McAfee Virtual Network Security Platform

Solução completa para detecção de ameaças e prevenção de intrusões para redes na nuvem

O McAfee® Virtual Network Security Platform (McAfee vNSP) é um sistema completo de prevenção de intrusões (IPS) e ameaças a redes, construído de acordo com as necessidades específicas de nuvens públicas e privadas. Ele descobre e bloqueia rapidamente ameaças sofisticadas nas arquiteturas de nuvem com precisão e simplicidade, permitindo que as organizações protejam cargas de trabalho e restabeleçam a conformidade, com confiança. Suas tecnologias avançadas incluem detecção sem assinaturas, emulação em linha e correção de vulnerabilidades com base em assinaturas. Fluxos de trabalho simplificados, opções flexíveis de integração e licenciamento fácil permitem que as organizações gerenciem e expandam sua segurança sem dificuldades, satisfazendo necessidades atuais e futuras.

Segurança completa na nuvem pública

As nuvens públicas proporcionam conveniência, economia e a oportunidade de mudar de investimento em infraestrutura para um modelo de despesas operacionais. Elas também introduzem um novo nível de risco, no qual uma vulnerabilidade no software acessível publicamente pode permitir que um atacante penetre a nuvem e vaze informações confidenciais, ou expor acidentalmente dados de clientes para outros usuários da nuvem que utilizem o mesmo serviço. O McAfee vNSP é compatível com Amazon Web Services (AWS), Microsoft Azure e Oracle Cloud Infrastructure (OCI), atuais líderes em serviços de nuvem pública, proporcionando visibilidade total sobre ameaças e proteção para os dados que passam por um gateway de Internet ou de um servidor para outro (tráfego lateral).

Proteção de ambientes virtualizados

As corporações estão adotando rapidamente infraestruturas de TI virtualizadas (como nuvens públicas e privadas), nas quais servidores físicos podem hospedar simultaneamente várias máquinas virtuais (VMs) e cargas de trabalho virtualizadas. A comunicação entre máquinas virtuais resultante, juntamente com a migração, replicação e backup instantâneos dessas cargas de trabalho, contribuiu para aumentar consideravelmente o tráfego lateral dentro de nuvens públicas e privadas, bem como em data centers definidos por software (SDDC). Somando-se ao caos, a flexibilidade proporcionada pela virtualização de rede torna dinâmica e imprevisível essa escalada nos fluxos de tráfego. Para se manterem à altura do desafio, as soluções de segurança virtualizadas

Principais vantagens

- Proteção completa para nuvens públicas e privadas (AWS, Azure e OCI)
- Proteção autêntica para tráfego lateral
- Console de gerenciamento centralizado para controle e visibilidade
- Tecnologias avançadas de inspeção protegem contra ameaças conhecidas e desconhecidas
- Alta disponibilidade, recuperação de desastres e balanceamento de carga para melhor desempenho
- Compartilhamento de licenças na nuvem para flexibilidade entre nuvens privadas e públicas
- Integra-se com o portfólio da McAfee, proporcionando segurança do dispositivo à nuvem
- Disponível no **AWS Marketplace**
- Disponível no **Azure Marketplace**

Conecte-se conosco

precisam ser flexíveis e expansíveis, e o mais importante, precisam funcionar perfeitamente com as plataformas de rede definidas por software (SDNs) que coordenam essas cargas de trabalho e máquinas virtuais de vida normalmente curta.

Agilidade em nuvens privadas

O McAfee vNSP integra-se perfeitamente com plataformas populares de nuvem privada, incluindo SDN baseados em ambientes OpenStack e VMware NSX. O McAfee vNSP é a única solução específica de IPS virtual certificada para funcionar com o VMware NSX. A microssegmentação de máquinas virtuais e a inspeção profunda do tráfego lateral são mantidas automaticamente nos ambientes virtualizados, mesmo que as cargas de trabalho surjam, migrem e cessem rapidamente.

Prevenção contra ameaças avançadas

O McAfee vNSP baseia-se em uma arquitetura de inspeção de próxima geração desenvolvida para oferecer inspeção profunda de tráfego em redes virtuais. Ele utiliza uma combinação de tecnologias avançadas de inspeção, incluindo análise completa de protocolo, reputação de ameaças, análise comportamental e análise de malware avançado, para detectar e impedir ataques à rede, tanto conhecidos quanto desconhecidos (de dia zero).

Uma única tecnologia de detecção de malware não pode impedir todos os ataques. É por isso que o McAfee vNSP sobrepõe vários mecanismos de detecção com e sem assinaturas para ajudar a impedir que o malware indesejável cause desordem nas suas nuvens. Ele utiliza múltiplas tecnologias de inspeção, incluindo emulação em linha de navegador, detecção de callback de malware, JavaScript, arquivos Adobe, redes de bots, detecção de DDoS com base em comportamento e proteção contra ataques avançados, como scripts entre sites e injeção de SQL.

