



Estrategia McAfee Protection-in-Depth

Creación de soluciones de seguridad económicas para pequeñas y medias empresas

Índice

Resumen	3
¿De dónde surgen los riesgos a la seguridad?	3
Protección de su red — opiniones del mercado	3
Network Associates puede ayudarle a aumentar la seguridad de su red	4
Soluciones McAfee System Protection para empresas de pequeño y medio porte	4
McAfee System Protection—Active Virus Defense Small Business Edition	4
McAfee System Protection—VirusScan ASaP	4
McAfee System Protection—McAfee SpamKiller for Microsoft Exchange	5
Soluciones McAfee Network Protection para empresas de pequeño y medio porte	5
McAfee Network Protection—McAfee IntruShield 1200	5
McAfee Network Protection—Netasyst Network Analyzer Distributed	5
McAfee Network Protection—Netasyst Network Analyzer LAN	5
McAfee Network Protection—Netasyst Network Analyzer Wireless	5
McAfee Network Protection—Sniffer Portable	5
McAfee Network Protection—Sniffer Reporter	5
Conclusión	6

Resumen

El hecho de tener una pequeña o media empresa (PYMEs/SMB) no significa que usted no tenga las mismas necesidades de seguridad de red de las grandes empresas. Con empleados y contratados que trabajan para usted en oficinas domésticas, que se conectan a su red en localidades remotas o acceden a materiales en cuartos de hotel, la necesidad de ofrecerle seguridad ininterrumpida es cada vez mayor.

Lamentablemente, al implementar todas las tecnologías y protecciones de acceso remoto, la única diferencia entre las grandes empresas y las SMB es la cantidad de dinero y de recursos.

En este trabajo, discutiremos lo siguiente: cómo puede ser violada la seguridad de las redes; creación de una red segura, así como herramientas reconocidas por el mercado y, finalmente, mostraremos cómo Network Associates® tiene las soluciones ideales que se adaptan a las necesidades de seguridad de su red.

¿De dónde surgen los riesgos a la seguridad?

Con mucha frecuencia, el patrimonio de muchas empresas está en los sistemas de computadoras, los cuales exigen una protección especializada. Por eso, la primera preocupación del gerente de TI es la de solucionar de manera rápida y fácil los problemas de red y de seguridad. La clave para lograr la resolución de problemas de seguridad es saber de dónde surgen las amenazas. Veamos algunas formas por medio de las cuales la seguridad puede ser violada.

Una de las primeras cosas por hacer es conocer qué tipo de red existe en el momento. Por ejemplo, independientemente del nivel general de seguridad de su red, las LAN inalámbricas pueden ser el objetivo preferido, pues exigen poca invasión física y, muchas veces, imponen mucho menos barreras de seguridad para que sean transpuestas de que un ataque por Internet.

Además, se puede echar su empresa gravemente de operación debido a una infección por virus y *worms*, que llevará a la degradación del desempeño de su red o hasta a daños físicos por medio de la corrupción o exclusión de archivos. Pero no todas las violaciones de seguridad vienen de fuera. Los empleados descontentos, servidores defectuosos, fallas de hardware o simples accidentes también pueden comprometer la seguridad internamente.

Protección de su red – opiniones del mercado

La mejor defensa contra ataques externos es reforzar la protección de su red y de sus usuarios. Esa medida reducirá el número de puntos de entrada vulnerables para que usted pueda tomar la iniciativa de supervisarlos e implantar medidas antiinvasión, tales como barrido de virus, prevención contra invasiones, filtración de *spam* y *firewalls*.

Saber lo que acontece en su red 24 horas al día — y no sólo en los horarios de punta o durante el horario comercial — ayuda al fortalecimiento de esa protección. Con el monitoreo de los patrones de tráfico y de uso, se puede identificar quién

está en la red y a cuáles informaciones están accediendo. Al establecer un parámetro básico de la actividad de su red, usted puede detectar patrones inusuales de tráfico que indiquen una violación de seguridad, de qué manera sucedió la violación y qué puede hacerse para solucionarla.

