LEARNING MADE EASY

2ª Edição Especial da VMware

Virtualização de redes

para leigos

Por que você precisa virtualizar sua rede

Como funciona e como iniciar

Trazido para você por

vmware

Jonathan Morin

Shinie Shaw

Sobre a VMware

Os softwares da VMware alimentam a complexa infraestrutura digital do mundo. As ofertas de computação, nuvem, mobilidade, rede e segurança da empresa fornecem uma base digital dinâmica e uniforme para fornecer os aplicativos que alimentam a inovação nos negócios. A VMware está agilizando a jornada para negócios digitais para mais de 500 mil clientes globalmente, auxiliada por um ecossistema de 75 mil parceiros, liberando o valor das tecnologias atuais e permitindo a integração futura. Com a VMware, as organizações têm o poder de flexibilizar e aproveitar novas tecnologias rapidamente, sem interromper as operações nem introduzir riscos. Este ano, a VMware comemora 20 anos de inovações revolucionárias que beneficiam as empresas e a sociedade.

Para obter mais informações, visite **www.vmware.com**.

Virtualização de redes

2ª Edição Especial da VMware

Jonathan Morin e Shinie Shaw

para leigos®

Virtualização de redes para Leigos®, Segunda Edição Especial da VMware

Publicado por
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-59683-7 (pbk); ISBN 978-1-119-59684-4 (ebk)

Fabricado nos Estados Unidos da América

10 9 8 7 6 5 4 3 2 1

Para obter informações gerais sobre nossos outros produtos e serviços, ou sobre como criar um livro personalizado *For Dummies* para sua empresa ou organização, entre em contato com nosso Departamento de Desenvolvimento de Negócios nos EUA pelo telefone 877-409-4177, pelo e-mail info@dummies.biz ou visite www.wiley.com/go/custompub. Para obter informações sobre licenciamento da marca *For Dummies* para produtos ou serviços, entre em contato com BrandedRights&Licenses@Wiley.com.

Reconhecimentos da editora

Algumas das pessoas que ajudaram a colocar este livro no mercado:

Responsável por desenvolvimento: Becky Whitney

Editor do projeto: Elizabeth Kuball

Responsável por aquisições: Katie Mohr

Gerente editorial: Rev Mengle

Representante de desenvolvimento de negócios: Karen Hattan

Responsável pela produção: Magesh Elangovan

Índice

Introdução

Bem-vindo à *Virtualização de Redes para Leigos*, seu guia para uma abordagem nova e melhorada à rede.

Antes de irmos ao âmago da questão da virtualização de redes, vamos descrever brevemente alguns tópicos que abordaremos nessas páginas. Todos os requisitos a seguir vêm de uma necessidade de sair do passado da rede com fio para o mundo flexível da virtualização de redes, o qual descreveremos em detalhes no Capítulo 1:

- A rede precisa ser tão rápida quanto a empresa.
- A segurança da rede precisa ser mais rápida do que os criminosos cibernéticos.
- Os aplicativos precisam da flexibilidade para serem executados em qualquer lugar.

Então, como se chega lá? O primeiro passo é mergulhar nos conceitos dessa nova abordagem à rede. Esse é o assunto deste livro.

Sobre este livro

Não deixe o tamanho deste livro enganar você. Ele está repleto de informações que poderão ajudá-lo a entender e a lucrar com a virtualização de redes. Em uma linguagem simples e clara, explicaremos o que é a virtualização de redes, por que é um assunto tão importante, como você pode começar e as etapas que pode adotar para obter o melhor retorno sobre o seu investimento em TI.

Suposições tolas

Ao escrever este livro, fizemos algumas suposições sobre você. Supomos que você

- trabalha com TI, nuvem, projetos de aplicativos ou em uma função relacionada que envolve algum nível de rede.
- está familiarizado com a terminologia de rede.
- entende o conceito de virtualização.

Ícones usados neste livro

Para facilitar ainda mais a navegação até as informações mais úteis, esses ícones destacam o texto principal:

LEMBRE-SE

Esteja atento a esses pontos principais.

COISAS TÉCNICAS

Leia estas passagens opcionais se quiser uma explicação mais técnica.

DICA

Siga o alvo para obter dicas que podem poupar tempo.

Para onde ir agora

O livro foi escrito como um guia de referência, para que você possa lê-lo de capa a capa ou ir direto para os tópicos que mais lhe interessam. Seja qual for o caminho escolhido, não tem como errar. Ambos os caminhos levam ao mesmo resultado: um melhor entendimento da virtualização de redes e como ela pode ajudá-lo a melhorar a segurança, a agilidade e a flexibilidade em ambientes multi-cloud.

NESTE CAPÍTULO

- **Desafios das redes atuais**
- **Construção da base para uma virtualização de redes**
- **Introdução da rede virtual em nuvem**

Capítulo 1
A próxima evolução de redes: A ascensão da rede virtual em nuvem

Por que você deveria se preocupar com a virtualização de redes? Essa pergunta tem mais que uma única resposta. Este capítulo examina vários desafios atuais que apontam para uma única necessidade global: A rede e a segurança devem ser proporcionadas em software. Eis o porquê:

- Para se manterem competitivas, as empresas precisam da agilidade da nuvem.
- As arquiteturas de rede preexistentes limitam a agilidade das empresas, são mais vulneráveis a ameaças de segurança e aumentam os custos.
- Hardware dedicado para cada função de rede proíbe uma abordagem diferente.

A virtualização de redes está reescrevendo as regras sobre como os serviços devem ser fornecidos, desde o data center definido por software (SDDC) até a nuvem. Essa abordagem transforma as redes estáticas, inflexíveis e ineficientes em dinâmicas, ágeis e otimizadas.

Nesse novo mundo, a virtualização permite que a inteligência da infraestrutura passe de hardware para software. Com o SDDC, os elementos da infraestrutura do data center, incluindo computação, rede e armazenamento, são virtualizados e agrupados em pools de recursos. Esses recursos podem ser implantados automaticamente, com pouco ou nenhum envolvimento humano. Tudo é flexível, automatizado e controlado por software. A rede virtual na nuvem estende esses conceitos além do data center, para onde os aplicativos e os dados residem.

Com a virtualização de redes viabilizando o SDDC, não será necessário passar dias ou semanas aprovisionando a infraestrutura para dar suporte a um novo aplicativo. Agora é possível implantar ou atualizar aplicativos em minutos. Este livro coloca uma ênfase especial em como a virtualização de redes viabiliza o SDDC, além de abordar a base da rede virtual em nuvem, um modelo de rede que amplia a virtualização de redes entre nuvens, aplicativos e endpoints.

De acordo com o relatório "2018 State of the Cloud" da RightScale, 81% das empresas deverão ter uma estratégia multi-cloud, e as organizações usarão cinco nuvens em média. Para realizar essa estratégia, uma abordagem definida por software é essencial. É uma estrutura muito necessária para uma maior agilidade e fornecimento mais rápido de serviços de operações e desenvolvimento de TI, tudo isso por um custo menor. É essencial para entender o futuro do ambiente multi-cloud.

A empresa precisa de velocidade

Este capítulo começa com todas as boas notícias sobre a virtualização de redes. Eis o problema: As arquiteturas de rede com base no hardware não conseguem corresponder à velocidade e à agilidade do SDDC.

Organizações de todos os portes estão tendo um rápido aumento no ritmo de mudanças. Tudo precisa ser feito ontem; novas inovações e fornecimento de recursos, respostas competitivas, projetos críticos para a organização. Essa nova realidade tem grandes implicações para a rede.

Quando uma empresa quer impressionar seus clientes com um novo aplicativo, lançar uma promoção ou adotar uma nova rota para o mercado, ela precisa dos serviços de TI imediatamente, e não semanas ou mesmo dias depois. No mundo atual, ou você entra na onda ou perde completamente. Estamos na era da incrível janela de oportunidade.

Quando a empresa recorre à organização de TI para serviços essenciais, ela quer ouvir: "Dá para fazer. Tudo estará em funcionamento imediatamente." E cada vez mais, a empresa não quer nem precisar perguntar à TI.

Os requisitos de segurança estão aumentando

Há muito tempo, Bob Dylan aconselhou o mundo: "Não é necessário um meteorologista para saber de que lado o vento sopra". Hoje em dia, pode-se dizer praticamente a mesma coisa sobre a segurança de rede. Nas empresas atuais, um vento forte está soprando e servindo como um alerta de segurança.

Todos sabem que precisamos fazer mais para evitar violações dispendiosas que colocam informações confidenciais nas mãos dos criminosos cibernéticos. Nenhuma empresa está imune à ameaça. Pense em algumas das violações de segurança dos últimos anos, violações que derrubaram empresas enormes. Grandes marcas, desde empresas no setor de saúde e bancos de investimento até lojas e entretenimento, foram prejudicadas ao decepcionarem seus clientes. Todas as empresas estão agora envolvidas na mesma batalha dispendiosa para defender dados críticos.

É como um grande jogo de guerra. Uma empresa fortalece seu data center com um firewall novo e resistente, e os criminosos cibernéticos acabam entrando por uma porta dos fundos desconhecida (como uma simples vulnerabilidade em um sistema de cliente) e acessam livremente o data center. A estratégia tradicional de defender o perímetro precisa ser atualizada para incluir muito mais proteção dentro do data center.

Considere essas visões baseadas em pesquisas:

» De acordo com o relatório do CSIS de 2018, "Economic Impact of Cybercrime — No Slowing Down" (O impacto econômico do crime cibernético – sem indícios de desaceleração), as perdas

devido a problemas com a segurança aumentam ano após ano, apesar de cada vez mais gastos com a segurança.

- Em um comunicado à imprensa do Gartner de agosto de 2017, Sid Deshpande, o principal analista de pesquisa do Gartner, disse "... melhorar a segurança não é gastar com tecnologias novas. Como visto na recente onda de incidentes globais, fazer as coisas básicas corretamente nunca foi tão importante. As organizações podem melhorar significativamente sua postura de segurança apenas abordando a segurança básica e os elementos de higiene relacionados ao risco, como... a segmentação de rede interna.... "

Observações como essas destacam a necessidade de transformar a rede por meio da virtualização com segurança integrada.

Aplicativos e dados em várias nuvens

Não há mais uma única resposta simples sobre onde os aplicativos estão sendo executados e onde seus dados residem. Para muitas organizações, alguns aplicativos começam na nuvem, onde alguns desenvolvedores começam a codificar e testar. Muitos também acham que certos aplicativos são mais bem executados no data center privado, tanto pela eficiência de custos quanto pelo controle privado. Muitas outras organizações ainda movem aplicativos em qualquer direção, do data center privado para a nuvem pública para delegar gerenciamento, e da nuvem pública para o data center privado para controlar os custos da nuvem pública ou para aproveitar as vantagens de novos modelos de consumo da nuvem privada. Atualmente, as organizações sabem que precisam apoiar-se em vários ambientes.

A ascensão da virtualização de servidores tornou muitas grandes coisas possíveis em torno da mobilidade de aplicativos, mas tem havido um problema: a rede. Há algo que está impedindo de seguirmos à frente. A configuração de rede está vinculada ao hardware, portanto, mesmo que os aplicativos possam se mover com relativa facilidade, as conexões de rede com fio impedem isso.

Os serviços de rede tendem a ser muito diferentes de um data center ou de uma nuvem para outra. Isso significa que é preciso muita personalização para que os aplicativos funcionem em diferentes ambientes de rede. Essa é uma grande barreira à mobilidade de aplicativos, e mais um argumento para usar a virtualização para transformar a rede.

Arquiteturas de rede enraizadas em hardware não conseguem acompanhar o SDDC

O SDDC é a arquitetura mais ágil e adequada para o data center moderno. Isso é atingido movendo inteligência para o software em *todos os* elementos da infraestrutura. Então, vamos fazer um balanço de onde as coisas estão atualmente:

- A maioria dos data centers agora aproveita a virtualização de servidores para obter a melhor eficiência de computação. *Correto!*
- Muitos data centers otimizam seus ambientes de armazenamento por meio da virtualização. *Correto!*
- Muitas organizações virtualizaram seus ambientes de rede dentro do data center e em nuvens. *Muito progresso foi feito! Mas o potencial para fazer mais continua enorme*.

Embora as empresas estejam lucrando com a virtualização de servidores e de armazenamento, elas ainda são desafiadas pela infraestrutura de rede preexistente, a qual gira em torno de abordagens aprovisionadas manualmente e centradas em hardware que existem desde a primeira geração de data centers.

Nas seções a seguir, mostraremos alguns dos desafios específicos das arquiteturas preexistentes.

O aprovisionamento de rede física é lento por natureza

Embora alguns processos de aprovisionamento de rede possam ser roteirizados (e certos modelos de rede definida por software (SDN) prometam tornar isso realidade) com sistemas baseados em hardware, não há nenhuma conexão automática para virtualização de computação ou de armazenamento. Como resultado, não é possível aprovisionar automaticamente a rede quando a computação e o armazenamento associados são criados, movidos, capturados instantaneamente, excluídos ou clonados. Portanto, o aprovisionamento de rede continua lento, apesar do uso de ferramentas automatizadas.

Ao mesmo tempo, o que mais importa para os negócios, ou seja, que novos aplicativos estejam prontos para o uso, está sujeito a atrasos frequentes causados por processos manuais lentos e suscetíveis a erros usados para aprovisionar serviços de rede.

Isso é muito irônico quando você para e analisa o panorama geral: As limitações das redes preexistentes vinculam o mundo virtual dinâmico atual ao hardware inflexível e dedicado. A infraestrutura de servidores e de armazenamento que deve ser rapidamente reaproveitada precisa aguardar que a rede a alcance. O aprovisionamento então se torna um jogo de pressa e espera.

O posicionamento da carga de trabalho e a mobilidade são limitados

Nos ambientes empresariais atuais em constante evolução, os aplicativos precisam ter pernas. Eles precisam se locomover livremente de um lugar para outro. Isso pode significar uma replicação para um data center de backup e recuperação externo, uma movimentação de uma parte do data center corporativo para outra ou uma migração para dentro e para fora de um ambiente de nuvem.

A virtualização de servidores e de armazenamento possibilita esse tipo de mobilidade. Mas você tem que estar ciente de um outro problema: a rede. Quando se trata de mobilidade de aplicativos, os atuais silos de rede com fio tiram os tênis de corrida dos aplicativos. As cargas de trabalho, mesmo aquelas em máquinas virtuais, estão ligadas a hardware e topologias de rede física. Para complicar ainda mais, data centers diferentes têm abordagens diferentes para serviços de rede, por isso, pode ser necessário muito trabalho pesado para configurar um aplicativo em execução no data center A para um desempenho ideal no data center B.

Tudo isso limita o posicionamento da carga de trabalho e a mobilidade do aplicativo e torna a mudança não apenas difícil, mas arriscada. É sempre mais fácil, e mais seguro, simplesmente deixar as coisas do jeito que elas estão.

COISAS TÉCNICAS

A atual abordagem de rede centrada em hardware restringe a mobilidade da carga de trabalho a sub-redes físicas e zonas de disponibilidade individuais. Para alcançar os recursos de computação disponíveis no data center, os operadores de rede podem ser forçados a executar configurações individuais de switching, roteamento, regras de firewall, serviços de balanceamento de carga e assim por diante. Esse processo não é apenas lento e complexo, mas também acabará atingindo um limite de dimensionamento, seja nas limitações de memória endereçável de conteúdo ternário (TCAM) de quantos endereços MAC e IP os sistemas podem reter, seja nas limitações arquiteturais de construções como redes de área local virtual (VLAN), que ainda são usadas com

muita frequência como um mecanismo de segmentação, apesar das soluções alternativas e da limitação de escala de 4.096.

Limitações de hardware e dependências tecnológicas criam complexidade e rigidez

A atual abordagem de caixa preta fechada para redes – com sistemas operacionais personalizados, circuitos integrados específicos para aplicativos (ASICs), interfaces de linha de comandos (CLIs) e software de gerenciamento dedicado – complica as operações e limita a agilidade. Essa abordagem antiga não leva em conta a natureza dinâmica dos aplicativos atuais e deixa você preso, e não apenas com o fornecedor. Ela o prende nas complexidades da sua arquitetura de rede atual, limitando a capacidade da equipe de TI de se adaptar e inovar, o que, por sua vez, coloca os mesmos limites na empresa, porque a empresa não pode se locomover mais rápido que a TI.

