

McAfee Desktop Firewall

Defiende y controla los *desktops* corporativos de manera proactiva

McAfee® Desktop Firewall™ es un *firewall* avanzado para aplicaciones, con recursos de prevención contra invasiones, que defiende y controla anticipadamente los *desktops* y *laptops*, impidiendo nuevas amenazas que el antivirus por sí solo no consigue combatir. Al brindar amplios recursos de *firewall* de red y de aplicaciones aliados a una tecnología de prevención de invasiones, Desktop Firewall impide que sus sistemas envíen o reciban amenazas de tráfico de red o aplicaciones no-autorizadas. También impide que las aplicaciones autorizadas de su empresa sean manipuladas para enviar o recibir amenazas por la red.

Menor costo total de propiedad

Seguridad integrada al cliente

Desktop Firewall se integra al McAfee VirusScan® Enterprise y al McAfee ePolicy Orchestrator® (ePO™), y ofrece a su empresa protección integrada contra virus, administración general y elaboración de informes, hasta para las empresas de gran porte. La seguridad integrada del cliente le ofrece a su empresa interoperabilidad sin obstáculos, protección completa contra virus, *hackers* y amenazas, prevención contra robo de datos y costo total de propiedad reducido.

Gestión flexible de políticas para sistemas remotos

Políticas que tienen en cuenta la conexión

Desktop Firewall puede aplicar diferentes políticas de *firewall*, dependiendo del modo con el cual un sistema se conecta con la red. Por ejemplo, un administrador puede crear un grupo de conexión basado en VPN, y el Desktop Firewall apenas aplicará las reglas asociadas cuando un usuario intente conectarse con un VPN, ignorando así cualquier regla asociada cuando el usuario se conecte con la red por medio de algún otro método de conexión. Esa funcionalidad ofrece flexibilidad a los administradores para definir una variedad de criterios de conexión diferentes con base en políticas de *firewall*, incluyendo el tipo de conexión, dirección IP del *host*, *gateway* de destino, DNS, DHCP y servidores WINS.

Bloquea y detiene nuevas amenazas que el antivirus por sí solo no consigue

Firewall para filtración de paquetes

Desktop Firewall ofrece *firewall* en nivel de paquete, el cual puede filtrar todo el tráfico que entra y sale de la red. Desktop Firewall usa reglas definidas por el administrador y aprendidas automáticamente, para bloquear o autorizar el tráfico de la red. La filtración de paquetes permite que el Desktop Firewall impida que sus sistemas sean atacados o reciban tráfico no-autorizado de ataques potencialmente hostiles. Desktop Firewall soporta varios protocolos de red, incluso más de 120 protocolos basados en IP. Además, su administrador puede crear políticas para protocolos no-IP, incluso Wi-Fi (802.11x), NetBEUI, IPX y AppleTalk. La creación y aplicación de varias reglas de protocolo permiten niveles mayores de seguridad al filtrar gran parte del tráfico de la red.

Controla aplicaciones que acceden a la red

Firewall en la capa de aplicaciones

Desktop Firewall ofrece una capa de aplicaciones que puede filtrar todas las aplicaciones que generan tráfico en la red. Su administrador de sistema puede impedir el uso impropio y aumentar la política de seguridad controlando las puertas y los protocolos usados por aplicaciones confiables.

Impide programas no-autorizados y fiscaliza el COE

Monitoreo de aplicaciones

Desktop Firewall incluye el monitoreo de aplicaciones, y así ofrece a su empresa la capacidad de controlar y monitorear aplicaciones. Eso evita que las aplicaciones no-autorizadas sean ejecutadas o se vinculen a otras aplicaciones. Las reglas de aplicaciones pueden ser configuradas tanto manualmente como ser aprendidas automáticamente y bloqueadas para impedir alteraciones. Las reglas para creación de aplicaciones impiden que las aplicaciones no-autorizadas sean ejecutadas. Un ejemplo de eso sucede cuando un *software* legítimo, como el Instant Messenger, crea un riesgo de seguridad al acceder a la red y amenazas tales como caballos de Troya, *worms*, caballos de Troya de *backdoor* o programas espías resultan en daños al sistema, pérdida de productividad y pérdida de ingresos. Las reglas de aplicaciones también permiten que el administrador fiscalice el COE (Ambiente Operacional Común), impidiendo que los usuarios instalen o ejecuten *softwares* no-aprobados y creen vulnerabilidades adicionales a la seguridad. La detección de *hooking* de aplicaciones impide ataques sofisticados, como secuestro de navegador.

Impide que sistemas desprotegidos se conecten con la red

Modo cuarentena

El Modo cuarentena permite que Desktop Firewall sea interrogado por el ePolicy Orchestrator antes de que el cliente se conecte totalmente con la red. Si se detecta que el cliente está desactualizado o ejecutando políticas antiguas, el acceso a la red será restringido. Las políticas del Desktop Firewall y del VirusScan Enterprise, las actualizaciones de *software* y los archivos DAT pueden ser, entonces, aplicados y sus usuarios serán liberados de la cuarentena. El Modo cuarentena protege la red contra antivirus desactualizados y contra *softwares* y políticas del Desktop Firewall que dejan los sistemas vulnerables a ataques. Al colocar los sistemas en cuarentena hasta que sean actualizados se limitan los riesgos a la seguridad, manteniendo el tráfico potencialmente peligroso lejos de la red.