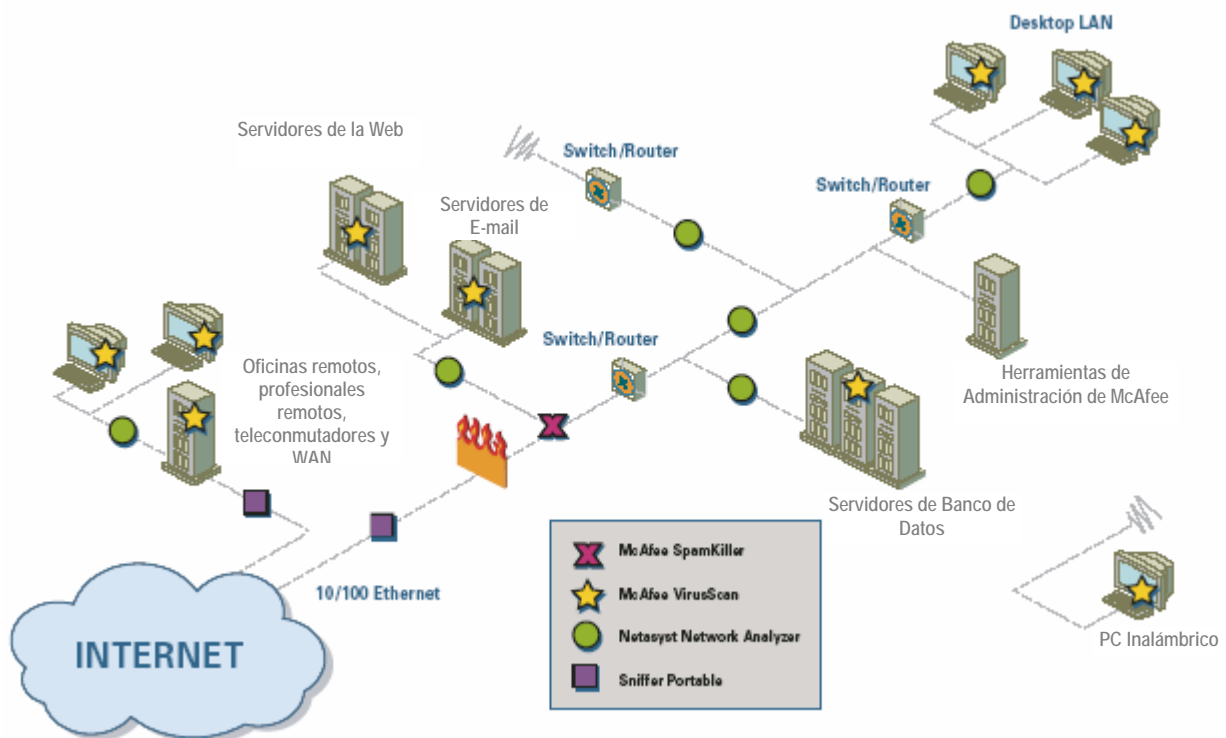
En el proceso de descubrimiento, no se sorprenda con el hecho de que el acceso remoto sea siempre un punto de vulnerabilidad, pues con el uso cada vez mayor de Internet para posibilitar el acceso remoto, muchas veces es difícil saber simplemente quién está intentando entrar. Un *firewall* en el punto de entrada es obligatorio para la seguridad de la red. Después de su implantación, hay diversas alternativas que pueden ser usadas para proporcionar un acceso remoto seguro. La opción más común puesta a disposición es la implementación de una red privada virtual (VPN), en la cual todos los datos son sometidos a criptografía y el acceso pasa por un elaborado sistema de identificación que emplea claves privadas específicas. Para garantizar la mayor eficacia de la VPN, todos los sistemas remotos deben tener un *firewall* personal.

Virus y *worms* pueden atacar por Internet, por *e-mail* o por *downloads* de la red, y una práctica recomendada es la de equipar cada PC y estación de trabajo de la red con un sistema de detección de virus.

Sin embargo, los *hackers* pueden emplear otros métodos para atacar a su red. El primero es un ataque de negación de servicio, mediante el cual inundan los sistemas con solicitudes de acceso hasta que estos no consigan más lograrlo. El segundo es un ataque que tiene por objetivo el acceso para fines malintencionados. En cualquiera de estos casos, hay productos que pueden ayudar a detectar esos ataques. Los sistemas de detección de invasiones de red (NIDS) son familias de productos que monitorean continuamente el tráfico que llega a la red, capaces de detectar ataques a la red, analizarlos para determinar la mejor reacción, con la finalidad de bloquear ataques en marcha, y, finalmente, implementar políticas capaces de impedir anticipadamente las invasiones en el futuro. Para aumentar la velocidad y la eficacia, muchas veces los sistemas son *appliances* de red autónomos.

Con el acceso protegido en el perímetro de la red, el próximo paso es pensar en la red corporativa. Para comprender los problemas de seguridad de la red, es importante ser capaz de comprender los patrones de tráfico de la red en *links* de LAN e inalámbrico. De esa forma, usted podrá usar esas informaciones para determinar y solucionar diversas situaciones de seguridad.

