

IntruShield Security Management de McAfee

Los productos para la seguridad de redes IntruShield® de McAfee® se basan en la primera arquitectura del sector para la detección y prevención de intrusiones en tiempo real en redes empresariales y públicas. La innovadora arquitectura IntruShield integra las técnicas patentadas de análisis de firmas, anomalías y denegación de servicio, que permiten una detección y prevención inteligentes y precisas de los ataques a velocidades de varios gigabits. Este aprovechamiento sin precedentes de tecnologías innovadoras permite proteger incluso las redes más exigentes contra la amenaza de ataques conocidos, iniciales (desconocidos) y de denegación de servicio.

La familia de productos IntruShield incluye IntruShield 4000, IntruShield 2600 e IntruShield 1200 — tres potentes dispositivos de detección y prevención de intrusiones que proporcionan el rendimiento y la funcionalidad necesarios para proteger redes que requieren un alto nivel de disponibilidad — y el sistema IntruShield Security Management (ISM), una solución potente y ampliable para la administración de la seguridad. ISM es una solución avanzada para administrar las implantaciones de dispositivos sensores IntruShield en redes de empresa grandes y distribuidas. Está disponible en dos versiones: IntruShield Global Manager e IntruShield Manager. IntruShield Global Manager es más adecuado para instalaciones globales de IDS de hasta varios centenares de sensores, mientras que IntruShield Manager admite instalaciones distribuidas de hasta seis detectores.

La solución ampliable IntruShield proporciona una protección integral que abarca el núcleo de la empresa, su perímetro y las redes de sucursales. Ofrece una atractiva relación precio-rendimiento para necesidades de ancho de banda comprendidas entre varias decenas de Mb/s y dos Gb/s.

Características Generales

- **Intrusion Intelligence™** — Capacidades sin precedentes que proporcionan una información detallada, precisa y fiable de la identificación, relevancia, dirección, efectos y análisis de las intrusiones
- **Administración Integral Centralizada Basada en la Red** — Una plataforma fácil de usar, centralizada y basada en la red permite una administración remota segura y ampliable de la instalación de IDS en toda la empresa
- **Actualizaciones Automatizadas de Amenazas en Tiempo Real** — Un proceso innovador y automatizado facilita actualizaciones de firmas a toda la empresa en tiempo real sin necesidad de reiniciar los sensores

El sistema IntruShield Security Management integra un completo conjunto de funciones de administración de la seguridad, lo que simplifica y racionaliza de forma espectacular las complejas tareas asociadas a la configuración de IDS y a la administración de políticas, amenazas y respuestas:

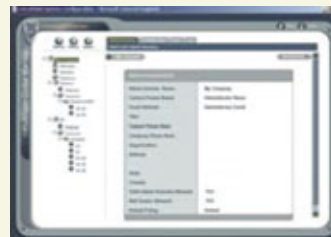
Vista de la Consola

Vigilancia y control de amenazas de un vistazo



Configuración del Sistema

Administración de políticas flexible y diferenciada



Visor de Alerta Inteligente

Análisis de intromisiones en tiempo real



Generador de Informes

Completa configuración de IDS, informes de amenazas



- **Dominios Administrativos** — Una administración ampliable de las políticas de seguridad con un control de accesos basado en la función del usuario permite delegar las responsabilidades administrativas
- **Administración Diferenciada de las Políticas de Seguridad** — Una administración muy flexible y personalizada de las políticas por sensor, o desde varios segmentos de red a hosts individuales, proporciona mejor detección y prevención de ataques
- **Administración Integral de Respuestas** — Un Completo conjunto de medidas de respuesta—que incluye respuestas definidas por el usuario y amplias posibilidades de informes—proporciona notificación y prevención preventivas de los ataques
- **Compatibilidad con los Administradores de Empresa** — Compatibilidad con las aplicaciones de gestión de empresa y con SIM (Security Information Management) para reducir el coste total de propiedad

