VMWARE NSX CLOUD

Sistema de rede e segurança consistentes para aplicativos executados de forma nativa nas nuvens públicas

VISÃO GERAL

O VMware NSX® Cloud oferece sistema de rede e segurança consistentes para aplicativos executados de forma nativa em nuvem pública. O NSX Cloud usa a mesma camada de gerenciamento e controle que o NSX Data Center, possibilitando uma única solução de sistema de rede e segurança, desde o data center privado até a nuvem pública.

PRINCIPAIS BENEFÍCIOS

Sistema de rede e segurança comuns, em nuvens públicas como AWS e Azure, melhoram significativamente o dimensionamento, o controle e a visibilidade, com OpEx reduzido.

- Dimensionamento simples em redes virtuais, zonas de disponibilidade, regiões e nuvens públicas.
- Controle preciso de serviços de segurança e sistema de rede trazem proteção e padronização aos aplicativos.
- Visibilidade completa de sistema de rede e segurança garante a integridade e a conformidade de aplicativos em nuvens públicas.

PREÇOS

- Assinatura com base em preço, disponível em licenças temporárias de 1 e de 3 anos.
- Baseado em vCPUs com consumo de cargas de trabalho ativas dentro da nuvem pública, independentemente do número de redes virtuais (como AWS VPCs, Azure VNets).
- A licença do NSX Data Center não é obrigatória para casos de uso exclusivos de nuvem.

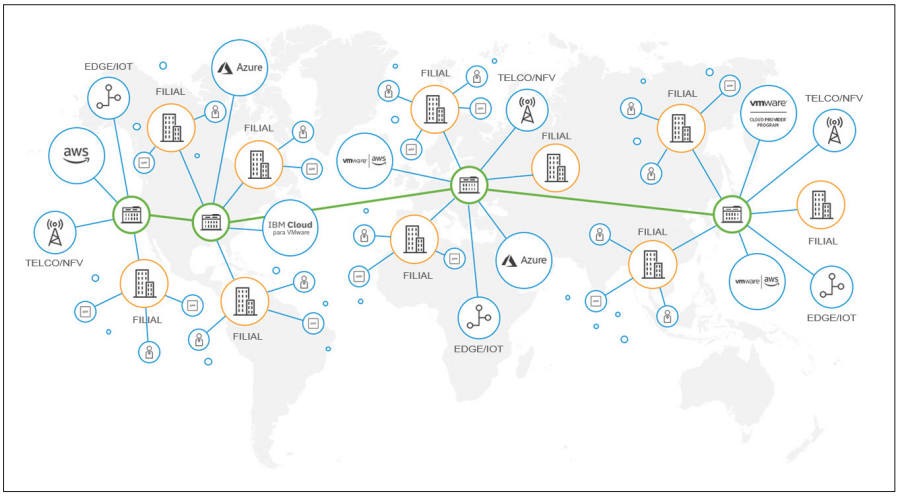

Figura 1: Virtual Cloud Network

Uma rede construída para os princípios da nuvem

O VMware NSX Cloud oferece sistema de rede e segurança consistentes para seus aplicativos executados de forma nativa em nuvens públicas. Juntamente com a família do VMware NSX, o VMware NSX Cloud habilita o Virtual Cloud Network, uma abordagem definida por software para o sistema de rede que se estende pelos data centers, nuvens, endpoints e objetos.

Casos de uso

Segurança consistente entre nuvens

O NSX Cloud capacita políticas em cargas de trabalho executadas em múltiplas nuvens públicas. O NSX Cloud aproveita a mesma camada de controle e caminho de dados que o NSX Data Center, habilitando o gerenciamento de políticas de ponta a ponta em data centers e nuvens. A política é definida uma vez e aplicada a cargas de trabalho em qualquer lugar: em redes virtuais de nuvem, regiões, zonas de disponibilidade e vários provedores de nuvem. As políticas de segurança são aplicadas dinamicamente a cada carga de trabalho baseada em atributos de aplicativo e marcas definidas pelo usuário. Cargas de trabalho não autorizadas ou comprometidas podem ser colocadas em quarentena automaticamente se elas não tiverem a política correta de segurança de microssegmentação aplicada.