De acordo com o relatório "Look Beyond Network Vendors for Network Innovation" (Veja além dos fornecedores de rede em busca de inovação de rede) de 2018 do Gartner, ele está observando que, à medida que seus clientes estão passando por uma transformação digital, suas equipes de rede "devem fornecer infraestrutura de rede de data centers rapidamente e sob demanda". Além disso, o Gartner está vendo que a rede do data center é um dos maiores desafios para seus clientes (com base em mais de três mil consultas e pesquisas de público em 2017).

Eis algumas conclusões bastante reveladoras do mesmo relatório:

- É comum que as solicitações da rede do data center demorem dias para serem atendidas.
- O número de portas ativas por equivalentes em tempo integral (FTE) da rede de área local (LAN) ficou menos eficiente ao longo do tempo, em mais de 10%, de 3.412 portas por FTE em 2013 para apenas 2.933 portas por FTE em 2016.

Processos de configuração são manuais, lentos e propensos a erros

No dia a dia, as redes físicas forçam sua equipe de rede a executarem muitas tarefas repetitivas e manuais, muitas das quais são desencorajadas ou exigem aprovações, devido às implicações de um erro. Se uma linha de negócios ou um departamento solicitar um novo aplicativo ou serviço, será necessário criar VLANs, mapear VLANs entre switches e

uplinks, criar grupos de portas, atualizar perfis de serviço e assim por diante.

Certos modelos SDN esperam ajudar aqui, permitindo hardware controlado programaticamente, mas isso ainda deixa você com muito trabalho pesado. Por exemplo, ainda é necessário criar várias pilhas de rede física idênticas para respaldar as suas equipes de desenvolvimento, teste e produção, e você ainda não tem a capacidade de implantar sua rede (baseada em hardware) em sincronia com o armazenamento e a computação virtualizados.

Há um alto preço associado a tudo isso. Como observou Andrew Lerner, diretor de pesquisa do Gartner, "A configuração e o gerenciamento de mudanças de equipamentos de rede continuam sendo basicamente um processo manual e trabalhoso. Essas práticas de rede menos favoráveis resultam em tempo de inatividade, reduzem a segurança, degradam o desempenho dos aplicativos e desperdiçam recursos humanos e de capital."

Claramente, há um caminho melhor: a automação de rede. Como a *Network World* observou em um artigo em 2018, "A automação de rede está ajudando as empresas a ampliarem-se e a reduzirem seus custos exponencialmente, dando a elas a capacidade necessária para se concentrarem em estratégia e inovação."

OpEx e CapEx são muito altos

As limitações das arquiteturas de rede preexistentes estão aumentando os custos do data center em termos de despesas operacionais (OpEx) e despesas de capital (CapEx).

OpEx

O uso pesado de processos manuais aumenta o custo das operações de rede. Basta considerar todas as tarefas manuais trabalhosas necessárias para configurar, aprovisionar e gerenciar uma rede física. Agora multiplique o esforço dessas tarefas em todos os ambientes que você precisa suportar: desenvolvimento, teste, preparação e produção; redes departamentais diferentes; ambientes de aplicativos diferentes; sites primários e de recuperação; e assim por diante. Tarefas que podem ser concluídas em minutos com processos automatizados, ou mesmo instantaneamente com a implantação *automática* de redes, levam horas, dias ou semanas em um mundo manual.

E, há também os custos ocultos que acompanham os erros de configuração introduzidos manualmente. Um erro pode causar um problema crítico de conectividade ou uma interrupção que afete a empresa diretamente. Considere estas constatações:

- Os estudos do Ponemon Institute constatam consistentemente que o erro humano é uma das maiores causas para interrupções não planejadas (Ponemon Institute Cost of Data Center Outages 2010, 2013, 2016).
- O impacto financeiro de uma indisponibilidade de data center não planejada pode ser enorme. O Ponemon Institute constatou que o custo de uma interrupção aumentou de 690 mil em 2013 para 740 mil de dólares em 2016, e aumentou 38% desde o estudo de 2010.

CapEx

Do lado do capital, as arquiteturas de rede preexistentes exigem que sua organização invista em soluções independentes para muitas das funções de rede e de segurança que são fundamentais para as operações do data center. Isso inclui roteamento, firewall e balanceamento de carga. O fornecimento dessas funções em todos os lugares em que elas são necessárias tem um preço alto.

Há também a questão da necessidade de aprovisionar hardware excessivamente para garantir que você atenda às demandas de pico, além da necessidade de implantar configurações ativo-passivo. Na verdade, é necessário comprar hardware duplicado para fins de disponibilidade e, às vezes, muito mais.

E depois disso, há o custo de atualizações completas. Para aproveitar as mais recentes inovações na tecnologia de rede, as operadoras de rede muitas vezes precisam descartar e substituir equipamentos preexistentes, e a maioria das organizações tem um ciclo de modernização de três a cinco anos. As arquiteturas de rede preexistentes baseadas em hardware também precisam de um excesso de aprovisionamento para levar em consideração os picos de uso. A incapacidade de redes baseadas em hardware para dimensionar automaticamente com base em demandas requer essa ineficiência. E os custos de rede sobem.

As arquiteturas de rede preexistentes também podem resultar em outras ineficiências. Em geral, os designers de rede devem reservar partes de uma rede para um uso específico com o intuito de acomodar

requisitos especiais de segurança ou de conformidade. Juntamente com a necessidade de excesso de aprovisionamento, as ineficiências são ampliadas, levando a faixas de "servidores escuros" e seus recursos de rede associados, mantidas "caso sejam necessárias", sem servir para qualquer finalidade útil. O resultado parece um disco rígido gravemente fragmentado.

Não é possível alavancar os recursos da nuvem híbrida

O modelo de nuvem pública provou que aplicativos e serviços podem ser aprovisionados sob demanda. Em toda parte, as empresas gostariam de desfrutar do mesmo nível de velocidade e agilidade. Com esse pensamento em mente, os executivos com visão de futuro visam usar nuvens híbridas para todos os tipos de casos de uso, desde armazenamento de dados e recuperação de desastres até desenvolvimento e testes de software.

Porém, mais uma vez, há um problema relacionado à rede: em busca por uma mudança para a nuvem, as empresas são prejudicadas pelo hardware de rede e pela topologia física específicos do fornecedor. Essas restrições que vêm com arquiteturas preexistentes de data center podem dificultar a implementação de nuvens híbridas. As nuvens híbridas dependem de uma extensão contínua do data center no local para um recurso de nuvem pública. Como atingir isso quando não é possível controlar a rede de nuvem pública para espelhar seus sistemas de rede de hardware?

As redes têm defesas inadequadas

Muitos dos ataques cibernéticos amplamente divulgados nos últimos anos têm uma característica comum: uma vez dentro do perímetro do data center, o código malicioso se move de servidor para servidor, onde dados confidenciais são coletados e enviados para os criminosos cibernéticos. Esses casos destacam uma debilidade dos data centers atuais: eles têm controles limitados de segurança de rede para impedir que os ataques se espalhem dentro do data center.

Os firewalls do perímetro são muito bons para impedir muitos dos ataques, mas não todos. Como os ataques recentes demonstram, as ameaças ainda estão entrando no data center por meio de pontos de acesso legítimos. Uma vez lá dentro, eles se espalham como um vírus mortal. Este tem sido um problema difícil de resolver por causa das realidades das arquiteturas de rede física. Simplificando, com sistemas de rede

preexistentes, é muito dispendioso fornecer um firewall para o tráfego entre *todas as* cargas de trabalho dentro do data center. Isso dificulta impedir que um ataque seja propagado lateralmente de um servidor para outro usando o tráfego leste-oeste.

LEMBRE-SE

Até este ponto, observamos que:

- Para permanecerem competitivas, as empresas precisam se mover rapidamente, mas suas redes não têm a agilidade necessária.
- Arquiteturas de rede antiquadas estão bloqueando o caminho para o SDDC e a rede de nuvem virtual.
- As arquiteturas de rede preexistentes limitam a agilidade das empresas, são mais vulneráveis a ameaças de segurança e aumentam os custos.

Estes temas apontam para uma única necessidade global: é hora de sair do passado e entrar na era da rede virtualizada.

NESTE CAPÍTULO

- Explicação dos fundamentos da virtualização de redes
- Destaques dos benefícios desta nova abordagem
- Descrição das principais características de uma rede virtualizada

Capítulo 2
É hora de virtualizar a rede

Neste capítulo, mergulhamos no conceito de virtualização de redes, o que é, como ele difere de outras abordagens de rede e por que é a hora certa para essa nova abordagem.

Para colocar as coisas em perspectiva, vamos começar com um pouco de informação sobre a virtualização de redes, o estado das redes atuais e como chegamos a esse ponto.

Como funciona a virtualização de redes

A virtualização de redes possibilita criar programaticamente, aprovisionar e gerenciar redes em software, ao mesmo tempo que continua a alavancar a rede física subjacente como o backplane de encaminhamento de pacotes. Os serviços de rede e de segurança em software são distribuídos a uma camada virtual (hypervisors, no data center) e "anexados" a cargas de trabalho individuais, como máquinas virtuais ou contêineres, de acordo com as políticas de segurança definidas para cada aplicativo conectado. Quando uma carga de trabalho é movida para outro host, seus serviços de rede e de segurança vão com ela. E quando novas cargas de trabalho são criadas para dimensionar um aplicativo, as políticas necessárias também são aplicadas dinamicamente a elas.

Semelhante a como uma máquina virtual ou um contêiner é uma construção de software que apresenta serviços lógicos para um aplicativo, uma *rede virtual* também é uma construção de software que apresenta serviços de rede lógica, ou seja, switches, roteamento, firewall, balanceamento de carga, redes virtuais privadas (VPNs) e muito mais, para as cargas de trabalho conectadas. Esses serviços de rede e de segurança são fornecidos em software e requerem apenas o encaminhamento de pacotes do protocolo de Internet (IP) da rede física subjacente. As próprias cargas de trabalho são conectadas por meio da rede lógica e implementadas pela rede de sobreposição. Isso permite que toda a rede seja criada no software (veja a Figura 2-1).

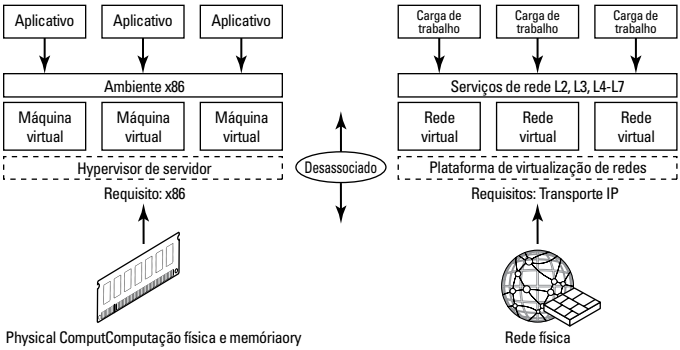


FIGURA 2-1: Computação e virtualização de redes.

A virtualização de redes coordena os switches virtuais nos vários ambientes (por exemplo, hypervisors, nuvens) junto com os serviços de rede (por exemplo, firewall, balanceamento de carga) para fornecer uma plataforma de rede e a criação de redes virtuais dinâmicas (veja a Figura 2-2).

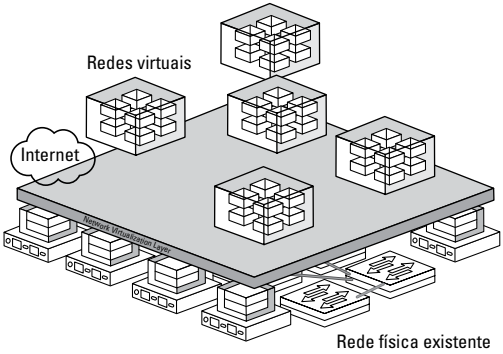


FIGURA 2-2: A plataforma de virtualização de redes.

Uma outra vantagem da virtualização de redes é que os recursos e os serviços de rede podem ser aprovisionados por meio de várias interfaces. Um conjunto de opções utiliza as interfaces nativas de usuário, a interface gráfica do usuário (GUI, graphical user interface) nativa e a interface da linha de comandos (CLI, command-line interface). Uma outra abordagem tira proveito da interface de programação de aplicativos (API, application programming interface) para criar scripts ou ferramentas domésticas. Novos modelos de aplicativos, como o Kubernetes, integram-se à virtualização de redes para que os serviços de rede sejam criados como novos aplicativos, pods e contêineres. Uma outra maneira de aprovisionar redes virtuais usa uma plataforma de gerenciamento de nuvem (CMP, cloud management platform), como o OpenStack ou o VMware vRealize Automation, para solicitar uma rede virtual e os serviços de segurança apropriados para novas cargas de trabalho. Em cada caso, o controlador distribui os serviços de rede necessários aos switches virtuais correspondentes e os conecta logicamente às cargas de trabalho correspondentes (veja a Figura 2-3).

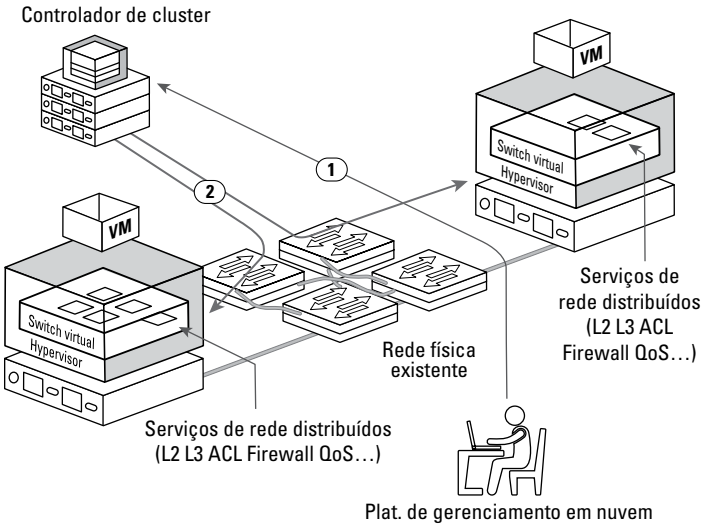


FIGURA 2-3: Aprovisionamento de rede virtual.

Essa abordagem não apenas permite que diferentes redes virtuais sejam associadas a diferentes cargas de trabalho no mesmo ambiente (por exemplo, cluster, pod, hypervisor, instância de aplicativo, nuvem privada virtual [VPC, virtual private cloud]), mas também permite a criação de tudo desde redes virtuais básicas que envolvem apenas dois nós

até construções muito avançadas que correspondem às topologias de rede complexas de múltiplos segmentos usadas para fornecer aplicativos de multicamadas.

Para cargas de trabalho conectadas, uma rede virtual se parece e opera como uma rede física tradicional (veja a Figura 2-4). As cargas de trabalho "veem" a mesma camada 2, camada 3 e camada 4 através dos serviços de rede da camada 7 que elas usariam em uma configuração física tradicional. A diferença é que esses serviços de rede são agora instâncias lógicas de módulos de software distribuídos sendo executados no software do host local e aplicados na interface virtual do switch virtual.

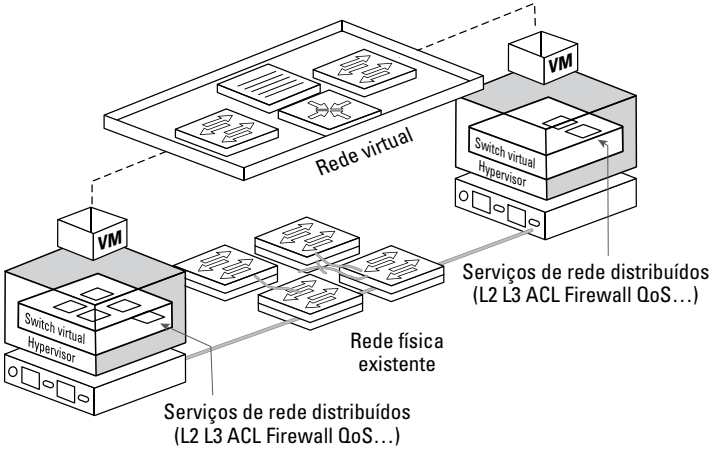


FIGURA 2-4: A rede virtual, da perspectiva da carga de trabalho (lógica).

