

# McAfee Desktop Firewall 8.0

*Defiende y controla los clientes de su red de manera proactiva*

De acuerdo con los laboratorios ISCA, más de doscientas nuevas amenazas malintencionadas son adicionadas mensualmente a las más de 72.500 amenazas ya existentes hoy en día. Además de las "tradicionales" amenazas de virus, ahora hay un número creciente de *worms* que reconocen la Internet, *mass mailers* (programa de envío de correo en masa), ataques DoS (Denegación de Servicio), caballos de Troya, troyanos de acceso remoto, zombis, *hackers* y vulnerabilidades del sistema operativo. Esas amenazas no son solo potencialmente más destructivas, sino también se esparcen con más rapidez. Un tiempo atrás, serían necesarias semanas o hasta meses para que una amenaza lograra amplia circulación. Actualmente, las amenazas como SQL Slammer se esparcen por todo el mundo en cuestión de minutos, explorando redes corporativas y la Internet.

## Seguridad integrada para el Cliente

### *Reduce el costo total de propiedad*

McAfee® Desktop Firewall™ se integra al McAfee VirusScan™ Enterprise y al ePolicy Orchestrator™, proporcionando protección integrada con virus, gestión y generación de informes globales. La seguridad integrada del cliente ofrece interoperabilidad sin obstáculos, protección completa contra virus, *hackers* y otras amenazas malintencionadas, prevención contra robo de datos y reducción del costo total de propiedad.

## Firewall para Filtrado de Paquetes

### *Impide y detiene las amenazas nuevas que el antivirus por sí solo no consigue neutralizar*

McAfee Desktop Firewall ofrece *firewall* al nivel de paquete que puede filtrar todo el tráfico que entra y sale de la red. Desktop Firewall usa reglas definidas por el administrador y aprendidas automáticamente para decidir si el tráfico de la red debe ser bloqueado o liberado. El filtrado de paquetes le permite impedir al Desktop Firewall que los clientes sean atacados o que reciban tráfico no-autorizado, lo cual podría ser un ataque hostil. Por ejemplo, puede impedir anticipadamente que las amenazas usen a la red para propagarse, una técnica usada por la mayoría de las grandes amenazas descubiertas en 2002. Desktop Firewall soporta varios protocolos de red, incluso más de 120 protocolos basados en IP. Además de ello, los administradores pueden crear políticas para protocolos no basados en IP, incluso WiFi (802.11x), NetBEUI, IPX y AppleTalk. El establecimiento de reglas para varios protocolos proporciona mayor seguridad a la red, pues permite el filtrado de gran parte del tráfico de la red.

## Firewall en la Capa de Aplicación

### *Controla las aplicaciones que acceden a la red*

McAfee Desktop Firewall ofrece un *firewall* en la capa de aplicación que puede filtrar todas las aplicaciones que generan tráfico en la red. Los administradores pueden evitar el uso impropio y fortalecer la seguridad controlando las puertas y los protocolos usados por las aplicaciones fiables.

## Monitoreo de Aplicaciones

### *Bloquea programas no-autorizados y mantiene el COE (Common Operating Environment)*

Desktop Firewall incluye monitoreo de aplicación, que proporciona la capacidad de controlar y monitorear aplicaciones, impidiendo que aplicaciones no-autorizadas sean ejecutadas o que se asocien a otras aplicaciones. Es posible configurar reglas para aplicaciones, lo que puede hacerse manualmente o ser aprendido automáticamente. Esas reglas pueden ser configuradas manualmente o aprendidas automáticamente y desactivadas para evitar alteraciones. Las reglas para creación de aplicaciones

impiden que sean ejecutadas aplicaciones no-autorizadas. Un ejemplo de esto es cuando software legítimo, como programas de intercambio de mensajes instantáneos, puede presentar un riesgo a la seguridad al acceder a la red al contener amenazas como caballos de Troya, *worms*, troyanos de acceso remoto o programas de espionaje que causan daños al sistema, pérdida de productividad y de ingresos. Las reglas de Aplicaciones también permiten que los administradores mantengan el Ambiente Operacional Común (COE), impidiendo que los usuarios instalen o ejecuten softwares no-aprobados y creen más vulnerabilidades a la seguridad. La detección de *hooking* en aplicaciones impide ataques sofisticados como secuestro de navegador.

