

McAfee Desktop Firewall 8.0

Defende e controla os clientes da sua rede de maneira proativa

De acordo com os laboratórios ISCA, mais de duzentas novas ameaças mal intencionadas são mensalmente adicionadas às mais de 72.500 ameaças existentes hoje em dia. Além das ameaças "tradicionais" de vírus, há agora um número crescente de worms que reconhecem a internet, mass mailers (programa de envio de correio em massa), ataques DoS (Negação de Serviço), cavalos de Tróia, zumbis, hackers e vulnerabilidades do sistema operacional. Essas ameaças não são apenas potencialmente mais destrutivas, mas também se espalham com mais rapidez. Há um tempo atrás, seria preciso semanas ou até meses para que uma ameaça atingisse ampla circulação. Atualmente, ameaças como SQLSlammer se espalham pelo mundo todo em questão de minutos, explorando redes corporativas e a Internet.

Segurança Integrada para o Cliente

Reduz o custo total de propriedade

O McAfee® Desktop Firewall™ integra-se ao McAfee VirusScan™ Enterprise e ao ePolicy Orchestrator™, proporcionando proteção integrada contra vírus, gerenciamento e geração de relatórios globais. A segurança integrada do cliente oferece interoperabilidade sem obstáculos, proteção completa contra vírus, hackers e outras ameaças mal intencionadas, prevenção contra roubo de dados e redução do custo total de propriedade.

Firewall para Filtragem de Pacotes

Impede e detém as ameaças novas que o antivírus sozinho não consegue barrar

O McAfee Desktop Firewall oferece firewall em nível de pacote que pode filtrar todo o tráfego que entra e sai da rede. O Desktop Firewall usa regras definidas pelo administrador e aprendidas automaticamente para decidir se o tráfego da rede deve ser bloqueado ou liberado. A filtragem de pacotes permite ao Desktop Firewall impedir que clientes sejam atacados ou recebam tráfego não-autorizado, o qual poderia ser um ataque hostil. Por exemplo, ele pode impedir antecipadamente que ameaças usem a rede para se espalhar, uma técnica usada pela maioria das grandes ameaças descobertas em 2002. O Desktop Firewall suporta vários protocolos de rede, inclusive mais de 120 protocolos baseados em IP. Além disso, os administradores podem criar políticas para protocolos não baseados em IP, inclusive WiFi (802.11x), NetBEUI, IPX e AppleTalk. O estabelecimento de regras para vários protocolos proporciona maior segurança à rede, pois permite a filtragem de grande parte do tráfego da rede.

Firewall na Camada de Aplicativo

Controla os aplicativos que acessam a rede

O McAfee Desktop Firewall oferece um firewall na camada de aplicativo que pode filtrar todos os aplicativos que geram tráfego na rede. Os administradores podem evitar o uso impróprio e fortalecer a segurança controlando as portas e os protocolos usados pelos aplicativos confiáveis.

Monitoramento de Aplicativos

Bloqueia programas não-autorizados & mantém o COE (Common Operating Environment)

O Desktop Firewall inclui monitoramento de aplicativo, proporcionando a capacidade de controlar e monitorar aplicativos, impedindo que aplicativos não-autorizados sejam executados ou se associem a outros aplicativos. É possível configurar regras para aplicativos, sendo que isso pode ser

quando softwares autênticos, como programas de troca de mensagens instantâneas, podem apresentar um risco à segurança ao acessar a rede, e ameaças como cavalos de Tróia, worms, troianos de acesso remoto ou programas espíões causam danos ao sistema, perda de produtividade e de receita. As regras de Aplicativos também permitem que os administradores mantenham o Ambiente Operacional Comum (COE), impedindo que os usuários instalem ou executem softwares não-aprovados e criem mais vulnerabilidades à segurança. A detecção de hooking em aplicativos impede ataques sofisticados como seqüestro de browser, tais como utilizar o browser para execução de aplicativos não-autorizados.