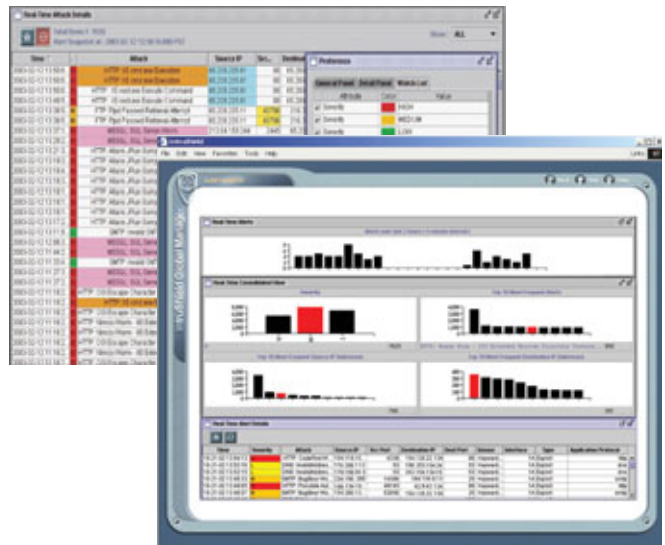
Intrusion Intelligence

El IDS IntruShield presenta las primeras capacidades Intrusion Intelligence del sector. Este conjunto de funciones sin precedentes proporciona una información detallada, precisa y fiable sobre la identificación, relevancia, dirección, efectos y análisis de las intrusiones. Intrusion Intelligence sienta las bases para que las empresas pasen de una capacidad de detección de intrusiones reactiva a una capacidad de prevención proactiva en la que los dispositivos de prevención detienen los ataques antes de que éstos alcancen sus objetivos.

Intrusion Intelligence consta de un exclusivo conjunto de funciones para analizar las características principales de una intrusión. Entre estas funciones se incluyen:

- **Identificación de Intrusiones** — IntruShield admite una amplia gama de métodos de detección de ataques, utilizando detección de firmas, de anomalías y de denegación de servicio. Se emplean funciones avanzadas, como el encapsulado de protocolo (tunneling) y el descubrimiento de protocolo, para detectar ataques *ocultos* diseñados para evitar un IDS. Una gran precisión en la detección y la amplitud de cobertura de ataques hacen posible una confianza sin precedentes en la correcta identificación de intrusiones o intentos de intrusión
- **Visor de Alerta Inteligente** — IntruShield ofrece una visión inteligente e intuitiva de las intrusiones, lo que simplifica la administración de alertas y datos sin renunciar a las potentes funciones de minería de datos. Las alertas se muestran en forma de tablas y gráficos en tiempo real, o se extraen de la base de datos para el análisis de alertas históricas. Unas listas de seguimiento codificadas por colores, configurables por el usuario, permiten hacer un seguimiento visual de la actividad sospechosa por ataque, por origen o por destino.

Potentes funciones de análisis facilitan la identificación de los incidentes relevantes con tan sólo un par de clics. Cada usuario de IntruShield puede adaptar a sus necesidades la codificación por colores y la estructura de la información presentada en el visor de alertas. La combinación de las funciones de dominio administrativo y de control de accesos basado en la función del usuario permite al administrador del sistema ofrecer una visión segmentada de la información a cada usuario final, en función de su nivel de delegación de dirección



El gestor intuitivo de IntruShield le permite controlar los datos en tiempo real.

- **Dirección de las Intrusiones** — Basándose en el análisis del tráfico bidireccional por estado de conexión (stateful), IntruShield puede determinar con precisión si el ataque es entrante o saliente. Adicionalmente, la función de política según dirección del tráfico permite a IntruShield aplicar políticas de seguridad diferentes en función de la dirección del tráfico, a fin de reducir los falsos positivos y proteger contra responsabilidades legales. Por ejemplo, una organización que sólo tenga servidores Linux instalados internamente puede reducir los falsos positivos mediante la aplicación de una política de seguridad personalizada que proteja exclusivamente contra ataques a Linux en el tráfico entrante. Al mismo tiempo, la organización puede aplicar una política no exclusiva al tráfico saliente para proteger contra ataques que se originen en la propia organización. Por ejemplo, un servidor Linux interno puede haberse visto comprometido y actuar, de forma inadvertida, como origen de ataques a Microsoft® Windows® de los que se podría hacer responsable a la organización



IntruShield puede diferenciar entre los ataques entrantes y salientes.

