uma carga de trabalho pode ser aprovisionada com políticas padrão de firewall, que permitem ou restringem o acesso a outros tipos de cargas de trabalho. A mesma política também pode definir que, se uma vulnerabilidade fosse detectada na carga de trabalho durante o curso normal de verificação da vulnerabilidade, uma política de firewall mais restritiva se aplicaria, restringindo o acesso da carga de trabalho apenas às ferramentas usadas para remediar as vulnerabilidades (consulte a barra lateral “Segmentação com inserção de serviço de segurança avançado, encadeamento e direção de tráfego”).



Os fornecedores de segurança podem aproveitar a plataforma de virtualização de redes para desencadear respostas de serviços de segurança avançados a partir de uma solução de tecnologia do fornecedor de segurança completamente diferente. Uma inovação que simplesmente não é possível sem a virtualização de redes.

Segmentação com inserção de serviços de segurança avançados, encadeamento e direcionamento de tráfego

A plataforma de virtualização de redes VMware NSX fornece recursos de firewall de inspeção stateful para fornecer segmentação nas redes virtuais. Em alguns ambientes, são exigidos recursos mais avançados de segurança de rede. Nessas instâncias, as organizações podem aproveitar a plataforma de data center definido por software (SDDC, Software Defined Data Center) para distribuir, permitir e aplicar serviços de segurança de rede avançados em um ambiente de rede virtualizada. A plataforma NSX distribui serviços de rede ao switch virtual para formar um caminho lógico de serviços aplicado ao tráfego de rede virtual. Os serviços de rede de terceiros podem ser inseridos nesse caminho, permitindo que serviços físicos ou virtuais sejam consumidos em sequência.

Cada equipe de segurança usa uma combinação exclusiva de produtos de segurança de rede para atender às necessidades do ambiente. A plataforma NSX está sendo utilizada pelo ecossistema inteiro dos provedores de soluções de segurança da VMware, já que as equipes de segurança de rede são frequentemente desafiadas a coordenar serviços interligados de segurança de rede de vários fornecedores. Outro benefício poderoso da abordagem do NSX é sua habilidade para criar políticas que utilizem a inserção, o encadeamento e o direcionamento

de serviços do NSX para orientar a execução de serviços no caminho lógico de serviços, com base no resultado de outros serviços, tornando possível coordenar serviços de segurança de rede de vários fornecedores, sem nenhuma relação entre eles.

Por exemplo, a integração da VMware à Palo Alto Networks aproveita a plataforma NSX para distribuir o firewall de última geração VM-Series da última, disponibilizando os recursos avançados localmente em cada hypervisor. As políticas de segurança de rede, definidas para cargas de trabalho de aplicativos aprovisionadas ou movidas para o hypervisor, são inseridas no caminho lógico da rede virtual. No tempo de execução, a inserção de serviços aproveita o recurso de firewall de última geração da Palo Alto Networks disponível localmente, definido para fornecer e aplicar controles e políticas baseados em aplicativos, usuários e conteúdo na interface virtual da carga de trabalho.

Outro exemplo poderia usar a Trend Micro para detecção de malware. Se malware é detectado sendo carregado em uma VM, a Trend Micro bloqueia o malware e dispara um alerta que adiciona a VM a uma política de um grupo de “quarentena”. Um snapshot da VM é imediatamente criado para fins de investi-

gação e todo o tráfego de e para a VM é redirecionado por meio de um IPS e, simultaneamente, espelhado para uma sessão de SPAN remoto (RSPAN) para coleta e análise forense.

Atualmente, a plataforma VMware NSX tem integração significativa com os parceiros, incluindo a Palo Alto Networks, Rapid7, Trend Micro, Symantec, CheckPoint, Intel Security e outras, permitindo uma segurança avançada nunca vista antes.

Elementos essenciais da microssegmentação

Como discutido mais adiante neste capítulo, o hypervisor de rede está exclusivamente posicionado para fornecer contexto e isolamento em todo o SDDC, não muito perto da carga de trabalho na qual ele pode ser desativado por um ataque, e não tão distante que não tenha contexto na carga de trabalho. Dessa forma, o hypervisor de rede é ideal para implementar três elementos-chave de microssegmentação: persistência, ubiquidade e extensibilidade.

Persistência

Os administradores de segurança precisam saber que quando aprovisionam segurança para uma carga de trabalho, a aplicação dessa segurança persiste apesar das mudanças no ambiente. Isso é essencial, já que as topologias do data center estão constantemente mudando: as redes são renumeradas, os pools de servidores são expandidos, as cargas de trabalho são movidas e assim por diante. A única constante em face de toda essa mudança é a própria carga de trabalho, juntamente com a sua necessidade de segurança. Mas em um ambiente de mudança, a política de segurança configurada quando a carga de trabalho foi implantada pela primeira vez, provavelmente, não é mais aplicável, especialmente se a definição dessa política considerou associações limitadas à carga de trabalho, como endereço IP, porta e protocolo. A dificuldade de manter essa segurança persistente é agravada por cargas de trabalho que se movem de um data center a outro ou mesmo para a nuvem híbrida (por exemplo, uma migração em tempo real ou para fins de recuperação de desastres).

A microssegmentação fornece aos administradores maneiras mais úteis para descrever a carga de trabalho. Em vez de depender

apenas dos endereços IP, os administradores podem descrever as características inerentes da carga de trabalho, relacionando essas informações à política de segurança:

- ✓ Que tipo de carga de trabalho é essa (por exemplo, Web, aplicativo ou banco de dados)?
- ✓ Qual a finalidade dessa carga de trabalho (por exemplo, para desenvolvimento, teste ou produção)?
- ✓ Que tipos de dados essa carga de trabalho tratará (por exemplo, informações de baixa sensibilidade, financeiras ou de identificação pessoal)?

A microsegmentação ainda permite que os administradores combinem essas características para definir atributos de políticas herdadas. Por exemplo, uma carga de trabalho que trata de dados financeiros obtém um determinado nível de segurança, mas uma carga de trabalho de produção que trata de dados financeiros recebe um nível ainda mais alto de segurança.

Ubiquidade

Arquiteturas de data center tradicionais priorizam a segurança para cargas de trabalho importantes, negligenciando muitas vezes sistemas de menor prioridade. A segurança de rede tradicional é cara para implantar e gerenciar e, por causa desse custo, os administradores de data center são forçados a uma situação em que eles têm de racionar a segurança. Os invasores aproveitam esse fato, tendo como alvo sistemas de menor prioridade com níveis menores de proteção como ponto de infiltração em um data center.

A fim de proporcionar um nível adequado de defesa, os administradores de segurança precisam depender de um alto nível de segurança disponível para todos os sistemas do data center. A microsegmentação torna isso possível, incorporando funções de segurança à própria infraestrutura do data center. Ao aproveitar essa infraestrutura de computação generalizada, os administradores podem contar com a disponibilidade de funções de segurança para o mais amplo espectro de cargas de trabalho no data center.

Extensibilidade

Além da persistência e ubiquidade, os administradores de segurança também contam com a microsegmentação para se adaptar a situações novas e imprevisíveis. Da mesma forma que

as topologias de data center estão mudando constantemente, o mesmo ocorre com as topologias de ameaças no interior do data center: novas ameaças ou vulnerabilidades são expostas, as antigas se tornam irrelevantes e o comportamento do usuário é a variável inexorável que constantemente surpreende os administradores de segurança.

Em face aos cenários de segurança emergentes, a microsegmentação permite que os administradores estendam as capacidades, integrando funções de segurança adicionais ao portfólio de defesas. Por exemplo, os administradores podem começar com firewall stateless distribuído por todo o data center, mas adicionar firewalls de última geração e prevenção contra intrusões para inspeção detalhada do pacote (DPI, Deep Packet Inspection) ou anti-malware sem agente para aumentar a segurança do servidor. Mas além de simplesmente adicionar mais funções de segurança, os administradores precisam dessas funções a fim de proporcionar segurança mais eficaz do que se fossem implantadas de maneira isolada. A microsegmentação aborda essa necessidade, permitindo o compartilhamento de inteligência entre as funções de segurança. Isso possibilita que a infraestrutura de segurança atue acertadamente para adequar as respostas a situações únicas.

Como um exemplo, com base na detecção de malware, um sistema antivírus em coordenação com a rede espelha o tráfego para um sistema de prevenção contra intrusões (IPS), que por sua vez, realiza verificações em busca de tráfego anormal. A extensibilidade da microsegmentação permite essa capacidade dinâmica. Sem isso, o administrador de segurança teria que pré-configurar uma cadeia estática diferente dos serviços iniciais, cada uma correspondendo a um possível cenário de segurança diferente. Isso exigiria uma ideia preconcebida para todo cenário de segurança possível durante a implantação inicial.

Como equilibrar isolamento e contexto

Muitos profissionais de segurança de TI tendem a ver inovações, como o SDDC, como um novo alvo em potencial. Mas a realidade com o SDDC é que o impacto positivo na segurança de TI é muito maior do que quaisquer mudanças para o que precisa ser protegido. Em outras palavras, para os profissionais de segurança de TI, o SDDC é uma ferramenta e não um alvo. A abordagem de SDDC fornece uma plataforma que soluciona de modo inerente algumas das limitações de arquitetura fundamentais no design de data center, que estiveram restritas a profissionais de segurança por décadas.

Considere o dilema da escolha entre contexto e isolamento nas abordagens tradicionais de segurança. Frequentemente, para obter contexto, colocamos controles no sistema operacional do host. Essa abordagem permite ver quais aplicativos e dados estão sendo acessados e quais usuários estão no sistema, resultando em um bom contexto. No entanto, como o controle fica no domínio de ataque, a primeira ação de um invasor será desativar o controle. Esse isolamento é ruim. Essa abordagem equivale a colocar o botão Liga/Desliga do sistema de alarme de uma residência do lado de fora.

Uma abordagem alternativa, que troca o contexto pelo isolamento, coloca o controle na infraestrutura física. Essa abordagem isola o controle do recurso que está sendo protegido, mas tem um contexto ruim porque os endereços IP, as portas e os protocolos são substitutos muito ruins para o contexto de usuários, aplicativos ou transações. Além disso, nunca houve uma camada de aplicação abrangente criada para a infraestrutura. Até agora.

A camada de virtualização do data center usada pelo SDDC oferece o local ideal para obter contexto e isolamento, combinado a uma aplicação abrangente. Os controles que funcionam na camada de virtualização do data center aproveitam o exame interno seguro do host, a capacidade de fornecer contexto de host sem agente e de alta definição, enquanto permanecem isolados no hypervisor, protegidos contra tentativas de ataque.

A posição ideal da camada de virtualização do data center entre o aplicativo e a infraestrutura física, combinada com o aprovisionamento automatizado e o gerenciamento de políticas de rede e segurança, o desempenho incorporado do kernel, a aplicação distribuída e a capacidade de dimensionamento horizontal, está próxima da transformação completa da segurança do data center e da permissão para que os profissionais de segurança do data center alcancem os níveis de segurança que eram operacionalmente inviáveis no passado.

Como implementar privilégio mínimo e confiança com microssegmentação

Pressupondo que as ameaças podem estar escondidas em qualquer lugar no data center, uma abordagem de segurança prudente requer um modelo de privilégio mínimo e confiança. Juntos,

privilegio mínimo e confiança no nível da unidade, alcançam um modelo de controle positivo que implementa uma estratégia de segurança “nunca confie, sempre verifique” em um nível muito detalhado até a carga de trabalho individual.



Um *modelo de controle positivo* define explicitamente o que é permitido na rede e bloqueia implicitamente todo o resto. Um *modelo de controle negativo* define explicitamente o que não é permitido na rede e permite implicitamente todo o resto.

