

# McAfee Desktop Firewall

## Defender e Controlar os Desktops Corporativos de Maneira Proativa

O McAfee® Desktop Firewall™ é um firewall avançado para aplicativos com recursos de prevenção contra invasões, que defende e controla antecipadamente os desktops e laptops, impedindo novas ameaças que o antivírus sozinho não consegue combater. Por fornecer recursos abrangentes de firewall de rede e de aplicativos aliado a uma tecnologia de prevenção de invasões, o Desktop Firewall impede que seus sistemas enviem ou recebam ameaças de tráfego de rede ou aplicativos não-autorizados. Ele também impede que aplicativos autorizados de sua empresa sejam manipulados para enviar ou receber ameaças pela rede.

### Menor Custo Total de Propriedade

#### Segurança integrada ao cliente

O Desktop Firewall se integra ao McAfee VirusScan® Enterprise e ao McAfee ePolicy Orchestrator® (ePO™), oferecendo à sua empresa proteção integrada contra vírus, gerenciamento geral e geração de relatórios, até mesmo para as empresas de grande porte. A segurança integrada do cliente oferece à sua empresa interoperabilidade sem obstáculos, proteção completa contra vírus, hackers e ameaças, prevenção contra roubo de dados e custo total de propriedade reduzido.

### Gestão Flexível de Políticas para Sistemas Remotos

#### Políticas que Levam em Conta a Conexão

O Desktop Firewall pode aplicar diferentes políticas de firewall, dependendo do modo como um sistema se conecta à rede. Por exemplo, um administrador pode criar um grupo de conexão baseado em VPN, e o Desktop Firewall apenas aplica as regras associadas quando um usuário tenta se conectar a um VPN, ignorando assim qualquer regra associada quando o usuário se conecta à rede por meio de algum outro método de conexão. Essa funcionalidade oferece flexibilidade aos administradores para definir uma variedade de critérios de conexão diferentes com base em políticas de firewall, incluindo o tipo de conexão, endereço IP do host, gateway de destino, DNS, DHCP e servidores WINS.

### Bloquear e conter novas ameaças que o antivírus sozinho não consegue

#### Firewall para filtragem de pacotes

O Desktop Firewall oferece firewall em nível de pacote, o qual pode filtrar todo o tráfego que entra e sai da rede. O Desktop Firewall usa regras definidas pelo administrador e aprendidas automaticamente, para bloquear ou autorizar o tráfego da rede. A filtragem de pacotes permite que o Desktop Firewall impeça que seus sistemas sejam atacados ou recebam tráfego não-autorizado de ataques potencialmente hostis. O Desktop Firewall suporta vários protocolos de rede, inclusive mais de 120 protocolos baseados em IP. Além disso, seu administrador pode criar políticas para protocolos não IP, inclusive Wi-Fi (802.11x), NetBEUI, IPX e AppleTalk. A criação e aplicação de várias

regras de protocolo permitem níveis maiores de segurança ao filtrar grande parte do tráfego da rede.

### Controlar Aplicativos que Acessam a Rede

#### Firewall na camada de aplicativos

O Desktop Firewall oferece uma camada de aplicativos que pode filtrar todos os aplicativos que geram tráfego na rede. Seu administrador de sistema pode impedir o uso impróprio e aumentar a política de segurança controlando as portas e os protocolos usados por aplicativos confiáveis.

### Impedir Programas Não-Autorizados e Fiscalizar o COE

#### Monitoramento de aplicativos

O Desktop Firewall inclui o monitoramento de aplicativos, oferecendo à sua empresa a capacidade de controlar e monitorar aplicativos. Isso evita que aplicativos não-autorizados sejam executados ou se vinculem a outros aplicativos. As regras de aplicativos podem ser configuradas manualmente ou aprendidas automaticamente e bloqueadas para impedir alterações. As regras para criação de aplicativos impedem que aplicativos não-autorizados sejam executados. Um exemplo disso ocorre quando um software legítimo como o Instant Messenger cria um risco de segurança ao acessar a rede, e ameaças como cavalos de Tróia, worms, cavalos de Tróia de backdoor ou programas espíões resultem em danos ao sistema, perda de produtividade e perda de receita. As regras de aplicativos também permitem que o administrador fiscalize o COE (Ambiente Operacional Comum), impedindo que os usuários instalem ou executem softwares não-approvados e criem vulnerabilidades adicionais à segurança. A detecção de hooking de aplicativos impede ataques sofisticados como seqüestro de navegador.

### Impedir que Sistemas Desprotegidos se Conectem à Rede

#### Modo quarentena

O Modo quarentena permite que o Desktop Firewall seja interrogado pelo ePolicy Orchestrator antes de o cliente se conectar totalmente à rede. Se for detectado que o cliente está desatualizado ou executando políticas antigas, o acesso à rede é restringido. As políticas do Desktop Firewall e do VirusScan Enterprise, as atualizações de software e os arquivos DAT podem ser, então, aplicados e seus usuários são liberados da quarentena. O Modo quarentena protege a rede contra antivírus desatualizados e contra softwares e políticas do Desktop Firewall que deixam os sistemas vulneráveis a ataques. Colocar os sistemas em quarentena até que sejam atualizados limita os riscos à segurança, mantendo o tráfego potencialmente perigoso longe da rede.

