RESUMO EXECUTIVO: QUATRO OBSTÁCULOS PARA A OBTENÇÃO DA SEGURANÇA EM NUVEM PÚBLICA/PRIVADA

Análise das armadilhas de segurança que ameaçam os ambientes virtuais atuais

Resumo

A virtualização e as arquiteturas em nuvem podem reduzir os custos e aumentar a eficiência e a agilidade operacional, mas enfrentam ameaças como malware cada vez maiores. A área de TI deve aplicar orçamentos limitados para proteger os ambientes em nuvem pública/privada das armadilhas comuns de segurança, incluindo:

- Incapacidade de visualização do tráfego dentro da VM
- Proliferação de políticas
- Proliferação virtual
- Restrições em nuvens pública

Iniciativas de negócio que estão impulsionando a migração para a virtualização

Diante dos mercados em rápida evolução, da concorrência feroz e de um ambiente de negócio acelerado, as organizações devem proteger a participação no mercado e também crescer. Mais do que nunca, a tecnologia da informação desempenha um papel central.

No "back-end", espera-se que a área de TI acompanhe as inovações tecnológicas, modernize os data centers e o ambiente de TI e otimize os serviços de TI para posicionar a organização para o sucesso. Isso inclui projetar, implementar e novas aplicações que capacitem os negócios corporativos, ferramentas e serviços de produtividade de usuários e arquiteturas de rede, como computação em nuvem pública/privada/híbrida, virtualização de funções de rede (NFV) e mobilidade. Igualmente importante, a área de TI também deve oferecer suporte e proteger esse ambiente de rede dinâmico e a equipe de trabalho móvel com um orçamento uniforme, se não reduzido.

No "front-end", a área de TI deve ter êxito em garantir que os engajamentos na Web, os serviços e o suporte da empresa estejam on-line 24 horas por dia, 7 dias por semana, 365 dias por ano. Isso envolve manter todas as propriedades da Web da organização seguras, sem interrupções e com seu melhor desempenho. A área de TI busca uma defesa de segurança acessível e inflexível. Isso exige uma segurança dinâmica que possa prevenir ataques

e fornecer a análise para proteção e resposta em toda a infraestrutura física e virtual da organização. A área de TI deve insistir em uma segurança flexível, seja ela com fio/wireless ou em nuvem pública/privada e de seu escritório central para seus campus remotos, filiais, subsidiárias ou ambientes de parceiros.

As vantagens e as desvantagens da virtualização

Há mais de uma década, a virtualização de servidores transformou a parte de computação da infraestrutura de TI do mundo físico para o mundo virtualizado. A virtualização ainda é proeminente hoje, pois continua avançando e aumentando os benefícios operacionais e econômicos de todo o data center, reduzindo os custos operacionais e de capital e permitindo que a equipe se concentre na infraestrutura crítica.

Os avanços contínuos nas ferramentas e nos serviços de virtualização, como a virtualização da função de rede, estão facilitando e agilizando o desenvolvimento e a colocação de cargas de trabalho virtualizadas em qualquer lugar da rede virtual (VN) pelos departamentos de TI. Além disso, a virtualização fornece para a área de TI mais recursos de autogerenciamento e programabilidade da rede, assim como a velocidade de provisionamento necessária para operar o data center com a eficiência aprimorada. Isso permite que as equipes de rede e aplicações personalizem e forneçam novos serviços e iniciem, movam, copiem, clonem, restaurem ou excluam instantaneamente os serviços hospedados em máquinas virtuais a qualquer momento para atender às necessidades operacionais específicas do seu data center. Esse nível mais alto de elasticidade e agilidade operacional reduz significativamente o custo do fornecimento de serviços de aplicações para toda a empresa.