Para a rede física, uma rede virtual parece e opera como uma rede física tradicional (veja a Figura 2-5). A rede física "vê" as mesmas estruturas de rede da camada 2 que usaria em uma rede física tradicional. A carga de trabalho virtualizada envia uma estrutura de rede de camada 2 padrão que é encapsulada no hypervisor de origem com IP adicional, protocolo de datagrama de usuário (UDP, user datagram protocol) e cabeçalhos de sobreposição de rede lógica (por exemplo, rede virtualmente extensível [VXLAN, virtual extensible local area network] ou encapsulamento genérico de virtualização de rede [GENEVE, generic network virtualization encapsulation]). A rede física encaminha a estrutura como uma estrutura de rede de camada 2 padrão e o ambiente de destino (por exemplo, hypervisor, plataforma de contêiner, nuvem) desencapsula os cabeçalhos e entrega a estrutura de camada 2 original à

carga de trabalho de destino (por exemplo, máquina virtual ou contêiner).

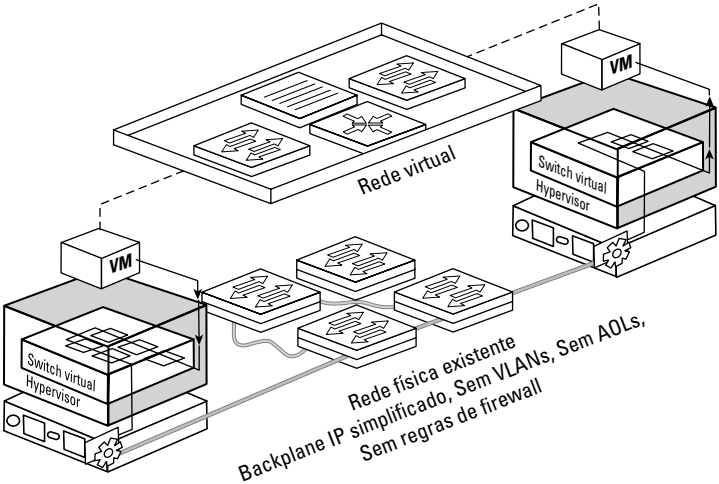


FIGURA 2-5: A rede virtual, da perspectiva da rede (física).

A capacidade de aplicar e impor serviços de segurança na interface virtual do switch virtual também elimina práticas como "hairpin" (consulte o Capítulo 3) em situações em que é necessário o tráfego leste-oeste entre dois endpoints no mesmo host físico, mas em sub-redes diferentes, para atravessar a rede para alcançar serviços essenciais, como roteamento e firewall.

QUAL É A DIFERENÇA ENTRE UMA REDE VIRTUAL E UMA REDE VIRTUAL LOCAL?

Se você trabalha com redes, deve saber tudo sobre redes locais virtuais (VLANs, virtual local area networks). Elas já estão disponíveis há muito tempo. Então, por que as VLANs não são suficientes? Vamos ver as diferenças entre as VLANs e as redes virtuais.

A abordagem da VLAN divide uma rede local física (LAN, local area network) em várias redes virtuais. Grupos de portas são isolados uns

(continued)

(continued)

dos outros como se estivessem em redes fisicamente diferentes. A abordagem VLAN é como dividir uma grande rede em muitas redes pequenas. Em termos prospectivos, à medida que sua rede cresce, você pode eventualmente chegar a um beco sem saída: a limitação de um total de 4.096 VLANs em uma única LAN.

Os problemas com as VLANs não param por aí. Uma outra grande limitação é que as VLANs não permitem salvar, criar snapshots, excluir, clonar ou mover redes. E há também o problema inerente da segurança com as VLANs; elas não permitem que você controle o tráfego entre dois sistemas na mesma VLAN. Isso significa que um ataque que atinja um sistema pode passar para outro sistema.

- As VLANs não oferecem uma abordagem holística para virtualizar a rede. Isso significa que:
- É necessária uma configuração em todos os saltos físicos e virtuais para estender uma VLAN.

Elas abordam apenas a segmentação de redes de camada 2, que tem imensas consequências de complexidade desnecessárias para outros serviços de rede, como roteamento, firewall e balanceamento de carga.

A virtualização de redes é muito mais do que as VLANs, possibilitando a criação de redes inteiras em software, incluindo switching, roteamento, firewall e balanceamento de carga, aproximando-se do aplicativo e orquestrando o processo por padrão. Essa abordagem oferece muito mais flexibilidade do que era possível no passado. Com todos os serviços de rede e de segurança disponibilizados em software e anexados ao aplicativo, os processos trabalhosos de gerenciamento e de configuração podem ser simplificados e automatizados, e as redes podem ser criadas automaticamente para atender às demandas da carga de trabalho.

Virtualização de redes e rede definida por software

A virtualização de redes se parece muito com a rede definida por software (SDN, software-defined networking), então qual é a diferença? Vejamos esses dois conceitos.

O termo *rede definida por software* significa coisas diferentes para pessoas diferentes, mas tudo começou com o objetivo de tornar a rede mais ágil através da definição de construções de rede em software. Nesse sentido, a virtualização de redes e a SDN são semelhantes. Existe uma grande variação sobre como a SDN se manifesta. Em alguns casos, o objetivo é gerenciar a configuração de dispositivos de rede física. Em outros, trata-se da orquestração mais ampla dos serviços de rede, unindo vários sistemas por meio de APIs (um pouco de software, um pouco de hardware). Em muitos casos, o hardware continua a ser a força motriz da rede, e isso se afasta do objetivo original.

A virtualização de redes tem uma definição mais específica e separa completamente os recursos de rede do hardware subjacente. Componentes e funções de rede são replicados no software. Os princípios de virtualização são aplicados à infraestrutura de rede física para criar uma reserva flexível de capacidade de transporte que pode ser alocada, usada e redefinida sob demanda.

Com seus recursos de rede desacoplados da infraestrutura física, praticamente não há necessidade de tocar no hardware subjacente para adicionar ou atualizar aplicativos, independentemente dos serviços de rede que eles precisem. Os endpoints podem se mover de um domínio lógico para outro sem que seja necessário reconfigurar a rede ou fazer conexões de domínio. Implementa-se a virtualização de redes em uma camada virtual dentro do domínio de computação, próximo ao aplicativo, em vez de em switches de rede. Conforme observado anteriormente, a rede física, ainda muito essencial, serve como um backplane de encaminhamento de pacotes, mas não é necessário mudá-la com cada mudança de aplicativo.

LEMBRE-SE

Originalmente, a SDN compartilhava o mesmo objetivo da virtualização de redes, o que tornava a rede mais ágil, mas a SDN é um termo mais amplo que adotou diversas definições, muitas das quais estão ligadas a arquiteturas de hardware e muitas delas não virtualizam totalmente a rede.

Appliances virtuais versus integração na camada virtual

Muitos provedores de serviços de rede e de segurança perceberam que o que era tradicionalmente oferecido com um appliance físico deveria se assemelhar ao aplicativo para ser mais ágil e mais eficiente. Com essa

finalidade, esses provedores também estão oferecendo opções virtualizadas. Esses são conhecidos como *appliances virtuais*. Em geral, os appliances virtuais são projetados para fornecer a funcionalidade de uma única função de rede, como um roteador, um acelerador de rede de longa distância (WAN, wide area network) ou um firewall de rede, mas no formato de uma máquina virtual dedicada.

Embora atendam a necessidades específicas, os appliances virtuais têm algumas características diferentes de uma abordagem de virtualização de redes mais ampla. Para começar, os appliances virtuais são executados como guests na parte superior de um hypervisor, e isso limita o desempenho. Eles também apresentam o desafio da expansão de appliances virtuais. Devido ao desempenho limitado dos dispositivos, pode ser necessário implantar dezenas, centenas ou até milhares de appliances virtuais para alcançar a capacidade de expansão do data center completo. Isso apresenta barreiras de despesas de capital (CapEx), bem como desafios operacionais.

O verdadeiro valor da virtualização de redes está na integração de todas as funções de rede em uma camada de rede virtual abrangente que inclui um mecanismo de orquestração (ou controlador) e uma profunda integração com a camada de computação virtual (por exemplo, hypervisor, orquestração de contêineres ou nuvem). Essa abordagem mais sofisticada permite que a rede e todas as diversas funções acompanhem as máquinas virtuais à medida que elas se movem de um servidor para outro. Não há necessidade de reconfigurar nenhuma conexão de rede, porque elas estão todas no software. Basicamente, a rede pode ir a qualquer lugar que seja virtualizado.

Há muitas outras vantagens na abordagem intrinsecamente virtual da virtualização de redes. Abrangemos isso no Capítulo 3. Por enquanto, vamos apenas dizer que essa nova abordagem à rede torna o seu data center, e o gerenciamento de aplicativos além do data center, muito mais ágil. É como passar de conexões com fio para conexões sem fio em sua rede residencial. Você está livre de uma restrição tradicional.

Por que é a hora certa para a virtualização de redes

Há anos que as pessoas falam sobre a virtualização de redes. Agora é hora de fazer a coisa acontecer, para atender às necessidades urgentes dos aplicativos atuais.

Aqui estão alguns dos motivos pelos quais a hora é certa para a virtualização de redes.

Satisfação das demandas de uma empresa dinâmica

Simplificando, software se move mais rápido que hardware. É muito mais fácil implantar serviços, fazer alterações e reverter para versões anteriores quando a rede está em software. As empresas modernas têm requisitos em constante mudança, e isso coloca demandas crescentes em TI para suportar essas mudanças. Quando o ambiente de rede é executado exclusivamente em software, ele é muito mais flexível em adaptar-se a mudanças, possibilitando que as organizações de TI atendam às demandas de negócios com mais eficiência.

Aumento da flexibilidade com a abstração de hardware

A virtualização de redes move a inteligência de hardware dedicado para um software flexível que aumenta a agilidade de TI e da empresa. Esse conceito é conhecido como *abstração*. Para explicar esse conceito, vamos começar no mundo consagrado da virtualização de servidores.

Com a virtualização de servidores, uma camada de abstração, ou hypervisor, reproduz os atributos do servidor físico, unidade de processamento central (CPU, central processing unit), memória de acesso aleatório (RAM, random access memory), disco e assim por diante, no software. A abstração permite que esses atributos sejam montados dinamicamente para produzir uma máquina virtual personalizada.

A virtualização de redes funciona da mesma maneira. Com a virtualização de rede, o equivalente funcional de um "hypervisor de rede" reproduz serviços de rede, como switching, roteamento, controle de acesso, firewall, qualidade de serviço (QoS, Quality of Service) e balanceamento de carga, no software. Com tudo em software, os serviços virtualizados podem ser montados em qualquer combinação para produzir uma rede virtual personalizada em questão de segundos.

Esse nível de agilidade é um dos grandes benefícios do data center definido por software (SDDC, software-defined data center), estendendo-se à rede em nuvem virtual e é um das grandes motivos para a virtualização de redes.

Aumento da segurança com a microssegmentação

Outro motivo para a virtualização de redes está na necessidade de maior segurança. A virtualização de redes aumenta a segurança, servindo de base para a *microssegmentação:* o uso de políticas refinadas e controle de rede para permitir a segurança *de cada aplicativo*. A microssegmentação permite a redução da segurança em torno de cada carga de trabalho, evitando a disseminação de ameaças laterais. Explicaremos mais sobre esse conceito no Capítulo 4.

Com a virtualização de redes, as redes são isoladas por padrão, o que significa que as cargas de trabalho em duas redes não relacionadas não têm possibilidade de se comunicar entre elas. O isolamento é fundamental para a segurança da rede, seja para conformidade, contenção ou simplesmente para impedir que os ambientes de desenvolvimento, teste e produção interajam. Quando as redes virtuais são criadas, elas permanecem isoladas umas das outras, a menos que você decida conectá-las. Elas não precisam de sub-redes físicas, VLANs, listas de controle de acesso (ACLs, access control lists) nem de configurações de firewall físico para permitir esse isolamento.

As redes virtuais também são isoladas da rede física subjacente. Esse isolamento não apenas dissocia as alterações em uma rede virtual para uma não afetar a outra, mas também protege a infraestrutura física subjacente de ataques iniciados a partir de cargas de trabalho em qualquer uma das redes virtuais. Mais uma vez, não é necessária nenhuma VLAN, ACL ou regras de firewall para criar esse isolamento. Porque a virtualização de redes funciona exatamente assim.

ANÁLISE DA MICROSSEGMENTAÇÃO

Para conhecer mais a fundo o conceito de microssegmentação, baixe uma cópia do documento *Microssegmentação para Leigos* (Wiley) em `www.vmware.com/go/MicrosegmentationForDummies.com`. Este livro, patrocinado pela VMware, fornece uma visão detalhada dos conceitos, tecnologias e benefícios da microssegmentação com a família de produtos VMware NSX.

Estabelecimento de uma plataforma para o data center definido por software

Conforme observamos no Capítulo 1, o SDDC é uma estrutura muito necessária para maior agilidade de TI e um fornecimento de serviços de TI mais rápido, tudo a um custo menor dentro do data center, e a rede virtual em nuvem estende esses conceitos para aplicativos em qualquer lugar.

A virtualização de redes é uma arquitetura transformadora que possibilita criar e executar redes inteiras em paralelo no hardware de rede existente. Isso resulta em uma implantação mais rápida de cargas de trabalho, bem como maior agilidade e segurança diante de data centers, nuvens e nós de borda cada vez mais dinâmicos.

Reavaliação da rede

Embora ela alavanque seu hardware de rede existente, a virtualização de redes é uma abordagem fundamentalmente nova para a rede. Isso significa que é preciso pensar sobre sua rede de novas maneiras. No passado, as funções de rede giravam em torno do hardware. Agora elas têm toda a flexibilidade do software.

Uma rede virtualizada deve permitir que use-se uma rede inteira, completa com todas as configurações e funções, e duplique-a no software.

DICA

É possível criar e executar sua rede virtualizada em paralelo no hardware existente da sua rede. Uma rede virtual pode ser criada, salva, excluída e restaurada, assim como você faria com as máquinas virtuais, mas neste caso você está fazendo isso com toda a rede.

LEMBRE-SE

Em termos mais específicos, uma rede virtualizada oferece a capacidade de:

- Desassociar a rede do hardware subjacente e aplicar os princípios de virtualização à infraestrutura de rede.
- Criar um pool flexível de capacidade de transporte que pode ser alocado, usado e redefinido sob demanda.
- Implantar redes em softwares totalmente isolados uns dos outros, bem como de outras mudanças no data center.
- Transferir, mover e replicar a rede, assim como pode-se fazer com recursos de computação e armazenamento virtualizados.

- Disponibilizar a funcionalidade de rede uniforme em qualquer lugar da empresa.

Então, como se chega lá? Abrangemos essa parte da história no Capítulo 3, onde analisaremos as tecnologias por trás da transformação da rede.

NESTE CAPÍTULO

- Explicação das principais funcionalidades de uma rede virtualizada
- Introdução das tecnologias para a virtualização de redes
- Descrição das principais características de uma rede virtualizada
- Benefícios funcionais e econômicos

Capítulo 3
Transformação da rede

Nos capítulos anteriores, introduzimos a virtualização de redes e fornecemos uma visão geral rápida. Neste capítulo, aprofundamos as tecnologias necessárias para levar os benefícios da virtualização ao seu ambiente de rede. Começamos introduzindo os conceitos por trás da virtualização de redes e concluímos com detalhes do VMware NSX Data Center, uma plataforma de virtualização de redes e segurança multi-cloud e com vários hypervisors.

As principais funcionalidades de uma rede virtualizada

Algumas das principais funcionalidades de uma rede virtualizada são: rede de sobreposição, bem como as funções tradicionais com as quais você provavelmente está mais familiarizado, como roteamento e balanceamento de carga, os quais agora são realizados no software, mais próximos do aplicativo.

Redes de sobreposição

A virtualização de redes faz uso das tecnologias de sobreposição, as quais ficam acima do hardware da rede física, permitindo uma rede lógica, conforme aparece na Figura 3-1.