O McAfee vNSP também pode identificar e bloquear os mais ocultos dos arquivos por meio de integração com o McAfee Advanced Threat Defense, no qual os arquivos são submetidos a análises comportamentais. O McAfee Advanced Threat Defense combina análise detalhada e estática de código, análise dinâmica (área restrita de malware) e **autoaprendizagem** para aumentar a detecção de ameaças de dia zero, incluindo ameaças que usam técnicas de evasão e ransomware. A McAfee também oferece suporte nativo para assinaturas do Snort para detecção e proteção contra malware.

Compartilhamento flexível de licenças de nuvem

As organizações corporativas espalham sua infraestrutura e seus recursos de TI por várias nuvens e plataformas para preservar a compatibilidade com aplicativos legados, para reduzir a dependência de um único fornecedor, por questão de redundância de sistemas ou para reduzir custos. O licenciamento de soluções de segurança para ambientes virtualizados pode ser complicado e caro, pois a maioria dos fornecedores exige a compra de licenças separadas para nuvens privadas e públicas e para plataformas SDN diferentes.

A McAfee simplifica o licenciamento e reduz os custos por meio do compartilhamento de licenças na nuvem, possibilitando às organizações compartilhar sua

Saiba mais

- **Proteção para suas redes virtuais Amazon Web Services**
- **Proteção para suas redes virtuais Microsoft Azure**

capacidade de processamento e suas licenças do McAfee vNSP por qualquer combinação de plataformas de nuvem pública e privada. O compartilhamento de licenças na nuvem também proporciona flexibilidade e melhora a segurança ao permitir que os administradores ofereçam rapidamente proteção para tráfego lateral e microssegmentação para cargas de trabalho virtuais, onde quer que estejam, sem passar por processos de aquisição demorados e processos de licenciamento complicados.

Análises e fluxos de trabalho simplificados

As ameaças modernas podem gerar grandes volumes de alertas e exceder rapidamente a capacidade do operador de segurança de priorizá-los e acompanhá-los. Se a resposta for muito lenta, ameaças reais podem passar sem serem detectadas. O McAfee vNSP inclui fluxos de trabalho decisivos e análises avançadas que correlacionam múltiplos alertas de IPS em um único evento decisivo, permitindo que os administradores identifiquem rapidamente as informações relevantes. Além disso, a integração com soluções de segurança adicionais da McAfee cria uma plataforma de detecção e resolução de ameaças de rede amplamente abrangente e conectada.

Gerenciamento centralizado para visibilidade e controle em tempo real

Um único appliance do McAfee Network Security Manager oferece gerenciamento centralizado, com base na Web, para visibilidade e controle em tempo real. O console avançado coloca você no controle de dados em tempo real através de um painel unificado. Você pode gerenciar, configurar e monitorar facilmente todos os appliances do McAfee Network Security Platform, virtuais ou físicos, bem como appliances do McAfee Network Threat Behavior Analysis, em ambientes de nuvem pública, de nuvem privada e tradicionais. Sua interface intuitiva também pode se expandir para gerenciar facilmente clusters de missão crítica amplamente distribuídos.

O McAfee Network Security Manager também pode ser distribuído como uma instância virtual em servidores VMware ESX e em ambientes AWS ou Azure. O McAfee vNSP é compatível com o AWS Identity and Access Management (IAM), possibilitando aos administradores gerenciar com facilidade e segurança o acesso a serviços e recursos do AWS de acordo com permissões atribuídas a usuários e grupos específicos.

Alta disponibilidade, recuperação de desastres e balanceamento de carga

O McAfee vNSP proporciona automaticamente controle, proteção e desempenho ininterruptos através de vários métodos. O McAfee Network Security Manager oferece alta disponibilidade monitorando proativamente o ambiente. Se um controlador ativo se torna indisponível, o McAfee Network Security Manager faz automaticamente o failover para um controlador reserva, proporcionando visibilidade e segurança ininterruptas. Além disso, um McAfee Network Security Manager reserva pode ser distribuído para recuperação de desastres em ambientes AWS, Azure e OCI.

O McAfee vNSP também oferece alta disponibilidade para sensores de IPS. Se um sensor se torna indisponível, a capacidade de autodimensionamento cria automaticamente um novo sensor de IPS virtual para uma proteção ininterrupta. Além disso, se o tráfego de rede aumenta, o balanceamento de carga automático entre sensores assegura que o desempenho seja otimizado e sensores adicionais podem ser distribuídos automaticamente para oferecer a capacidade exigida.

