VMware NSX for Horizon

RESUMO GERAL

O VMware NSX™ for Horizon® traz velocidade e simplicidade para a rede de VDI. Em segundos, os administradores de TI podem criar políticas que acompanham desktops virtuais de forma dinâmica, sem a necessidade de um demorado aprovisionamento de rede. Estendendo a política de segurança do data center para o desktop e o aplicativo, essa solução conjunta também fornece uma plataforma extensível que se integra às principais soluções de segurança do setor.

BENEFÍCIOS

- Aumente a segurança de desktops virtuais que residem em meio a outras cargas de trabalho do data center.
- Simplifique e agilize a administração da rede e da política de segurança para usuários com base em agrupamento lógico, função ou tag.
- Associe automaticamente a política a um desktop assim que ele é criado, acompanhando a VM independentemente da infraestrutura subjacente.
- Integre às principais soluções do setor para antivírus, malware, prevenção contra intrusões e serviços avançados de segurança.

Rede e segurança para desktops virtuais e aplicativos: rápidas, fáceis e extensíveis

Muitas organizações implementam a virtualização de desktops e aplicativos para melhorar a segurança da computação do cliente e oferecer maior mobilidade corporativa. A centralização de desktops e aplicativos protege dados estáticos, impede o acesso não autorizado a aplicativos e fornece um modo mais eficiente de aplicar patches, fazer a manutenção e o upgrade de imagens.

No entanto, com a virtualização de desktops e aplicativos, novas preocupações de segurança podem surgir com relação ao firewall do data center, onde residem centenas ou até milhares de desktops. Esses desktops ficam perto de outros usuários e cargas de trabalho essenciais, deixando-os muito mais suscetíveis a malware e outros ataques. Esses ataques podem se mover do desktop para o servidor, expondo uma grande superfície de ataque no data center. O cenário de ameaças "leste-oeste" é um cenário comum que afeta muitos clientes hoje em dia, principalmente aqueles com rígidos requisitos de segurança e conformidade.

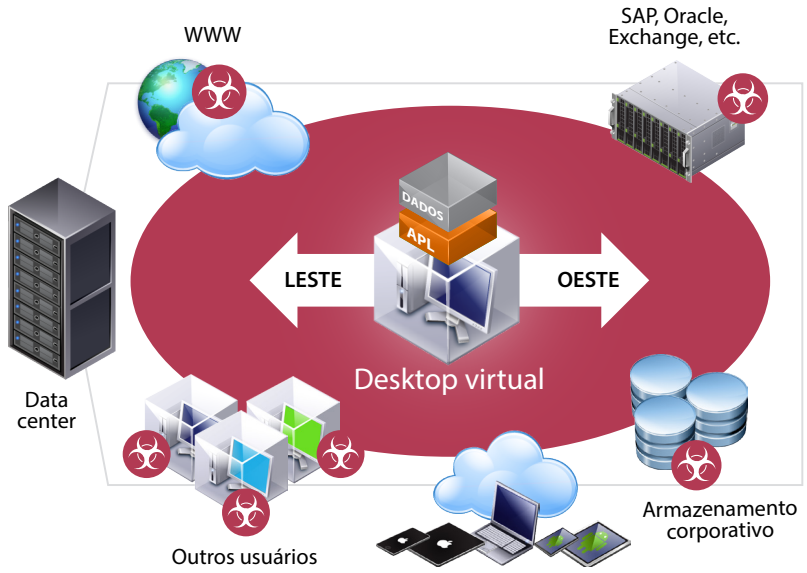

Figura 1: preocupações de segurança no cenário leste-oeste no data center

As organizações que buscam administrar a rede e a política de segurança e acompanham de forma persistente usuários e cargas de trabalho também costumam investir significativamente em uma arquitetura centralizada em hardware que gera muitas despesas de capital, é complexa de operar e lenta para se adaptar ao típico ambiente de negócios dinâmico.

VMware NSX for Horizon

O VMware NSX for Horizon protege com eficiência o tráfego leste-oeste no data center, além de garantir que a equipe de TI possa administrar com rapidez e facilidade a rede e a política de segurança que acompanha de forma dinâmica os desktops virtuais e aplicativos dos usuários finais em infraestruturas, dispositivos e locais diferentes.