Entretanto, apesar dessas muitas vantagens, o outro lado do uso de tecnologias de virtualização são as muitas implicações e preocupações de segurança que a área de TI deve enfrentar. (Consulte a Tabela 2 abaixo.) A virtualização, por sua própria natureza, acrescenta muitas camadas de infraestrutura e complexidade operacional. Questões como uso compartilhado de armazenamento, dispositivos de roteamento, segmentos de rede e canais de comunicação demonstraram ser vulneráveis a ataques cibernéticos, como ataques de uso indevido de recursos compartilhados, ataques a máquinas virtuais cruzadas, ataques de canal lateral e vulnerabilidades comuns de aplicações e protocolos baseados em rede. Essas ameaças atingem todas as partes da estrutura virtual, incluindo hypervisor ou monitor de máquina virtual (VMM), máquinas virtuais (VMs), sistemas operacionais (OSs) em VMs, aplicações em execução nesses OSs e os componentes de rede virtual do ambiente virtualizado. A proteção incorreta de todo o ambiente virtual pode resultar em prejuízos imensuráveis para uma organização.

Tabela 2 – Relacionamentos entre vulnerabilidades e ameaças em ambientes de virtualização da rede

Categorias de ameaças		Vulnerabilidades	Ameaças
Divulgação	Vazamento de informações	Ausência de proteção da tabela ARP	Envenenamento da tabela ARP
		Inserção de regras de firewall em nós virtuais	Subversão de regras de firewall
	Interceptação de informações	Ausência de proteção da tabela ARP	Envenenamento da tabela ARP
		Transmissão de dados em padrões previsíveis	Ataques de análise de tráfego
		Manipulação não controlada de múltiplas solicitações sequenciais de rede virtual de uma única entidade	Inferência e divulgação de informações topológicas confidenciais
		Troca desprotegida de informações de roteamento entre roteadores virtuais	Divulgação de informações confidenciais de roteamento
	Exploração de introspecção	Introspecção não controlada	Roubo de dados
Fraude	Fraude de identidade	Tratamento incorreto de identidades:	
		– em redes individuais	Injeção de mensagens maliciosas com fontes falsificadas
		– entre redes federadas	Atendimento de segundo nível de privilégios
		– durante procedimentos de migração	Abuso de remoção de nó e readição para obter novas identidades (limpas)
	Perda de entradas do registro	Operações não controladas de reversão	Perda de entradas do registro
	Ataques de reprodução	Ausência de identificadores exclusivos de mensagem	Ataques de reprodução
Interrupções	Sobrecarga dos recursos físicos	Alocação não controlada de recursos	Queda de desempenho
			Consumo abusivo de recursos
		Tratamento não controlado das solicitações da rede virtual	Esgotamento de recursos em partes específicas da infraestrutura
		Ausência de estratégias proativas ou reativas de recuperação	Ataques de negação de serviço
	Falha de recursos físicos	Ausência de estratégias proativas ou reativas de recuperação	Falha de roteadores/redes virtuais
		Realocação não controlada de recursos após falhas	Sobrecarga dos roteadores virtuais restantes após falhas
Usurpação	Fraude de identidade	Tratamento incorreto de identidades e privilégios associados	Atendimento de segundo nível de privilégios
	Exploração de vulnerabilidades do software	Atendimento de segundo nível de privilégio em monitores de máquina virtual	Controle não autorizado de roteadores físicos

Fonte: "Segurança da rede virtual: ameaças, contramedidas e desafios" (Em inglês) Journal of Internet Services and Applications, dezembro de 2015

Os danos podem incluir:

- Controle não autorizado dos sistemas virtuais para execução de ações maliciosas
- Acesso não autorizado a ativos de dados protegidos
- Roubo de informações
- Interrupção ou degradação do serviço de parte ou de todo o ecossistema virtual

A virtualização é atualmente um campo ativo de pesquisa de ameaças e vulnerabilidades na academia, programas de recompensa por bugs, hacking ético e comunidades organizadas de crimes cibernéticos. Novas ameaças são identificadas regularmente. A vulnerabilidade VENOM, CVE-2015-3456, é um desses exploits que afetam plataformas populares de virtualização, como Xen e KVM.