O privilegio mínimo começa sem um nível de confiança padrão para qualquer entidade ou objeto no data center, incluindo segmentos de rede, cargas de trabalho de servidores, aplicativos e usuários. A confiança no nível da unidade exige que as empresas estabeleçam limites de confiança que efetivamente compartilhem diferentes segmentos do ambiente do data center em um nível muito detalhado e movam os controles de segurança o máximo possível para perto dos recursos que necessitam de proteção.

O privilegio mínimo e a confiança no nível da unidade requerem monitoramento contínuo e inspeção de todo o tráfego do data center quanto a ameaças e atividades não autorizadas. Isso inclui o tráfego norte-sul (cliente a servidor) e o tráfego leste-oeste (servidor a servidor). A microssegmentação permite a implementação de uma estratégia de segurança eficaz de privilégio mínimo e confiança no nível da unidade por meio da criação de vários limites de confiança em um nível extremamente alto de detalhamento e aplicação de políticas e controles apropriados para cargas de trabalho individuais no data center.



A microssegmentação permite que as organizações adotem uma estratégia de privilégio mínimo e confiança no nível da unidade que efetivamente limite a capacidade de um invasor de mover-se lateralmente no interior do data center e extrair dados sensíveis.

O que não é microssegmentação

O conceito de microssegmentação não é nada novo. A realidade de alcançar a microssegmentação é nova e possível pela primeira vez com a virtualização de redes e segurança distribuída para o hypervisor. Infelizmente, como acontece com qualquer nova inovação tecnológica, muitas vezes há uma grande confusão sobre as capacidades e limites da microssegmentação. Portanto, é hora de derrubar alguns mitos sobre essa abordagem.

Primeiro, a microssegmentação e, mais especificamente, os serviços de rede e segurança de uma plataforma de virtualização de redes, não é um substituto de firewalls de hardware implantados no perímetro do data center. A capacidade de desempenho das plataformas de firewall de hardware é projetada para controlar o fluxo de tráfego de e para centenas ou milhares de sessões simultâneas de carga de trabalho do data center.



Não obstante o desempenho dos firewalls de hardware implantados no perímetro do data center, o desempenho dos firewalls e a capacidade da plataforma NSX da VMware, por exemplo, para o tráfego leste-oeste no data center é impressionante. A plataforma NSX fornece 20 Gbps de throughput de firewall e oferece suporte a mais de 80.000 conexões por segundo, por host. Esse desempenho é aplicado apenas às VMs em seu hypervisor e, sempre que outro host é adicionado à plataforma de SDDC, a capacidade de outros 20 Gbps de throughput é adicionada.

Em seguida, a microssegmentação não é possível com ferramentas e tecnologias existentes e não pode ser efetivamente implementada em uma rede virtualizada porque há falta de contexto. A microssegmentação eficaz requer agrupamento inteligente de cargas de trabalho individuais, de modo que as políticas de rede e segurança possam ser aplicadas de forma dinâmica em um nível extremamente alto de detalhamento, completamente independente da topologia da rede física subjacente (consulte a Figura 2-2).

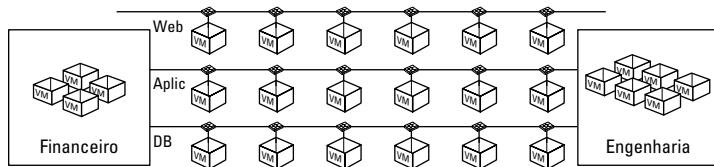


Figura 2-2: O agrupamento inteligente de cargas de trabalho do data center em um ambiente multicamadas que seja completamente independente da rede física subjacente só é possível com a microssegmentação.

A microssegmentação permite que as organizações definam grupos de formas criativas que antes nunca fora possível. Devido à natureza ubíqua do hypervisor de rede e a visibilidade única e compreensão das cargas de trabalho individuais no data center, os grupos inteligentes de política de rede e segurança são baseados em características (consulte a Figura 2-3), tais como

- ✓ Sistema operacional
- ✓ Nome da máquina
- ✓ Serviços
- ✓ Camadas de aplicação
- ✓ Requisitos normativos
- ✓ Contêineres do Active Directory
- ✓ Tags exclusivas

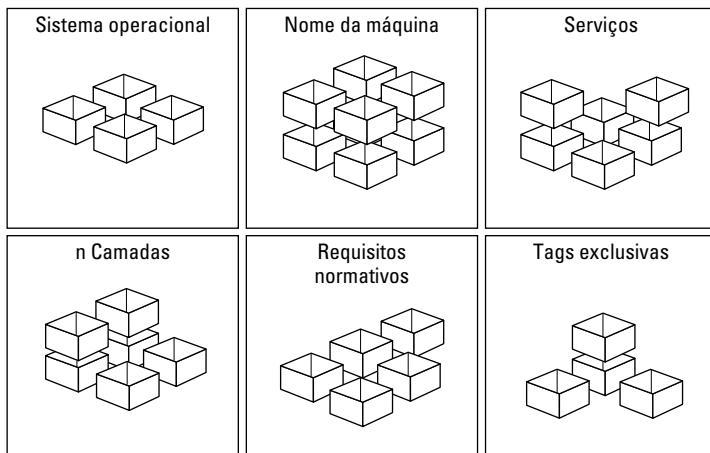


Figura 2-3: Agrupamento inteligente definido por critérios personalizados.

Esse nível de detalhamento exigiria, provavelmente, a implantação de milhares de firewalls (físicos, virtuais ou ambos) no interior do data center, o que não é viável, financeira nem operacionalmente, para a maioria das organizações. Embora a microssegmentação permita implantação e gerenciamento centralizado, automação e orquestração de centenas de milhares de firewalls individuais no nível da carga de trabalho individual, a microssegmentação não é uma solução definida por hardware nem um appliance virtual. Além disso, a automação e o gerenciamento de regras de firewall são capacidades importantes que permitem a microssegmentação, mas não definem a microssegmentação em si mesmas.

Finalmente, a microssegmentação não pode ser alcançada com segurança baseada em agente instalada em cargas de trabalho individuais. A microssegmentação utiliza uma abordagem baseada em grupo para aplicar os serviços de rede e segurança em cargas

de trabalho individuais. Essas políticas se movem e mudam dinamicamente à medida que os requisitos de negócios e técnicos de uma carga de trabalho individual mudam. Por exemplo, um banco de dados que não processar, armazenar e transmitir informações do titular do cartão não poderá ser considerado parte do ambiente de dados do titular do cartão (CDE, Cardholder Data Environment) e, portanto, não estará sujeito aos requisitos de conformidade dos Padrões de segurança de dados (DSS, Data Security Standards) do setor de cartões de pagamento (PCI, Payment Card Industry). No entanto, se as informações do titular do cartão forem erroneamente armazenadas no banco de dados em algum momento, a política de segurança precisará ser atualizada. A microssegmentação permite que essa alteração de política ocorra automaticamente, movendo o banco de dados para o grupo apropriado no SDDC. Uma abordagem baseada em agente exigiria atualização manual da política de segurança para esse banco de dados específico. Além disso, a segurança baseada em agente não tem o nível adequado de isolamento porque muitas vezes é o primeiro componente que o invasor desativará, anulando efetivamente o alarme.

No Capítulo 3, você aprenderá como uma plataforma de virtualização de redes permite a microssegmentação no data center.

Capítulo 3

Como migrar o data center para software

Neste capítulo

- ▶ Como reconhecer os atuais desafios de rede e segurança
 - ▶ Como estender a virtualização para a infraestrutura de redes
 - ▶ Como funciona a virtualização de redes
 - ▶ Juntando as peças da virtualização de redes
-

Os data centers corporativos atuais estão aproveitando os enormes benefícios da virtualização de servidores nas áreas de processamento e armazenamento para consolidar e otimizar a utilização dos recursos de infraestrutura, reduzir a complexidade operacional, além de alinhar e dimensionar sua infraestrutura de aplicativos de forma dinâmica, de acordo com as prioridades dos negócios. No entanto, as aéreas de rede segurança do data center não acompanharam o mesmo ritmo e continuam estáticas, complexas, proprietárias e fechadas às inovações. Tais barreiras impossibilitam explorar todo o potencial da virtualização e mover o data center para software.

Neste capítulo, você descobrirá como a Virtualização da Redes pode transformar o data center e construir a base necessária para microssegmentação.

Principais motivadores para a transformação do data center

As soluções de virtualização de processamento e armazenamento transformaram dramaticamente o data center, proporcionando economia operacional significativa através da automação, economia em novos investimentos através da independência e da

consolidação de hardware, bem como maior agilidade através das abordagens de provisionamento sob demanda e através de autoatendimento. No entanto, as equipes de rede e segurança, que continuam sob pressão para inovar e agilizar, são restringidas por um modelo de tecnologia baseado em hardware e processos de operações manuais. Ao trabalhar com uma arquitetura tradicional, as equipes de rede e segurança lutam para se adaptar de forma rápida o suficiente para atender aos requisitos de negócios e manter o ritmo em um cenário de ameaças em constante mudança.



A abordagem através de software cria uma plataforma comum de redes e segurança que permite a integração de soluções de fabricantes diferentes com o objetivo de garantir uma operação mais eficiente e efetiva em todo o data center.

O modelo operacional atual resulta em um provisionamento lento, manual e propenso à erros de configuração dos serviços de rede e segurança que suportam a implantação das aplicações. Os operadores de rede dependem de recursos como terminal serial, do teclado, dos scripts de configuração e das interfaces de linha-de comando (CLIs) para manipular diversas VLAN, regras de firewall,平衡adores de carga, listas de controle-de acesso (ACLs), qualidade de serviço (QoS), instâncias de VRF e tabelas MAC e ARP. A complexidade e os riscos aumentaram, pois é necessário garantir que as alterações na rede necessárias por uma aplicação não impactem outras aplicações.

Devido à complexidade dessa situação, não é de se admirar que estudos recentes apontam que erros de configuração manual são responsáveis por mais de 60% dos casos de indisponibilidade de rede e de violações de segurança. O resultado é que, além dos frequentes e inevitáveis erros de configuração, o departamento de TI leva muito tempo para atender às solicitações da empresa, uma vez que a infraestrutura de processamento e armazenamento que foi rapidamente realocada ainda precisa esperar pela infraestrutura de rede e segurança.

Já se foi o tempo de uma única infraestrutura monolítica de aplicativos podia ser provisionada de forma isolada em um servidor físico e vinculada a uma política de segurança estática. As aplicações atuais exigem mobilidade das cargas de trabalho, velocidade para chegar ao mercado e um nível de acessibilidade que não existia antes do data center incorporar o processamento definido por software. No entanto, a abordagem atual de redes e segurança centradas em hardware limita a mobilidade das cargas de trabalho à zonas de disponibilidade baseadas em subnets físicas individuais.

Para acessar os recursos de processamento disponíveis no data center, os administradores de rede e segurança são obrigados a configurar as VLANs uma a uma, e o mesmo acontece para as ACLs, regras de firewall e etc. Esse processo, além de lento e complexo, é bastante limitado, como por exemplo, ao limite total de 4.096 VLANs. As empresas geralmente acabam optando por soluções sobredimensionadas para as células de processamento de suas aplicações, resultando no desperdício e na baixa utilização dos recursos disponíveis.

Esse desequilíbrio entre o ritmo dinâmico de mudanças dos negócios e a estagnação dos modelos de rede e segurança atuais criou um gargalo significativo (geralmente de semanas ou meses) para a implantação de novas aplicações e serviços. Além disso, é comum a exigência de novas mudanças depois do provisionamento de uma nova carga de trabalho, e essa realidade força a empresa a repetir o inevitável ciclo de reconfiguração manual de infraestrutura e acaba desgastando o relacionamento entre o modelo de negócio da empresa e o departamento de TI (veja a Figura 3-1).