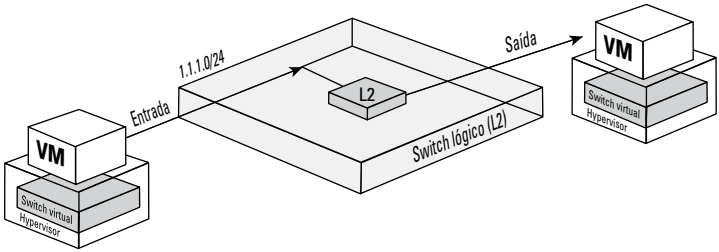


FIGURA 3-1: Rede lógica através do uso de sobreposições.

As sobreposições de rede possibilitam a execução de redes inteiramente no software, abstraídas da infraestrutura de rede física de suporte. No caso da rede do data center, elas criam túneis entre os endpoints dentro da camada virtual.

Fluxo de pacotes do remetente ao destinatário

Conforme observamos em outros lugares, as redes virtuais usam a rede física subjacente como o backplane de encaminhamento de pacotes e deixam decisões de rede mais específicas mais próximas do aplicativo. Quando os endpoints de aplicativos (por exemplo, duas máquinas virtuais [VMs]) se comunicam entre si, o pacote é encapsulado com o endereço do Protocolo de Internet (IP, Internet Protocol) do endpoint virtual de destino. A rede física entrega a estrutura ao host ou hypervisor de destino, que pode remover o cabeçalho externo e, em seguida, a instância do switch virtual local entrega a estrutura ao endpoint do aplicativo de destino.

Dessa forma, a comunicação usa a rede física subjacente como um backplane de IP simples, ou seja, um que não precisa de muita complexidade como STP (Spanning Tree Protocol) ou listas de controle de acesso (ACLs), pois isso agora podem ser feito mais perto do aplicativo pela plataforma de virtualização de redes. Essa abordagem simplifica consideravelmente o gerenciamento de configuração e elimina as mudanças físicas de rede do processo de aprovisionamento de rede, o que é uma grande coisa.

Tecnologias de sobreposição

Existem várias tecnologias de sobreposição. Uma tecnologia padrão do setor é chamada de rede local virtualmente extensível (VXLAN). A VXLAN fornece uma estrutura para a sobreposição de redes de camada 2 virtualizadas sobre redes de camada 3, definindo um mecanismo de encapsulamento e um plano de controle. Uma outra é o encapsulamento genérico de virtualização de rede (GENEVE), que usa os mesmos conceitos, mas os torna mais extensíveis por ser flexível a vários mecanismos de plano de controle.

Há também outras, incluindo a virtualização de redes usando o encapsulamento genérico de roteamento (NVGRE, generic routing encapsulation). A NVGRE é semelhante à VXLAN em seus objetivos, mas usa abordagens diferentes para criar a sobreposição. A NVGRE teve adoção limitada em comparação com a VXLAN e a GENEVE.

Uma introdução à VXLAN e GENEVE

Esta seção esclarece questões relacionadas à VXLAN e GENEVE – como são semelhantes e como são diferentes.

Encapsulamento

VXLAN e GENEVE são tecnologias de sobreposição que encapsulam as estruturas Ethernet originais geradas por cargas de trabalho (virtuais ou físicas) conectadas ao mesmo segmento de camada lógica 2, geralmente denominado switch lógico. Elas também são tecnologias de encapsulamento da camada 2 sobre a camada 3 (L2oL3). A estrutura Ethernet original gerada por uma carga de trabalho é encapsulada com um cabeçalho externo, seguido pelos cabeçalhos Protocolo de Datagrama de Usuário (UDP, User Datagram Protocol), IP e Ethernet para garantir que ele possa ser transportado pela infraestrutura de rede interconectando os endpoints VXLAN ou GENEVE (normalmente endpoints do aplicativo, como uma máquina virtual ou um pod de contêiners).

Dimensionamento

É possível ampliar além da limitação da rede local dinâmica (VLAN) de 4.096 nos switches tradicionais através de um identificador de 24 bits, denominado VNI (identificador de rede VXLAN em VXLAN ou identificador de rede virtual em GENEVE), o qual está associado a cada segmento de camada 2 criado no espaço lógico. Esse valor é colocado dentro do cabeçalho de sobreposição e é normalmente associado a uma sub-rede IP, semelhante ao que tradicionalmente acontece com as VLANs.A comunicação entre dispositivos da mesma sub-rede ocorre entre dispositivos conectados à mesma rede virtual (switch lógico).

Como atravessar a rede

É realizado hashing dos cabeçalhos das camada 2, camada 3 e camada 4 presentes na estrutura Ethernet original para derivar o valor da porta de origem para o cabeçalho UDP externo. Isso é importante para garantir o balanceamento de carga do tráfego de sobreposição em caminhos de custo igual potencialmente disponíveis dentro da infraestrutura de rede de transporte.

Término dos túneis

Os endereços IP de origem e de destino usados no cabeçalho IP externo identificam exclusivamente os hosts que originam e terminam o encapsulamento de sobreposição de estruturas. Essa funcionalidade está no endpoint de encapsulamento (em GENEVE) ou VXLAN Tunnel EndPoint (VTEP, em VXLAN).

Tamanho da estrutura

O encapsulamento da estrutura Ethernet original em um pacote UDP aumenta o tamanho do pacote IP. Isso resulta em um dos poucos requisitos para a infraestrutura de rede física: Recomenda-se aumentar o tamanho da unidade de transmissão máxima (MTU, Maximum Transmission Unit) para um mínimo de 1.700 bytes para todas as interfaces que transportarão o tráfego de rede de sobreposição. A MTU para os uplinks do switch virtual dos endpoints de encapsulamento que realizam o encapsulamento VXLAN ou GENEVE é automaticamente aumentada ao preparar o endpoint de encapsulamento para VXLAN ou GENEVE.

A Figura 3-2 descreve (em alto nível) as etapas necessárias para estabelecer a comunicação da camada 2 entre os endpoints do aplicativo, aproveitando a funcionalidade de sobreposição, neste caso, digamos que duas máquinas virtuais se comunicando em VXLAN:

- A VM1 origina uma estrutura destinada à parte da VM2 do mesmo segmento lógico da camada 2 (sub-rede IP).
- O VTEP de origem identifica o VTEP de destino no qual a VM2 está conectada e encapsula a estrutura antes de enviá-lo à rede de transporte.
- A rede de transporte só é necessária para permitir a comunicação IP entre os VTEPs de origem e de destino.
- O VTEP de destino recebe a estrutura VLXLAN, realiza o desencapsulamento da estrutura e identifica o seu respectivo segmento da camada 2.
- A estrutura é entregue à VM2.

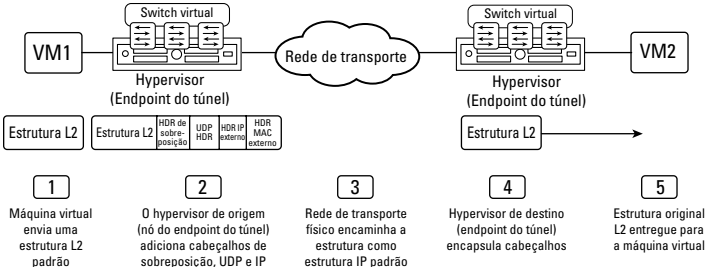


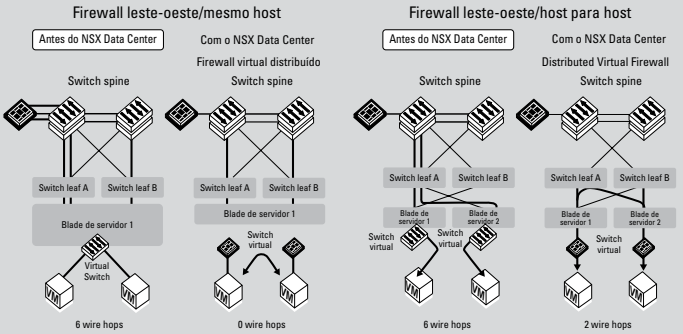
FIGURA 3-2: Estabelecimento da comunicação da camada 2 entre máquinas virtuais com VXLAN.

VIRTUALIZAÇÃO DA REDE EM AÇÃO: UM EXEMPLO

Eis um dos muitos possíveis exemplos de como a virtualização de redes facilita a vida dos administradores de segurança e de rede.

A comunicação em uma rede convencional pode ser ineficiente quando serviços, como o firewall, são aplicados. O tráfego deve ser roteado para fora do ambiente virtual, passado pelo firewall físico e, em seguida, redirecionado de volta para o ambiente virtual. Este processo é muitas vezes conhecido como *hairpinning* ou *tromboning*, ou seja, ele sai e volta, antes mesmo de chegar ao seu destino. Isso dá maior complexidade e latência, reduzindo o desempenho e aumentando a instabilidade, dificultando a movimentação dos endpoints dos aplicativos.

Por outro lado, quando os serviços de rede são integrados a uma camada de virtualização de redes, não há necessidade desse processo de "*hairpinning*". Esses conceitos são ilustrados na figura a seguir.



Funções da rede virtual

A rede de sobreposição é muito poderosa, mas é apenas uma parte da história sobre a virtualização de redes. As sobreposições basicamente permitem que sejam tomadas decisões de rede no software, em uma camada virtual, abstraída do hardware físico com todos os benefícios que acompanham. Mas e depois? Como são essas decisões? É aí que entram as funções de rede virtual. Na verdade, muitas delas podem obter os benefícios sem a necessidade de implantar uma rede de sobreposição.

Quais funções? Bem, a maneira como funciona a rede IP não está necessariamente mudando, então ainda é necessário um roteador no espaço virtual. Como você está aproximando a rede do aplicativo, ela também pode se beneficiar de um novo modelo de balanceamento de carga. Essas podem ser funções centralizadas (pense em um único roteador) ou funções distribuídas (como tem sido feito há anos com switching virtual distribuído). E por fim, algo que realmente revolucionou a segurança é o firewall virtual distribuído. Analisaremos cada uma dessas funções mais a fundo à medida que explicarmos as arquiteturas e os casos de uso.

COISAS TÉCNICAS

Funções de Redes Virtuais é um termo importante no campo da Virtualização de Funções de Rede (NFV, Network Function Virtualization). Esse campo dedica-se à virtualização das funções de rede física exigidas pelas redes de provedores de serviços e redes de operadoras móveis. Na verdade, é muito parecido com o modo como as funções estão passando para software no espaço do data center e em outros lugares, mas também é diferente em muitos aspectos, por isso vale a pena esclarecer que não estamos necessariamente falando sobre NFV aqui, embora estarmos discutindo como levar funções de rede para o software.

O grande retorno

A virtualização de redes ajuda as organizações a alcançarem grandes avanços em velocidade, agilidade e segurança, automatizando e simplificando muitos dos processos que envolvem a execução de uma rede de data center e o gerenciamento de redes e de segurança na nuvem.

Eis uma lista de alguns dos principais benefícios com essa nova abordagem para a rede. A virtualização de redes ajuda a:

- Reduzir o tempo de aprovisionamento de rede de semanas para minutos.
- Alcançar maior eficiência operacional ao automatizar processos manuais.
- Colocar e mover cargas de trabalho independentemente da topologia física.
- Melhorar a segurança da rede no data center.

Conheça o VMware NSX Data Center: Introdução da virtualização de redes ao SDDC

Primeiro, uma definição simples: O VMware NSX é uma família de produtos de rede da VMware que realiza a virtualização de redes do data center para a nuvem até a borda. O NSX Data Center é a plataforma de virtualização de redes e de segurança para o data center definido por software (SDDC). O NSX Data Center reproduz todo o modelo de rede no software. Esse modelo completo permite que qualquer topologia de rede, desde redes simples até multicamadas complexas, seja criada e aprovisionada em segundos. Ele oferece todo o lado bom da virtualização de redes que abrangemos até agora, e muito mais, que abordaremos mais tarde.

Além do NSX Data Center aumentar a agilidade e simplificar sua abordagem à rede, ele também melhora a segurança dentro do data center. Esses ganhos de segurança são fornecidos por meio de políticas automatizadas refinadas que envolvem controles de segurança em torno de cada endpoint de aplicativo. Esta é uma abordagem completamente nova. Ela possibilita uma rede intrinsecamente segura, evitando ataques que se movem lateralmente dentro do data center, de carga de trabalho a carga de trabalho, com pouco ou nenhum controle para bloquear a propagação. Com o NSX Data Center, as cargas de trabalho podem ser isoladas umas das outras, como se cada uma estivesse em sua própria rede.

Como funciona

Nesta seção, analisaremos o VMware NSX Data Center com mais detalhes.

Arquitetura do NSX Data Center

A abordagem do NSX à virtualização de redes no data center permite que sua rede física seja tratada como uma reserva de capacidade de transporte que pode ser consumida e redefinida sob demanda. As redes virtuais são criadas, aprovisionadas e gerenciadas no software, usando sua rede física como um simples backplane de encaminhamento de pacotes.

Os serviços de rede virtualizados são distribuídos para cada endpoint de aplicativo independentemente do hardware ou da topologia de rede subjacente. Isso significa que as cargas de trabalho podem ser adicionadas ou movidas rapidamente e todos os serviços de rede e de segurança anexados ao aplicativo se movem com elas, em qualquer lugar do data center. Seus aplicativos existentes operam sem modificações. Eles não veem nenhuma diferença entre uma rede virtual e uma conexão de rede física.

Integração com a infraestrutura de rede existente

O NSX Data Center trabalha com sua infraestrutura de computação e de rede, aplicativos e produtos de segurança existentes. Pode-se implantar o NSX Data Center sem interrupções sobre a infraestrutura atual.

E acima de tudo, o NSX Data Center não é uma abordagem de tudo ou nada. Você não precisa virtualizar toda a sua rede. Há a flexibilidade de virtualizar partes da rede simplesmente adicionando hypervisors, hosts novos e até nuvens à plataforma NSX.

Redes simplificadas

Depois da implantação do NSX Data Center, pouca interação com a rede física é necessária. Não é preciso mais lidar com a configuração de rede física de VLANs, ACLs, árvores de extensão, conjuntos complexos de regras de firewall e padrões complicados de tráfego porque eles não são mais necessários quando a rede é virtualizada.

LEMBRE-SE

À medida que implantar redes virtuais do NSX, será possível otimizar cada vez mais a configuração e o design da rede física. A dependência de fornecedor torna-se coisa do passado porque a rede física só precisa entregar encaminhamento confiável de pacotes de alta velocidade. Isso significa que pode-se misturar e combinar hardware de diferentes linhas de produtos e fornecedores.

Um ecossistema mais amplo de recursos de rede e de segurança

O NSX Data Center é extremamente flexível, altamente extensível e amplamente compatível. Um poderoso recurso de direcionamento de tráfego, chamado de *inserção de serviço*, permite que qualquer combinação de serviços de rede e segurança seja encadeada em qualquer ordem. Tudo é definido pelas políticas de aplicativos que você define para cada carga de trabalho.

Esse alto grau de flexibilidade se aplica não apenas aos serviços nativos do NSX Data Center, mas também à uma ampla variedade de soluções compatíveis de terceiros, incluindo instâncias físicas e virtuais de firewalls de próxima geração, controladores de entrega de aplicativos e sistemas de prevenção contra intrusões.

Vamos dar um passo atrás e considerar a perspectiva mais ampla aqui. A disponibilidade de muitos produtos compatíveis com NSX de parceiros da VMware é um sinal de suporte do setor para o novo modelo operacional fornecido pela plataforma NSX Data Center. Isso lhe dá mais confiança à medida que você entra no campo da rede virtualizada. Você tem um amplo ecossistema do seu lado. Para obter mais detalhes, consulte o Capítulo 6 e a seção "Integrando-se aos parceiros do ecossistema de serviços de rede".

O que faz: Os principais recursos do NSX Data Center

Vejamos alguns dos principais recursos técnicos do VMware NSX Data Center. No início, tenha isso em mente: O NSX Data Center virtualiza todas as funções de rede. Além disso, muitos que são cobertos e muitos que não são, também estão disponíveis no ecossistema de parceiros. Nesse sentido, o NSX é como uma camada mágica que permite um espectro de recursos em todo o seu ambiente.

Tudo no software

LEMBRE-SE

Eis algumas das principais características do VMware NSX Data Center:

- **Switching lógico distribuído:** O NSX Data Center possibilita a reprodução da funcionalidade completa de switching da camada 2 e da camada 3 em um ambiente virtual, dissociado do hardware subjacente.