Por isso, a área de TI tem motivos para se preocupar intensamente com sua postura atual de segurança. Muitas organizações acreditam que o sistema de defesa atual não tem os recursos e os controles dinâmicos de segurança necessários para proteger adequadamente as infraestruturas de rede virtual de forma contínua. Isso dificulta a garantia do tempo de atividade operacional, do fornecimento e disponibilidade de serviços e da conformidade com os requisitos regulamentares para a área de TI.

Cenário prático

Para fornecer uma perspectiva mais práticas, vamos analisar um cenário no qual o ambiente virtual de uma organização reside em uma arquitetura de segurança de firewall físico. A Figura 1 (acima à direita) descreve o canal do fluxo de comunicação da VM da aplicação para a VM do banco de dados na máquina host da VM. A aplicação pode ser um Microsoft SharePoint realizando uma leitura/gravação em um banco de dados SQL. Neste cenário, a área de TI deve garantir o fornecimento seguro dos serviços da aplicação.

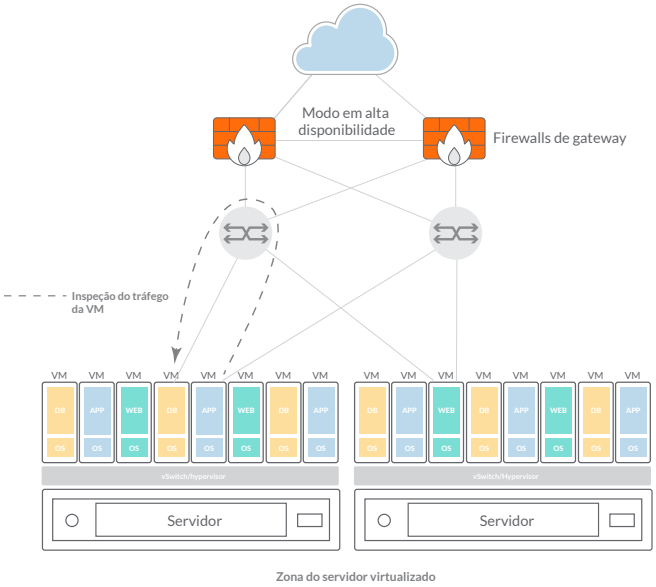

Figura 1: ambiente virtual com firewall físico

Ambiente virtual com firewall físico

A área de TI tem duas abordagens de inspeção com métodos legados. Um caminho possível é rotear o tráfego entre as VMs por meio do switch virtual (vSwitch) ao norte para a malha de roteamento externa e, em seguida, para um firewall externo que retorna o mesmo canal ao sul. O direcionamento do tráfego dessa forma apresenta muitos hops e pode causar problemas como degradação do desempenho, latência, perda de pacotes e as preocupações de controle de segurança mencionadas anteriormente. A segunda abordagem é usar um firewall baseado em software e executá-los como agentes em cada VM. Esse método apresenta desafios semelhantes, com baixo desempenho e aumento da complexidade de gerenciamento à medida que a quantidade de VMs aumenta.

Ao analisar o desafio de segurança dos firewalls físicos em um mundo dinâmico virtualizado, as armadilhas comuns que a área de TI vai enfrentar são:

1. Incapacidade de visualização do tráfego entre as máquinas virtuais
2. Proliferação de políticas
3. Proliferação virtual
4. Ambiente em nuvem pública

Incapacidade de visualização do tráfego entre as máquinas virtuais

Quando você tem dezenas de VMs comunicando-se em um sistema virtual, um firewall de perímetro físico pode não visualizar o tráfego lateral, porque o tráfego nunca pode sair desse servidor virtual devido a configurações de roteamento ou isolamentos de VM. Do ponto de vista da segurança, isso significa que o monitoramento de anomalias e eventos incomuns nesses cenários se torna impossível.