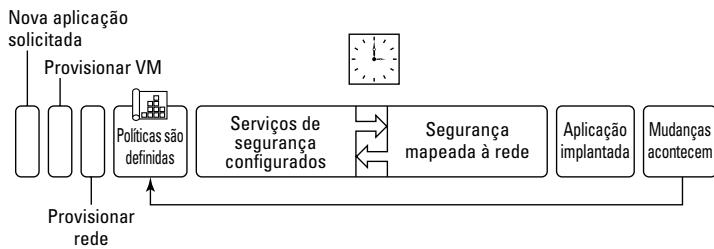


Figura 3-1: As políticas de segurança mapeadas de forma rígida à topologia da rede não conseguem acompanhar o ritmo das mudanças de negócios.

Ao mesmo tempo, a demanda por mais segurança no data center permanece constante e cada vez mais importante no modelo de negócio atual. Atualmente, as grandes violações de segurança, ameaças cada vez mais sofisticadas e requisitos de conformidade normativa cada vez mais complexos e rigorosos são preocupações constantes de diretores de segurança da informação (CISO, Chief Information Security Officer) e demais profissionais dessa área. Tornou-se praticamente impossível manter uma postura de segurança proativa e eficaz no data center que ao mesmo tempo permita um ambiente ágil e dinâmico para os negócios.

Transformando seu data center com a virtualização de redes

A abordagem por software apresentada pelo SDDC estende as principais tecnologias de virtualização a todo o data center. Essa mesma abordagem por software transforma a economia envolvida no data center e a agilidade do modelo de negócio através da automação e de sua implementação não disruptiva que aproveita os investimentos existentes em infraestrutura de processamento físico, conectividade e armazenamento.

Da mesma forma que a virtualização de servidor cria, realiza “snapshots”, exclui e restaura as máquinas virtuais baseadas em software, a virtualização de redes cria, realiza “snapshots”, exclui e restaura as redes virtuais baseadas em software. O resultado é uma abordagem completamente transformadora para a área de redes, que não só permite que os gerentes de data center a alcancem excelentes níveis de agilidade e economia, mas também permite um modelo operacional altamente simplificado para a infraestrutura de redes física.



A virtualização de redes é uma solução que permite sua adoção de forma não disruptiva e que pode ser implantada em qualquer rede IP, incluindo as arquiteturas de rede tradicionais existentes como também as arquiteturas de fabric de última geração de qualquer fabricante.

A virtualização de servidores (server hypervisor) cria uma camada de abstração que reproduz os atributos de um servidor físico x86 (interfaces de processadores, memória, armazenamento e rede) em software, permitindo que eles sejam montados de forma programática em qualquer combinação aleatória para criar uma máquina virtual ou VM customizada (veja a Figura 3-2).

A virtualização de redes (network hypervisor) tem um modelo de funcionamento equivalente, que reproduz o conjunto completo dos serviços de rede da camada 2 à camada 7, tais como switching, roteamento, firewall e balanceamento de carga em software. Dessa forma, é possível criar quantas topologias de rede forem necessárias, de forma arbitrária, conforme a demanda. Isso também permite o encadeamento de serviços, ou service chaining, utilizando tecnologias de segurança avançadas, em qualquer combinação ou ordem, para fornecer os controles de segurança mais eficazes possíveis (leia o Capítulo 2 para saber mais sobre esse recurso).

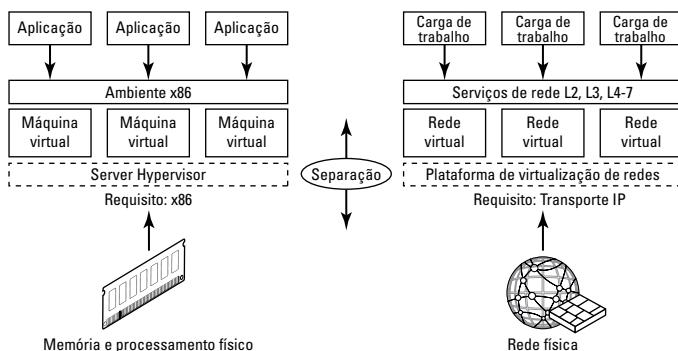


Figura 3-2: Virtualização das camadas de processamento e de conectividade.

Além disso, a virtualização de redes permite distribuir esses serviços de rede e segurança da camada 2 à camada 7 em todas as cargas de trabalho do data center. Essa abordagem distribuída disponibiliza os serviços avançados de rede e segurança em qualquer lugar e minimiza o impacto de qualquer tipo de falha. Essa abordagem também permite que você dimensione sua capacidade de acordo com a inclusão de cada carga de trabalho. Por exemplo, com cada nova carga de trabalho adicionada ao data center é adicionada também mais capacidade de firewall.

Evidentemente, benefícios semelhantes são obtidos com a virtualização de redes e com a virtualização de servidores. Por exemplo, assim como as VMs são independentes da plataforma x86 e permitem que o departamento de TI trate os hosts físicos como um pool de capacidade de processamento, as redes virtuais são independentes da infraestrutura de conectividade física e permite que a TI trate da rede física como um pool de capacidade de transporte que pode ser consumido e adaptado sob demanda.

Ao contrário das arquiteturas de rede tradicionais, as redes virtuais podem ser provisionadas, alteradas, armazenadas, excluídas e restauradas programaticamente, sem a reconfiguração dos equipamentos físicos ou da topologia existente. Ao entregar os recursos e benefícios derivados de soluções conhecidas de virtualização de armazenamento e processamento, essa abordagem inovadora revela todo o potencial do SDDC.

Como funciona a virtualização de redes

A virtualização de redes cria, provisiona e gerencia redes virtuais de maneira programática, utilizando a rede física como um backplane de encaminhamento de pacotes. Os serviços de rede e segurança em software são distribuídos nos hypervisores e aplicados às VMs individuais de acordo com políticas definidas para cada aplicação conectada. Quando uma VM é transferida de um host para outro, seus serviços de rede e segurança a acompanham. Quando novas VMs são criadas para dimensionar a capacidade de uma aplicação, as políticas necessárias também são aplicadas a elas de forma dinâmica.

Assim como uma máquina virtual é um contêiner em software que apresenta serviços lógicos de processamento para uma determinada aplicação, uma rede virtual é um contêiner em software que apresenta serviços lógicos de rede (switching, roteamento, firewall, VPN e平衡amento de carga, entre outros) para as cargas de trabalho conectadas. Esses serviços de rede e segurança são fornecidos em software e exigem somente o encaminhamento de pacotes IP da rede física.

A virtualização de redes coordena os switches virtuais e serviços de rede recebidos pelas VMs presentes nos hypervisores de servidor de modo a oferecer uma plataforma (“network hypervisor”) que crie redes virtuais de forma eficaz (veja a Figura 3-3).

Uma maneira de provisionar as redes virtuais é utilizando uma plataforma de gerenciamento de nuvem (CMP, Cloud Management Platform) para solicitar os serviços de rede e segurança virtuais para as cargas de trabalho correspondentes (veja a Etapa 1 ou a Figura 3-4). Em seguida, o controlador distribui os serviços necessários para os switches virtuais correspondentes e os conecta logicamente às respectivas cargas de trabalho (veja a Etapa 2 ou a Figura 3-4).

Essa abordagem não só permite que diferentes redes virtuais sejam associadas a diferentes cargas de trabalho no mesmo hypervisor, como também possibilita a criação de tudo, desde redes virtuais básicas com apenas dois nós à estruturas mais avançadas com topologias de rede complexas de vários segmentos usadas em aplicações multicamadas.

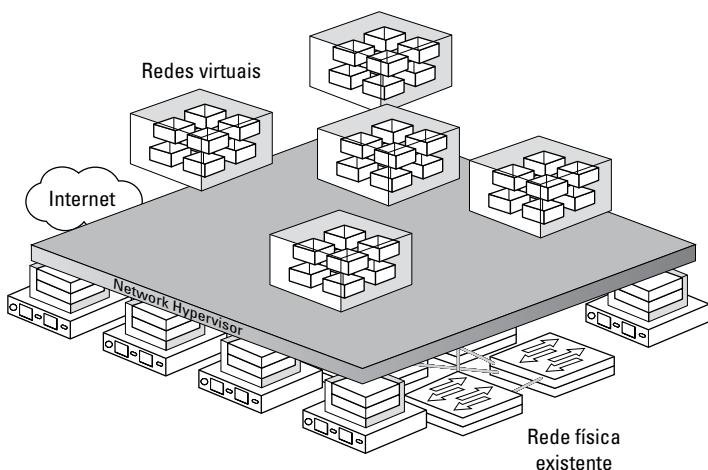


Figura 3-3: O “network hypervisor”.

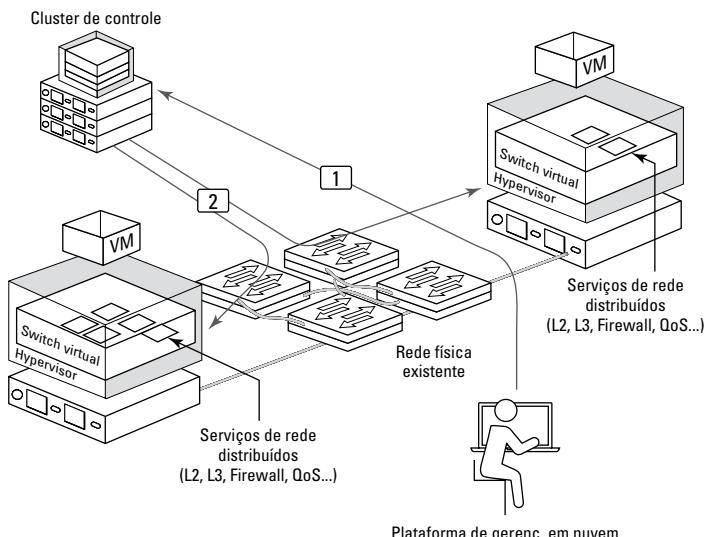


Figura 3-4: Provisionamento de rede virtual.

Para as cargas de trabalho conectadas, uma rede virtual se parece e funciona exatamente como uma rede física tradicional (veja a Figura 3-5). As cargas de trabalho reconhecem os mesmos serviços de rede existentes nas camadas 2 a 7 que reconheceriam em uma

rede tradicional. A única diferença é que esses serviços de rede agora são instâncias lógicas de módulos de software distribuídos que estão em execução no hypervisor no host local e aplicados nas interfaces do switch virtual.

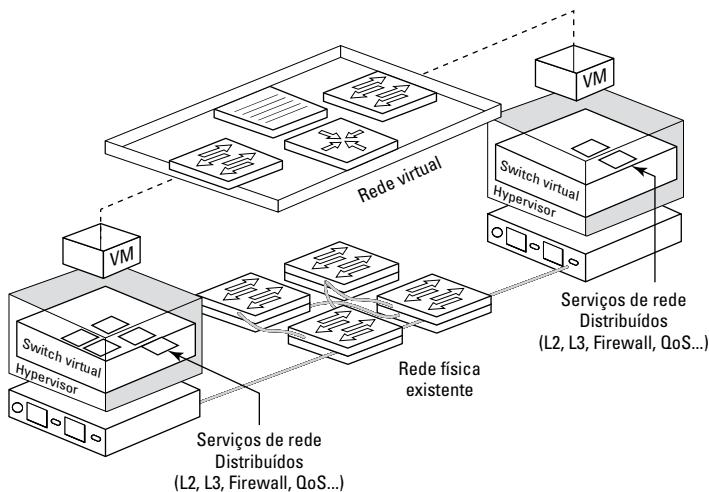


Figura 3-5: A rede virtual, da perspectiva da carga de trabalho (lógica).

Para a rede física, uma rede virtual parece e funciona como uma rede física tradicional (veja a Figura 3-6). A rede física “vê” os mesmos frames de rede de camada 2 que estariam em uma rede física tradicional. A VM envia um frame de rede de camada 2 padrão que é encapsulado no hypervisor de origem que apresenta externamente novos cabeçalhos IP, UDP e VXLAN (Virtual Extensible LAN). A rede física encaminha o frame como um frame de camada 2 padrão, e o hypervisor de destino desencapsula os cabeçalhos e fornece o frame de camada 2 original à VM de destino.