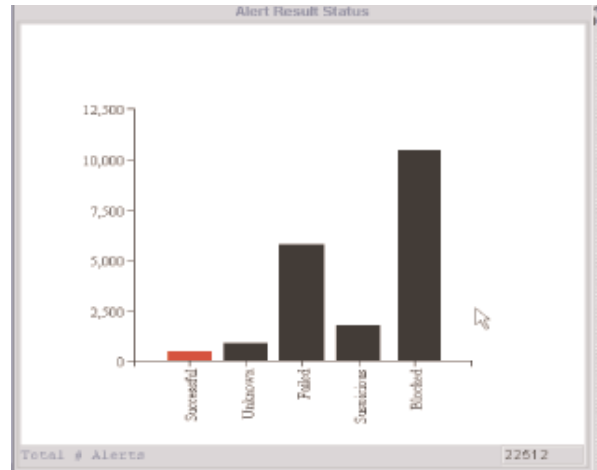
- Relevancia de las Intrusiones** — Una combinación de IDS virtual y administración de políticas diferenciadas permite al sistema tener en cuenta la relevancia de un ataque para un determinado entorno en el momento de generar una alerta o de bloquear selectivamente un ataque relevante, reduciendo los falsos positivos de forma significativa. Se pueden crear políticas altamente diferenciadas para alertar sobre ataques que son relevantes para un sistema operativo determinado o para aplicaciones concretas usadas en recursos específicos. Por ejemplo, el empleo de una sola interfaz de sensor permite proteger un grupo de servidores Web NT aplicando una política de servidores Web, mientras que un servidor de correo de la misma red se puede proteger mediante otra política personalizada de denegación de servicio
- Efectos de las Intrusiones** — IntruShield proporciona información precisa acerca de los efectos de un ataque. La innovadora función de verificación de ataques puede determinar si un ataque ha conseguido su objetivo mediante la vigilancia del tráfico bidireccional por estado de conexión (stateful) y el análisis del tráfico de respuesta originado por la posible víctima. La verificación de ataques clasifica cada ataque en una de las siguientes categorías:

- Conseguido
- Fallido
- Bloqueado
- Desconocido
- Sospechoso

Esta clasificación reduce espectacularmente los falsos positivos y permite a los analistas de seguridad dedicar su tiempo y sus recursos a los incidentes relevantes o de alta prioridad.

Después de un ataque conseguido, se pueden utilizar las funciones de *caja negra* (análisis forense) de IntruShield para registrar la comunicación posterior al ataque entre el

intruso y la víctima, lo que permite a los analistas de seguridad analizar con precisión los efectos de dicho ataque. Por ejemplo, el sistema puede capturar los comandos específicos ejecutados en el equipo de la víctima o registrar en su totalidad la transferencia de información confidencial de la víctima al intruso



IntruShield informa en tiempo real sobre los efectos de los ataques.

- Caja Negra (Análisis Forense)** — IntruShield incluye funciones de *caja negra* muy detalladas y potentes para capturar y analizar toda la información relacionada con una posible intrusión. El sistema permite registrar con gran precisión los paquetes de datos o sesiones durante el ataque y después del mismo. Después del ataque se pueden registrar todas las comunicaciones del intruso, de la víctima o las que tienen lugar entre ambos. Con un solo clic se puede ver la totalidad de los paquetes o sesiones registrados desde el visor de alertas, usando Ethereal o cualquier otra herramienta capaz de leer información en formato PCAP

Alert	Exploit	Response	Configured Response	Signature	Description
Attack Name:	HTTP Protocol Discovered on a Non-Standard Port			Attack Description	
Sensor ID:	realSensor [det. 3/13/03 10:56 AM]	Interface:	subnet204		
Severity:	Informational	State:	Unacknowledged		
Time:	2003-02-28 15:52:08.000 PST	Alert ID:	4467910908730115069		
Domain:	My Company/HR	Director:	Outbound		
Category:	Policy Violation	Subcategory:	19		
Detection Mechanism:	209	Result Set:	Suspicious		

IntruShield incluye funciones de *caja negra* muy detalladas.