- **Gateway NSX:** Esse gateway da camada 2 possibilita uma conexão perfeita com cargas de trabalho físicas e VLANs preexistentes.
- **Roteamento lógico:** O roteamento entre switches lógicos fornece um roteamento dinâmico dentro de diferentes redes virtuais.
- **Firewall lógico distribuído:** O NSX Data Center possibilita a criação de um firewall distribuído, integrado à camada de rede virtual e acondicionando a segurança em torno de cada carga de trabalho. Isso vem acompanhado da identificação de aplicativos da camada 7, bem como o firewall com base no usuário.
- **Balanceador lógico de carga:** O NSX Data Center oferece um balanceador de carga completo com terminação SSL.
- **VPN lógica:** O NSX Data Center oferece suporte a redes privadas virtuais (VPNs, virtual private networks) de site para site e acesso remoto no software.
- **API do NSX:** Essa API baseada em REST possibilita a integração em qualquer plataforma de gerenciamento de nuvem.
- **Integração com plataformas de gerenciamento de nuvem:** A integração é possível com automação completa por meio de plataformas como o OpenStack ou o VMware vRealize Automation.
- **Inserção de serviço:** O NSX Data Center possibilita conectar funções de serviços de terceiros, não apenas como uma chamada à API e direção ao norte, mas como um serviço encadeado para cada fluxo de pacote.
- **Rede e segurança multi-cloud e em vários sites:** Você pode ampliar esses conceitos fora de um único domínio do data center para vários sites e nuvens.
- **Planejamento, visibilidade e ferramentas de operações:** Ferramentas como o Application Rule Manager permitem capturar tráfego e usar essa visibilidade para criar políticas de rede, enquanto o Traceflow possibilita fazer um passeio de pacotes para depuração, por exemplo.

Isolamento essencial, segmentação e serviços avançados de segurança

Todos os anos, as empresas gastam bilhões de dólares para proteger os perímetros de seus data centers. E adivinhe o que acontece? As violações continuam a acontecer. Embora seja uma parte essencial de uma estratégia de segurança, a proteção de perímetro não faz tudo que seria necessário. Precisamos de um novo modelo para a segurança do data center. A microssegmentação, um conceito apresentado no Capítulo 2, fornece esse modelo.

O NSX Data Center oferece segurança dentro do data center com políticas automatizadas e refinadas, vinculadas a endpoints de aplicativos, como máquinas virtuais. As políticas de segurança de rede são aplicadas por controles de firewall integrados à camada virtual, como o hypervisor, que já está distribuído por todo o data center. O hypervisor, por exemplo, serve como um local ideal para impor essas políticas, estando ele próximo mas, ao mesmo tempo, isolado do aplicativo. Essas políticas de segurança são movidas quando as máquinas virtuais são movidas e se adaptam dinamicamente a mudanças no data center.

As redes virtuais podem operar em seus próprios espaços de endereços ou ter espaços de endereços sobrepostos ou duplicados. Tudo isso sem interferir uma na outra. As redes virtuais são inerentemente isoladas de todas as outras redes virtuais e da rede física subjacente, por padrão. Cada rede virtual é como uma ilha em um mar do data center. Essa abordagem possibilita isolar as redes umas das outras com segurança. Você acaba tendo um modelo de segurança inerentemente melhor para o data center. Softwares maliciosos que passam pelo seu firewall não podem mais saltar de um servidor para outro.

Obviamente isso não significa que você possa desistir de suas soluções favoritas de segurança de rede. O NSX Data Center é uma plataforma para trazer as principais soluções de rede e de segurança do setor para o SDDC. Graças à forte integração com a plataforma do NSX Data Center, produtos e soluções de terceiros podem ser implantados conforme necessário e podem se adaptar dinamicamente às condições em constante mudança no data center.

LEMBRE-SE

Esses recursos de virtualização de redes possibilitam as três principais funções de microssegmentação:

- **Isolamento:** Nenhuma comunicação entre redes não relacionadas
- **Segmentação:** Comunicação controlada dentro de uma rede

- **Segurança com serviços avançados:** Possibilitada pela integração com soluções de segurança de terceiros

Desempenho e dimensionamento

O NSX Data Center proporciona desempenho e dimensionamento comprovados. Visto que as funções de rede estão incorporadas na camada virtual, o NSX Data Center apresenta uma arquitetura de expansão que permite o dimensionamento contínuo de capacidade adicional e, ao mesmo tempo, oferece disponibilidade e confiabilidade sólidas.

Veja um exemplo da extrema capacidade de expansão do NSX Data Center: Em uma implantação do NSX Data Center, um único cluster de controladores está sendo usado para fornecer mais de 10 mil redes virtuais, que por sua vez suportam mais de 100 mil máquinas virtuais. Isso não é necessário nem faz sentido para a maioria das redes, mas muitas têm limitações de capacidade de expansão que agora são abordadas.

No ambiente do NSX Data Center:

- O processamento necessário para a execução de serviços de rede distribuídos é incremental ao que o vSwitch já está fazendo com as cargas de trabalho conectadas.
- O vSwitch é um módulo integrado ao kernel do hypervisor, juntamente com todos os serviços de rede e de segurança do NSX Data Center.
- A capacidade de transporte da rede virtual é dimensionada linearmente (junto com o endpoint do aplicativo ou a capacidade da máquina virtual) com a introdução de cada novo hypervisor/host, adicionando 20 Gbps de capacidade de switching e roteamento e 19,6 Gbps de capacidade de firewall.

Visibilidade de rede inigualável

O NSX Data Center leva a visibilidade da rede a um nível totalmente novo. Com as abordagens convencionais de rede, a configuração e o estado de encaminhamento são distribuídos em vários dispositivos de rede diferentes. Essa fragmentação pode ofuscar sua visão e complicar a solução de problemas.

Por outro lado, o NSX Data Center fornece todas as informações de configuração e estado para todas as conexões e serviços de rede em um único local. O status e os registros de conectividade de todos os componentes do NSX Data Center e dos elementos de rede virtual (switches

lógicos, roteadores e semelhantes) estão prontamente acessíveis, assim como o mapeamento entre topologias de rede virtual e a rede física subjacente. Isso possibilita uma visibilidade total do tráfego entre os endpoints do aplicativo, mesmo quando as máquinas virtuais ou os contêineres em comunicação estão no mesmo host e o tráfego de rede nunca chega à rede física.

LEMBRE-SE

Além disso, o NSX Data Center dá acesso a ferramentas avançadas de solução de problemas, como o Traceflow. Essa função injeta um pacote sintético em uma porta de switch virtual, proporcionando a oportunidade de observar o caminho da rede à medida que atravessa sistemas de rede físicos e lógicos. Isso possibilita que os administradores identifiquem o caminho completo que um pacote faz e solucionem problemas em qualquer ponto ao longo do caminho em que o pacote for descartado (por exemplo, devido a políticas de firewall).

Esse nível de visibilidade não é possível se você estiver executando hardware de rede física tradicional e definitivamente não seria possível com a rede física em situações em que duas máquinas virtuais estão se comunicando no mesmo host.

Os principais benefícios do VMware NSX Data Center

Agora vamos falar das coisas realmente boas. Esta seção analisa algumas das maneiras pelas quais a sua organização pode lucrar com os recursos de virtualização de redes do VMware NSX Data Center. Eles podem ser divididos em: benefícios funcionais e benefícios econômicos.

Benefícios funcionais

Os benefícios funcionais do NSX Data Center giram em torno de quatro pilares do SDDC: velocidade, agilidade, segurança e confiabilidade. Veja como esses benefícios são fornecidos:

- **Criação de redes inteiras no software em segundos:** O NSX Data Center tem uma biblioteca de elementos e serviços lógicos de rede, como switches lógicos, roteadores, firewalls, balanceadores de carga, VPN e segurança de carga de trabalho. Pode-se misturar e combinar esses componentes para criar topologias de rede virtual isoladas em segundos.

- **Minimização do impacto financeiro das violações de dados:** Pode-se usar o NSX Data Center para isolar cargas de trabalho, cada uma com suas próprias políticas de segurança. Esse recurso ajuda a conter ameaças e bloqueia a movimentação de softwares mal-intencionados no data center. Uma melhor segurança interna pode ajudar a evitar ou a reduzir os custos de violações de dados.
- **Aceleração da entrega de serviços de TI e da comercialização:** Com a virtualização de rede, pode-se reduzir o tempo necessário para aprovisionar serviços de rede e de segurança multicamadas de semanas para minutos. Algumas empresas usam o NSX Data Center para fornecer às equipes de aplicativos recursos completos de aprovisionamento por autoatendimento. Além disso, os recursos de automação e de orquestração do NSX Data Center ajudam a evitar o risco de erros de configuração manual.
- **Simplificação dos fluxos de tráfego de rede:** Pode-se usar o NSX Data Center para diminuir a carga de tráfego de servidor para servidor (tráfego leste-oeste) no núcleo com excesso de solicitações. Com uma rede virtual, as máquinas virtuais se comunicam entre si por meio do vSwitch ou da malha de agregação. Isso reduz o tráfego leste-oeste e ajuda a evitar as armadilhas de padrões de tráfego complicados. A ideia é fazer melhor uso dos ativos atuais e evitar os custos para aumentar a capacidade do núcleo com mais hardware.
- **Aumento da disponibilidade do serviço:** Os data centers ampliados em nuvem têm poucas interrupções porque têm malhas mais planas com roteamento de vários caminhos de custo igual entre qualquer ponto da rede. As malhas simplificadas leaf-spine tornam os elos ou os dispositivos individuais inconsequentes. A rede pode suportar várias falhas simultâneas de dispositivos sem nenhuma interrupção. Com os recursos de virtualização de redes do NSX Data Center, pode-se obter a mesma alta disponibilidade no data center.

Benefícios econômicos

Os benefícios econômicos da virtualização de redes com o NSX Data Center estão relacionados com os gastos de capital e operacionais:

- **Redução do risco de violações dispendiosas:** Historicamente, a implantação de firewalls para controlar um volume crescente de tráfego leste-oeste dentro do data center tinha um custo

proibitivo para muitas empresas. Além disso, o grande número de dispositivos necessários e o esforço necessário para configurar e gerenciar uma matriz complexa de regras de firewall tornavam essa abordagem operacionalmente inviável. Os recursos de microssegmentação que acompanham a virtualização de redes tornam tudo isso não apenas factível, mas também acessível. Agora pode-se reduzir o risco de violações de segurança em vários data centers, evitando gastos altos de capital com hardware e software adicionais.

- **Redução de tempo e esforço:** A virtualização de redes pode reduzir bastante o esforço e o tempo necessários para realizar tarefas de rede. Geralmente, o NSX Data Center reduz o esforço de horas para minutos e a duração de ciclo de dias para minutos. Ao considerar todas as tarefas manuais necessárias para aprovisionar e gerenciar uma rede física (em ambientes de desenvolvimento, teste, preparação e produção), e o fato de o NSX Data Center automatizar essas tarefas, haverá muitas oportunidades para reduzir os custos operacionais.
- **Melhoria da utilização de ativos do servidor:** Em topologias tradicionais, cada cluster de rede tem sua própria capacidade de computação. Muitas vezes, os administradores de TI aumentam a capacidade de aprovisionamento da computação para evitar a reconfiguração de rede demorada e propensa a erros, a qual é necessária para atingir a capacidade disponível em outro cluster. O NSX Data Center oferece uma maneira melhor de fazer as coisas. Pode-se usar o NSX Data Center para unir dois ou mais clusters de rede e implantar cargas de trabalho para a capacidade não utilizada. Ao aproveitar melhor a capacidade do servidor existente, pode-se evitar a necessidade de comprar novos servidores físicos.
- Melhoria em economia de preço/desempenho: Muitas empresas estão usando os recursos do NSX Data Center e a virtualização de redes para substituir hardware patenteado caro por uma infraestrutura de baixo custo que possa ser comprada de vários fornecedores, ou seja, de quem tiver o melhor preço/desempenho.
- **Extensão do ciclo de vida do hardware:** Pode-se usar o NSX Data Center para extrair mais valor da sua infraestrutura de rede existente. Veja como: o NSX Data Center transfere um volume crescente de tráfego leste-oeste do núcleo da rede. Isso permite estender a vida útil do hardware sem precisar adicionar uma capacidade dispendiosa. Com o NSX Data Center, o

hardware de rede subjacente se torna um backplane de encaminhamento de IP simples. Em vez de atualizar o seu equipamento de rede no final do ciclo de depreciação contábil, é possível usá-lo por períodos mais longos. Com essa abordagem, você só mexe no hardware para adicionar mais capacidade ou para substituir dispositivos individuais quando eles falham.

NESTE CAPÍTULO

- Reavaliação da segurança
- Sistema de automação
- Redes multi-cloud

Capítulo 4
Casos de uso de virtualização de redes

A virtualização de redes melhora profundamente o status quo, criando um grande impacto e amplo em várias categorias. Neste capítulo, analisaremos essas categorias, dando uma série de exemplos de como as pessoas estão colocando a virtualização de redes em ação.

LEMBRE-SE

Ao examinar esses casos de uso, lembre-se que: Conforme observamos no Capítulo 3, a virtualização com o NSX Data Center não é uma abordagem de tudo ou nada. Você não precisa virtualizar toda a sua rede. É possível virtualizar partes da rede para casos de uso específicos e, em seguida, expandir o uso da virtualização ao longo do tempo.

E eis um fato interessante: Em geral, as empresas podem justificar o custo do NSX Data Center por meio de um único caso de uso, ao mesmo tempo que estabelecem uma plataforma estratégica que automatiza a TI e impulsiona casos e projetos de uso adicionais ao longo do tempo.

Nas seções a seguir, detalharemos alguns dos casos de uso mais comuns, para mostrar como é possível usar a virtualização de redes para acelerar processos, reforçar a segurança e manter seus aplicativos em funcionamento.

Proteção do data center

Conforme observamos em outros lugares, a segurança é uma preocupação cada vez maior para as empresas. A virtualização de redes fornece uma camada ideal para segurança (próxima mas isolada de aplicativos) que possibilita uma nova arquitetura de infraestrutura com segurança intrínseca, reduzindo drasticamente os riscos de violações de dados.

Microssegmentação: Limitação do movimento lateral no interior do data center

Os ataques modernos exploram as fraquezas inerentes às estratégias tradicionais de segurança de rede centrada no perímetro para se infiltrar nos data centers corporativos. Após contornar com sucesso as defesas de perímetro do data center, um ataque pode mover-se lateralmente no seu interior, de carga de trabalho para outra, com pouco ou nenhum controle para bloquear sua propagação.

A microssegmentação da rede do data center restringe o movimento lateral não autorizado, mas até agora, esse controle não era operacionalmente viável em redes de data center devido às características dos firewalls tradicionais.

Os firewalls tradicionais de filtro em pacotes e os mais avançados firewalls (da nova geração) implementam controles como pontos de obstrução físicos ou virtuais na rede. À medida que o tráfego de carga de trabalho do aplicativo passa por esses pontos de controle, seus pacotes de rede são bloqueados ou permitidos atravessar o firewall com base nas regras de firewall configuradas naquele ponto de controle.

Há duas barreiras operacionais para a microssegmentação usando firewalls tradicionais: capacidade de taxa de transferência e gerenciamento de segurança. Além disso, elas geralmente não usam a virtualização de redes como uma nova camada ideal para implementar e reforçar a segurança.

As limitações na capacidade de transporte podem ser superadas, mas a um custo significativo. É possível comprar firewalls físicos ou virtuais suficientes para fornecer a capacidade necessária para atingir a microssegmentação, mas na maioria das organizações (se não em todas), o número de firewalls necessário para uma microsegmentação eficiente não é financeiramente viável. Estamos falando de um firewall separado por máquina virtual (VM, virtual machine). Quantas máquinas virtuais

o seu data center tem? Centenas? Milhares? Isso significaria potencialmente milhares de firewalls para um data center típico.