### Proteger Contra Técnicas Conhecidas de Ataque à Rede

#### Prevenção de Invasão Baseada na Assinatura

A prevenção de invasão proporciona ao Desktop Firewall meios para detectar os comportamentos dentro do tráfego

legítimo da rede ou as atividades de aplicativos que indicam um ataque aos sistemas. Isso tem como base regras fornecidas por um arquivo de definição de assinatura da McAfee. Se o Desktop Firewall identificar um ataque interno ou externo na empresa, pode bloquear o ataque, alertar e registrar o evento para impedir futuros ataques. A prevenção de invasões permite que o Desktop Firewall proteja os usuários contra ataques e impede que eles sejam usados para atacar outros. O Desktop Firewall é capaz de impedir vários métodos comuns de ataque, tais como IP Spoofing, Ping Flood, WinNuke, SYN Flood e muitos outros.

## Fiscalização Global de Políticas

### Gerenciamento Centralizado

O Desktop Firewall está disponível como uma solução isolada ideal para empresas de pequeno porte ou para usuários que precisam manter o controle de suas próprias políticas, e como uma solução ePO para a empresa. Integrado ao ePO, o administrador pode gerenciar de maneira centralizada o Desktop Firewall a partir de um único console. O ePO pode implementar e definir políticas para o Desktop Firewall e enviar atualizações normais do produto e alterações na política. O gerenciamento centralizado fornecido pelo ePO permite que o administrador economize dinheiro, tempo e largura de banda com o aproveitamento do investimento feito em um único console para gerenciar não apenas o Desktop Firewall, como também o antivírus corporativo e a avaliação de vulnerabilidade a vírus.

## Visibilidade Global

### Geração de relatórios gráficos

O ePO gera robustos relatórios gráficos sobre toda a empresa, inclusive com modelos de relatório padrão ou personalizados. Os relatórios padrão incluem: todas as invasões, alvo e fonte das invasões, os dez principais alvos de ataque, os dez principais invasores e resumos de invasões de acordo com o tipo, o ano, o mês ou a semana. Os relatórios permitem que o administrador faça uma análise detalhada das invasões na rede e dos ataques recebidos, e identifique a origem do ataque. Além disso, o ePO também permite que seu administrador destaque os problemas, permitindo que ações rápidas resolvam os problemas de segurança de rede.

## Implementação Simplificada na Empresa e Criação da Política

### Aprendizagem Automática e Modo de Auditoria

O Desktop Firewall pode aprender a atividade automaticamente sem solicitar que o usuário permita ou negue as regras. Depois, o administrador de sistema pode

realizar uma auditoria de políticas do Desktop Firewall para visualizar as regras aprendidas. As políticas podem então ser modificadas, agrupadas e distribuídas aos usuários, como um conjunto-padrão de regras. Além disso, o administrador pode criar rapidamente políticas personalizadas para a empresa, que podem ser copiadas para a empresa inteira, simplificando o processo de implementação da política.

## McAfee PrimeSupport

O McAfee PrimeSupport® é essencial para otimizar o retorno do investimento no Sistema McAfee e nas Soluções de Proteção da Rede. A equipe do PrimeSupport da McAfee está preparada para oferecer os recursos certos para qualquer solicitação de serviço. Entre os recursos do PrimeSupport estão:

- Entrega de todas as versões de manutenção e atualizações de produto disponíveis
- Acesso a um conjunto abrangente de recursos de auto-atendimento on-line
- Suporte telefônico ao vivo 24/7/365
- Disponibilidade de gerentes de conta de suporte técnico dedicados
- Uma variedade completa de soluções de suporte de software e hardware, adaptadas a empresas de qualquer tamanho

## Requisitos de Sistema

Nota: A seguir são apresentados os requisitos gerais de sistema, que podem variar de acordo com a natureza do seu ambiente.

Sistemas operacionais:

- Windows® 98 SE (Second Edition)
- Windows NT Workstation 4.0 com Service Pack 6 ou mais recente
- Windows NT Server 4.0 com Service Pack 6 ou mais recente
- Windows 2000 Professional com Service Pack 2
- Windows 2000 Server com Service Pack 2
- Windows 2000 Advanced Server com Service Pack 2
- Windows 2003 Advanced Server
- Windows ME (Millennium Edition)
- Windows XP Home Edition
- Microsoft® Windows XP Professional

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, [www.mcafee.com](http://www.mcafee.com)

Os produtos da McAfee® denotam anos de experiência e compromisso com a satisfação do cliente. A equipe PrimeSupport® da McAfee de atenciosos e altamente qualificados técnicos de suporte oferece soluções sob medida e assistência técnica detalhada na gestão do sucesso de projetos essenciais — tudo isso com níveis de serviço que atendem às necessidades de cada empresa cliente. A McAfee Research, líder mundial em sistemas de informação e pesquisa de segurança, continua na vanguarda da inovação no desenvolvimento e refino de todas as nossas tecnologias.

McAfee, Desktop Firewall, ePolicy Orchestrator, ePO, VirusScan, Protection-in-Depth e PrimeSupport são marcas comerciais, registradas ou não, da McAfee, Inc. e/ou das suas afiliadas nos EUA e/ou em outros países. A cor vermelha usada em relação à segurança é marca distintiva dos produtos que levam a marca McAfee®. Todas as outras marcas comerciais, registradas ou não, mencionadas neste documento pertencem exclusivamente aos seus respectivos titulares. © 2005 McAfee, Inc. Todos os direitos reservados. 1-sps-f85-002-0405