- Notificación de Intrusiones** — Las completas funciones de notificación de IntruShield ofrecen vistas globales y detalladas de la administración y análisis de intrusiones de la empresa en informes intuitivos y gráficos. La amplia gama de opciones incluye informes resumidos para directivos, informes detallados de alertas de seguridad, informes de configuración del sistema e informes de análisis de tendencias a largo plazo. La función de notifi-

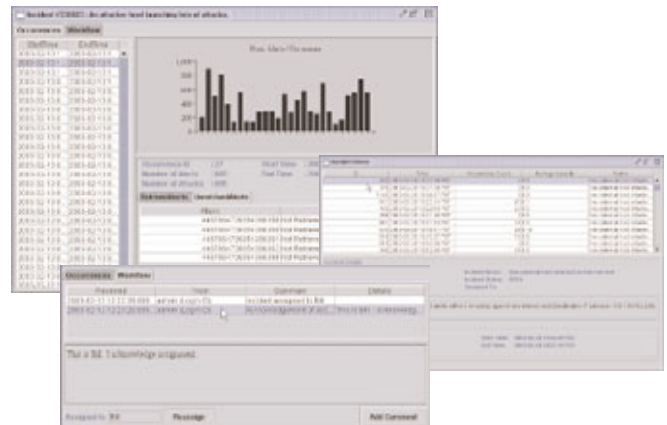
cación definida por el usuario (UDR) permite una generación de informes altamente personalizada y flexible mediante el filtrado de la información, definido por el usuario, por origen, destino, ataque, gravedad, sensor, IDS virtual, tipo de alerta y estado de la alerta, para satisfacer las necesidades de la dirección y las de los analistas de seguridad.

Los informes de tendencias ofrecen un análisis a largo plazo de diversos parámetros, que incluyen el número de ataques único, las direcciones de origen/destino únicas, la gravedad de la alerta o las categorías de alertas. Los informes se pueden generar en formato HTML o PDF, en tiempo real o siguiendo una programación predeterminada. Los informes programados pueden guardarse localmente en el Manager o distribuirse automáticamente por correo electrónico; cada informe se puede distribuir a un grupo de usuarios personalizado. Los datos de IntruShield se pueden integrar fácilmente con herramientas de notificación externas como Crystal Reports



IntruShield ofrece una amplia variedad de informes de fácil interpretación.

- **Gestión de Incidentes de Intrusiones** — A menudo, un mismo ataque genera cientos de eventos de seguridad a medida que avanza en su ciclo de vida. La potente función de correlación agrupa en un solo incidente un gran número de eventos IntruShield relacionados con una misma intrusión, centuplicando la eficiencia de la administración de alertas y datos. La gestión de incidentes ofrece una administración intuitiva del flujo de trabajo, en la que un incidente se puede asignar a un analista de seguridad y éste puede hacer comentarios al mismo o eliminarlo. El sistema puede hacer el seguimiento de varias apariciones de un incidente y presentarlas visualmente, ofreciendo una visión macroscópica de las actividades subyacentes



IntruShield puede agrupar miles de incidentes en un solo ataque.

Gestión Integral Basada en la Red

ISM es un sistema de administración intuitivo y fácil de usar, pero potente. El acceso seguro a ISM hace posible la administración remota de un gran número de sensores instalados por toda la red de la empresa. Todas las tareas asociadas a la configuración de IDS y a las funciones de administración de políticas, amenazas y respuestas se pueden realizar a distancia, sin necesidad de acceso físico al Manager ni a los sensores. Un solo Manager admite políticas de seguridad heterogéneas para los distintos sensores y para los recursos de interfaz física y subinterfaz virtual dentro de cada sensor. El Manager permite asimismo un acceso diferenciado de los usuarios a dichos recursos, definido por los dominios administrativos.

Actualizaciones Automatizadas de Amenazas en Tiempo Real

IntruShield Manager proporciona la protección más actualizada mediante técnicas innovadoras para salvaguardar contra unagama de amenazas en rápido cambio.