Controle preciso sobre o sistema de rede da nuvem

O VMware NSX Cloud foi projetado para ambientes de nuvem pública como o Amazon (AWS) e o Microsoft Azure. O NSX Cloud complementa os serviços nativos disponibilizados pelos provedores de nuvem pública. Com o NSX Cloud, é possível continuar a usar a infraestrutura do provedor de nuvem pública e os serviços de aplicativo para cargas de trabalho sem limitações (como AWS ELB/balanceador de carga do Azure, AWS Route53/Azure DNS, AWS Direct Connect/Azure ExpressRoute e Amazon RDS/banco de dados do Azure). O aprovisionamento e o gerenciamento da configuração podem ser automatizados via solicitações de API REST utilizando suas ferramentas existentes de automação.

PARA OBTER MAIS INFORMAÇÕES OU ADQUIRIR OS PRODUTOS VMWARE

LIGUE PARA

877-4-VMware (fora da América do Norte, ligue para +1-650-427-5000),

ACESSE O SITE

www.vmware.com/br/products/nsx-cloud.html ou http://www.vmware.com/br/products para pesquisar um revendedor autorizado on-line.

Controle e visibilidade operacional completos

O VMware NSX Cloud oferece interfaces e protocolos padrão para acessar os dados de rede e segurança das redes em nuvem. Informações de fluxo, pacote e evento estão disponíveis via IPFIX, Traceflow, espelhamento de porta e Syslog. Esses dados podem ser consumidos por ferramentas de operações no local existentes e utilizados para permitir a visibilidade aprofundada e completa para monitoramento, solução de problemas e auditoria. Os dados avançados de operação ajudam a encurtar drasticamente o tempo necessário para identificar e resolver problemas de conectividade de rede, desempenho e segurança em toda a implantação de nuvem híbrida, incluindo aplicativos no local e na nuvem pública.

Principais recursos

Sistema de rede e segurança multi-cloud, em vários locais: O NSX Cloud traz recursos de sistema de rede e segurança a endpoints em várias nuvens e, ao integrar-se com o NSX Data Center, habilita o gerenciamento de sistema de rede e segurança em locais de nuvem e data center.

Microssegmentação: Controle sobre o tráfego leste-oeste entre as cargas de trabalho de aplicativos sendo executados nativamente nas nuvens públicas.

Grupos de segurança: As regras e os grupos de segurança podem ser definidos com base em conceitos avançados de políticas, como nome de instância, tipo de sistema operacional, ID de AMI e marcas definidas pelo usuário.

Política dinâmica: A política de segurança é aplicada automaticamente e reforçada com base nos atributos de instância e nas marcas definidas pelo usuário. As políticas seguem as instâncias automaticamente quando estas são movidas dentro das nuvens e entre as nuvens.

Instâncias em quarentena: Coloque em quarentena as cargas de trabalho comprometidas e não autorizadas que estejam em execução na nuvem pública sem a segurança da microssegmentação. As instâncias em quarentena não podem se comunicar na rede da nuvem.

Arquitetura distribuída: A arquitetura distribuída de firewall do NSX Cloud elimina o tráfego e os saltos de rede adicionais, porque as políticas são aplicadas à interface de rede virtual de cada instância, em vez de roteadas pelo firewall externo.

Firewall do Edge: O NSX Cloud proporciona firewall sem estado que filtra o tráfego norte-sul que flui entre as instâncias nas redes virtuais e na internet pública.

API RESTful: API RESTful e ferramentas de automação para aprovisionar e configurar de modo programático a infraestrutura de segurança e de sistema de rede sob demanda.

Criação de templates: Use as ferramentas existentes de automação e orquestração para criar templates padronizados de aplicativos e simplificar o aprovisionamento e o gerenciamento dos serviços de segurança e sistema de rede nas nuvens públicas.

Visibilidade do tráfego leste-oeste: Use as ferramentas existentes de operações do segundo dia para obter visibilidade do tráfego leste-oeste dentro dos VPCs.

Registro de segurança em log: Visibilidade e auditoria em tempo real dos eventos de segurança, como incidentes de permissão/recusa e quarentena. Envie as informações sobre os eventos de segurança para um servidor Syslog ou SIEM.

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