A capacidade de aplicar serviços de segurança nas interfaces dos switches virtuais também elimina a necessidade de topologias de hairpin (consulte o Capítulo 1). Essa prática é comum em situações nas quais o tráfego leste-oeste entre duas VMs que estão no mesmo hypervisor, mas em subnets diferentes, precisa atravessar a rede para acessar serviços essenciais, como roteamento e firewall.

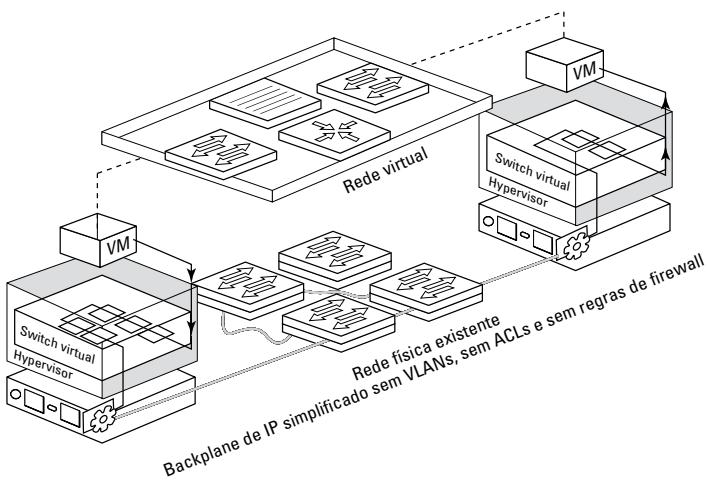


Figura 3-6: A rede virtual, da perspectiva da rede física.

Elementos essenciais para virtualização de redes

A virtualização de redes distribui serviços de conectividade e segurança da camada 2 à camada 7 em todas as cargas de trabalho no ambiente, incluindo switching, roteamento, balanceamento de carga e firewall. Essa abordagem distribuída é a solução dos problemas da segurança da informação: controle centralizado com aplicação granular. A arquitetura distribuída juntamente com a virtualização de redes também reduz drasticamente os pontos de falha do data center em todo o ambiente para que nenhum ponto único de falha cause um problema mais grave. Uma plataforma de virtualização de redes consiste em um plano de gerenciamento, um plano de controle e um plano de dados que usam um protocolo de encapsulamento para abstrair componentes de rede físicos ou virtuais para promover um backplane de transporte baseado em IP.



Ao contrário da rede definida-por software (SDN, Software-Defined Networking), em que o hardware continua a ser a principal força motriz, a tecnologia de virtualização de redes é totalmente agnóstica ao hardware e promove os recursos de rede de forma independente à rede física. Os princípios da virtualização são aplicados à infraestrutura de rede física, abstraindo os serviços de rede para criar um pool de transporte flexível que pode ser alocado, utilizado e redefinido sob demanda.

Alguns planos... de dados, de controle e de gerenciamento

O plano de *controle* em uma rede virtual é executado em um controlador e é responsável por rotear o tráfego pela rede. A camada de controle também executa encapsulamento do tráfego de rede nas tecnologias de virtualização de redes que usam os protocolos VXLAN e NVGRE (explicados mais adiante neste capítulo). Vários nós de controlador podem ser implementados para adicionar alta disponibilidade e dimensionamento ao ambiente.

O plano de *gerenciamento* fornece configuração e administração centralizadas das redes virtuais e pode ser integrado a uma plataforma de gerenciamento de nuvem para implementar novas aplicações e aprovisionar serviços funcionais de rede e segurança, incluindo os seguintes:

- ✓ **Switching:** Permite a extensão de um segmento de camada 2 ou sub-rede IP em qualquer lugar da rede física independente de seu design.
- ✓ **Roteamento:** O roteamento entre subnets IP pode ser realizado logicamente, sem que o tráfego saia para o roteador físico. Esse roteamento é executado pelo kernel do hypervisor e fornece um caminho de dados ideal para o roteamento do tráfego na infraestrutura virtual (comunicação leste-oeste) e para a rede externa (comunicação norte-sul).
- ✓ **Firewall distribuído:** A microssegmentação permite a aplicação de segurança através do kernel a nível de interface da rede virtual. Isso permite a aplicação de regras de firewall de modo altamente escalável em alta velocidade com performance próxima à wire-speed, sem criar gargalos em appliances físicos.
- ✓ **Balanceador de carga lógico:** Suporte ao balanceamento de carga da camada 4 à camada 7 com os recursos de SSL (Secure Sockets Layer) Termination.
- ✓ **VPN (Virtual Private Network):** Serviços de SSL VPN de camada 2 e camada 3.
- ✓ **Conectividade com as redes físicas:** As funções de gateway de rede nas camadas 2 e 3 fornecem comunicação entre as cargas de trabalho localizadas em ambientes lógicos e ambiente físicos.

O *plano de dados* transporta o tráfego de rede. Em uma rede virtualizada, as funções do plano de dados são geralmente implementadas em um switch virtual. Um switch virtual abstrai a rede física e fornece comutação no próprio hypervisor. Ele é crucial para a virtualização da camada de conectividade porque promove redes lógicas que não dependem de estruturas físicas, como VLANs. Veja alguns dos benefícios de um switch virtual:

✓ **Supporte para redes baseadas em overlay e configuração centralizada:** As redes baseadas em overlay permitem os seguintes recursos:

- Criação de uma de camada 2 lógica sobre a infraestrutura IP física atual sem a necessidade de repensar a arquitetura novamente
- Provisionamento ágil de comunicação (leste-oeste e norte-sul) mantendo o isolamento em ambientes multi-tenant
- Cargas de trabalho e máquinas virtuais que são agnósticas quanto às redes virtuais e operam como se estivessem conectadas a uma rede física tradicional de camada 2

✓ **Crescimento transparente de hypervisors**

✓ **Um kit de ferramentas completo para gerenciamento, monitoramento de tráfego e troubleshooting em uma rede virtual:** Vários recursos disponíveis, tais como espelhamento de portas, NetFlow e IPFIX (IP Flow Information Export), backup e restauração de configurações, verificação de integridade da rede, qualidade de serviço (QoS) e LACP (Link Aggregation Control Protocol).

Além disso, o plano de dados possui dispositivos que atuam como gateway, fornecendo comunicação entre os ambientes lógico e físico. Essa comunicação pode ocorrer na camada 2 (bridging) ou camada 3 (roteamento).

Encapsulamento

Os protocolos de encapsulamento (ou “overlay”) separam a conectividade do ambiente lógico da infraestrutura do ambiente físico. Os dispositivos conectados às redes lógicas podem aproveitar as funções de rede (incluindo switching, roteamento, firewall,平衡amento de carga, VPN e conectividade com o ambiente físico), independentemente da configuração da infraestrutura física utilizada.

A rede física se torna um backplane utilizado para transportar o tráfego de overlay.

Esse tipo de separação soluciona muitos dos desafios que os tradicionais ambientes de data center enfrentam, como os seguintes:

- ✓ **Provisionamento rápido e ágil de aplicativos:** O design de rede tradicional representa um gargalo que atrasa a implementação de novas aplicações no ritmo exigido pelas empresas. O tempo necessário para provisionar a infraestrutura de rede necessária para suportar uma nova aplicação costuma ser contado em dias ou até em semanas.
- ✓ **Mobilidade da carga de trabalho:** A virtualização da camada de processamento permite a mobilidade de cargas virtuais entre diferentes servidores físicos conectados à rede do data center. Em designs tradicionais de data center, isso exige estender os domínios de camada 2 (VLANs) em toda a infraestrutura de rede do data center, o que afeta o dimensionamento geral e pode prejudicar a resiliência do design como um todo.
- ✓ **Ambientes Multi-tenant de larga escala:** O uso de VLANs como forma de criar redes isoladas é limitado a quantidade máxima de 4094 instâncias. Esse número, apesar de parecer alto para implantações comuns de empresas, está se tornando um gargalo sério para a maioria dos provedores de nuvem.

O encapsulamento permite que as funções de rede disponíveis no ambiente lógico sejam abstraidas das protocolos existentes na camada física ao encapsular os frames com as informações do protocolo da camada superior mais próxima. Para a virtualização de redes, há quatro protocolos de encapsulamento disponíveis no momento:

- ✓ O **VXLAN (Virtual Extensible LAN)** encapsula os frames da camada 2 nos datagramas UDP de camada 4. Os fabricantes que oferecem suporte ao desenvolvimento da VXLAN incluem: Arista Networks, Broadcom, Cisco, Dell, Juniper Networks, OpenBSD, Red Hat, VMware, entre outros.
- ✓ O **NVGRE (Network Virtualization using Generic Routing Encapsulation)** usa encapsulamento de roteamento genérico (GRE, Generic Routing Encapsulation) para encapsular os frames de camada 2 nas redes de camada 3. Os fabricantes que oferecem suporte ao desenvolvimento da NVGRE incluem: Arista Networks, Broadcom, Dell, Emulex, F5 Networks, Intel, Hewlett-Packard, Microsoft, entre outros.

- ✓ O Geneve (**G**eneric **N**etwork **V**irtualization **E**ncapsulation) especifica um esquema do plano de dados e separa o encapsulamento da camada de controle para fornecer flexibilidade em diferentes cenários de implementação. Os fabricantes que oferecem suporte ao desenvolvimento do Geneve incluem Intel, Microsoft, Red Hat e VMware.
- ✓ O STT (**S**tateless **T**ransport **T**unneling) usa o recurso TCP Segmentation Offload (TSO) nas interfaces de rede para aceleração de hardware e desacopla o encapsulamento da camada de controle. Os fabricantes que oferecem suporte ao desenvolvimento de STT são Broadcom, eBay, Rackspace e Yahoo!, entre outros.



Não tem certeza de qual protocolo de encapsulamento usar? Não se preocupe, todos eles são compatíveis e podem coexistir na mesma rede. Você pode utilizar qualquer protocolo de encapsulamento que seja compatível com sua própria tecnologia de virtualização de redes.

Um resumo sobre VXLAN

O VXLAN (Virtual Extensible LAN) tornou-se o protocolo padrão de overlay (ou encapsulamento) com amplo suporte do mercado. O VXLAN é a chave para a criação de redes lógicas que fornecem adjacência de camada 2 entre cargas de trabalho, sem problemas ou preocupações com escalabilidade encontrados nas tecnologias tradicionais de camada 2.

O VXLAN é uma tecnologia que encapsula os frames Ethernet originais gerados por cargas de trabalho (físicas ou virtuais) conectados ao mesmo segmento lógico de camada 2, normalmente chamado de switch lógico (LS, Logical Switch).

O VXLAN é uma tecnologia de encapsulamento de camada 2 sobre camada 3 (L2oL3). O frame Ethernet original gerado por uma carga de trabalho é encapsulado adicionando-se ao frame novos cabeçalhos Ethernet, IP, UDP e VXLAN externos que permitem o transporte do frame original através da infraestrutura de rede que interliga os end-points VXLAN (máquinas virtuais).

Permite o dimensionamento além da limitação dos switches tradicionais de 4094 VLANs através de um identificador de 24 bits, denominado VNI (VXLAN Network Identifier), que está associado a cada segmento de camada 2 criado no ambiente lógico. Esse valor é colocado dentro

(continuação)

(continuação)

do cabeçalho VXLAN e é, em geral, associado a uma subnet IP, semelhante ao que acontece tradicionalmente com a segmentação por VLANs. A comunicação entre dispositivos da mesma subnet ocorre na mesma rede virtual (switch lógico).