A sobrecarga do gerenciamento de segurança também aumenta exponencialmente com o número de cargas de trabalho e a natureza cada vez mais dinâmica dos data centers atuais. Se as regras de firewall precisarem ser adicionadas, excluídas e/ou modificadas manualmente sempre que uma nova máquina virtual for adicionada, movida ou desativada, a frequência de alteração rapidamente sobrecarregará as operações de TI. É essa barreira que representa o fim dos planos dos melhores esquemas da maioria das equipes de segurança para criar uma estratégia confiável de microssegmentação abrangente ou no nível de unidade com privilégios mínimos no data center. (Discutiremos o conceito de privilégio mínimo posteriormente neste capítulo.)

O data center definido por software (SDDC, software-defined data center) aproveita uma plataforma de virtualização de redes para oferecer várias vantagens significativas em relação às abordagens tradicionais de segurança de rede. Isso inclui aprovisionamento automatizado, movimentação/acréscimo/alteração automatizada para cargas de trabalho, aplicação distribuída em cada interface virtual e desempenho de firewall com dimensionamento horizontal, distribuição para cada hypervisor e incorporação à plataforma.

O crescimento do tráfego leste-oeste no interior do data center

Durante a última década, cada vez mais os aplicativos têm sido implantados em infraestruturas de servidores com multicamadas, e as comunicações leste-oeste de servidor a servidor agora representam significativamente mais tráfego de data center do que as comunicações norte-sul (cliente-servidor). Na verdade, o tráfego no interior do data center agora é responsável por até 80% de todo o tráfego da rede. Essas infraestruturas de aplicativos com multicamadas geralmente são projetadas com pouco ou nenhum controle de segurança para restringir as comunicações entre os sistemas.

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

Visibilidade

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 a atravessar um firewall usando técnicas como redirecionamento ("hairpinning") para redirecionar o tráfego através de um ponto de obstrução, o resultado é um caminho de comunicação complexo e ineficiente que prejudica o desempenho da rede em todo o data center.

A inovação em virtualização de servidores superou em muito as construções subjacentes de rede e de segurança nos data centers tradicionais. A implantação de várias cargas de trabalho virtuais em um único host físico configurado com várias placas de interface de rede (NICs, network interface cards) é comum em ambientes de servidores virtuais. Sem os switches virtuais, o tráfego que vai e volta das máquinas virtuais 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.

A camada de rede virtual está unicamente posicionada para ver todo o tráfego no data center, até o nível de cargas de trabalho virtualizadas individuais (por exemplo, máquinas virtuais e contêineres). Esse nível de visibilidade e de contexto possibilita a microssegmentação com base em atributos exclusivos para cada carga de trabalho, tais como o sistema operacional, o nível de patch, serviços em execução e muitas outras propriedades. Essa capacidade, por sua vez, possibilita que decisões mais inteligentes de políticas de segurança e de rede possam ser definidas com uma compreensão do propósito específico de cada carga de trabalho individual no data center.

Por exemplo, as políticas exclusivas podem ser especificamente definidas para a camada web de um aplicativo de recebimento de pedidos ou para um sistema corporativo de gerenciamento de recursos humanos, com base nas necessidades da carga de trabalho individual, e não nas restrições da topologia de rede subjacente.

Indo um pouco mais adiante, o NSX Data Center não apenas fornece visibilidade do tráfego de rede por padrão, mas também oferece ferramentas para depurar (por exemplo, Traceflow) e construir estratégias

de microssegmentação baseadas nessa visibilidade (por exemplo, o Application Rule Manager), possibilitando implementar políticas em apenas alguns cliques.

Ciente do contexto

As políticas tradicionais de segurança de rede eram baseadas em construções de infraestrutura, como endereços de IP (Internet Protocol) e portas TCP (Transmission Control Protocol), que são mais um resultado da infraestrutura estática do que o contexto do aplicativo. Ao colocar a segurança mais próxima do aplicativo, integrando-a a hypervisors de virtualização e a plataformas de nuvem, a virtualização de redes permite políticas de segurança baseadas, de fato, no contexto do aplicativo. Isso não é apenas inerentemente mais seguro (porque chega ao ponto da política em vez de um artefato de infraestrutura), mas também mais fácil de gerenciar (porque não é mais necessário gerenciar várias camadas de abstrações para escrever ou entender uma política).

Eis alguns exemplos de contexto de aplicativo nos quais se basear uma política de segurança:

- **Contexto de carga de trabalho:** Em qual sistema operacional o aplicativo está sendo executado? Como você rotulou essa carga de trabalho usando tags internas?
- **Contextos do usuário:** Quem está acessando este servidor? Eles deveriam estar acessando? Qual o papel que eles têm de acordo com seu esquema do Active Directory?
- **Comportamento do aplicativo:** O que o aplicativo está fazendo? Isso é uma consulta SQL ou uma autenticação ou um tráfego da Web? Isso é melhor identificado na camada 7, depois da porta da camada 4, que só pode ser adivinhada, mas é claro que será usada para enganá-lo no caso de um ataque mal-intencionado.
- **Terceiros:** O que os sistemas de terceiros têm a dizer a respeito desse aplicativo, além do rico contexto que a plataforma de virtualização de rede, a plataforma na nuvem ou o hypervisor já sabe?

Isolamento

O isolamento é um princípio importante para a segurança da 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 firewall em dispositivos físicos têm sido tradicionalmente usados para estabelecer e impor o isolamento nas redes de data center.

COISAS TÉCNICAS

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

As redes virtuais são inerentemente isoladas de outras redes virtuais e da rede física subjacente desde a concepção. Esse conceito é distintamente diferente da abordagem preexistente de assumir algum nível padrão de confiança no interior do data center. O isolamento é inerente à virtualização de redes e não são necessárias sub-redes físicas, LANs virtuais (VLANs), ACLs ou regras de firewall para permitir esse isolamento. As redes virtuais são criadas em isolamento e permanecem isoladas, a menos que sejam deliberadas e explicitamente conectadas.

Eis uma outra coisa que é crítica com essa abordagem: As políticas de firewall no firewall distribuído, embora mais próximas do aplicativo e aproveitando o contexto do aplicativo, também são isoladas de ataques porque não ficam no guest. Elas são executadas no kernel, no hypervisor.

Qualquer rede virtual isolada pode ser composta de cargas de trabalho distribuídas em qualquer lugar do data center, e as cargas de trabalho na mesma rede virtual podem residir nos mesmos hypervisors ou em hypervisors separados. Além disso, as cargas de trabalho em várias redes virtuais isoladas podem residir no mesmo hypervisor. O isolamento entre as redes virtuais também possibilita a sobreposição de endereços IP. Assim, é possível, por exemplo, ter redes virtuais de desenvolvimento, de teste e de produção isoladas, cada uma com uma versão de aplicativo diferente, mas com os mesmos endereços IP, todas operando ao mesmo tempo na mesma infraestrutura física subjacente.

E por fim, as redes virtuais também são isoladas da infraestrutura física subjacente. Como o tráfego entre hypervisors é encapsulado, os

dispositivos de rede física operam em espaços de endereço completamente diferentes das cargas de trabalho conectadas às redes virtuais.

Por exemplo, uma rede virtual poderia suportar cargas de trabalho de aplicativos IPv6 em uma rede física IPv4. Esse isolamento protege a infraestrutura física subjacente de qualquer ataque possível iniciado por cargas de trabalho em qualquer rede virtual. Novamente, tudo isso é independente de quaisquer VLANs, ACLs ou regras de firewall que tradicionalmente seriam necessárias para criar esse isolamento.

Segmentação

A segmentação está relacionada ao isolamento, mas é aplicada em uma rede virtual de multicamadas. Tradicionalmente, a segmentação de rede é obtida com um roteador ou firewall físico que permite ou nega o tráfego entre segmentos ou camadas de rede, por exemplo, segmentando tráfego entre uma camada web, uma camada de aplicativo e uma camada de banco de dados. A segmentação é um princípio importante no design de segurança porque permite que as organizações definam diferentes níveis de confiança para diferentes segmentos de rede e reduz a superfície de ataque caso um invasor viole as defesas do perímetro. Infelizmente, os segmentos de rede do data center costumam ser grandes demais para serem eficazes, e os processos tradicionais para definir e configurar a segmentação são demorados e propensos a erros humanos, muitas vezes resultando em violações de segurança.

Uma segmentação de rede, como o isolamento, é um recurso fundamental de uma plataforma de virtualização de redes. Uma rede virtual pode suportar um ambiente de rede multicamadas, vários segmentos de camadas 2 com segmentação de camada 3 (ou microssegmentação) em um único segmento de camada 2, usando o firewall distribuído definido por políticas de segurança de carga de trabalho. Isso poderia, por exemplo, representar uma camada web, uma camada de aplicativo e uma camada de banco de dados.

Em uma rede virtual, os serviços de rede e de segurança, como camada 2, camada 3, ACLs, firewall e qualidade de serviço (QoS, Quality of Service), aprovisionados com uma carga de trabalho são criados e distribuídos de modo programático para o switch virtual do hypervisor e aplicados na interface virtual. A comunicação em uma rede virtual nunca sai do ambiente virtual, eliminando a necessidade de configuração e de 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 os data centers.

Igualmente importante, se o aplicativo for excluído, suas 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 regras de firewall obsoletas e desatualizadas em operação, muitas vezes resultando em problemas de segurança e degradação do desempenho.

As empresas também podem aplicar uma combinação de diferentes recursos de parceiros, encadeando serviços avançados de segurança e impondo serviços diferentes com base em diferentes situações de segurança. Isso permite que as organizações integrem as tecnologias de segurança já existentes para criar um recurso de segurança mais abrangente e correlacionado no interior do data center. As tecnologias de segurança já existentes funcionam melhor com a microssegmentação porque têm uma maior visibilidade e contexto do tráfego da máquina virtual de carga de trabalho individual no interior do data center, e as ações de segurança podem ser personalizadas para cargas de trabalho de máquinas virtuais individuais como parte de uma solução de segurança completa.

Por exemplo, uma carga de trabalho pode ser aprovisionada com políticas de firewall padrão, que permitem ou restringem o acesso a outros tipos de cargas de trabalho. A mesma política também pode determinar que, se uma vulnerabilidade for detectada na carga de trabalho durante a verificação normal de vulnerabilidades, uma política de firewall mais restritiva será aplicada, restringindo a carga de trabalho apenas às ferramentas usadas para remediar as vulnerabilidades.

DICA

Os fornecedores de segurança podem aproveitar a plataforma de virtualização de redes para desencadear respostas de serviços avançados de segurança a partir de uma solução de tecnologia de um fornecedor de segurança completamente diferente. Uma inovação que é acelerada com a virtualização de redes.

Inserção de serviços e introspecção de guests

Como um componente fundamental da infraestrutura, o NSX Data Center tem uma posição privilegiada para capacitar outras soluções de segurança para proteger melhor o ambiente. Os firewalls da nova geração ou os sistemas de prevenção contra intrusões (IPSs, Intrusion Prevention Systems) podem ser inseridos e o tráfego pode ser dinamicamente direcionado pelo NSX Data Center para esses sistemas, o que aumenta a eficiência do fluxo de tráfego ao mesmo tempo que mantém a segurança. Para obter mais informações sobre a integração com os parceiros do ecossistema de serviços de rede, consulte o Capítulo 6.

Ambientes seguros de usuários: Microssegmentação para VDI

Muitas empresas implantaram a infraestrutura de desktop virtual (VDI, Virtual Desktop Infrastructure) para alavancar as tecnologias de virtualização além do data center. A microssegmentação permite que essas organizações compartilhem muitas das 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 de segurança no gerenciamento de VDI
- Eliminação de políticas e topologias complexas necessárias para diferentes usuários de VDI
- Definição de regras de firewall e filtragem de tráfego, e atribuição de políticas para agrupamentos lógicos
- Separação de políticas de segurança da topologia de rede para simplificar a administração

Devido à sua capacidade de implementar a microssegmentação, o NSX Data Center permite que cada desktop virtual tenha seu próprio firewall. Isso possibilita um nível muito mais granular de segurança, o qual se estende até a interface de rede virtual. Com base nas políticas, todo o tráfego que chega e sai da máquina virtual pode ser protegido, impedindo a comunicação não autorizada entre máquinas virtuais ou outras cargas de trabalho. Se a área de trabalho virtual de um usuário final for comprometida, a exposição poderá ser facilmente contida apenas para esse usuário específico.

Automação dos processos de TI

Em grandes data centers, os processos manuais são a ruína da existência do administrador de TI e um dreno no orçamento do gerente. A virtualização de redes ajuda a enfrentar esses desafios, automatizando tarefas trabalhosas, propensas a erros e associadas à configuração de rede, aprovisionamento, gerenciamento e muito mais.

Automação de TI

Com o NSX Data Center, os poderosos recursos de orquestração distribuem os serviços de rede em paralelo com as máquinas virtuais. Pode-se usar o NSX Data Center para padronizar e manter modelos predefinidos que consistem em topologias e serviços de rede. Com a abordagem de modelo, os ambientes podem ser aprovisionados em segundos com configuração e segurança uniformes.

DICA

Ao trabalhar com os recursos de automação de TI do NSX Data Center, você está pronto para três coisas:

- Reduzir despesas operacionais.
- Acelerar o tempo de lançamento no mercado.
- Acelerar o fornecimento de serviços de TI

Nuvem de desenvolvedores

O NSX Data Center é ideal para uso como uma plataforma para nuvens de desenvolvedores de autoatendimento, bem como outras iniciativas de Infraestrutura como Serviço (IaaS, Infrastructure-as-a-Service). É possível usar a rede automatizada e o aprovisionamento de serviços para fornecer às equipes de desenvolvimento e de teste o acesso rápido à infraestrutura que precisam, para que possam disponibilizar os aplicativos e as atualizações de software aos usuários em menos tempo.

O NSX Data Center pode fornecer milhares de redes isoladas para ambientes de desenvolvimento, de teste e de preparação, tudo na mesma infraestrutura física. Nesse novo modo de fazer negócios, o NSX Data Center remove as tarefas manuais e o tempo de ciclo associados à aquisição, instalação e configuração da infraestrutura de rede. As redes são implantadas em sincronia com suas cargas de trabalho, como transações de autoatendimento totalmente auditadas. Os aplicativos passam rapidamente pelo desenvolvimento, teste, preparação e produção sem alterações em seus endereços de IP.

Infraestrutura multi-tenant

Graças à virtualização, o aprovisionamento de uma infraestrutura de rede para equipes de desenvolvimento/teste não é mais um afunilamento que atrasa os negócios e o tempo de lançamento no mercado.

Em ambientes de nuvem multi-tenant, pode-se usar os recursos de microssegmentação e de isolamento do NSX Data Center para manter o isolamento entre os tenants. O NSX Data Center permite criar redes virtuais e isolá-las completamente de qualquer outra rede virtual e da rede física subjacente. É possível ter dois tenants diferentes em execução nos mesmos endereços IP na mesma infraestrutura física sem ter nenhum conflito entre esses endereços IP, porque as redes virtuais nem sabem da existência da outra e desconhecem a existência da rede física.

Para uma solução mais ampla, pode-se adicionar serviços avançados com base em rede virtual, segmento de rede ou grupo de segurança. Por exemplo, é possível adicionar uma inspeção profunda de pacotes por meio de firewalls, como os da Palo Alto Networks. Com esse serviço, é possível definir de forma granular os fluxos de tráfego que serão redirecionados para o firewall da série VM da Palo Alto Networks para inspeção e fiscalização. O tráfego permitido pelo VM-Series Firewall então volta ao switch virtual do NSX Data Center para a entrega no destino final (máquina virtual guest ou dispositivo físico).

Aplicativos nativos em nuvem

Os desenvolvedores estão cada vez mais contornando a TI e criando aplicativos na nuvem. Eles estão usando novas construções como contêineres, criando aplicativos em arquiteturas de microsserviços e usando plataformas de orquestração de contêineres para criar e dimensionar seus aplicativos. As organizações estão encontrando maneiras de inserir algum nível de visibilidade e controle nesse processo, sem diminuir a velocidade das equipes de desenvolvimento ou impondo-lhes barreiras para ultrapassar que provavelmente serão ignoradas.

O NSX Data Center se conecta diretamente às plataformas de orquestração de aplicativos e contêineres, como Kubernetes ou Cloud Foundry, para fornecer visibilidade à organização mais amplamente e aplicar políticas já no NSX Data Center ao domínio do contêiner. Isso permite que as organizações ajudem a depurar no nível do contêiner quando algo em um aplicativo do produto der errado. Ele também permite que as políticas centradas nos negócios, por exemplo, conformidade com PCI para transações de pagamento, sejam aplicadas no aplicativo, inerentemente captadas dos manifestos dos desenvolvedores à medida que os aplicativos são criados.

