

Intelligent Application Gateway 2007

Los productos Forefront™ de Seguridad Perimetral y Accesos, Internet Security and Acceleration (ISA) Server 2006 y Intelligent Application Gateway (IAG) 2007, contribuyen a proteger su entorno de IT frente a amenazas procedentes de Internet y además posibilitan un acceso de los usuarios rápido y controlado mediante políticas, a las aplicaciones y datos corporativos.

- **Acceso remoto seguro:** para empleados, partners y clientes desde prácticamente cualquier sitio y dispositivo.
- **Seguridad en redes de oficinas:** mejor conectividad y seguridad para centros de trabajo remotos.
- **Protección del acceso a Internet:** mayor resistencia de la infraestructura de IT frente a amenazas basadas en tecnologías de Internet.

Control de los accesos

Acceso seguro mediante el navegador de Internet a las aplicaciones y datos de la empresa desde más sitios y más dispositivos sin necesidad de instalar ni aprovisionar software de cliente.

Protección de Activos

Protección integrada de aplicaciones que asegura la integridad y seguridad de la infraestructura de red y aplicación bloqueando el tráfico potencialmente dañino y los ataques detectados.

Salvaguarda de la información

Aplicación intensiva de políticas que permite dar cumplimiento a las directivas legales e internas con respecto al uso de la información, las restricciones y obligaciones a que debe someterse todo acceso a los datos sensibles de la empresa.

Entorno completo de acceso seguro

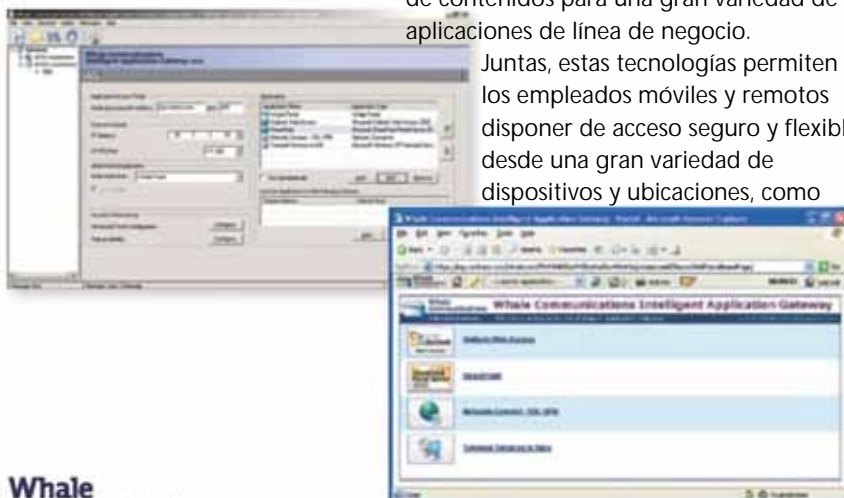
El Intelligent Application Gateway (IAG) con Optimizadores de Aplicación le ofrece VPN basada en SSL, firewall para aplicaciones Web y gestión completa de la seguridad del extremo de conexión que permite un mejor control de accesos, autorización e inspección de contenidos para una gran variedad de aplicaciones de línea de negocio.

Juntas, estas tecnologías permiten a los empleados móviles y remotos disponer de acceso seguro y flexible desde una gran variedad de dispositivos y ubicaciones, como

Kioscos, PCs y dispositivos móviles. IAG además facilita la aplicación de directivas de seguridad para cumplir con las normativas sobre uso de la información y las aplicaciones mediante políticas de acceso remoto basadas en el dispositivo, el usuario, la aplicación u otros criterios internos.