Detecção de Invasão Baseada em Assinatura

Protege contra técnicas conhecidas de ataque à rede

A detecção de invasão fornece meios para que o Desktop Firewall detecte comportamentos anormais no tráfego da rede ou atividades de aplicativos que indiquem um ataque ao cliente. Essa detecção baseia-se em regras fornecidas por um arquivo de definição por assinatura da McAfee Security. As assinaturas IDS podem ser atualizadas automática ou manualmente para garantir que o Desktop Firewall esteja equipado para defendê-lo contra técnicas emergentes. Se o Desktop Firewall identifica ataques na entrada ou na saída, ele pode bloquear a invasão, alertar e registrar a ocorrência. A detecção de invasão permite que o Desktop Firewall proteja o cliente contra ataques mal intencionados e impede que eles sejam usados para atacar outros. O Desktop Firewall é capaz de impedir os métodos mais comuns de ataques, como IP Spoofing, Ping Flood, SYN Flood e muitos outros.

Modo Quarentena

Impede que clientes desprotegidos se conectem à rede

O modo quarentena permite que o Desktop Firewall seja interrogado pelo ePolicy Orchestrator antes de o cliente se conectar à rede. Se for descoberto que o cliente está com o software desatualizado ou executando políticas antigas, o acesso à rede é vedado. As políticas do Desktop Firewall e do VirusScan Enterprise, as atualizações ao software e os arquivos DAT podem ser implementados e o cliente será liberado de sua quarentena. O modo quarentena protege a rede contra, softwares e políticas Desktop Firewall e antivírus desatualizados, o que deixa os clientes vulneráveis a ataques. Manter os clientes em quarentena até que estejam atualizados limita riscos à segurança, mantendo o tráfego potencialmente perigoso longe da rede.

Gerenciamento Centralizado

Aplicação global de políticas

O Desktop Firewall apresenta duas opções: uma solução independente, ideal para pequenas empresas ou usuários que precisam manter o controle de suas próprias políticas; e a solução corporativa McAfee ePolicy Orchestrator. Integrado ao McAfee ePolicy Orchestrator, o Desktop Firewall pode ser gerenciado centralmente, a partir de um único console. O ePolicy Orchestrator pode implementar e estabelecer políticas para o Desktop Firewall e distribuir atualizações do produto e alterações às políticas regularmente. O gerenciamento centralizado oferecido pelo ePolicy Orchestrator permite que os administradores economizem dinheiro, tempo e largura de banda, aproveitando o investimento já feito em um único console para gerenciar não apenas o Desktop Firewall, mas também o antivírus corporativo e a avaliação de vulnerabilidade

McAfee Desktop Firewall 8.0

Defende e controla os clientes da sua rede de maneira proativa

viral. A aplicação de políticas garante que os clientes do Desktop Firewall não alterem ou mexam nas configurações.

Geração de Relatórios Gráficos

Visibilidade global

O ePolicy Orchestrator oferece geração de relatórios gráficos sólidos de toda a empresa, dispondo, inclusive, de modelos de relatórios padrão ou personalizados. Os modelos padrão incluem: Todas as Invasões, Alvo e Origem da Invasão, 10 Principais Alvos de Ataque, 10 Principais Invasores e resumos de invasões baseados em tipo, ano, mês ou semana.

Os relatórios permitem que os administradores realizem uma análise detalhada das invasões e dos ataques feitos à rede, e identifiquem a origem do ataque. Além disso, o ePolicy Orchestrator também permite que os administradores identifiquem as questões mais importantes, o que possibilita tomar medidas rapidamente para solucionar problemas de segurança da rede.

Modo de Aprendizado

Cria regras dinâmicas para o Desktop Firewall

O Desktop Firewall aprende automaticamente o que pode entrar ou sair, o tráfego da rede e a atividade do aplicativo. No modo de aprendizado, o Desktop Firewall solicita que o usuário ou administrador escolha entre autorizar e bloquear tanto atividades de aplicativos como da rede. Ele também permite que o administrador crie regras personalizadas rapidamente, sem barrar a atividade legítima do cliente, sendo ideal para novas implementações.