El análisis del tráfico de la red puede identificar la presencia de otros servidores no-autorizados. Normalmente, el exceso de tráfico en la red indica alguna forma de violación de seguridad, sea causada por un *worm*, un virus u otra fuente malintencionada. Servidores, procesadores o usuarios no-autorizados pueden ser aislados de la red y pueden realizarse análisis más minuciosos para establecer la raíz del problema.



Las soluciones de McAfee se combinan para proporcionar seguridad completa a la red

La mayor parte de las PYMEs/SMB posee un servidor interno de *e-mail* implantado. Aunque no se trate necesariamente de una amenaza directa a la seguridad, el *spam* — mensajes de *e-mail* indeseados que, según encuestas internas, ya responde por casi un 50% de todos los *e-mails* — es una amenaza general a la productividad de toda la empresa. Una solución anti-*spam* implantada en el servidor de *e-mail* puede ser usada para reducir considerablemente o eliminar el *spam* de los buzones postales de todos los usuarios de la red.

Network Associates puede ayudarle a aumentar la seguridad de su red

Network Associates ofrece la mejor combinación de soluciones de administración de seguridad de sistemas y redes para PYMEs/SMB por medio de dos familias de productos: McAfee® System Protection Solutions y McAfee Network Protection Solutions. El diagrama de arriba muestra algunas de las soluciones descritas a continuación usadas simultáneamente para brindar total seguridad a la red.

Soluciones McAfee System Protection para empresas de pequeño y medio porte

Las empresas de pequeño y medio porte son tan vulnerables a virus y *hackers* cuanto las grandes empresas. Con los sistemas de negocios conectados a Internet, su empresa está siempre a merced de actividades malintencionadas, las cuales pueden derrumbar los sistemas de computación,

afectando negativamente los negocios o, simplemente, paralizándolos. Las soluciones de McAfee ayudan a reducir esos riesgos con software y servicios proyectados teniendo en consideración a su pequeña empresa. Vea algunas de esas soluciones:

McAfee System Protection—Active Virus Defense Small Business Edition

McAfee Security ofrece protección máxima contra virus para las pequeñas y medias empresas. Normalmente, las empresas con menos de 250 empleados no poseen los recursos para una administración completa de antivirus. McAfee Security soluciona ese problema con la Small Business Edition del Active Virus Defense, que cuenta con McAfee VirusScan®, WebShield® y NetShield®, proyectados para defender todas las capas de su red. Además, integra el control del ePolicy Ochestraor® (ePO™), que fiscaliza la política antivirus de su preferencia y ofrece una visibilidad sin precedentes de la defensa antivirus en su red. El Active Virus Defense Small Business Edition evita epidemias, promueve la productividad y protege su presupuesto antivirus.

McAfee System Protection—VirusScan ASaP

McAfee VirusScan ASaP es el servicio antivirus remoto líder de mercado que protege *desktops* y servidores continuamente contra códigos malintencionados, utilizando las protecciones más actualizadas. Usando la tecnología de barrido de última generación de McAfee Security, VirusScan ASaP detecta archivos infectados accedidos en *desktops* o

servidores, limpiándolos, poniéndolos en cuarentena o excluyéndolos automáticamente para proteger su ambiente. Con sus actualizaciones automáticas, VirusScan ASaP protege sistemas que no tienen conexión con Internet, y puede hasta distribuir protección antivirus avanzada a usuarios de líneas discadas. Diseñado para proteger hasta 200.000 computadoras, VirusScan ASaP permite que usted delegue el fardo de administrar el software antivirus, reduce los costos operacionales y le ayuda a que vuelva a dedicarse al éxito de sus negocios.

McAfee System Protection—McAfee SpamKiller for Microsoft Exchange

Ajustado para operar en alta velocidad, McAfee Security SpamKiller® “powered by McAfee SpamAssassin™” ofrece protección incomparable para servidores Microsoft® Exchange 2000 y 2003, proporcionando hasta 95% de detección de *spam* sin ningún ajuste especial. McAfee SpamKiller puede ayudarle a reducir los costos asociados al barrido del *spam*, aplicando el barrido a los *e-mails* así que llegan al servidor Exchange. Después del barrido, el *spam* puede ser colocado en cuarentena en una carpeta de basura electrónica en el servidor o en la carpeta de basura electrónica del usuario. Al detectar el *spam*, usted evita que sus usuarios tengan que enfrentarse con mensajes indeseados, lo que les aumenta la productividad.