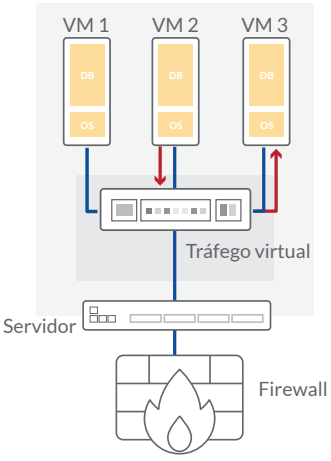

Figura 2: tráfego entre as VMs

SONICWALL®

Proliferação de políticas

Quando as propriedades virtualizadas são criadas ou movidas, muitas alterações complexas na configuração de rede são necessárias para direcionar o tráfego dessas VMs ao firewall físico. Isso envolve regras de NAT e roteamento, portas e protocolos que são suportados por aplicações. As diretrizes de gerenciamento de mudanças exigem que as mudanças de políticas passem por um processo de fluxo de trabalho manual e trabalhoso de verificação, aprovação, auditoria e teste antes da implantação na produção. Isso é altamente ineficiente, operacionalmente exigente e caro, por causa do número de pessoas envolvidas.

Além disso, com novas regras somando-se a outras centenas de regras obscuras que nunca foram auditadas e removidas, as políticas de segurança se tornam complexas e incontroláveis. A área de TI pode começar a ver lacunas de políticas aparecerem e aumentarem, ameaças perdidas e/ou queda do desempenho.

Proliferação virtual

A proliferação virtual refere-se a um problema comum no qual o número de propriedades virtuais em um ambiente atinge um ponto que dificulta muito o rastreamento e o controle. Quando VMs são copiadas, clonadas ou movidas (e, em muitos casos, suspensas e esquecidas), isso cria riscos de segurança e deixa o ambiente aberto e vulnerável, uma vez que os controles e as políticas de segurança são desassociados. E não é prático fixar uma regra de segurança em um endereço IP estático da VM, considerando que os endereços IP das máquinas virtuais geralmente mudam. Esse é um problema comum, e os hackers estão explorando ativamente as vulnerabilidades. Assim, um ambiente virtual dinâmico requer controles de segurança dinâmicos, com um processo de mudança completamente regulado e auditável para garantir que as VMs cumpram as políticas de segurança e configuração adequadas.

Ambiente em nuvem pública

Outro caso de uso problemático é quando os serviços de aplicações da organização residem em nuvem pública, como Amazon Web Services (AWS) ou Microsoft Azure. Em um ambiente em nuvem, a área de TI da organização não pode colocar um appliance de firewall físico no data center protegido do fornecedor. São instalações extremamente controladas, e mesmo que a área de TI consiga colocar um dispositivo fixo no local, ela simplesmente não consegue impor o padrão do tráfego, de modo que o firewall fique na frente do tráfego de aplicações da organização. Nesse caso, o firewall também precisa ser virtual, então a área de TI pode usar rede definida por software (SDN) configurações manuais de engenharia de tráfego para colocar o firewall virtualizado entre seus serviços de aplicações e o resto do mundo, nos caminhos de entrada e/ou saída do data center.

Conclusão

A segurança é um fator fundamental em qualquer análise de custo-benefício das iniciativas de virtualização. As vantagens de economia e eficiência devem ser comparadas com os possíveis danos devido a ameaças crescentes e armadilhas comuns. A área de TI precisa explorar novas soluções além de abordagens e tecnologias legadas que possam efetivamente garantir o sucesso da segurança da virtualização.

Saiba mais: leia nosso resumo de solução "O que procurar em um firewall virtual de próxima geração" (Em inglês) e visite www.sonicwall.com/virtual-firewall.

Sobre nós

A SonicWall tem combatido o setor do crime cibernético por mais de 25 anos, defendendo desde pequenas e médias empresas até grandes corporações mundialmente. A nossa combinação de produtos e parceiros propiciou uma solução de defesa cibernética em tempo real, associada às necessidades específicas de mais de 500.000 empresas, em mais de 150 países, o que permite que você faça mais negócio com menos preocupações.

Se você tiver dúvidas sobre o possível uso deste material, entre em contato com:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Acesse o nosso site para obter mais informações.
www.sonicwall.com