## Detección de Intrusos basada en Firmas

### *Protege contra técnicas conocidas de ataque a la red*

La detección de intrusos provee medios para que Desktop Firewall detecte comportamientos anormales en el tráfico de la red o actividades de aplicaciones que indiquen un ataque al cliente. Esa detección está basada en reglas provistas por un archivo de definición por firmas, de McAfee Security. Las firmas IDS pueden ser actualizadas automática o manualmente para garantizar que Desktop Firewall esté equipado para defenderlo contra técnicas emergentes. Si Desktop Firewall identifica ataques en la entrada o en la salida, puede bloquear la invasión, alertar y registrar el evento. La detección de intrusos permite que Desktop Firewall proteja al cliente contra ataques malintencionados e impide que sean usados para atacar a otros. Desktop Firewall es capaz de impedir los métodos más comunes de ataques, como IP Spoofing, Ping Flood, SYN Flood y muchos otros.

## Modo Cuarentena

### *Impide que clientes desprotegidos se conecten a la red*

El modo cuarentena permite que Desktop Firewall sea interrogado por el ePolicy Orchestrator antes de que el cliente se conecte a la red. Si se descubre que el cliente está con el *software* desactualizado o ejecutando políticas antiguas, el acceso a la red le es denegado. Las políticas del Desktop Firewall y del VirusScan Enterprise, las actualizaciones al *software* y los archivos DAT pueden ser forzados y el cliente será liberado de su cuarentena. El modo cuarentena protege a la red contra software y políticas no actualizados en el antivirus y el Desktop Firewall que dejan a los clientes vulnerables a ataques. Al mantener los clientes en cuarentena hasta que estén actualizados se limitan riesgos a la seguridad, alejando de la red el tráfico potencialmente peligroso.

## Gestión centralizada

### *Aplicación global de políticas*

Desktop Firewall presenta dos opciones: una solución independiente, ideal para pequeñas empresas o usuarios que precisan mantener el control de sus propias políticas; y una solución corporativa McAfee ePolicy Orchestrator. Integrado al McAfee ePolicy Orchestrator, Desktop Firewall puede ser administrado centralmente, a partir de una única consola. El ePolicy Orchestrator puede implementar y establecer políticas para Desktop Firewall y distribuir actualizaciones del producto y alteraciones a las políticas, regularmente. La gestión centralizada ofrecida por ePolicy Orchestrator permite que los administradores economicen dinero, tiempo y ancho de banda, aprovechando la inversión ya realizada en una única consola para administrar no sólo al Desktop Firewall como, también, el antivirus corporativo y la evaluación de vulnerabilidad

# McAfee Desktop Firewall 8.0

*Defiende y controla los clientes de su red de manera proactiva*

viral. La aplicación de políticas garantiza que los clientes del Desktop Firewall no alteren ni cambien las configuraciones.

## Generación de Informes Gráficos

### Visibilidad global

El ePolicy Orchestrator ofrece generación de informes gráficos sólidos de toda la empresa, y dispone, además, de modelos de informes patrón o personalizados. Los modelos patrón incluyen: Todas las Intrusiones, Blanco y Origen de la Intrusión, 10 Principales Blancos de Ataque, 10 Principales Intrusos y resúmenes de intrusos basados en tipo, año, mes o semana.

Los informes permiten que los administradores realicen un análisis detallado de las intrusiones y de los ataques hechos a la red, y que identifiquen el origen del ataque. Además de ello, ePolicy Orchestrator también permite que los administradores identifiquen las cuestiones más importantes, lo que hace posible la toma de medidas rápidamente para solucionar problemas de seguridad de la red.

## Modo de Aprendizaje

### Crea reglas dinámicas para Desktop Firewall

Desktop Firewall aprende automáticamente lo que puede entrar o salir, el tráfico de la red y la actividad de la aplicación. En el modo de aprendizaje, Desktop Firewall solicita que el usuario o administrador elija entre autorizar y bloquear tanto actividades de aplicaciones como de la red. También permite que el administrador cree reglas personalizadas rápidamente, sin impedir la actividad legítima del cliente, lo cual es ideal para nuevas implementaciones.