Soluciones McAfee Network Protection para empresas de pequeño y medio porte

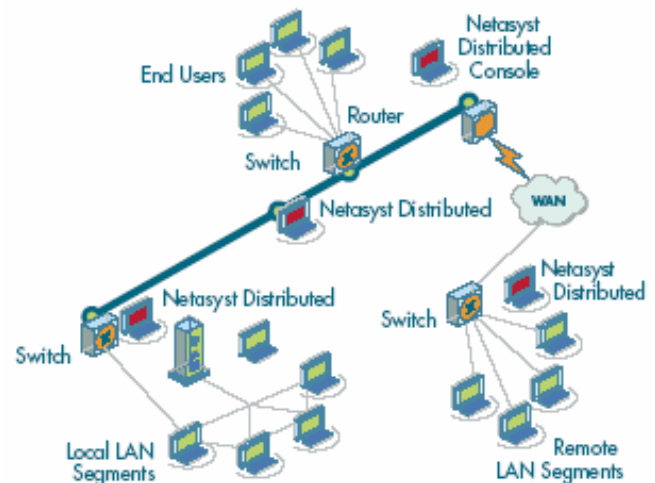
La familia de soluciones McAfee Network Protection fue creada para administrar y resolver proactivamente los problemas de su red. Esas soluciones ofrecen varios productos para la administración de su red. Las soluciones de protección de red que le ayudan a identificar y resolver problemas de manera rápida, fácil, económica y adecuada son:

McAfee Network Protection — McAfee IntruShield 1200

McAfee IntruShield® 1200 (I-1200) es un poderoso *appliance* sensor para detección y prevención contra invasión de redes que proporciona una implementación económica para redes de medio porte, de oficinas remotas o de filiales. La administración centralizada por la Web para implantaciones de IDS en toda la empresa reduce drásticamente los costos operacionales. El I-1200 posee dos puertos de detección Fast Ethernet, exploradores de red Fast Ethernet incorporados, una puerta Fast Ethernet para reacción y otra para administración, además de operar a una velocidad de hasta 100 Mb/s.

McAfee Network Protection — Netasyst Network Analyzer Distributed

El software Netasyst™ Distributed es una solución fiable, flexible y económica para resolver problemas remotamente y administrar redes LAN 10/100 LAN. La solución puede ser instalada en PC dedicados e implantada en toda su empresa en segmentos de LAN 10/100 para proporcionar una visibilidad ininterrumpida de su red. Con la interfaz de



usuario (UI) en el estilo Windows, usted puede tener acceso a informaciones sobre la red a cualquier momento, en cualquier lugar, además de administrar proactivamente toda su red a partir de un único lugar. Netasyst Distributed es una solución “Powered by Sniffer Technologies” que utiliza los decodificadores y los análisis avanzados que las grandes empresas vienen empleando para administrar, proteger y planear el crecimiento de las redes pertenecientes a esas corporaciones.

McAfee Network Protection — Netasyst Network Analyzer LAN

Los productos Netasyst para LAN mantienen su red Ethernet 10/100 funcionando en velocidad máxima. El analizador captura paquetes, creando, al mismo tiempo, un banco de datos de objetos de red a partir del tráfico observado para detectar anomalías en la red. Después que Netasyst aísla, analiza y califica un problema, le alerta, explicando el problema y recomendando medidas de corrección. Netasyst utiliza el sistema Expert Analysis de Sniffer® Technologies para optimizar la automatización de la administración, para ampliar las informaciones sobre la solución de los eventuales problemas y aumentar la visibilidad de la red.

McAfee Network Protection — Netasyst Network Analyzer Wireless

Los productos Netasyst para redes inalámbricas proporcionan una solución amplia para la administración de aplicaciones e implementaciones en redes 802.11a y 802.11b. Con la capacidad de decodificar el tráfico con Privacidad Equivalente a la de Redes Cableadas (WEP), sea antes o después de la captura, Netasyst le ofrece una flexibilidad incomparable para solucionar problemas. El análisis avanzado específico para ambientes inalámbricos permite que los productos Netasyst para redes inalámbricas detecten rápidamente violaciones de seguridad en radiofrecuencias por usuarios móviles no-autorizados o por puntos de acceso desprotegidos. Siguiendo todo el comportamiento de la red inalámbrico y exhibiendo todas las

informaciones conocidas, los productos Netasyst pueden determinar rápidamente si un ambiente está sobrecargado o con un desempeño eficaz. Esa función garantiza la corrección de problemas de velocidad, la retirada de equipos inalámbricos desprotegidos y el descubrimiento de usuarios móviles no-autorizados para que no representen más una amenaza a la seguridad de la red.