É realizado hashing dos cabeçalhos das camadas 2, 3 e 4 presentes no frame Ethernet original para derivar o valor da porta de origem para o cabeçalho de UDP externo. Isto é importante para garantir o equilíbrio dos fluxos de tráfego VXLAN pelos caminhos múltiplos caminhos de mesmo custo potencialmente disponíveis dentro da infraestrutura de transporte de rede.

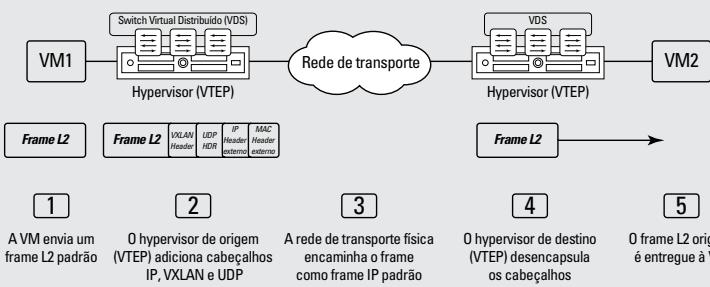
Os endereços IP de origem e de destino utilizados no cabeçalho IP externo identificam exclusivamente os hosts que originam e terminaram o encapsulamento VXLAN dos frames originais. Essa funcionalidade lógica baseada em hypervisor geralmente é referida como VXLAN VTEP (VXLAN Tunnel EndPoint).

O encapsulamento do quadro Ethernet original em um pacote UDP aumenta o tamanho do pacote de IP. É recomendado aumentar o tamanho geral da MTU (Maximum Transmission Unit) para um mínimo

de 1600 bytes para todas as interfaces na infraestrutura física que transportarão os frames VXLAN. A MTU para os uplinks do switch virtual dos VTEPs que realizam o encapsulamento VXLAN é automaticamente aumentado na preparação do host.

A figura a seguir descreve (em alto nível) as etapas necessárias para estabelecer a comunicação de camada 2 entre as VMs que utilizam a funcionalidade de overlay baseada em VXLAN:

1. A VM1 origina um frame destinado à VM2 do mesmo segmento lógico de camada 2 (subnet IP).
2. O VTEP de origem identifica o VTEP de destino no qual a VM2 está hospedada e encapsula o frame antes de enviá-lo à rede de transporte.
3. A rede de transportes só é necessária para permitir a comunicação IP entre os VTEPs de origem e destino.
4. O VTEP de destino recebe o quadro da VLXLAN, realiza o desencapsulamento do frame e identifica o seu respectivo segmento da camada 2.
5. O frame é entregue à VM2.



Capítulo 4

Como automatizar as tarefas de segurança

Neste capítulo

- ▶ Como identificar diferentes abordagens de política de segurança
- ▶ Como criar políticas de rede e segurança de acordo com a carga de trabalho de novas aplicações
- ▶ Como acompanhar as mudanças do ambiente dinamicamente
- ▶ Como automatizar as respostas contra as ameaças ao data center
- ▶ Como simplificar o gerenciamento de firewalls

Este capítulo mostrará como a virtualização de redes e o Data Center Definido por software (SDDC) tornaram possível a microsegmentação, viabilizando assim a realização de tarefas de segurança, tais como, provisionamento de novas regras, movimentação e alteração de regras existentes, configuração de respostas às ameaças dinamicamente e a simplificação do gerenciamento. Esse conjunto de fatores melhorou de uma maneira precisa segurança geral no data center.

Como criar políticas de segurança para o data center definido por software

A virtualização de redes permite microsegmentar o Data Center Definido por Software, atribuindo ao ambiente uma postura de segurança eficaz, agrupando de forma inteligente diversas cargas de trabalho, baseadas nos atributos das aplicações permitindo assim a atribuição de políticas de segurança adequadas.

As regras de política de segurança podem ser criadas de várias maneiras com a virtualização de redes, conforme mostrado na Figura 4-1.

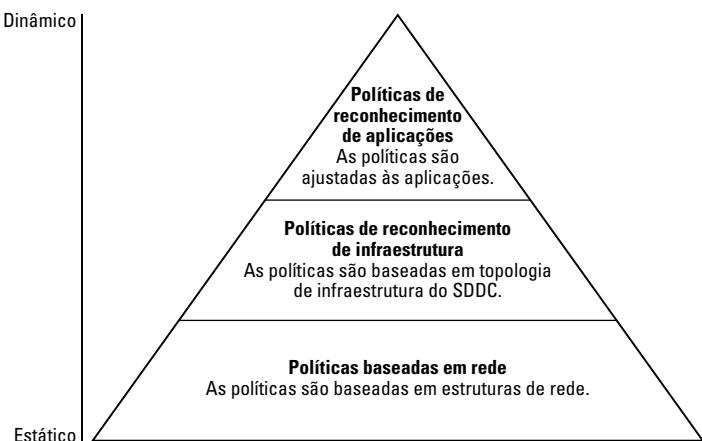


Figura 4-1: Políticas de segurança baseadas em rede, infraestrutura e aplicação. As políticas baseadas em rede destinam-se a ambientes estáticos. Em ambientes virtualizados mais dinâmicos, as políticas precisam evoluir com a natureza dinâmica das aplicações.

Políticas de segurança baseadas em rede

As políticas de segurança baseadas em rede agrupam elementos da Camada 2 ou Camada 3, tais como endereços físicos (MAC, Media Access Control) ou endereços lógicos (IP, Internet Protocol).

A equipe de segurança precisa estar ciente da infraestrutura de rede para implementar as políticas baseadas nessa variável. Quando o agrupamento baseado em atributos dinâmicos deixa de ser usado há uma alta probabilidade de proliferação de regras de segurança. O método de agrupamento estático funciona muito bem se você está apenas migrando regras já existentes de firewalls de fornecedores diferentes mas traz complexidade ao ambiente com o passar do tempo.

Em ambientes dinâmicos, como o provisionamento de recursos de TI através de portal de autoatendimento e implementações automatizadas em nuvem, nos quais é possível adicionar e remover Máquinas Virtuais (VMs) e as topologias das aplicações mudam rapidamente, o agrupamento baseado em endereços MAC pode não ser adequado pois pode haver um atraso entre o provisionamento de uma nova VM e a adição do endereço MAC ao grupo.

Nos ambientes de Data Center com alta mobilidade de cargas de trabalho (migração de VMs e alta disponibilidade por exemplo), a abordagem de agrupamento baseado em endereços IP de Camada 3 também podem ser inadequadas.

Políticas de segurança baseadas em infraestrutura

As políticas de segurança baseadas em infraestrutura agrupam elementos físicos ou lógicos participantes da infraestrutura do data center. Um exemplo dessa política baseada em infraestrutura seria agrupar o ambiente de dados dos Titulares de Cartões de Crédito (CDE, Cardholder Data Environment) do Setor de Cartões de Pagamento (PCI, Payment Card Industry) em uma rede local virtual (VLAN) com regras de segurança adequadas aplicadas com base no nome da VLAN. Outro exemplo poderia usar switches lógicos no data center para agrupar todas as VMs associadas a um aplicativo específico em um único switch lógico. Políticas baseadas em infraestrutura eficazes requerem uma coordenação rigorosa entre as equipes de segurança e de aplicativos para entender os limites lógicos e físicos no data center.

Se não há limites físicos ou lógicos no data center, uma abordagem de política baseada em infraestrutura não é viável. Você também precisa estar ciente do local em que os aplicativos podem ser implantados nesse cenário. Por exemplo, se for necessário flexibilidade para implantar uma carga de trabalho PCI em qualquer cluster que tenha recursos de processamento adequados e disponíveis, a postura de segurança pode não estar vinculada a um cluster específico. Em vez disso, a política de segurança deve se mover com a aplicação.

Políticas de segurança baseadas em aplicação

As políticas de segurança baseadas em aplicação agrupam elementos do data center com base em uma ampla variedade de mecanismos de personalização, tais como o tipo de aplicação (por exemplo, VMs com tag como “Servidores_Web”), ambiente da aplicação (por exemplo, todos os recursos marcados como “Zona_Produção”) e postura de segurança da aplicação. A vantagem dessa abordagem é que a postura de segurança da aplicação não está vinculada às estruturas de rede ou de data center. As políticas de segurança podem se mover com o aplicativo, independentemente dos limites de rede ou infraestrutura e os modelos de política podem ser

criados e reutilizados em todos os tipos de aplicação e workloads semelhantes.

Para implementar políticas de segurança baseadas em aplicação, a equipe de segurança só precisa estar ciente da aplicação que deve ser protegida com base nessas políticas. Essas políticas de segurança seguem o ciclo de vida da aplicação, desde a criação da política (que acompanha a implementação da aplicação) até a exclusão (que acompanha a desativação da aplicação). A abordagem de políticas de segurança baseadas em aplicação permite um modelo de TI de autoatendimento. As regras e moldes de segurança reutilizáveis e concisos podem ser criados sem o conhecimento da topologia subjacente.



As políticas baseadas em infraestrutura e aplicações fornecem a melhor segurança em redes virtualizadas através da microssegmentação.

Aprovisionamento

A virtualização de redes fornece o modelo operacional já consolidado na utilização de VMs para a camada de redes, agilizando o provisionamento dos serviços de conectividade e segurança de semanas para segundos. A virtualização de redes reduz significativamente o tempo e o esforço manual associados à aquisição, instalação e configuração de hardware de rede tradicional (consulte o Capítulo 6).

As capacidades de orquestração avançada em uma plataforma de virtualização de redes distribui programaticamente os serviços de rede na etapa de associação de VMs. As empresas usam esses recursos para padronizar e manter modelos predefinidos que consistem em serviços e topologias de rede e segurança.

Por exemplo, um engenheiro de redes pode criar um modelo de uma aplicação multicamadas para fins de desenvolvimento. O ambiente pode ser provisionado para um desenvolvedor de aplicações em questão de segundos através de um portal de autoatendimento. O mesmo pode ser feito em ambientes de produção, validação e controle de qualidade (QA, Quality Assurance), em diversas aplicações e serviços, com configuração consistente e segurança. Esses recursos de automação reduzem as despesas operacionais, aceleram o tempo de colocação de produtos no mercado e agilizam o fornecimento de serviços de TI.

A virtualização de redes também simplifica as operações, consolidando o estado de configuração e os dados de operação para todas

as conexões de rede, tanto virtual quanto física. Os administradores têm visibilidade operacional completa sobre o que está ocorrendo em toda a infraestrutura de rede. Isso simplifica o gerenciamento, o monitoramento, a identificação e a correção de problemas.

Como se adaptar às mudanças dinamicamente

A mudança é constante em todos os lugares no mundo atual, exceto no data center moderno, que é relativamente estático, do tipo “configure e esqueça”. Como não?!

Já sei, os data centers estão mudando constantemente e as organizações de TI estão se esforçando para acompanhar os requisitos de negócios cada vez mais dinâmicos e exigentes. Esta falta de capacidade e fornecimento de serviços tornou-se muito clara e ainda mais intensa pelas tendências atuais, tais como virtualização de servidor e computação em nuvem — tendências que permitem maior agilidade nos negócios e, portanto, mais mudanças (consulte o Capítulo 2 para saber mais sobre essas tendências e desafios). As equipes de rede e segurança, em particular, sentiram a tensão quando foram forçados a usar ferramentas e soluções que não mantiveram o ritmo com as demandas dos negócios e das outras áreas funcionais de TI.

A virtualização de redes libertou as aplicações e serviços da infraestrutura de rede física, tornando as redes tão portáteis e ágeis quanto as VMs. Com a virtualização da camada de conectividade, as redes são virtualizadas no mesmo switch virtual (vSwitch) conectado às VMs. Quando uma aplicação se move, ela é acompanhada dos serviços de rede e segurança automaticamente.