Redes multi-cloud

De acordo com o "State of the Cloud Report" de 2018 da RightScale, em média, as organizações valem-se de cinco nuvens diferentes. *Cinco*. Até mesmo as organizações que não usam nuvens públicas devido a problemas de regulamentação ainda gerenciam várias nuvens privadas de data center para melhorar a continuidade dos aplicativos e manter as empresas em operação. As organizações que usam nuvens públicas podem ter um desenvolvedor criando um aplicativo no Amazon Web Services (AWS) enquanto outro está fazendo isso no Google Cloud Platform. Enquanto isso, toda uma equipe separada pode ter um projeto completo no Microsoft Azure.

O gerenciamento de processos de TI, o planejamento de desastres e a garantia da segurança em vários data centers privados e/ou nuvens públicas são agora uma obrigação empresarial. A boa notícia é que a virtualização de redes torna isso possível e elimina barreiras que costumavam apresentar desafios nessa área. Ao ampliar a rede para várias nuvens e gerenciar a segurança em um único lugar em nuvens, a rede e a segurança cross-cloud tornam-se tecnicamente possíveis e operacionalmente viáveis.

Recuperação de desastres

O processo de recuperação é automatizado, orquestrado e totalmente integrado em computação, armazenamento, rede e segurança. O NSX Data Center é compatível com várias ferramentas de orquestração de recuperação de desastres (DR, Disaster Recovery), como o VMware Site Recovery Manager, o Dell EMC RP4VM, o Zerto e o Veeam.

O NSX Data Center proporciona segurança e uma rede lógica uniforme em sites protegidos e de recuperação, e isso reduz o objetivo de tempo de recuperação (RTO, Recovery Time Objective) no caso de um desastre. Com redes e segurança abrangendo vários sites de maneira uniforme, os aplicativos podem se recuperar no site de recuperação e manter suas configurações de rede e de segurança.

Além disso, o NSX Data Center pode ser usado para facilmente criar redes de teste que podem ser usadas para testar planos de recuperação sem interromper o ambiente de produção. O teste ocorre em um ambiente isolado e mantém os mesmos endereços IP e as políticas de segurança do aplicativo no site de recuperação.

Reserva de vários locais e extensão do data center

A criação de pools em vários locais cria um pool de infraestrutura unificada, contínua e resiliente para executar aplicativos em vários data centers e em nuvens, habilitado por uma única plataforma de rede uniforme. Da mesma forma, os aplicativos podem ser implantados em qualquer local e conectados a recursos localizados em locais para acomodar a prevenção de desastres, interrupções planejadas e não planejadas ou melhor utilização de recursos.

Além disso, a maior mobilidade de cargas de trabalho em uma rede comum significa que o tempo de inatividade pode ser planejado com mais eficiência e que a ampliação de data centers existentes ou a incorporação de novos on-line ou a integração de novas fusões e aquisições é significativamente simplificada. Isso tem sido um caso de uso predominante para o NSX Data Center em implantações em vários locais.

Segurança uniforme em várias nuvens

Depois que a rede é virtualizada, ampliar seus benefícios para a nuvem se torna um complemento simples. O VMware NSX Cloud faz exatamente isso, adicionando cargas de trabalho de nuvem nativas à base do VMware NSX Data Center, usando um portal de gerenciamento para cargas de trabalho no local e na nuvem. Isso permite a microssegmentação do tráfego leste-oeste entre cargas de trabalho de aplicativos em execução na nuvem ou no data center privado.

Agora é possível definir uma política de segurança e aplicá-la a cargas de trabalho em qualquer lugar, em redes virtuais em nuvem, regiões, zonas de disponibilidade e vários data centers privados e em nuvens públicas. As políticas de segurança são aplicadas dinamicamente com base nos atributos de carga de trabalho e aplicadas no nível da instância. As regras de segurança seguem as cargas de trabalho quando elas são movidas. É possível definir políticas com base em construções ricas, como atributos de carga de trabalho e tags definidas pelo usuário. Pode-se também fazer coisas como responder a ameaças normalmente com uma quarentena de endpoints de nuvem maliciosos ou comprometidos.

NESTE CAPÍTULO

- Introdução do conceito de operacionalização
- Análise de um caso de uso de implantação de virtualização de redes
- Questões relacionadas a funcionários e empregos

Capítulo 5
Operacionalização da virtualização de redes

A operacionalização da virtualização de redes envolve a otimização de pessoas, processos e tecnologia para maximizar a rede e os recursos de segurança que ela permite.

A empresa deve ser bem-sucedida na operacionalização da virtualização de redes para obter os benefícios abrangentes de velocidade, agilidade e segurança. Quanto melhor for a operacionalização da virtualização de redes, mais rápido serão os benefícios mensuráveis de TI e de negócios – o objetivo final.

A operacionalização da virtualização de redes deve ser vista como uma jornada cultural e técnica gradual, em que a organização alcança maturidade e sofisticação crescentes à medida que passa de um data center definido por hardware para um data center definido por software (SDDC, Software-Defined Data Center). É uma jornada que trará muitos benefícios, assim como a virtualização computacional fez na década anterior.

O objetivo deste capítulo não é fornecer todas as respostas sobre o que é necessário para operacionalizar o NSX Data Center (isso daria um livro inteiro), mas sim apresentar o tópico e destacar algumas das principais áreas que devem ser consideradas na jornada para a virtualização de redes.

DICA

Ao embarcar nessa jornada de virtualização de redes, defina claramente sua visão de longo prazo para o SDDC totalmente otimizado. Pense em como você precisa desenvolver seus funcionários, processos e ferramentas para chegar onde deseja.

Áreas de investimento de operações

Deve-se considerar três principais áreas de investimento de operações na jornada rumo à virtualização de redes. Esses investimentos ajudam a obter o máximo valor de negócios para sua organização e o valor máximo de carreira para sua equipe de TI.

Adote uma abordagem holística que englobe esses conceitos, cada um deles abordado em detalhes nas seguintes seções:

- Pessoas
- Processo
- Ferramentas

Pessoas e processo

As operações do SDDC afetam a maior parte da organização de TI. Essas operações abrangem computação, rede, armazenamento, segurança e pessoal, incluindo operadores, administradores, técnicos e arquitetos.

DICA

Ao operar a virtualização de redes, inclua todas as pessoas necessárias no processo e seja transparente.

Veja algumas outras práticas recomendadas relacionadas à sua organização de TI e a seus funcionários:

- **Suas equipes de rede e segurança existentes assumem o NSX Data Center.** Não há necessidade de mudar suas equipes ou de criar equipes novas. Os papeis funcionais também permanecem os mesmos (por exemplo, arquitetos, técnicos, operadores, administradores). Os papeis e as responsabilidades existentes evoluem para incluir a virtualização de rede.
- **Considere como criar uma equipe de nuvem mais mesclada** com habilidades interdisciplinares e em vários domínios, metas e princípios operacionais comuns, treinamento e desenvolvimento dentro da equipe e alinhamento em relação ao fornecimento de serviços para a empresa.

- **Considere esses papéis de rede e de segurança para sua rede em nuvem:** Arquitetura, segurança, orquestração e automação, desenvolvimento e integração, administração, operações, e suporte e dimensionamento.
- **Obtenha o suporte da sua equipe.** Certifique-se de que todos os funcionários da sua equipe entendam a proposta de valor e o que isso significa para eles, pessoal e profissionalmente, à medida que novas oportunidades para trabalhar em projetos mais interessantes e estratégicos são disponibilizadas.
- **Tranquilize sua equipe de rede sobre a segurança de seus empregos.** Deixe claro para sua equipe de rede que eles não perderão seus empregos para sistemas automatizados e que suas funções não serão movidas para a equipe de virtualização. Sua equipe de rede existente assume a virtualização de redes. Apenas eles têm o conhecimento de rede necessário.
- **Envolva sua equipe de operações em nuvem no início do processo de avaliação.** Dessa forma, eles podem aprender como o NSX Data Center facilitará seus trabalhos e poderão se tornar defensores do projeto. Não os surpreenda antes que você queira implantar.
- **Inclua a segurança no início da avaliação.** A equipe de segurança precisa aprender como as redes virtuais isoladas são tão seguras quanto as redes físicas. Eles precisam aprender que a microssegmentação não substitui os firewalls de perímetro existentes pelo tráfego norte-sul, mas permite que a organização controle o tráfego leste-oeste no interior do data center.

DICA

Tire vantagem dos recursos focados em operações da VMware (guias técnicos, workshops, treinamento e certificações) para obter as especializações, os conhecimentos e as habilidades necessários para a virtualização de redes e o SDDC.

Processos e ferramentas

Um dos principais benefícios da virtualização de redes é que os processos que antes eram manuais podem ser automatizados. Isso exige, no entanto, um investimento inicial nas ferramentas apropriadas. Algumas tarefas de automação podem ser realizadas diretamente no NSX Manager, enquanto outras funções de automação são fornecidas por outras ferramentas, como uma plataforma de gerenciamento em nuvem.

O NSX Data Center fornece um ponto central de controle, o NSX Manager, para a criação, o gerenciamento e o monitoramento de redes virtuais. A operação de um ambiente do NSX Data Center naturalmente se concentrará no NSX Manager, seja por meio da interface do usuário (UI, User Interface) ou por meio de chamadas da interface de programação de aplicativos (API, Application Programming Interface) feitas no NSX Manager por outras ferramentas (como o VMware vRealize Automation, VMware vRealize Operations , OpenStack e outras ferramentas de terceiros).

Além disso, será necessário o gerenciamento da infraestrutura subjacente, que inclui os componentes do NSX Data Center (controladores, nós de borda, hypervisors) e a infraestrutura de rede (a base). O NSX Data Center fornece seu próprio recurso para gerenciar esses elementos, e as ferramentas de terceiros também podem desempenhar um papel central no gerenciamento da infraestrutura.

DICA

Ao operacionalizar a virtualização de redes, reflita e considere todas as implicações para seus processos e ferramentas. Em particular, mantenha estas práticas recomendadas em mente:

- **Analise seus processos existentes de rede e de segurança e os entenda em detalhes.** Determine como simplificar e otimizar seus processos por meio de orquestração e automação.
- **Considere o impacto que a virtualização de redes tem em atividades como monitoramento, solução de problemas, gerenciamento de mudanças, gerenciamento de versões e gerenciamento de capacidade.** Entenda como essas importantes atividades funcionam hoje e como elas podem ser simplificadas.
- **Determine suas prioridades para automatizar os processos de rede e padronizar ambientes (por exemplo, configurações e políticas) para reduzir o esforço e as despesas operacionais.** A automação e o aprovisionamento baseado em políticas de redes e serviços eliminam erros de configuração comuns e melhoram o rastreamento de alterações para auditoria e conformidade.
- **Determine se deve usar suas ferramentas de gerenciamento e de operações existentes ou se deve avaliar alternativas modernas.** Essas alternativas modernas fornecem uma visão completa da integridade do aplicativo em computação, armazenamento e rede. Obtenha visibilidade dos

relacionamentos de objetos entre componentes virtuais e físicos.

- **Identifique as ferramentas da VMware e de terceiros para o gerenciamento de componentes virtuais e físicos.** Avalie como você pode aproveitar os recursos e APIs nativos do NSX Data Center para uma profunda integração com ferramentas existentes, tais como plataformas de gerenciamento em nuvem e ferramentas de orquestração e de automação.
- **Use suas ferramentas existentes para operar redes virtuais.** As redes virtuais fornecem todas as informações operacionais esperadas das redes físicas (por exemplo, contadores de pacotes e de bytes, exportação do NetFlow). Muitas ferramentas existentes podem aproveitar as informações fornecidas pelo NSX Data Center para tarefas operacionais.
- **Use suas ferramentas existentes favoritas para monitorar e solucionar problemas.** Uma abordagem de fornecedor único nem sempre lhe dá a melhor visibilidade. Você pode descobrir que o uso de várias ferramentas (por exemplo, vRealize Network Insight, vRealize Operations, Splunk, Wireshark ou NetFlow) permitirá que você monitore e solucione problemas da sua infraestrutura de rede.

Alguns exemplos

Há várias coisas para as quais pode-se usar a virtualização de redes. Para fins ilustrativos, esta seção apresenta três exemplos de estado atual versus estado ideal possibilitados pela virtualização de redes.

Gerenciamento de aprovisionamento e de configuração

A infraestrutura virtualizada e as APIs trazem a automação para o aprovisionamento, o gerenciamento de configuração e as ferramentas de conformidade.

Estado atual

- Empilhe dispositivos físicos e configure-os manualmente por meio de interfaces de linha de comando (CLIs, Command-Line Interfaces) ou scripts.

- Sistemas de tickets (por exemplo, Service Now) geram várias solicitações e rastreiam o status.
- Gerenciamento de configuração de rede (NCM, Network Configuration Management), banco de dados de gerenciamento de configuração (CMDB, Configuration Management Database; por exemplo, HPNA) e ferramentas de conformidade rastreiam itens de configuração e seus relacionamentos.

Estado ideal

- Ferramentas de plataforma de gerenciamento de nuvem/orquestração (CMP, Cloud Management Platform) (por exemplo, vRealize Automation, Chef ou Puppet) fornecem automação para o gerenciamento de aprovisionamento e de configuração.
- Portais de autoatendimento fornecem catálogos de serviços e automação com APIs.
- Modelos padronizados incluem relacionamentos integrados. Pode-se alavancar as APIs para descobrir a topologia e verificar a garantia de configuração por meio de ferramentas externas.

Gerenciamento de incidentes e de capacidade

O monitoramento, a solução de problemas e o gerenciamento de capacidade são fornecidos por meio de ferramentas de contexto virtuais e físicas, e cientes do aplicativo.

Estado atual

- As ferramentas de monitoramento e de solução de problemas ficam na infraestrutura física.
- Várias ferramentas consomem granularidade diferente de informações sem correlação.
- Gerente de Gerentes (MoMs, Manager of Managers) centralizado e vinculado a sistemas de emissão de tickets gera alertas automatizados.

Estado ideal

- Monitoramento em nível de aplicativo, resolução de problemas e gerenciamento de capacidade abrangem domínios e a infraestrutura virtual e física.
- Uma interface de usuário simplificada fornece uma visão unificada e correlacionada da infraestrutura do SDDC.
- A correção automática é fornecida por meio de ferramentas externas de monitoramento através de uma estrutura de API. O dimensionamento da capacidade do NSX Data Center é baseado na utilização.

Microssegmentação

Essa técnica de segurança permite que políticas de segurança refinadas sejam atribuídas a aplicativos, até o nível da carga de trabalho.

Estado atual

Do ponto de vista prático, a microssegmentação só é viável quando um data center está usando uma abordagem virtualizada, somente de software.

Estado ideal

- Entenda o tráfego de rede com o monitoramento em nível de aplicativo (por exemplo, VMware vRealize Network Insight) para automatizar um processo tradicionalmente manual e trabalhoso de identificar quais aplicativos estão se comunicando entre si.
- Implemente regras de firewall depois de selecionar o aplicativo de destino (por exemplo, usando o Gerenciador de Regras de Aplicativos integrado do NSX Data Center).
- Continue a monitorar o tráfego de rede e solucione problemas em todo o ambiente (por exemplo, vRealize Network Insight, VMware vRealize Log Insight e as ferramentas integradas do NSX Data Center: Monitoramento de Fluxo e Monitoramento de Endpoints). Repita com o próximo aplicativo.

Desenvolvimento da mentalidade certa

Mudar não é fácil, especialmente quando envolve algo pessoal. Infelizmente, porém, isso acontece quer gostemos, quer não. No mundo da tecnologia da informação, tudo está sempre em constante mudança. *A automação de TI, a microssegmentação, a disponibilidade de aplicativos e os serviços cross-cloud* não são mais chavões em materiais de marketing e reuniões executivas. Essas são realidades projetadas e implantadas em alguns dos maiores ambientes de TI do mundo. Os elementos em comum desses conceitos são os novos recursos de rede e de segurança criados pela família NSX.

A virtualização de redes está transformando a maneira como as empresas abordam os problemas empresariais tradicionais e está resolvendo novos problemas empresariais provenientes da transformação digital de uma empresa.