McAfee Network Protection — Sniffer Portable

Sniffer Portable es una familia de soluciones para administración de fallas y desempeño de red que les permite a los profesionales de red mantener, solucionar problemas, ajustar y expandir redes con varias topologías y varios protocolos. Esa solución portátil puede ser incluida en una red, en cualquier lugar en que sea necesaria para resolver problemas. Configure el software Sniffer Portable y las opciones del mismo en cuestión de minutos para comenzar a controlar todas las informaciones que entran o salen de su red por medio del *gateway* de Internet, y que transitan en las subredes internas. Opera prácticamente en todas las topologías de red local (LAN) y red remota (WAN), desde la Ethernet 10/100 hasta los más recientes *backbones* ATM (Modo Asíncrono de Transferencia) y Gigabit de alta velocidad. El software Sniffer Portable funciona en *desktops*, portátiles o *notebooks*, y puede utilizar componentes de hardware avanzados y personalizados para garantizar recursos de captura en alta velocidad.

McAfee Network Protection — Sniffer Reporter

Sniffer Reporter es una aplicación opcional de emisión de informes que perfecciona la solución Netasyst Network Analyzer. También es ofrecido acompañando a la solución Sniffer Portable. Genera informes gráficos con base en los datos recolectados por los productos Netasyst y/o Sniffer Portable. Son informes predefinidos, fáciles de generar, que exhiben rápidamente estadísticas globales, tablas de *host* e informes de matriz, así como distribución de protocolos en el segmento de red monitoreado. Esos datos ayudan a los gerentes de red a proyectar necesidades futuras de ancho de banda y a redistribuir recursos de red. Junto con el análisis

avanzado del Sniffer, el Sniffer Reporter identifica y corrige la degradación de la red antes que ello conduzca a una grave indisponibilidad.

Resumen

Aunque el cuadro general de la administración de la seguridad de redes pueda parecer asustador al comienzo, subdividirlo y analizar sus necesidades en todos los niveles reduce significativamente la complejidad. Además, Network Associates posee una gama completa de herramientas fiables para ayudarle a mantener su red con seguridad máxima 24 horas por día, 365 días por año.

Con o inalámbrico, el montaje de una red puede llevar su SMB a un nivel más alto en materia de comunicaciones por Internet, colaboración en tiempo real, hospedaje de la Web y comercio electrónico — o simplemente ser configurada para conectar una serie de estaciones de trabajo a una impresora compartida.

Las empresas de pequeño y medio porte tienen las mismas necesidades de seguridad que las grandes empresas, pero no cuentan con recursos humanos que puedan dedicarse en tiempo integral a la tarea. Por eso, el software desempeña un papel fundamental en la implementación de una red segura y protegida. Network Associates ofrece las soluciones McAfee System Protection (para proteger *desktops* y servidores) y las soluciones McAfee Network Protection (para garantizar la protección y la velocidad de la red corporativa).

No importa si su oficina cuenta con 25 ó 500 empleados, nosotros -de Network Associates- entendemos que sus negocios dependen de la seguridad ininterrumpida de su red, y nuestro compromiso es el de ser un aliado valioso para mantener su red operando sin problemas.

Entonces, PARE de preocuparse con seguridad de sistemas y COMIENCE a pensar en aumentar la productividad de los sistemas y usuarios.

Si quiere obtener más información sobre las soluciones para SMB, visite http://www.nai.com/us/audiences/small_buisness_home.asp.

McAfee Security 3965 Freedom Circle, Santa Clara, CA 95054, 800.338.8754

Los productos de Network Associates® traen junto con ellos años de experiencia y compromiso con la satisfacción del cliente. El equipo PrimeSupport®, compuesto por atentos y altamente cualificados técnicos de soporte, ofrece soluciones a la medida, proporcionando asistencia técnica detallada para administrar el éxito de proyectos fundamentales — todo con niveles de servicio insuperables para atender a las necesidades de cada empresa cliente. McAfee® Research, líder mundial en sistemas y seguridad de la información, continúa en la vanguardia de las innovaciones en el desarrollo y refinamiento de todas nuestras tecnologías.

Network Associates, McAfee, VirusScan, WebShield, NetShield, ePolicy Orchestrator, ePO, SpamKiller, Powered by SpamAssassin, IntruShield, Netasyst, Sniffer y PrimeSupport son marcas comerciales, registradas o no, de Network Associates, Inc. y/o de sus afiliadas en EE.UU. y/o en otros países. Los productos que llevan la marca Sniffer® son producidos exclusivamente por Network Associates, Inc. Todas las otras marcas comerciales, registradas o no, presentadas en este documento pertenecen exclusivamente a sus respectivos titulares. ©2004 Networks Associates Technology, Inc. Todos los derechos reservados. 6-net-smb-001-0304