As empresas usam a virtualização de redes para migrar facilmente as aplicações de um host para outro ou de um data center para outro. Os casos de uso do mundo real incluem o movimento de uma aplicação de um host sobrecarregado para aproveitar a capacidade ociosa em outro local, respeitando às leis de residência de dados, migração para um novo data center ou realização de manutenção ou atualização da infraestrutura física.

Por exemplo, as topologias de rede físicas normalmente exigem a mudança de endereços IP quando as aplicações são movidas. Em alguns casos, as aplicações têm endereços IP fixos, o que pode exigir mudanças de configuração de endereçamento e testes de rollback. Com a virtualização de redes, as empresas têm liberdade para

movimentar rapidamente as aplicações sem reconfiguração. Essas facilidades reduzem significativamente as despesas operacionais e melhoram a agilidade de TI e diminuem o tempo de resposta.

Como responder às ameaças dinamicamente

Os ataques modernos ao data center são eventos sofisticados que estão evoluindo rapidamente e também exigem uma resposta rápida e que se adapte de forma ágil e dinâmica. Tal resposta só pode ser alcançada de forma eficaz automatizando as tarefas de segurança. O adversário atual tem as ferramentas e os recursos necessários para modificar automaticamente uma ameaça ou ataque, a fim de contornar os controles de segurança estáticos e as medidas corretivas de reação no data center. A microssegmentação fornece a possibilidade de responder com a mesma capacidade e frustrar os ataques com controles de segurança detalhados e igualmente sofisticados, além de tarefas específicas aplicadas às cargas de trabalho individuais no data center.

Por exemplo, a microssegmentação permite que as equipes de segurança apliquem uma política que proporcione ao mesmo tempo velocidade e segurança em uma determinada aplicação com arquitetura multicamadas. Em condições normais de funcionamento, essa política pode realizar o controle de acesso de segurança básica e a verificação de malwares com um impacto mínimo no desempenho do aplicativo. No entanto, se uma ameaça de malware é detectada, a política de segurança pode isolar imediatamente a aplicação e seus componentes afetados do restante da rede, a fim de evitar uma exposição maior da aplicação ou de quaisquer outras aplicações no data center. A política recém-aplicada pode então exigir uma inspeção detalhada do pacote (DPI, Deep Packet Inspection) por um Firewall de Nova Geração (NGFW, Next Generation Firewall) integrado a solução, a fim de identificar quaisquer outras ameaças que possam estar usando táticas, como ocultação de SSL (Secure Sockets Layer) ou mesmo “port-hopping” para evitar a detecção e extraír as informações sensíveis.

As Figuras 4-2 e 4-3 ilustram um exemplo de visão física e lógica, respectivamente, da microssegmentação em uma Aplicação multicamadas.

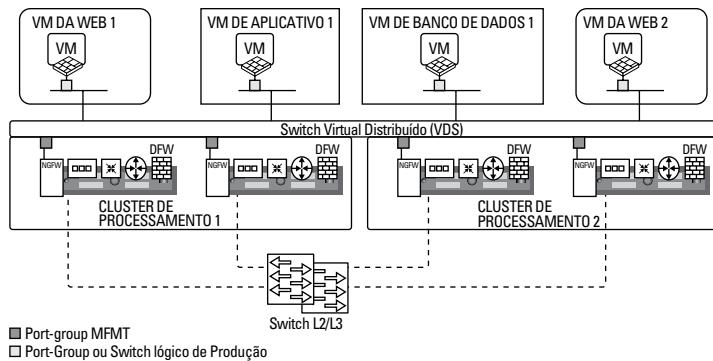


Figura 4-2: Visão física de microssegmentação em uma Aplicação multicamadas

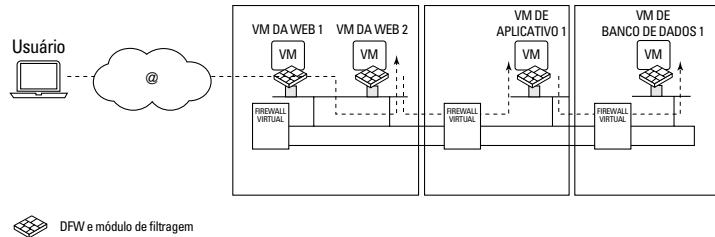


Figura 4-3: Visão lógica da microssegmentação em uma Aplicação multicamadas.



Saiba mais sobre os recursos de inserção de serviços avançados de segurança, sequenciamento e direção possíveis com a microssegmentação no Capítulo 2.

Como criar firewalls para dezenas de milhares de cargas de trabalho com um único firewall lógico

Por último, a plataforma de virtualização de redes possibilita gerenciar literalmente milhares de firewalls nas redes do SDDC a partir de um único "painel de controle" como se fossem um único firewall. Os administradores de segurança podem automatizar tarefas, políticas e conjuntos de regras e configurar outros recursos avançados de firewall e, em seguida, distribuir essas alterações de configuração para milhares de firewalls simultaneamente, com o objetivo de

proteger o data center no interior do perímetro e em todas as partes. Em outras palavras, a virtualização de redes permite a aplicação de políticas de segurança distribuídas com gerenciamento centralizado.

Capítulo 5

Microssegmentação: Como começar

Neste capítulo

- ▶ Implantando microssegmentação no seu data center
 - ▶ Explorando os casos de uso de segurança através da microssegmentação
-

Neste capítulo, você aprenderá a implementar a microssegmentação no seu data center e examinará alguns casos de uso comuns aderentes à essa tecnologia.

Como obter a microssegmentação

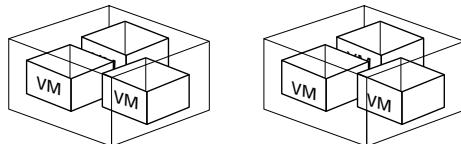
Seja projetando um novo data center com arquitetura definida por software (SDDC, Software-Defined Data Center) ou adicionando recursos de SDDC à um data center existente com arquitetura definida por hardware, a plataforma de virtualização de redes permite que os arquitetos da empresa criem uma infraestrutura otimizada para segurança e desempenho através da microssegmentação.

Os princípios de design de um SDDC com microssegmentação (consulte a figura 5-1) incluem:

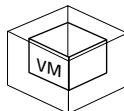
- ✓ Isolamento e segmentação
- ✓ Nível de confiança/menor privilégio
- ✓ Ubiquidade e controle centralizado

Princípios de design

1. Isolamento e segmentação



2. Nível de confiança/menor privilégio



3. Ubiquidade e controle centralizado

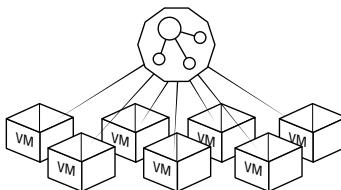


Figura 5-1: Microssegmentação, um novo modelo para o data center definido por software.



Consulte o Capítulo 2 para obter mais informações sobre os princípios de microssegmentação.

O design tradicional de um data center definido por hardware cria uma infraestrutura de conectividade limitada ao redor dos recursos físicos e direcionam o tráfego por meio de caminhos e pontos de segurança predeterminados. O SDDC pode ser implementado sob uma infraestrutura convencional que fornece apenas conectividade física — liberando os arquitetos do data center para desenvolver regras de segurança que aproveitam os fluxos de tráfego de forma mais eficiente e simples em todo o ambiente.

Para atingir um modelo “zero-trust” de segurança (veja o Capítulo 2) através da microssegmentação, comece entendendo os fluxos de tráfego dentro do data center. Em seguida, analise as relações entre as cargas de trabalho. Por fim, crie um modelo de política que esteja alinhado às necessidades de segurança de cada carga de trabalho.

Determine os fluxos de rede

Entender o fluxo de tráfego da rede que entra e sai do data center é um primeiro passo importante, pois costuma demonstrar falhas ou vulnerabilidades de segurança que podem ser exploradas e que podem permanecer desapercebidas por anos.

Comece a análise de tráfego verificando as regras atuais nos firewalls do seu perímetro e separando os tráfegos norte-sul e leste-oeste. Várias ferramentas de monitoramento de fluxo, como IPFIX (NetFlow) ou SYSLOG, podem ajudar você a coletar e analisar esses fluxos de tráfego e permitirão a correlação com o firewall atual.

Os padrões de fluxo identificados como “hairpin” (consulte o Capítulo 1) geralmente indicam os fluxos de tráfego leste-oeste. A análise das regras de firewall atuais ajuda a entender como substituir o tráfego “hairpin” por switches e roteadores lógicos usando a arquitetura de redes virtualizadas.



Identifique padrões e relações

As regras dos firewalls de perímetro atuais, quando correlacionadas com os padrões de fluxo coletados das ferramentas de monitoramento, fornecem o conjunto inicial de políticas de segurança para o modelo de microsegmentação.

Os padrões de fluxo encontrados fornecem a introspeção necessária para conhecer as relações existentes no seu data center. Por exemplo, você pode ver como cada carga de trabalho interage com os serviços de TI compartilhados, com outros aplicativos ou usuários e em diferentes ambientes (como produção ou desenvolvimento/teste). Entender essas relações ajudará você a definir os microsegmentos adequados, bem como as regras que controlarão a interação entre elas. Por exemplo, é possível criar um microsegmento para cada aplicativo e, em seguida, controlar a comunicação com outros microsegmentos, tais como serviços de TI compartilhados como Active Directory (AD), o Domain Name Service (DNS), o Network Time Protocol (NTP) e outros.



Exemplos comuns de definições de microsegmentos incluem por departamento ou locatário comercial, aplicativo, acesso de usuário e classificação de dados ou conformidade normativa.

Crie e aplique o modelo de política

Para permitir um ambiente de segurança “zero-trust” com microssegmentação, comece com um modelo de política de “bloco padrão”, no qual não é permitida nenhuma comunicação entre as várias relações de carga de trabalho no data center. Em outras palavras, comece fazendo uma verificação completa. Com base na sua análise de padrões e relações de fluxo de tráfego, defina políticas de segurança que ampliem cada vez mais os canais de comunicação entre cargas de trabalho, conforme necessário. Essa é a melhor prática recomendada para proteger o data center através microssegmentação.

Nem todos os fluxos e relações de tráfego no data center podem ser totalmente compreendidos. Nesses casos limitados e com maior discrição, use uma política de “permissão padrão” — basicamente sem impor restrições — para impedir a interrupção involuntária de qualquer serviço. Em seguida, bloquee todos os canais de comunicação impróprios que já foram identificados, a fim de eliminar o tráfego entre esses microssegmentos.

Como os contextos de carga de trabalho e aplicativo/usuário/dados mudam com o tempo, ajuste o seu modelo de política de segurança de acordo com as necessidades de segurança de cada carga de trabalho para garantir controles de segurança relevantes e atualizados.

Casos de uso de segurança

As empresas estão usando a virtualização de redes para oferecer uma infinidade de novos casos de uso de segurança e resultados de TI com alto valor agregado, algo que não era possível com a infraestrutura de rede tradicional. A TI também está realizando operações existentes de modo mais rápido e econômico do que nunca. As empresas muitas vezes podem justificar o custo da virtualização da rede por meio de um único caso de uso. Ao mesmo tempo, elas estabelecem uma plataforma estratégica que automatiza a TI e orienta outros casos de uso ao longo do tempo.

Casos de uso conhecidos incluem ambientes de “Disaster Recovery” (DR), nuvens de autoatendimento para pesquisa e desenvolvimento (P&D), portabilidade de aplicativos na nuvem e migração de data center, automação e orquestração de TI e otimização e atualização de infraestrutura. As seções a seguir

destacam três outros casos de uso: comunicação lateral entre servidores, ambientes “multitenancy” e infraestrutura de desktop virtual (VDI, Virtual Desktop Infrastructure).

Segurança de rede dentro do data center

A microssegmentação traz segurança para o data center com políticas automatizadas e granulares associadas a cargas de trabalho individuais. A microssegmentação é capaz de eliminar a movimentação lateral de ameaças dentro do data center e reduz significativamente a superfície total de ataques.