Como profissional de TI, seu sucesso a longo prazo depende da sua capacidade de se adaptar a novas tecnologias e soluções. As soluções NSX são conflituosas em relação ao estado atual mas, ao mesmo tempo, é uma oportunidade para seus administradores, engenheiros e arquitetos se tornarem líderes em um novo paradigma de rede e de segurança. Isso requer uma mentalidade focada em encontrar oportunidades em vez de acreditar que suas habilidades são fixas.

Pronto para atingir o próximo nível da sua carreira? Confira o capítulo 6 para aprender como.

Foco na visão do futuro

Como qualquer grande iniciativa de TI, a virtualização de redes muda muitas coisas no data center. Mas uma coisa que não muda é a sua segurança no emprego. Profissionais de rede são essenciais para o sucesso de um ambiente de rede virtualizado. Não é possível atingir sucesso sem eles.

Ao fazer parte de uma iniciativa de virtualização de redes, você tem a oportunidade de participar e de contribuir para a transformação da rede e da segurança em sua empresa. O resultado será benéfico para você, assim como para quem trabalhou e construiu suas carreiras em virtualização computacional. Aceite esta importante oportunidade de liderança.

DICA

Ao virtualizar e automatizar a infraestrutura, você estará livre para trabalhar em iniciativas mais interessantes e estratégicas. Por exemplo, em vez de passar o tempo no trabalho rotineiro de configurar um roteador ou atualizar regras de firewall, é possível trabalhar no design de uma rede spine-leaf, automatizar fluxos de trabalho de segurança e de rede ou talvez construir uma nuvem de desenvolvedor.

A participação em uma iniciativa de virtualização de redes irá enriquecê-lo profissionalmente, prepará-lo para o futuro e torná-lo mais valioso no mercado de trabalho, assim como a virtualização de servidores fez para os administradores de servidores há uma década atrás.

LEMBRE-SE

A virtualização de redes desenvolve sua carreira, permitindo que você passe mais tempo em arquitetura de rede, design e engenharia de tráfego:

- **Ao implementar a virtualização de redes, você não perderá seu emprego para um sistema automatizado.** Em vez disso, seu emprego será transformado para permitir que você trabalhe em projetos mais interessantes e estratégicos.
- **Seu emprego não irá para a equipe de virtualização.** O NSX Data Center usa os mesmos conceitos e tecnologias de rede que as redes físicas, por isso requer experiência em rede e segurança.
- **A virtualização não dificultará seu trabalho.** A sobreposição virtual, combinada com a automação e uma base física simplificada, simplifica o aprovisionamento e o gerenciamento da rede.

Para obter mais informações sobre a operacionalização da virtualização de redes, confira a biblioteca dos recursos do NSX Dia 1 em `www.vmware.com/go/runnsx`.

NESTE CAPÍTULO

- Destaque de recursos repletos de informações valiosas
- Teste do NSX Data Center
- Implantação do NSX Data Center em seu ambiente

Capítulo 6
Dez (ou em torno de) maneiras de começar uma virtualização de redes

Este capítulo informa o que você sempre quis saber sobre a introdução à virtualização de redes, mas teve receio de perguntar. Aqui, forneceremos uma biblioteca de recursos sobre a virtualização de redes, destacando oportunidades para implantar a plataforma VMware NSX Data Center com a infraestrutura da Cisco e explicaremos como o NSX Data Center foi projetado para integração com sua infraestrutura existente e soluções de terceiros para serviços de rede, tais como dispositivos de balanceamento de carga e firewalls de próxima geração.

O capítulo começa com uma visão geral sobre alguns dos recursos disponíveis para ajudá-lo a compreender a virtualização de redes, os componentes de uma rede virtualizada e as ferramentas disponíveis para ajudá-lo a começar.

Noções básicas

A VMware oferece uma ampla variedade de recursos para ajudá-lo a entender os fundamentos da virtualização de redes:

- **Vídeo de introdução ao VMware NSX Data Center** (`https://youtu.be/gqcwJEhIiqs`): Este rápido vídeo de três minutos explica como o NSX Data Center serve como base para uma plataforma de virtualização de redes que fornece o modelo operacional de uma máquina virtual.
- **Página do produto VMware NSX Data Center** (`www.vmware.com/go/nsx`): A página do produto NSX Data Center resume os recursos básicos, as funções e os benefícios da plataforma NSX Data Center. Ela também serve como um portal com links para uma ampla variedade de ativos com mais detalhes, incluindo informações técnicas e conteúdo focado em empresas.
- **Canal do VMware NSX no YouTube** (`www.youtube.com/vmwarensx`): O canal do NSX no YouTube fornece uma ampla variedade de vídeos, visões gerais animadas, histórias de clientes, orientações básicas e curtas, produtos em mais detalhes e muito mais.
- ***Microssegmentação para Leigos*** (`http://learn.vmware.com/41021_REG`): Este e-book fornece uma visão detalhada do caso de uso da microssegmentação para a virtualização de redes, incluindo o básico sobre como ela funciona, as tecnologias envolvidas e os amplos benefícios de segurança. Aprenda a desenvolver um data center inerentemente seguro que ajuda a impedir a propagação lateral de ataques no interior do seu data center.

Compreensão mais profunda

A VMware também oferece uma ampla variedade de recursos técnicos para ajudá-lo a entender a um nível mais aprofundado:

- **VMware NSX Data Center para o guia de design de virtualização de redes do vSphere** (`https://communities.vmware.com/docs/DOC-27683`): Para ter acesso a um material técnico realmente aprofundado, baixe o guia de design. Este documento é voltado para arquitetos de virtualização e de rede interessados em implantar a solução de virtualização de redes

do NSX Data Center em um ambiente vSphere. Este guia inclui informações detalhadas sobre o NSX Data Center para componentes funcionais, serviços funcionais e considerações de design do vSphere.

- **Guia inicial do NSX Data Center para vSphere** (`https://communities.vmware.com/docs/DOC-27705`): Este recurso fornece exemplos passo a passo que demonstram como configurar serviços de rede no NSX Data Center para vSphere, incluindo o seguinte:
  - Switches lógicos
  - Roteadores lógicos distribuídos
  - Firewalls distribuídos
  - Roteadores lógicos centralizados (borda) com roteamento dinâmico e com Tradução de Endereços de Rede (NAT, Network Address Translation) muitos para um
  - Balanceadores de carga lógicos (borda)
- **Guia de design de referência do VMware NSX-T Data Center** (`https://communities.vmware.com/docs/DOC-37591`): Este guia de design não pressupõe familiaridade com o NSX Data Center para vSphere e trata o conhecimento da plataforma de forma independente. Este guia inclui informações detalhadas sobre implantações novas de nó de borda e design de cluster, cobrindo implantações ESVi multi-vCenters (incluindo apenas designs de máquina virtual baseada em kernel [KVM, Kernel-based Virtual Machine]).
- **Guias dos dias 1 e 2 do VMware Press NSX Data Center** (`www.vmware.com/go/runnsx`): Nossos especialistas publicaram e-livros sobre tópicos essenciais de rede e de segurança para ajudá-lo a começar a usar o NSX Data Center:
  - *Dia 1 de microssegmentação do NSX*
  - *Dia 2 de microssegmentação do NSX*
  - *Criação de nuvens e data centers com tecnologia do VMware NSX para empresas de pequeno e médio porte*
  - *Operacionalização do VMware NSX*
  - *Automação do NSX para o vSphere com o PowerNSX*

  Novos e-livros são publicados trimestralmente, por isso, confira periodicamente os novos tópicos.

- **Blog de virtualização de redes** (`http://blogs.vmware.com/networkvirtualization`): Confira este blog para tudo, desde as últimas notícias até conhecimentos técnicos profundos e dicas sobre virtualização de redes. Ele serve como uma fonte importante do setor para notícias precisas e informações factuais sobre a virtualização de redes.

NSX Data Center em laboratórios práticos

Para conhecer melhor uma plataforma como o NSX Data Center, sempre ajuda experimentar antes:

- **Laboratório prático do VMware NSX** (`www.vmware.com/products/nsx/nsx-hol.html`): Os laboratórios práticos da VMware oferecem um ambiente de desktop em tempo real totalmente operacional para você experimentar produtos VMware sem a necessidade de configuração. Com a orientação por clique e todos os produtos pré-instalados, você pode se concentrar nos recursos do produto que são mais importantes para você. Essa é uma ótima maneira de conhecer de perto os recursos do NSX Data Center sem instalar nenhum software em seu sistema.

  Eis alguns exemplos dos laboratórios práticos neste site:

  - Laboratório de introdução ao VMware NSX Data Center
  - VMware NSX Data Center - firewall distribuído com microssegmentação
  - Introdução ao vRealize Network Insight
  - Laboratório avançado do VMware NSX Data Center
  - Horizon e NSX Data Center para o setor de saúde
  - Introdução ao NSX-T Data Center

Visibilidade

Você não pode proteger o que não consegue ver. Entenda quais aplicativos estão se comunicando uns com os outros com o Virtual Network Assessment (VNA, `www.vmware.com/go/vna-field`), o qual impulsiona o produto VMware Network Insight. Receba informações dentro de 24 horas. O VNA irá:

- Mostrar sua distribuição de tráfego de rede por tipo (leste-oeste, Internet, roteado, máquina virtual para máquina virtual) e por serviços (web, banco de dados, intermediários, infraestrutura).
- Fornecer uma amostra das recomendações de microssegmentação acionáveis do NSX Data Center para sua rede.
- Ressaltar suas oportunidades para otimizar o desempenho da rede com o NSX Data Center.

Como implantar o NSX Data Center em seu ambiente

Quando estiver pronto para investigar suas opções de implantação, comece aprendendo sobre a virtualização de redes e o NSX Data Center por meio de recursos sob demanda. A VMware oferece várias maneiras de conhecer os benefícios da virtualização de redes e do NSX Data Center, desde cursos on-line, seminários on-line ao vivo, até cursos individualizados sob demanda.

Comece sua jornada aprendendo sobre os fundamentos da virtualização de redes e os desafios empresariais que o NSX Data Center pode ajudá-lo a solucionar. Depois disso, você poderá fazer um curso individualizado sob demanda que fornecerá uma amostra de como instalar, configurar e gerenciar o NSX Data Center. Para obter mais informações, confira o seguinte:

- **Coursera (gratuito;** `http://vmware.com/go/coursera`**):** Continue sua formação em "Arquitetura de segurança e de rede com o VMware NSX" no Coursera. Este curso on-line gratuito dá aos alunos informações sobre a virtualização de redes básica com o VMware NSX Data Center. Para aproveitar ao máximo esse curso, você deverá estar familiarizado com os conceitos genéricos de TI de roteamento, switching, firewall, recuperação de desastres, continuidade de negócios, nuvem e segurança.
- **Fundamentos da virtualização de redes** (`https://mylearn.vmware.com/mgrreg/courses.cfm?a=det&id_course=240782&ui=www_edu`): Comece com um curso on-line individualizado de três horas que lhe dará uma compreensão fundamental da rede virtual e dos desafios empresariais que ela soluciona.

- **Certificação em virtualização de redes** (`https://mylearn.vmware.com/mgrReg/plan.cfm?plan=48389&ui=www_edu`): Avalie seu nível de habilidade projetando, implementando e gerenciando um ambiente do NSX Data Center. Você pode encontrar o seguinte:
  - **VMware NSX: Instalar, configurar, gerenciar:** Um curso de cinco dias no qual você aprende como usar switching e roteamento lógicos, serviços de gateway, configurações de firewall e serviços de segurança.
  - **VMware NSX: Projetar e implantar:** Um curso de cinco dias que o prepara para liderar projetos de design e de implantação do NSX Data Center, dando-lhe uma compreensão de processos e estruturas gerais de design.
  - **VMware NSX:** Solução de problemas e operações: Um curso no qual você aprende como isolar problemas e identificar resoluções através de um processo sistemático.
  - **VMware NSX para especialistas em redes - curso acelerado:** Um curso para aqueles que já possuem uma certificação Cisco Certified Internetwork Expert (CCIE). Você aprenderá o que o NSX Data Center tem em comum com as funções de virtualização de uma infraestrutura baseada em Cisco em arquiteturas de acesso de agregação de núcleos tradicionais e spine-leaf.

Implantação do NSX Data Center em sua infraestrutura de rede existente

O NSX Data Center foi projetado para ser executado em qualquer hardware de rede e, na maioria dos casos, ele também se integra para unir os mundos físico e virtual usando a funcionalidade de gateway de nível 2. Essas integrações reconhecem que, no ambiente hiperdinâmico do data center moderno, a rede de transporte subjacente e as soluções de virtualização de redes de sobreposição são atores codependentes no que diz respeito ao desempenho, à confiabilidade e ao dimensionamento ideais.

Para possibilitar essas integrações, a VMware trabalha ativamente com seus parceiros de switching de nível 2 para criar arquiteturas de referência e guias de design para usar o NSX Data Center como uma sobreposição ágil que aproveita os recursos da infraestrutura subjacente.

Veja uma amostra dos recursos técnicos disponíveis para guiar a integração do NSX Data Center com sua infraestrutura de rede existente:

- **Arista:** Guia de design de referência de virtualização de redes VMware e Arista para ambientes VMware vSphere (`https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-arista-nsx-design-guide.pdf`)
- **Cisco 9K:** Design de referência: Implantação do NSX com o Cisco UCS e a Infraestrutura Nexus 9000 (`https://communities.vmware.com/docs/DOC-29373`)
- **Dell:** Virtualização de redes com infraestrutura Dell e Arquitetura de Referência VMware NSX (`https://communities.vmware.com/docs/DOC-27684`)
- **Juniper:** Conexão de redes físicas e virtuais com plataformas VMware NSX e Juniper (`https://communities.vmware.com/docs/DOC-27610`)

Integração com parceiros do ecossistema de serviços de rede

Além de se integrar à infraestrutura de rede existente, o NSX Data Center foi projetado para integrar-se a soluções para vários serviços de rede, como dispositivos de balanceamento de carga e firewalls e serviços de próxima geração:

- **Serviços físicos a virtuais do data center:** Arista Networks, Rede aberta EMC da Dell, Extreme Networks, HPE, Huawei, Juniper Networks
- **Serviços de segurança:** Bitdefender, CA Technologies, Check Point, ESET, Fortinet, HyTrust, Juniper Networks, Kaspersky, McAfee, Palo Alto Networks, Symantec, Trend Micro
- **Operações e visibilidade do data center definido por software (SDDC):** AlgoSec, Dell EMC, Firemon, ForeScout, Gigamon, NetScout, RedSeal, Riverbed, Skybox, Tufin

DICA

Para obter uma lista atualizada de parceiros e recursos da tecnologia VMware, acesse `www.vmware.com/products/nsx/technology-partners.html`.

Faça a virtualização de redes funcionar para você

De muitas maneiras, a rede está presa em um passado com cabos. Com as abordagens convencionais para a rede, os serviços ainda exigem aprovisionamento manual e estão ancorados em hardware específico de fornecedores. Essa maneira antiga de fazer as coisas aumenta o tempo de implantação do aplicativo e bloqueia o caminho para o data center definido por software. A virtualização de redes altera isso. As redes virtualizadas são criadas, aprovisionadas e gerenciadas inteiramente em software, trazendo novos níveis de agilidade, eficiência e segurança às operações do data center.

Dentro...

- Saiba o que é a virtualização de redes
- Veja como ela difere das arquiteturas de rede convencionais
- Descubra como a virtualização de redes pode ajudar você a operar com mais eficiência
- Entenda a arquitetura e as melhores práticas

vmware®

Jonathan Morin trabalha há mais de 15 anos com redes, projetando redes de provedores de serviços e desenvolvendo produtos de rede em data centers e campi. Ele é graduado pela UNH e tem MBA pela UC Berkeley Haas.

Shinie Shaw tem mais de 5 anos de experiência em redes com Cisco e VMware e 10 anos em indústrias reguladas. Ela é graduada pela Northwestern University e tem MBA pela UC Berkeley Haas.

Acesse Dummies.com®
para ver vídeos, fotos passo a passo, artigos how-to ou para fazer compras!

ISBN: 978-1-119-59683-7

para leigos®

Também disponível como e-book

WILEY END USER LICENSE AGREEMENT

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