Figura 2: o NSX for Horizon oferece rede e segurança de VDI rápidas, fáceis e extensíveis

Com essa solução, as organizações aproveitam os benefícios da rapidez e da simplicidade da segurança e da rede de VDI. Em segundos, os administradores de TI podem criar políticas que acompanham desktops virtuais de forma dinâmica, sem a necessidade de um demorado aprovisionamento de rede.

Estendendo a política de segurança do data center para desktops e aplicativos, essa solução também fornece uma plataforma extensível que pode se integrar ao ecossistema da VMware de parceiros de segurança líderes do setor para fornecer aos clientes defesa avançada para proteger o desktop inteiro.

Como funciona

O VMware NSX for Horizon melhora a segurança da virtualização de desktops e ajuda a combater as ameaças do tráfego leste-oeste, permitindo que os administradores definam a política de forma centralizada. Essa política é distribuída para a camada do hypervisor em cada host do vSphere e associada automaticamente a cada desktop virtual assim que o desktop é criado. Para proteger desktops virtuais e cargas de trabalho adjacentes no data center, o VMware NSX implementa a "microssegmentação", fornecendo a cada desktop a defesa do seu próprio perímetro. Essa "segurança enxuta" usa o recurso de firewall virtual distribuído do VMware NSX para policiar o tráfego de entrada e saída de cada VM, eliminando o acesso não autorizado entre desktops e cargas de trabalho adjacentes. Se o desktop virtual for movido de um host para outro, ou no data center, a política irá acompanhá-lo automaticamente.

Recursos e benefícios

O VMware NSX for Horizon proporciona agilidade e simplicidade à rede de VDI com uma política de segurança que acompanha dinamicamente os usuários finais em qualquer infraestrutura, dispositivo e local.

Rede de VDI rápida e simples

Com o VMware NSX for Horizon, os administradores podem criar, alterar e gerenciar políticas de segurança em todos os desktops virtuais com apenas alguns cliques. As políticas de segurança podem ser mapeadas rapidamente para grupos de usuários para agilizar a integração do desktop virtual. Com a possibilidade de implantar funções de rede virtualizada (como alternância, roteamento, aplicação de firewall e balanceamento de carga), os administradores podem criar redes virtuais para VDI sem a necessidade de complexas VLANs, ACLs ou sintaxe de configuração de hardware.

Política automatizada que acompanha usuários finais e desktops de forma dinâmica

Os administradores podem definir políticas que se adaptam de forma dinâmica ao ambiente de computação do usuário final, com serviços de segurança de rede que são mapeados para o usuário com base em função, agrupamento lógico, sistema operacional do desktop e muito mais, independentemente da infraestrutura de rede subjacente. A política administrada de forma centralizada é associada automaticamente a cada VM do desktop assim que o desktop é criado. Dessa forma, as organizações podem se expandir com confiança, contando com uma segurança que acompanha com persistência o desktop virtual no data center.

Plataforma de segurança avançada

O VMware NSX oferece uma plataforma extensível que pode ser integrada aos melhores recursos do setor em um ecossistema estabelecido de parceiros de segurança. Adicionando serviços de forma dinâmica, a segurança do desktop virtual pode ser estendida do data center ao desktop e ao aplicativo. Esse ecossistema de parceiros, incluindo Trend Micro, Intel Security e Palo Alto Networks, oferece soluções que protegem o sistema operacional, o navegador, o e-mail e muito mais, com antivírus, malware, prevenção contra intrusões e serviços de segurança avançados.

Saiba mais

Para obter mais informações sobre o Horizon e o VMware NSX, acesse o site da VMware e siga-nos no Twitter.

Recursos do VMware Horizon

Web: http://www.vmware.com/br/products/horizon-view

Blog: http://blogs.vmware.com/euc/

Twitter: @VMwareHorizon

Recursos do VMware NSX

Web: http://www.vmware.com/br/products/nsx/

Blog: http://blogs.vmware.com/networkvirtualization/

Twitter: @VMwareNSX

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Rua Surubim, 504 4º andar CEP: 04571-050 Cidade Monções – São Paulo – SP Tel: +55 11 5509 7200 www.vmware.com/br