- **Actualizaciones de Firmas en Tiempo Real** — En función de la configuración de las políticas, el IntruShield Manager del equipo cliente solicita las nuevas firmas automáticamente, y éstas se pueden distribuir a los sensores en tiempo real. Los sensores IntruShield utilizan dinámicamente las firmas más recientes sin necesidad de ser restaurados o reiniciados, a fin de ofrecer una protección ininterrumpida contra los ataques
- **Programador** — IntruShield Manager puede distribuir nuevas firmas o software a los sensores en cuanto la actualización está disponible o bien a una hora programada
- **Descargas de Software** — En el servidor existen versiones actualizadas del software de los sensores, que se pueden descargar y aplicar desde dentro de IntruShield Manager

- **Firmas Definidas por el Usuario** — IntruShield Manager proporciona al usuario una interfaz gráfica fácil de usar para definir e implementar firmas personalizadas a sus entornos específicos. Las firmas definidas por el usuario pueden aprovechar la información detallada relativa a los campos de estado de comunicaciones y protocolos obtenida durante el análisis de protocolos

Dominios Administrativos

Un dominio administrativo representa un conjunto de recursos físicos o lógicos que quedan bajo un mismo dominio de dirección. Los dominios administrativos permiten aplicar una política de seguridad personalizada y conceder derechos administrativos diferenciados a las distintas entidades de una misma empresa: departamento, unidad de negocio o emplazamiento geográfico. Gracias a la capacidad de IDS virtual de IntruShield, un mismo sensor físico puede participar en varios dominios administrativos. Los dominios administrativos hacen posible una administración ampliable de las políticas de seguridad al permitir al usuario delegar un subconjunto de las tareas de administración de políticas de la empresa a varias entidades internas y conservar el control centralizado.



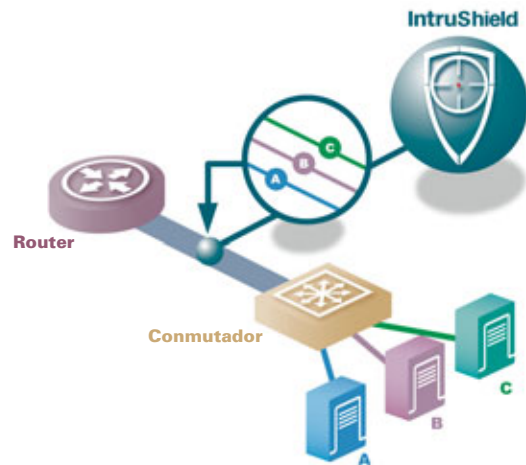
El IDS virtual de IntruShield permite la creación de múltiples políticas de seguridad personalizadas dentro de una misma red.

- **Control de Accesos Basado en la Función** — El control de accesos basado en la función del usuario hace posible el acceso diferenciado a los recursos de un dominio administrativo. A una persona se le puede conceder

acceso a todos los recursos de un dominio administrativo o a un subconjunto de los mismos. Aparte de esto, el nivel de acceso de cada usuario puede variar desde sólo lectura hasta el acceso administrativo total, lo que permite la administración de las políticas de seguridad. El Manager incluye una serie de funciones de usuario predefinidas con diferentes privilegios

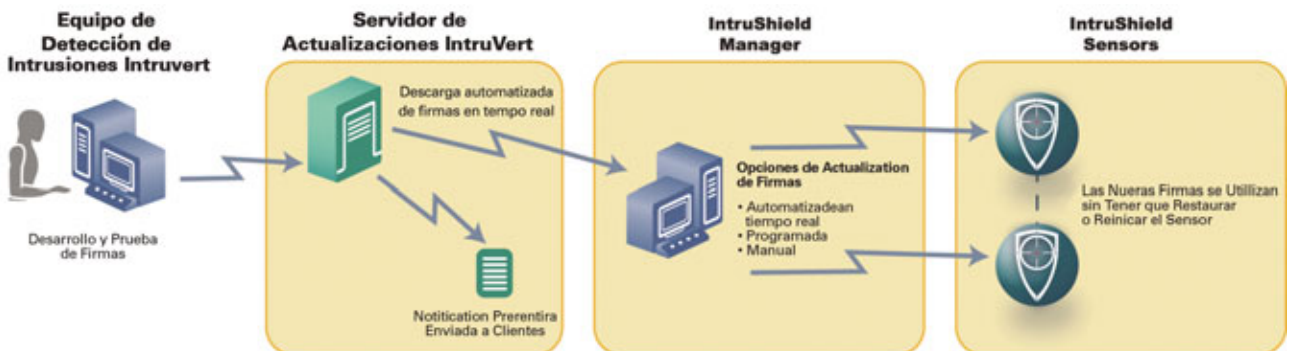
Administración Diferenciada de las Políticas de Seguridad

