VMWARE NSX

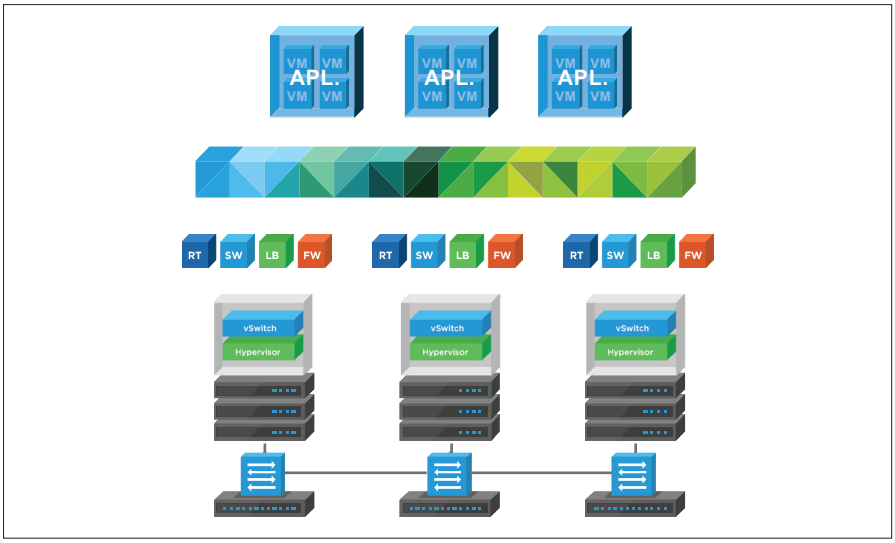
A plataforma de virtualização de redes e segurança

VISÃO GERAL

O VMware NSX® é a plataforma de virtualização de redes e segurança do data center definido por software (SDDC, Software-Defined Data Center), que leva o modelo operacional da máquina virtual para redes inteiras. Com o NSX, as funções de rede, como switch, roteamento e firewall, são incorporadas ao hypervisor e distribuídas em todo o ambiente. Isso cria efetivamente um "hypervisor de rede" que funciona como uma plataforma para sistemas de redes virtuais e serviços de segurança. De maneira semelhante ao modelo operacional de máquinas virtuais, as redes virtuais são aprovisionadas programaticamente e gerenciadas sem depender do hardware subjacente. O NSX reproduz todo o modelo de rede no software, permitindo que qualquer topologia de rede (de redes simples a complexas com diversas camadas) seja criada e aprovisionada em segundos. Os usuários podem criar várias redes virtuais com diversos requisitos, aproveitando uma combinação dos serviços que o NSX oferece para desenvolver ambientes inerentemente mais seguros.

PRINCIPAIS BENEFÍCIOS

- Microssegmentação e segurança detalhada fornecidas à carga de trabalho individual
- Redução do tempo de aprovisionamento de rede de dias para segundos e eficiência operacional aprimorada por meio de automação
- Mobilidade de carga de trabalho independente da topologia da rede física em todos os data centers
- Segurança aprimorada e serviços avançados de sistema de rede em um ecossistema de fornecedores externos líderes do setor



Virtualização de redes, segurança e SDDC

O VMware NSX fornece um modelo operacional totalmente novo para o sistema de rede que estabelece a base do data center definido por software. Como o NSX cria redes no software, os operadores de data center podem atingir níveis de agilidade, segurança e economia que não eram possíveis com as redes físicas. O NSX oferece um conjunto completo de serviços e elementos lógicos de sistema de rede que incluem switch, roteamento, firewall, balanceamento de carga, VPN, qualidade de serviço (QoS, Quality of Service) e monitoramento lógicos. Esses serviços são aprovisionados em redes virtuais por qualquer plataforma de gerenciamento de nuvem que utiliza as interfaces de programação de aplicativos do NSX. As redes virtuais são implantadas continuamente em qualquer hardware de sistema de rede existente.

Recursos principais do NSX

Alternância	Ative extensões lógicas de sobreposição de camada 2 em uma malha roteada (L3) nos limites do data center. Suporte para sobreposições de rede baseadas em VXLAN.
Roteamento	Roteamento dinâmico entre redes virtuais executado de maneira distribuída no kernel do hypervisor, roteamento de dimensionamento horizontal com failover ativo-ativo com roteadores físicos. Compatível com protocolos de roteamento estático e dinâmico (OSPF, BGP).
Firewall distribuído	Firewall sem estado distribuído, incorporado ao kernel do hypervisor, para até 20 Gbps da capacidade do firewall por host do hypervisor. Suporte a Active Directory e monitoramento de atividades. Além disso, o NSX também pode fornecer um recurso de firewall norte-sul por meio do NSX Edge™.