Protección contra técnicas conocidas de ataque a la red

Prevención de invasión basada en la firma

La prevención de invasión le proporciona al Desktop Firewall medios para detectar los comportamientos dentro del tráfico legítimo de la red o las actividades de aplicaciones que

indican un ataque a los sistemas. Eso tiene como base reglas dadas por un archivo de definición de firmas de McAfee. Si el Desktop Firewall identifica un ataque interno o externo en la empresa, puede bloquear el ataque, alertar y registrar el evento para impedir futuros ataques. La prevención de invasiones permite que Desktop Firewall proteja a los usuarios contra ataques e impide que sean usados para atacar a otros. Desktop Firewall es capaz de impedir varios métodos comunes de ataque, tales como IP Spoofing, Ping Flood, WinNuke, SYN Flood y muchos otros.

Fiscalización global de políticas

Administración centralizada

Desktop Firewall está disponible como una solución aislada ideal para empresas de pequeño porte o para usuarios que precisan mantener el control de sus propias políticas, y como una solución ePO para la empresa. Integrado al ePO, el administrador puede administrar de manera centralizada el Desktop Firewall a partir de una única consola. El ePO puede implementar y definir políticas para Desktop Firewall y enviar actualizaciones normales del producto y alteraciones en la política. La administración centralizada brindada por el ePO permite que el administrador economice dinero, tiempo y anchura de banda con el aprovechamiento de la inversión hecha en una única consola para administrar no sólo el Desktop Firewall, como también el antivirus corporativo y la evaluación de la vulnerabilidad frente a virus.

Visibilidad global

Elaboración de informes gráficos

El ePO genera robustos informes gráficos sobre toda la empresa, incluso con modelos de informe estándar o personalizados. Los informes estándar incluyen: todas las invasiones, el objetivo y la fuente de las invasiones, los diez principales objetivos de ataque, los diez principales invasores y resúmenes de invasiones de acuerdo con el tipo, el año, el mes o la semana. Los informes permiten que el administrador haga un análisis detallado de las invasiones en la red y de los ataques recibidos, e identifique el origen del ataque. Además, el ePO también posibilita que su administrador destaque los problemas, permitiendo resolver los problemas de seguridad de red con medidas rápidas.

Implementación simplificada en la empresa y creación de la política

Aprendizaje automático y Modo de auditoría

Desktop Firewall puede aprender una actividad automáticamente sin solicitar que el usuario permita o niegue las reglas. Después, el administrador de sistema puede realizar una auditoría de políticas del Desktop Firewall para

visualizar las reglas aprendidas. Entonces, las políticas pueden ser modificadas, agrupadas y distribuidas a los usuarios, como un conjunto patrón de reglas. Además, el administrador puede crear rápidamente políticas personalizadas para la empresa, que pueden ser copiadas para la empresa entera, simplificando el proceso de implementación de la política.

McAfee PrimeSupport

McAfee PrimeSupport® es esencial para optimizar el retorno de inversión en el Sistema McAfee y en las Soluciones de Protección de la Red. El equipo del PrimeSupport de McAfee está preparado para ofrecer los recursos ciertos para cualquier solicitud de servicio. Entre los recursos del PrimeSupport están:

- Entrega de todas las versiones de mantenimiento y actualizaciones de producto disponibles
- Acceso a un conjunto amplio de recursos de auto-atención *on-line*
- Auxilio telefónico al vivo 24/7/365
- Disponibilidad de gerentes de cuenta de soporte técnico dedicados
- Una variedad completa de soluciones de soporte de *software* y *hardware*, adaptadas a empresas de cualquier tamaño

Requisitos de Sistema

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

Sistemas operativos:

- Windows® 98 SE (Second Edition)
- Windows NT Workstation 4.0 con Service Pack 6 o más reciente
- Windows NT Server 4.0 con Service Pack 6 o más reciente
- Windows 2000 Professional con Service Pack 2
- Windows 2000 Server con Service Pack 2
- Windows 2000 Advanced Server con 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

Los productos de McAfee® evidencian años de experiencia y compromiso con la satisfacción del cliente. El equipo PrimeSupport® de McAfee de técnicos de soporte atentos y altamente calificados ofrece soluciones a la medida y asistencia técnica detallada en la gestión del éxito de proyectos esenciales — todo eso con niveles de servicio que atienden a las necesidades de cada empresa cliente. McAfee Research, líder mundial en sistemas de información e investigación de seguridad, continúa a la vanguardia de la innovación en el desarrollo y refino de todas nuestras tecnologías.

McAfee, Desktop Firewall, ePolicy Orchestrator, ePO, VirusScan, Protection-in-Depth y PrimeSupport son marcas comerciales, registradas o no, de McAfee, Inc. y/o de sus afiliadas en EE.UU. y/o en otros países. El color rojo usado con relación a la seguridad es una marca distintiva de los productos que llevan la marca McAfee®. Todas las otras marcas comerciales, registradas o no, mencionadas en este documento pertenecen exclusivamente a sus respectivos titulares. © 2005 McAfee, Inc. Todos los derechos reservados. 1-sps-f85-002-0405