## Modo de Autoaprendizaje y Auditoría

### Implementación corporativa y creación de políticas simplificadas

Desktop Firewall puede aprender actividades automáticamente, sin solicitar que el usuario autorice o bloquee las reglas. En este caso, el administrador puede realizar una auditoría de las políticas del Desktop Firewall para visualizar las reglas aprendidas. Las políticas pueden, entonces, ser modificadas, bloqueadas y distribuidas para otros clientes como un conjunto patrón de reglas. Los administradores pueden crear rápidamente políticas personalizadas que deben ser replicadas para toda la empresa, simplificando su proceso de implementación.

## Compatibilidad con VPN (Red Virtual Privada)

### Interoperación con otros proveedores

Desktop Firewall fue proyectado para fortalecer la protección de la VPN y fue probado para ejecutar *software* en clientes de VPN, incluso Checkpoint, Cisco, Nortel y Microsoft®. La compatibilidad garantiza que sus clientes actuales de VPN interoperen con Desktop Firewall.

## Servicios Expert

### Maximizando su inversión en seguridad

Las empresas están cada vez más dependientes de la tecnología de la información, y las técnicas de ataque están cada vez más avanzadas, por eso, la evaluación de la situación de la seguridad, la implementación de tecnologías de seguridad y la adopción de políticas de seguridad ejecutables son esenciales para el éxito de las empresas actuales. Los Servicios Expert, de Network

Associates, ofrecen ayuda especializada y objetiva en todas las fases de la gestión del programa de seguridad, desde el proyecto y la evaluación hasta la implantación de la tecnología y la respuesta a emergencias. Como proveedores de servicios de optimización y seguridad de red, tenemos la visión única de que la disponibilidad es un objetivo comercial tan crucial para el éxito como la seguridad. Esa comprensión nos habilita a proveer soluciones que crean un equilibrio entre operaciones de red eficaces y controles seguros. El resultado final son medidas de seguridad que pretenden organizar, y no dificultar.

## Requisitos de Sistema

Nota: A continuación, se encuentran requisitos generales de sistema, los cuales pueden variar de acuerdo con la naturaleza de su ambiente.

- Un procesador Intel® Pentium de 166 MHz o más veloz
- Mínimo de 64MB de RAM
- Mínimo de 32MB de espacio en el disco rígido
- Uno de los siguientes sistemas operativos:
  - Microsoft Windows® 98 SE (Segunda Edición)
  - Microsoft Windows NT Workstation 4.0, con Service Pack 6 o más reciente
  - Microsoft Windows NT Server 4.0, con Service Pack 6 o más reciente
  - Microsoft Windows 2000 Professional, con Service Pack 2
  - Microsoft Windows 2000 Server, con Service Pack 2
  - Microsoft Windows 2000 Advanced Server, con Service Pack 2
  - Microsoft Windows ME (Millennium Edition)
  - Microsoft Windows XP Home Edition
  - Microsoft Windows XP Professional

Todos los productos de Network Associates® cuentan con el respaldo de nuestro programa PrimeSupport® y de los Laboratorios de Network Associates. Personalizados para adecuarse a las necesidades de su empresa, los servicios PrimeSupport® ofrecen conocimiento de producto esencial y soluciones técnicas rápidas y fiables para mantenerlo en plena operación. Los Laboratorios de Network Associates, líder mundial en sistemas de información y seguridad, son su garantía de desarrollo y perfeccionamiento continuos de todas nuestras tecnologías.

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

networkassociates.com



YOUR NETWORK. OUR BUSINESS™

Network Associates, McAfee, ePolicy Orchestrator, VirusScan, Desktop Firewall y PrimeSupport son marcas registradas o comerciales de Network Associates, Inc. y/o sus afiliadas en EE.UU. y/u otros países. Los productos de la marca Sniffer® son hechos apenas por Network Associates, Inc. Todas las otras marcas registradas o marcas comerciales no registradas mencionadas en este documento pertenecen exclusivamente a sus respectivos propietarios. ©2003 Network Associates Technology, Inc. Todos los Derechos Reservados.