Una estructura de administración de políticas compleja y diferenciada hace posible aplicación de políticas de seguridad individualizadas que respondan a las necesidades de las distintas entidades de una empresa, como una unidad de negocio o un emplazamiento geográfico. Una configuración de entornos altamente personalizable permite identificar con precisión los recursos a proteger, lo que aumenta la precisión de la detección de ataques y reduce los falsos positivos.



IntruShield ofrece funciones de IDS virtual sin precedentes.

- **IDS Virtual (VIDS)** — Los sensores IntruShield incorporan el innovador y potente concepto de IDS virtual. El IDS virtual permite segmentar un sensor IntruShield en un gran número de sensores virtuales completamente personalizables con políticas de seguridad diferenciadas, incluidas la selección individualizada de ataques y las medidas de respuesta asociadas. El IDS virtual se puede definir como un bloqueo de direcciones IP, una o más etiquetas VLAN o puertos específicos de un sensor.



Mediante la utilización del IDS virtual, una sola interfaz de un sensor puede dividirse en un gran número de subinterfases, cada una de las cuales representa un host, un conjunto de hosts, un edificio, un departamento, un emplazamiento geográfico o una unidad de negocio de una misma empresa. Pueden combinarse varias interfaces en grupos para vigilar los enlaces que transportan tráfico para la red a proteger

- **Políticas de Seguridad** — El entorno a proteger se puede definir de forma muy detallada. Los hosts individuales o los grupos de hosts se pueden identificar con detalles específicos de su plataforma de hardware, sistemas operativos o servicios de aplicación subyacentes. Se pueden crear políticas de seguridad que incluyan las firmas que protegen el entorno concreto y omitan las firmas irrelevantes, con lo que se reducen los falsos positivos. Se pueden especificar políticas independientes para cada dirección del tráfico. Se pueden identificar las medidas de respuesta por firma, y la gravedad de los ataques se puede personalizar para el entorno del usuario final.

IntruShield Manager ofrece funciones avanzadas para reducir los costes operativos de la administración de políticas en toda la empresa. Los administradores pueden elegir entre varias políticas de seguridad predefinidas o adaptarlas y ajustarlas a su entorno con rapidez. Es posible aplicar modificaciones globales de políticas de detección y respuesta a intrusiones a múltiples sensores agrupados en un mismo dominio administrativo, lo que permite un importante ahorro de tiempo en la administración de políticas de grupo. Los cambios y actualizaciones de políticas se pueden distribuir fácilmente con un solo clic desde una consola de administración centralizada a un gran número de sensores

Administración Integral de Respuestas

Una combinación de respuestas automáticas o manuales iniciadas por el sensor y el administrador proporciona un amplio marco para detectar amenazas, responder las mismas y neutralizarlas, además de gran cantidad de opciones de notificación. Se pueden personalizar las medidas de respuesta para cada dominio administrativo. La administración de respuestas se puede dividir en tres grandes grupos:

- **Bloqueo selectivo de ataques** —

Al detectar un ataque, el sensor puede:

- Bloquear selectivamente los paquetes o sesiones malintencionados sin afectar al tráfico legítimo
- Poner fin a las sesiones inadecuadas

- Reconfigurar las listas de control de acceso del firewall
- Registrar los paquetes o sesiones
- Generar alertas y notificaciones

El bloqueo de ataques puede ser iniciado por el usuario o automatizado como parte de la política de seguridad

- **Notificación de Alertas** — Además de la notificación visual de alertas en la pantalla del Manager, los profesionales de la seguridad pueden recibir notificaciones de alerta por correo electrónico, agenda electrónica y buscapersoas. La notificación se puede personalizar para reflejar la gravedad de la alerta, controlada por el usuario, o para ciertos ataques seleccionados por el usuario
- **Medidas Definidas por el Usuario** — Además de la notificación de alertas, IntruShield Manager admite acciones definidas por el usuario (por ejemplo, la ejecución de scripts en el Manager), que contribuyen a permitir notificaciones complejas y mejoran las medidas de respuesta preventiva



IntruShield ofrece una gama completa de políticas de seguridad, incluso desde un mismo sensor.