A comunicação leste-oeste entre os servidores se torna cada vez maior, à medida que as infraestruturas de aplicações multicamadas desenvolvidas em plataformas de servidores virtualizados são implantadas.

Esse tráfego de rede costuma ser livre de controles de segurança tradicionais; em vez disso, ele é otimizado para máximo desempenho e throughput devido a uma falha no design de segurança, que pressupõe que as ameaças são impedidas no firewall do perímetro e que tudo o que está dentro do data center é confiável. As falhas desse design de segurança ficaram expostas com o acontecimento de grandes violações de segurança denunciadas pela mídia popular, as organizações lutam para remediar esse tipo de situação com práticas pouco eficazes, tais como redirecionar o tráfego leste-oeste para appliances de firewall através de “hairpin” criando pontos de gargalo. Como a microssegmentação pressupõe um modelo de segurança “zero-trust” que bloqueia todos os canais de comunicação por padrão e exige a permissão explícita do tráfego lateral, essas preocupações básicas de segurança são eliminadas.



Consulte o Capítulo 1 para obter uma discussão completa sobre redirecionamento e o Capítulo 2 para saber mais sobre o modelo “zero-trust”.

Uma plataforma de virtualização de redes permite que as organizações de TI eliminem práticas como “hairpin” ao implementar políticas extremamente granulares para cargas de trabalho individuais no data center usando microssegmentação.

DMZ em qualquer lugar

A economia global cada vez mais rápida faz com que as empresas disponibilizem acesso ao data center para seus usuários a qualquer hora, em qualquer lugar e a partir de qualquer dispositivo. Para capacitar de maneira segura o negócio de cada empresa e disponibilizar acesso em qualquer lugar, a área de TI precisa dispor de uma DMZ flexível, podendo estar presente em qualquer lugar.

A microssegmentação permite que os controles de segurança sejam atribuídos às cargas de trabalho individuais das VMs em vez de atribuídos à infraestrutura da rede física. Esse recurso permite aplicar os serviços avançados de segurança e restringir ou permitir o acesso à Internet de qualquer sistema dentro do data center, independentemente da sua localização na rede física. Dessa forma, o perímetro da rede e a área de DMZ não são mais definidos por appliances de firewall físicos entre a Internet e o data center; em vez disso, eles são definidos de acordo com as características individuais das cargas de trabalho no interior do data center.

Ambientes seguros de usuários

Muitas empresas implantaram ambientes de VDI para aproveitar os benefícios da virtualização além do data center (consulte a Figura 5-2). A microssegmentação permite que as organizações compartilhem as vantagens de segurança do SDDC com o ambiente de desktop — e até mesmo para ambientes móveis — incluindo os seguintes:

- ✓ Integração dos principais recursos de rede e segurança com o gerenciamento do ambiente VDI
- ✓ Eliminação de políticas de segurança e topologias complexas necessárias para atender diferentes usuários de VDI
- ✓ Aplicação das regras de firewall, filtragem de tráfego e políticas de segurança de forma eficaz através de grupos lógicos
- ✓ Separação políticas de segurança da dependencia da topologia de rede física para simplificar a administração

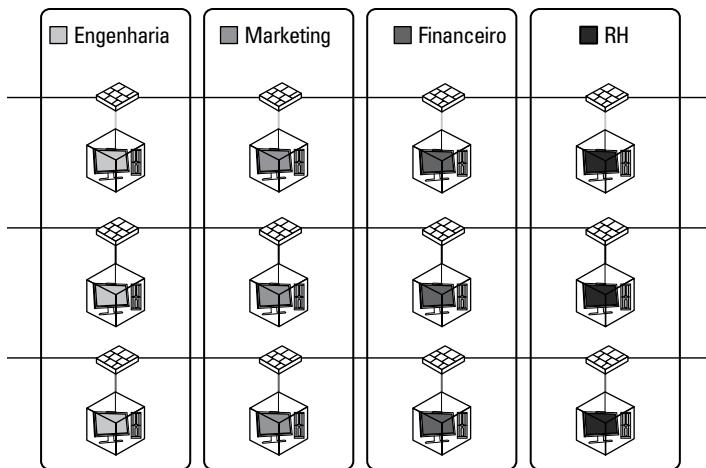


Figura 5-2: Microssegmentação em um ambiente VDI.

Esses casos de uso de segurança e microssegmentação são apenas alguns exemplos que demonstram as muitas vantagens da virtualização de redes. Outros casos de uso incluem a automação de processos de TI com o objetivo de acompanhar os requisitos de negócios, garantindo assim a flexibilidade e a segurança de infraestruturas “multi-tenant”, facilitando a criação de ambientes de “disaster recovery”, promovendo a continuidade dos serviços e mais.

No Capítulo 6, você saberá mais sobre os benefícios que segurança através da microssegmentação podem promover no data center.

60 Microsegmentação Para Leigos, Edição especial VMware _____

Capítulo 6

Dez (ou mais) benefícios da microssegmentação

A microssegmentação transforma drasticamente a segurança de rede no interior do data center. Neste capítulo, você saberá tudo sobre os detalhes de sua operação e os principais benefícios da microssegmentação.

Minimize o risco e o impacto das violações de segurança do data center

Se uma ameaça se infiltra no data center, a microssegmentação limita e bloqueia sua movimentação lateral para outros servidores, o que reduz consideravelmente a superfície de ataque e o risco para o negócio. A microssegmentação isola cada carga de trabalho com a sua própria política de segurança, impedindo que os invasores explorem outros sistemas e roubem dados valiosos.

Ao reduzir a superfície de ataque, a microssegmentação ajuda as organizações a evitar ou minimizar o prejuízo financeiro e o impacto operacional quando uma violação de dados ocorre, incluindo:

- ✓ Custos jurídicos diretos, tais como danos reais e punitivos, multas e honorários advocatícios com base no tamanho e na dimensão da violação de dados
- ✓ Perda de clientes e diminuição do volume de negócios
- ✓ Despesas operacionais de análise forense e de caráter investigativo
- ✓ Diminuição de produtividade

- ✓ Despesas diversas, tais como relatórios de análise e risco de crédito, validação de identidade e serviços de atendimento ao cliente



Como observado no Capítulo 1, o custo médio de uma violação de dados para empresas nos EUA foi estimado em aproximadamente US\$ 6 milhões. Além disso, é importante observar que várias violações de destaque nos últimos anos superaram e muito o valor de US\$ 100 milhões.

Automatize o fornecimento de serviços da TI e acelere a entrega de seus produtos no mercado

Assim como a virtualização de servidores transformou o modelo operacional da camada de processamento, a camada de conectividade foi transformada pela virtualização de redes, essa tecnologia permitiu microssegmentar a infraestrutura, a que por sua vez, transformou a segurança no data center. As empresas estão usando a microssegmentação para provisionar os serviços de segurança com a mesma agilidade, velocidade e controle que as máquinas virtuais (VMs) são provisionadas na camada de processamento.

Com a microssegmentação, as empresas podem provisionar serviços de segurança para aplicações tradicionais ou já nativas da nuvem em questão de segundos. As equipes de aplicação podem ter acesso integral ao portal de autoatendimento para provisionar novos recursos, sem terem que esperar dias ou semanas para que o hardware seja adquirido, a rede instalada e a segurança configurada. Além disso, os recursos de automação e orquestração eliminam o risco de erros de configuração manual que podem resultar em problemas de desempenho ou, pior ainda, brechas de segurança.



Consulte os Capítulos 2 e 3 para ver uma discussão completa sobre como a virtualização de servidores cria novos desafios de negócios para as equipes de rede e segurança, e como a virtualização de redes e a microssegmentação tratam desses desafios.

Por último, a microssegmentação reduz significativamente o tempo que se leva para entregar de forma segura novos serviços e aplicações geradoras de receita para o mercado. Esse novo patamar de velocidade e agilidade impulsiona a rápida inovação e a vantagem competitiva.

Simplifique os fluxos de tráfego de rede

O volume de tráfego de um servidor a outro (leste-oeste) gerado por aplicações modernas no interior do data center continua a crescer exponencialmente, o que resulta em maior consumo de banda de rede, aumento da latência, maior complexidade e uma relação elevada de over-subscription na comunicação com o core da rede.

A virtualização de redes e a microssegmentação permitem a comunicação leste-oeste direta entre os servidores virtuais por meio de switches virtuais ou uma malha de agregação que:

- ✓ Reduz significativamente os saltos de tráfego leste-oeste para o melhor desempenho das aplicações (comunicação praticamente “wire-speed” entre VMs em um mesmo host físico)
- ✓ Elimina o ineficiente redirecionamento de tráfego “hairpin” (que força o tráfego leste-oeste através de firewalls físicos), que por sua vez cria pontos de concentração e obstrução, servidores gerando tráfego retorno excessivo, além de aumentar a complexidade e contribuir para a proliferação de regras de firewall
- ✓ Permite a mobilidade de cargas de trabalho, permitindo que políticas de segurança customizadas sejam atribuídas a cada uma delas em qualquer lugar no data center, em vez de atribuir essa responsabilidade à topologia de rede física



Consulte o Capítulo 1 para saber sobre tráfego leste-oeste, “hairpinning”, e mobilidade de cargas de trabalho no data center.

Ative funções avançadas de segurança através do Desvio de Tráfego e da Inserção e Encadeamento de Serviços

Os ambientes que exigem avançados recursos de segurança de rede a nível da aplicação podem aproveitar a microssegmentação para distribuir, habilitar e aplicar serviços avançados de segurança em um contexto de rede virtualizada. A virtualização de redes distribui serviços de conectividade e segurança diretamente para as interfaces de rede virtuais (vNIC) individuais das VMs. Essa característica cria e entrega uma pilha lógica de serviços, que protege de forma detalhada as aplicações contra ameaças.

Essa pilha lógica permite que serviços sejam inseridos, encadeados ou que o tráfego seja desviado para que seja tratado de forma mais específica de acordo com a política atribuída ao tráfego ou de acordo com o resultado de um dos serviços da pilha. Essa capacidade torna possível coordenar e correlacionar de forma eficaz serviços de segurança de rede de vários fornecedores que anteriormente não tinham qualquer relação.

Aproveite a infraestrutura já existente

A microssegmentação não é uma proposta de tudo ou nada. Como não é necessário realizar alterações de configuração na infraestrutura rede física para implementar a virtualização de redes (além de permitir pacotes encapsulados de virtualização de redes através de firewalls existentes), elas podem coexistir de forma transparente, com mais ou menos microssegmentação das cargas de trabalho das aplicações existentes conforme necessário.

Os departamentos de TI têm a flexibilidade de virtualizar e segmentar partes da rede simplesmente adicionando nós de hypervisor à plataforma de virtualização. Além disso, existem gateways disponíveis em modelo de software ou em modelos de hardwares através de switches Topo de Rack que permitem interconectar diretamente redes virtuais e físicas. Os gateways podem ser usados, por exemplo, para permitir que as cargas de trabalho conectadas a redes virtuais accessem a Internet ou para a comunicação direta com VLANs ou cargas de trabalho existentes no ambiente físico.

As empresas estão usando a microssegmentação e a virtualização de redes para interligar e simplificar data centers de forma não disruptiva. A microssegmentação é compatível com arquiteturas tradicionais do tipo “Core - Agregação - Acesso” e também com as novas tecnologias de Fabric com arquitetura “Spine-Leaf”. O resultado é uma plataforma comum com o mesmo modelo lógico de gerenciamento, segurança e conectividade. As empresas também estão usando a microssegmentação e a virtualização de redes para a otimização e consolidação de diversos cenários. Por exemplo, integrando e protegendo sistemas de informação após fusões e aquisições, maximizando o compartilhamento de hardware entre clientes em nuvens “Multi-Tenant” e acessando ilhas de capacidade de processamento não utilizados.