Balanceamento de carga	Balanceador de carga L4–L7 com transferência de SSL e passagem direta, verificações de integridade do servidor e regras de aplicativo para programabilidade e manipulação de tráfego.
VPN	Recursos de site a site e VPN de acesso remoto, VPN não gerenciada para serviços de gateway em nuvem.
Gateway do NSX	Suporte a pontes de VXLAN a VLAN para conexão contínua a cargas de trabalho físicas. Esse recurso é nativo ao NSX e fornecido por switches top of rack de um parceiro do ecossistema.
API do NSX	Interface de programação de aplicativos (API) do RESTful para integração com qualquer plataforma de gerenciamento de nuvem ou automação personalizada.
Operações	Recursos de operações nativas, como interface central de linha de comando, traceflow, SPAN e IPFIX, para solucionar problemas e monitorar a infraestrutura proativamente. Integração com ferramentas, como VMware vRealize® Operations™ e vRealize Log Insight™, para técnicas de análise avançadas e solução de problemas. O NSX Application Rule Manager e o Endpoint Monitoring permitem a visualização completa do fluxo de tráfego de rede para a Camada 7, permitindo que as equipes de aplicativos identifiquem endpoints do data center intra e inter e respondam criando as regras de segurança apropriadas.
Microssegmentação com reconhecimento de contexto	O NSX permite que grupos dinâmicos de segurança sejam criados e que as políticas associadas baseiem-se em fatores que vão além de endereço IP e MAC, incluindo objetos e marcas do VMware vCenter™, tipo de sistema operacional e informações de aplicativos de camada 7 para permitir a microssegmentação com base no contexto do aplicativo. A política baseada em identidade, que usa informações de login das VMs, do Active Directory e da integração do gerenciamento de dispositivos móveis, possibilita a segurança com base no usuário, incluindo segurança no nível de sessão em ambientes de desktop remoto e virtual.
Gerenciamento de nuvem	Integração nativa com o vRealize Automation™ e o OpenStack.
Integração com parceiros externos	Suporte à integração de gerenciamento, camada de controle e integração do caminho de dados com parceiros externos nas mais variadas categorias, tais como firewall de próxima geração, IDS/IPS, antivírus sem agente, controladores de fornecimento de aplicativos, switch, operações e visibilidade, segurança avançada etc.
Sistema de rede e segurança no vCenter	Amplie o sistema de rede e a segurança nos limites do vCenter e do data center, independentemente da topologia física subjacente, permitindo recursos como recuperação de desastres e data centers ativo-ativo.
Gerenciamento de logs	Acelere a resolução de problemas com a visibilidade avançada do vRealize Log Insight para NSX. Visualize tendências de eventos, dispare alertas e muito mais, tudo em tempo real.

Casos de uso

Segurança

O NSX permite que as organizações dividam o data center logicamente em segmentos de segurança distintos até o nível da carga de trabalho individual, independentemente da sub-rede ou VLAN da carga de trabalho. Em seguida, as equipes de TI podem definir políticas e controles de segurança para cada carga de trabalho com base em grupos de segurança dinâmicos, o que garante respostas imediatas a ameaças no data center e aplicação em cada máquina virtual. Ao contrário das redes tradicionais, quando um invasor consegue passar pelos perímetros de defesa do data center, as ameaças não podem se mover lateralmente.

Automação

O NSX soluciona os desafios de aprovisionamento de rede demorado, erros de configuração e processos caros, pois automatiza as tarefas trabalhosas e propensas a erros. O NSX cria redes no software, eliminando gargalos associados a redes baseadas em hardware.

A integração nativa do NSX com plataformas de gerenciamento de nuvem, como vRealize Automation ou OpenStack, permite maior automação.

Continuidade de aplicativos

Como o NSX abstrai o sistema de rede do hardware subjacente, as políticas do sistema de rede e da segurança estão anexadas às cargas de trabalho associadas. As organizações podem replicar facilmente todos os ambientes de aplicativos para data centers remotos para recuperação de desastres, movê-los de um data center corporativo a outro ou implantá-los em um ambiente de nuvem híbrida, tudo isso em questão de minutos, sem interromper os aplicativos e sem tocar na rede física.

Edições do VMware NSX

Standard

Para organizações que precisam de agilidade e automação da rede

Advanced

Para organizações que precisam da edição Standard e também de um data center fundamentalmente mais seguro com microssegmentação

Enterprise

Para organizações que precisam da edição Advanced e também de sistema de rede e segurança em vários domínios

ROBO

Para organizações que buscam virtualizar e proteger os aplicativos no escritório remoto ou na filial

SAIBA MAIS

Para obter mais informações, acesse www.vmware.com/go/nsx.

Mais detalhes sobre os recursos de edição de licenciamento do NSX podem ser encontrados em https://kb.vmware.com/kb/2145269.

Para obter informações sobre todos os produtos da VMware ou adquiri-los, ligue para 877-4VMWARE (fora da América do Norte, ligue para +1-650-427-5000), acesse o site www.vmware.com/br/products ou procure um revendedor autorizado na Internet.

	STANDARD	ADVANCED	ENTERPRISE	ROBO
Switch distribuído	•	•	•	•*
Roteamento distribuído	•	•	•	
Firewall do NSX Edge	•	•	•	•
NAT	•	•	•	•
Ponte L2 do software para ambiente físico	•	•	•	
Roteamento dinâmico com ECMP (ativo-ativo)	•	•	•	•
Automação orientada por interface de programação de aplicativos	•	•	•	•
Integração com o vRealize e o OpenStack	•	•	•	•
Gerenciamento de logs com o vRealize Log Insight para NSX	•	•	•	•
Automação de políticas de segurança com o vRealize		•	•	•
Balanceamento de carga do NSX Edge		•	•	•
Firewall distribuído (incluindo integração com o Active Directory)		•	•	•
Monitoramento de atividade dos servidores		•	•	•
Inserção de serviços (integração de terceiros)		•	•	•
Integração com o VMware AirWatch®		•	•	•
Application Rule Manager		•	•	•
No vCenter NSX			•	
Otimizações de vários sites do NSX			•	
VPN (IPSEC e SSL)			•	•
Gateway remoto			•	
Integração com endpoints de túnel de VXLAN (VTEPs, VXLAN Tunnel EndPoint) de hardware			•	
Monitoramento de endpoint			•	
Firewall distribuído com camada 7			•	

*Baseado em VLAN

vmware®

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