Compatibilidad con los Administradores de Empresa

IntruShield Manager se puede integrar en un marco más amplio de administración de red dentro de una empresa. El Manager permite reenviar alertas por SNMP a aplicaciones de administración de redes empresariales como HP OpenView, IBM Tivoli o CA Unicenter. El Manager también permite reenviar alertas a servidores syslog para una visión y administración integradas. Cualquiera de estas formas de reenvío de alertas se puede personalizar para cada dominio administrativo y en función de la gravedad de los ataques. IntruShield Manager se integra con los principales productos SIM (Security Information Management).

Especificaciones de Los Productos Manager

	<i>IntruShield Global Manager</i>	<i>IntruShield Manager</i>
Plataformas Compatibles	Windows 2000	Windows 2000
Bases de Datos Compatibles	MySQL, Oracle	MySQL
Número de Sensores Admitidos	Ilimitado	6

Información para Pedidos

<i>Referencia</i>	<i>Descripción</i>
ICVS04KADEA	Dispositivo sensor IntruShield 4000
ITV-F04K-NA-100	Configuración de migración tras error para el dispositivo sensor IntruShield 4000
ICVS26KADEA	Dispositivo sensor IntruShield 2600
ITV-F26C-NA-100	Configuración de migración tras error para el dispositivo sensor IntruShield 2600
ICVS12KADEA	Dispositivo sensor IntruShield 1200
IMGCU-AD-A	Software de IntruShield Global Manager
IMSCUED-A	Software de IntruShield Manager
ITV-RPS4-NA-100	Fuente de alimentación CA redundante para el Sensor IntruShield 4000

McAfee PrimeSupport

McAfee ha seguido una estrategia que consiste en ofrecer la mejor tecnología para cada tipo de aplicación de gestión del rendimiento y la seguridad; ahora bien, la estrategia Protection-in-Depth™ va más allá de la instalación y aplicación de las mejores soluciones actuales. La prevención es sin duda nuestra prioridad principal, pero es inevitable que tenga usted que reaccionar ante un problema.

El programa PrimeSupport® de McAfee es fundamental para aprovechar al máximo su inversión en las soluciones de protección de redes y sistemas de McAfee. El equipo

PrimeSupport de McAfee cuenta con todos los recursos adecuados y puede ofrecerle en todo momento la solución de servicio que necesita. Entre los recursos de PrimeSupport se encuentran: autorización para acceder a todas las nuevas versiones de mantenimiento y actualizaciones de producto disponibles; acceso a una serie completa de funciones adicionales de autoasistencia en línea; asistencia telefónica en vivo accesible las 24 horas del día, los 7 días de la semana y los 365 días del año; disponibilidad de directores de cuenta asignados para prestar asistencia, y toda una serie de soluciones de asistencia para el software y el hardware que pueden adaptarse a sus necesidades.



McAfee S.A. Avda de Bruselas 22., 28108 Alcobendas. Madrid, +34 91 347 85 00, www.mcafee.com

Los productos de McAfee® significan años de experiencia y compromiso con la satisfacción del cliente. El equipo McAfee PrimeSupport® de técnicos de soporte especializados proporciona soluciones personalizadas y presta asistencia técnica pormenorizada, todo ello con niveles de servicio que responden a las necesidades de cualquier cliente. McAfee Research, líder mundial en investigación de seguridad y sistemas de información, continúa a la cabeza de la innovación en el desarrollo y el refinamiento de todas nuestras tecnologías.

McAfee, IntruShield, Intrusion Intelligence, Protection-in-Depth y PrimeSupport son marcas comerciales registradas o marcas comerciales de McAfee, Inc. y/o sus afiliados en Estados Unidos y/o en otros países. El color rojo es, en relación con la seguridad, distintivo de los productos de la marca McAfee®. El resto de las marcas registradas y no registradas que puedan aparecer en este documento son propiedad exclusiva de sus respectivos propietarios. © 2004 Networks Associates Technology, Inc. Reservados todos los derechos. 1-sps-ism-sp-002-1104