Tudo isso significa que as organizações podem implantar a microssegmentação no data center no ritmo que se ajuste às

necessidades dos seus negócios, como em uma prova de conceito de um projeto piloto, em uma aplicação Multicamada de alto valor ou na criação de um novo Data Center Definido por Software (SDDC) completo.



O Capítulo 5 explica como começar com a microssegmentação no data center.

Com a microssegmentação, as organizações podem aproveitar seus equipamentos de rede e segurança físicos já existentes e, em muitos casos, prolongar significativamente a vida útil da infraestrutura adquirida. Por exemplo, você conseguirá evitar a despesa com a expansão da capacidade dos equipamentos físicos, eliminando o tráfego excessivo que atravessam os firewalls devido aos complexos padrões de tráfego dos data center atuais, tais como o redirecionamento “hairpinning” e o tráfego de retorno existente na comunicação leste-oeste entre os servidores. A Figura 6-1 fornece um exemplo da economia típica que uma empresa pode esperar estendendo a vida útil da infraestrutura de rede e segurança já existente.

Ciclo de atualização tradicional									Custo total acima de 8 anos
Ano 1	Ano 2	Ano 3	Ano 4 - Atualizar	Ano 5	Ano 6	Ano 7	Ano 8 - Atualizar		
Switches de rede									
Novos	10	1,50	1,73	11,98	2,28	2,62	3,02	14,97	48
Custo	US\$ 180.000	US\$ 27.000	US\$ 31.050	US\$ 215.708	US\$ 41.064	US\$ 47.223	US\$ 54.307	US\$ 269.453	US\$ 885.804
Balanceadores de carga									
Novos	15	2,25	2,59	17,98	3,42	3,94	4,53	22,45	72
Custo	US\$ 450.000	US\$ 67.500	US\$ 77.625	US\$ 539.269	US\$ 102.659	US\$ 118.058	US\$ 135.767	US\$ 673.632	US\$ 2.164.509
Firewalls									
Novos	30	4,50	5,18	35,95	6,84	7,87	9,05	44,91	144
Custo	US\$ 4.050.000	US\$ 607.500	US\$ 698.625	US\$ 1.953.419	US\$ 923.932	US\$ 1.062.521	US\$ 1.221.899	US\$ 6.022.694	US\$ 19.480.581
Total	US\$ 4.680.000	US\$ 702.000	US\$ 807.300	US\$ 5.608.395	US\$ 1.067.654	US\$ 1.227.802	US\$ 1.411.973	US\$ 7.005.869	US\$ 22.510.893
Ciclo de vida estendido com NSX									Custo total acima de 8 anos
Ano 1	Ano 2	Ano 3	Ano 4	Ano 5	Ano 6	Ano 7	Ano 8		
Switches de rede									
Novos	10	1,50	1,73	1,98	2,28	2,62	3,02	3,47	27
Custo	US\$ 180.000	US\$ 27.000	US\$ 31.050	US\$ 35.708	US\$ 41.064	US\$ 47.223	US\$ 54.307	US\$ 62.453	US\$ 478.804
Balanceadores de carga									
Novos	15	2,25	2,59	2,98	3,42	3,94	4,53	5,20	40
Custo	US\$ 450.000	US\$ 67.500	US\$ 77.625	US\$ 89.269	US\$ 102.659	US\$ 118.058	US\$ 135.767	US\$ 156.132	US\$ 1.197.009
Firewalls									
Novos	30	4,50	5,18	5,95	6,84	7,87	9,05	10,41	80
Custo	US\$ 4.050.000	US\$ 607.500	US\$ 698.625	US\$ 803.419	US\$ 923.932	US\$ 1.062.521	US\$ 1.221.899	US\$ 1.405.184	US\$ 10.773.081
Total	US\$ 4.680.000	US\$ 702.000	US\$ 807.300	US\$ 928.395	US\$ 1.067.654	US\$ 1.227.802	US\$ 1.411.973	US\$ 1.623.769	US\$ 12.448.893
Economia de CapEx com NSX									
Pré-requisitos									
Taxa de crescimento anual:	10%	Switch de rede:		US\$ 18.000					
Taxa de falha anual:	5%	Balancedor de carga:		US\$ 30.000					
		Firewalls:		US\$ 135.000					

Reduza as despesas de capital (CapEx)

A implantação de firewalls físicos adicionais para controlar os volumes crescentes de tráfego leste-oeste no interior do data center tem um custo proibitivo para a maioria das empresas. Além disso, o grande número de dispositivos necessários e o esforço exigido para configurar e gerenciar uma complexa matriz de regras de firewall tornam essa abordagem operacionalmente impraticável. A microsegmentação permite o controle completo de cargas de trabalho individuais no data center sem comprar firewalls físicos adicionais para cada carga de trabalho, resultando em economia significativa para os data centers corporativos. A Figura 6-2 ilustra esse caso de uso para um típico data center corporativo.

Ambiente e capacidade	
Número de VMs	2.500
VMs por CPU	5
CPUs por servidor	2
Servidores	250
% de VMs que exigem regras de FW	40%
Gbps - Throughput médio de aplicação por host	7
Gbps - Throughput de firewall necessário em Gbps para todas as VMs	1.750
Gbps - Throughput de firewall necessário eficiente	700
Firewalls (20 Gbps cada x2 para alta disponibilidade)	70
Custo de hardware	
Preço de lista de cada Firewall físico de 20 Gbps	US\$ 135.000
Custo total de Firewall Físicos (mas operacionalmente impraticável)	US\$ 9.450.000
Custo do NSX	
Lista de custo por CPU com NSX	US\$ 5.995
Custo total do NSX	US\$ 2.997.500
Economia de CapEx com NSX	
	US\$ 6.452.500
	68%

Figura 6-2: A microsegmentação elimina a necessidade de firewalls físicos adicionais.

Reduza as despesas operacionais (OpEx)

A microsegmentação reduz drasticamente o esforço manual e o ciclo de tempo das tarefas de segurança, incluindo provisão, alteração/adaptação, dimensionamento e solução de problemas/correção.

Geralmente, a microssegmentação reduz o esforço de horas para minutos e os ciclos de tempo de dias para minutos. Se considerar todas as tarefas manuais necessárias para provisionar e gerenciar a segurança de uma rede física, por meio de ambientes de desenvolvimento, teste, validação e produção, e o fato de que a microssegmentação automatiza essas tarefas, você começará a ver todas as oportunidades para reduzir as despesas operacionais.

Conforme a análise na Figura 6-3 mostra, a microssegmentação agiliza drasticamente o provisionamento inicial dos serviços de segurança. Com hardware tradicional, o ciclo de tempo associado ao aprovisionamento de serviços de segurança para uma nova aplicação força as empresas a esperar cerca de 23 dias.

A virtualização de redes reduz isso para minutos, quase uma redução de 100% e um ganho gigantesco no tempo de colocação de produtos e serviços no mercado. Da mesma forma, aprovisionamento de serviços de segurança para uma nova aplicação leva em torno de 14 horas ou cerca de dois dias de trabalho de uma pessoa. A microssegmentação reduz isso para menos de duas horas - uma redução significativa de 87%.

	Esforço com tarefas (horas)		Ciclo de Tempo (dias)	
	Manual	Automatizado - NSX	Manual	Automatizado - NSX
Solicitar e analisar rede e recursos de segurança	1,00	0,00	1	0
Definir ambiente de rede e segurança	4,50	1,00	3	0
Determinar as alterações necessárias (disponibilidade de capacidade)	4,50	0,00	3	0
Revisar e aprovar processo (alterar conselho de aprovação)	0,50	0,50	5	0
Alterar programação de pedido	0,50	0,00	5	0
Configurar a rede (VLAN, roteamento)	1,00	0,00	2	0
Configurar a segurança (Firewall)	1,00	0,00	2	0
Configurar o平衡ador de carga	1,00	0,00	2	0
Provisionar o ambiente	0,30	0,30	0	0
Total	14,30	1,80	23	0
Economia de OpEx com NSX	12,50 horas		23 dias	
	87%		100%	

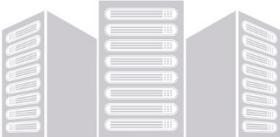
Figura 6-3: Reduções de despesas operacionais com automação de TI.

Ative de modo seguro a agilidade comercial

Os benefícios da microssegmentação através da virtualização de redes são imensos. As empresas têm sido forçadas historicamente a escolher entre velocidade e segurança, uma vez que as equipes de segurança são injustamente reconhecidas muitas vezes por

inibir a agilidade comercial em vez de habilitá-la com segurança. Esse conflito torna tensa a relação entre as equipes de segurança e as unidades de negócios, muitas vezes levando a jogos prejudiciais de cão e gato entre os usuários, que tentam driblar os controles para que possam desempenhar suas funções de trabalho, e os administradores de segurança que tentam proteger esses usuários de si mesmos aplicando políticas de segurança um tanto pesadas e criticadas, ou pior, respondendo a incidentes de segurança resultantes.

A virtualização de redes torna a microssegmentação no data center definido por software uma realidade e permite que as empresas inovem rapidamente para obter vantagem competitiva, mantendo a *segurança* onipresente e persistente no data center. As empresas em todos os lugares estão aproveitando os diversos benefícios de segurança e desempenho da microssegmentação no data center e vão continuar descobrindo novos usos e novas aplicações para essa tecnologia inovadora.



vmware®

VIRTUALIZAÇÃO E SEGURANÇA DE REDES

O data center definido por software é essencial para a TI moderna como um ponto de enfoque para a inovação.

A virtualização de redes é um componente fundamental do SDDC, já que oferece controles de segurança nativos para a infraestrutura, o que proporciona mais agilidade, proteção de seus ativos e melhor segurança.

Proteção de firewall distribuída e virtualizada,
integrada à arquitetura

Infraestrutura independente de hardware

Recursos potentes



Micros-
segmentação



Ambientes seguros
para usuários



Recuperação
de desastres



TI automatiza
a TI



Nuvem de
desenvolvedores



Pool de
recursos

COMEÇAR AGORA

Obtenha mais informações sobre como virtualizar a rede de seu data center em www.vmware.com/products/nsx

One CLOUD. Any APPLICATION. Any DEVICE.™

A microssegmentação é a nova base de segurança para bloquear ameaças dentro do data center

A microssegmentação transforma consideravelmente a segurança da rede dentro do perímetro do data center ao conter e bloquear a propagação lateral de ameaças a outros servidores. Este livro explica como implementar a microssegmentação com a sua infraestrutura de data center atual para reduzir consideravelmente a superfície de ataques ao data center e os riscos para os seus negócios.

- *Descubra o que há de errado com a base de segurança do data center e como corrigir o problema com microssegmentação*
- *Torne a confiança zero no data center uma realidade com confiança no nível da unidade e políticas de segurança definidas no nível da carga de trabalho individual*
- *Automatize os fluxos de trabalho de segurança e combine diferentes tecnologias ao vincular serviços avançados de segurança para melhorar a resposta e o desempenho de segurança*
- *Entenda os benefícios de segurança da microssegmentação e como ela transforma a segurança do data center com casos de uso inovadores*

Lawrence Miller trabalhou em segurança da informação em vários setores por mais de 25 anos. **Joshua Soto** é gerente de marketing de produto da plataforma VMware NSX.



Abra o livro e descubra:

- **Por que a microssegmentação no data center não era viável até agora**
- **Como os invasores se movem lateralmente no data center e como aproveitam a explosão de tráfego de data center leste-oeste para ampliar os ataques**
- **Como aproveitar a microssegmentação com a sua infraestrutura atual e melhorar a segurança e o desempenho do data center**

Acesse [Dummies.com](#) para saber mais!

WILEY



Também disponível
como e-book

ISBN: 978-1-119-28482-6
Não destinado à revenda

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley's ebook EULA.