Modo de Auto-Aprendizagem & Auditoria

Implementação corporativa e criação de políticas simplificadas

O Desktop Firewall pode aprender atividades automaticamente, sem solicitar que o usuário autorize ou bloqueie as regras. Nesse caso, o administrador pode realizar uma auditoria das políticas do Desktop Firewall para visualizar as regras aprendidas. As políticas podem, então, ser modificadas, bloqueadas e distribuídas para outros clientes como um conjunto padrão de regras. Os administradores podem criar rapidamente políticas personalizadas que devem ser replicadas para toda a empresa, simplificando seu processo de implementação.

Compatibilidade com VPN (Rede Virtual Privada)

Interoperação com outros fornecedores

O Desktop Firewall foi projetado para fortalecer a proteção da VPN e foi testado para executar softwares em clientes da VPN, inclusive Checkpoint, Cisco, Nortel e Microsoft®. A compatibilidade garante que seus clientes atuais de VPN interoperem com o Desktop Firewall.

Serviços Expert

Maximizando seu investimento em segurança

As empresas estão cada vez mais dependentes da tecnologia da informação, e as técnicas de ataque estão cada vez mais avançadas, por isso, a avaliação da situação da segurança, a implementação de tecnologias de segurança e a adoção de políticas de segurança executáveis são essenciais para o êxito das empresas atuais. Os Serviços Expert da Network

Associates oferecem ajuda especializada e objetiva em todas as fases do gerenciamento do programa de segurança, desde o projeto e a avaliação até a implementação da tecnologia e a resposta a emergências. Como provedora de serviços de otimização e segurança da rede, temos a visão única de que a disponibilidade é um objetivo comercial tão crucial para o sucesso quanto a segurança. Essa compreensão nos habilita a fornecer soluções que criam um equilíbrio entre operações de rede eficientes e controles seguros. O resultado final são medidas de segurança que pretendem organizar, e não atrapalhar.

Requisitos de Sistema

Nota: A seguir, encontram-se requisitos gerais de sistema, os quais podem variar de acordo com a natureza do seu ambiente.

- Um processador Intel® Pentium de 166 MHz ou mais veloz
- Mínimo de 64MB de RAM
- Mínimo de 32MB de espaço no disco rígido
- Um dos seguintes sistemas operacionais:
 - Microsoft Windows® 98 SE (Second Edition)
 - Microsoft Windows NT Workstation 4.0, com Service Pack 6 ou mais recente
 - Microsoft Windows NT Server 4.0, com Service Pack 6 ou mais recente
 - Microsoft Windows 2000 Professional, com Service Pack 2
 - Microsoft Windows 2000 Server, com Service Pack 2
 - Microsoft Windows 2000 Advanced Server, com Service Pack 2
 - Microsoft Windows ME (Millennium Edition)
 - Microsoft Windows XP Home Edition
 - Microsoft Windows XP Professional

Todos os produtos da Network Associates® contam com o respaldo do nosso programa PrimeSupport® e dos Laboratórios da Network Associates. Personalizado para se adequar às necessidades da sua empresa, os serviços PrimeSupport® oferecem conhecimento de produto essencial e soluções técnicas rápidas e confiáveis para mantê-lo em plena operação. Os Laboratórios da Network Associates, líder mundial em sistemas de informação e segurança, são a sua garantia de desenvolvimento e aperfeiçoamento contínuos de todas as nossas tecnologias.

3965 Freedom Circle | Santa Clara, CA 95054 | 800.764.3337 main

networkassociates.com



Network Associates, McAfee, ePolicy Orchestrator, VirusScan, Desktop Firewall e PrimeSupport são marcas registradas ou comerciais da Network Associates, Inc. e/ou suas afiliadas nos EUA e/ou outros países. A marca dos produtos Sniffer® são feitos apenas pela Network Associates, Inc. Todas as outras marcas registradas ou marcas comerciais não registradas mencionadas neste documento pertencem exclusivamente aos seus respectivos proprietários. ©2003 Networks Associates Technology, Inc. Todos os Direitos Reservados.