Segurança integrada

Ataques sofisticados não respeitam limites entre produtos e aproveitam rapidamente qualquer brecha na infraestrutura, especialmente entre produtos de segurança. O McAfee vNSP é o único IPS a se integrar perfeitamente com múltiplos produtos de segurança, aproveitando dados e fluxos de trabalho com eficiência para uma segurança melhor, mais proteção e maior retorno do investimento. Como exemplos da integração de soluções da McAfee, podemos citar:

- **McAfee ePolicy Orchestrator® (McAfee ePO™):** visibilidade total de todos os alertas e eventos de IPS dos endpoints
- **McAfee Endpoint Intelligence Agent:** combina perspectivas de rede e de endpoint para deter vazamentos de dados
- **McAfee Enterprise Security Manager:** compartilhamento de dados ricos e quarentena de IPS para alertas de IPS
- **McAfee Threat Intelligence Exchange:** aprendizagem compartilhada entre diversos tipos de dispositivos
- **McAfee Global Threat Intelligence:** maior e mais ativo serviço de reputação do mundo
- **McAfee Network Threat Behavior Analysis:** estenda a visibilidade pela rede
- **McAfee Virtual Advanced Threat Defense:** oferece inspeção detalhada para detecção de ameaças evasivas
- **McAfee Cloud Threat Detection:** um serviço que se integra às soluções de segurança existentes da McAfee para detectar malware avançado
- **McAfee Management for Optimized Virtual Environments (McAfee MOVE):** uma solução antivírus para ambientes virtuais
- **Mecanismos de varredura de vulnerabilidades de terceiros:** análises de host e de risco para endpoints

Recursos adicionais

Prevenção contra ameaças avançadas

- Mecanismo de emulação do McAfee Gateway Anti-Malware
- Mecanismo de emulação de código JavaScript incorporado em arquivos PDF (área restrita leve)
- Mecanismo de análise comportamental do Adobe Flash
- Proteção avançada contra evasão

Proteção contra callback de malware e rede de bots

- Detecção de callback de fluxo rápido em servidores de nome de domínio (DNS)/algoritmos de geração de domínios (DGA)
- "Sinkholing" de DNS
- Detecção heurística de bots
- Correlação de ataques múltiplos
- Banco de dados de comando e controle

Prevenção avançada de intrusões

- Desfragmentação de IP e remontagem de fluxo TCP
- Assinaturas da McAfee, definidas pelo usuário e de código aberto
- Quarentena de host e limitação de taxa
- Inspeção de ambientes virtuais
- Prevenção de negação de serviço (DoS) e negação de serviço distribuído (DDoS)
- Aperfeiçoamentos de listas negras e listas brancas como suporte para Structured Threat Information eXpression (STIX)
- Detecção com base em heurística e limites
- Limitação de conexão com base no host
- Suporte nativo para assinaturas do Snort
- Autoaprendizagem e detecção com base no perfil

McAfee Global Threat Intelligence

- Reputação de arquivos
- Reputação de IP
- Acesso restrito com base em geolocalização
- Controle de acesso com base em endereço IP

	Tipo de sensor 1	Tipo de sensor 2
Plataforma	VMware ESX 5.5/6.0/6.5	AWS Azure OCI VMware vSphere 6.5 e NSX 6.3
Modelo de sensor de IPS virtual	**IPS-VM600**	**IPS-VM600-VSS**
Tipo de distribuição de IPS virtual	Independente	Distribuído
Suporte para VMware NSX	Não	Sim
Suporte para AWS	Não	Sim
Suporte para Azure	Não	Sim
Suporte para OCI	Não	Sim
Número de CPUs lógicas	4	AWS 4, Azure 5
Memória necessária	7 GB	7 GB
Armazenamento	8 GB	8 GB
Especificações dos sensores virtuais		
Taxa de transferência máxima	Até 1 Gbps	Até 1 Gbps
Número de pares de portas de monitoramento	3	1 (porta de monitoramento, não um par de portas)
Interfaces virtuais (VIDS) por sensor	100	100
Perfis de DoS	300	300
Porta de gerenciamento	Sim	Sim
Porta de resposta	Não	Não
Modos de distribuição	Inspeção entre máquinas virtuais, inspeção de máquina física para virtual, inspeção de máquina física para física, inspeção de porta em linha/SPAN	

McAfee
Together is power.

Av. Nações Unidas, 8.501 – 16º andar
Pinheiros – São Paulo – SP
CEP 05425-070, Brasil
+(11) 3711-8200
www.mcafee.com/br