Equipo integrado

Intelligent Application Gateway es un equipo completo de alto rendimiento para la gestión de la seguridad y acceso a aplicaciones, diseñado para mantener un correcto equilibrio entre las demandas de seguridad, funcionalidad de las aplicaciones y acceso generalizado a los usuarios. Con las ventajas de un firewall de nivel de red (Microsoft® Internet Security and Acceleration Server 2006) y acceso VPN basado en SSL, IAG ofrece un entorno gestionado mediante políticas que unifica la seguridad del extremo de conexión, el acceso a las aplicación y el control de los accesos remotos, todo dentro de una plataforma muy escalable para poder responder a las necesidades de entornos complejos y de grandes dimensiones. IAG puede escalar hasta un número casi ilimitado de usuarios, soportando hasta 64 nodos en un mismo array de alta disponibilidad, permite definir esquemas de autenticación complejos, establecer configuraciones para la eliminación de elementos residuales de nivel de sesión y atender a requisitos específicos y personalizados para el cumplimiento de normativas en los extremos de conexión. La plataforma soporta múltiples portales en un mismo gateway, lo que facilita la personalización de la experiencia de usuario y la creación de configuraciones de políticas diferentes para cada portal.





Control de Accesos

- VPN sobre SSL flexible y adaptada a las aplicaciones, desde cualquier sitio y dispositivo.
- Acceso diferenciado y gestionado mediante políticas para una amplia gama de recursos de red, servidores y datos.
- Políticas de acceso y seguridad granulares
- Experiencia de portal Web personalizada, basada en la identidad del usuario

Protección de activos de IT

- Su integración con la infraestructura corporativa garantiza la integridad y seguridad de los recursos de red y aplicaciones.
- El firewall de aplicación Web adaptable impone filtros específicos de aplicación para protegerlas frente a PCs y redes no gestionados.
- Entorno completo de monitorización y registro de log para un mejor cumplimiento de normativas

Salvaguarda de la información

- Gestión intensiva de la seguridad y verificación que garantizan el cumplimiento de directivas y control de sesión en el extremo de conexión.
- Control más granular sobre el acceso de los usuarios a la Web y a otros recursos.
- Contribuye a garantizar la aplicación de las directivas corporativas sobre uso de la información mediante limpieza de la cache del cliente.

Optimizadores de Aplicaciones

IGAG incorpora diversos Optimizadores de Aplicación Inteligentes, que son módulos de software integrados con parámetros preconfigurados para garantizar el acceso remoto seguro a una amplia gama de aplicaciones. Los optimizadores protegen el punto de conexión, permiten la publicación de aplicaciones y aplican filtros a las peticiones al servidor de forma individual para garantizar el correcto equilibrio entre el rendimiento general de las aplicaciones y los niveles de seguridad exigidos para la red y los datos. Incluyen políticas granulares de seguridad específicas para Microsoft Exchange Server, SharePoint® Portal Server y muchas otras aplicaciones como SAP, IBM Domino y Lotus Notes.

Funciones	Conectividad		Políticas de Acceso	Seguridad del entorno de aplicación		Seguridad en el punto de conexión
	SSO (Logon Único)	Uso como página de Portal		Funciones de bloqueo	Firewall de nivel de aplicación	
Optimizador de Aplicación			Acceso limitado a áreas de aplicación			Eliminador de archivos adjuntos
Exchange Outlook® Web Access	Sí	N/D	Sí	Subida/descarga	Lógica positiva parcial	Sí
SharePoint Portal Server	Sí	Sí	Sí	Subida/descarga Edición	Lógica positiva completa	Sí
Domino Web Access	Sí	N/D	Sí	Subida/descarga	Lógica positiva completa	Sí
IBM WebSphere	Sí	Sí	Sí	Subida/descarga Edición	Lógica positiva parcial	Sí
Portal SAP	Sí	Sí	Sí	Subida/descarga Edición	Lógica negativa únicamente	Sí
Microsoft Dynamics	Sí	N/D	Sí	Subida/descarga Edición/Exportac.	Lógica positiva parcial	Sí



Aplicación	Características
<p>Optimizador de Aplicación para Microsoft SharePoint Portal Server</p> <p>El módulo de software preconfigurado para SharePoint ofrece funcionalidades para extender el acceso a SharePoint desde la extranet desde cualquier dispositivo con conexión a Internet.</p> <p>El Optimizador permite:</p> <ul style="list-style-type: none"> • Disponer de un acceso controlado a SharePoint desde extremos de conexión no gestionados, ampliando las posibilidades de acceso a partners y clientes • Plena compatibilidad con Microsoft Office sin necesidad de descargar componentes de túnel para establecer la conexión. • Integrar aplicaciones de terceros, antiguas o cliente/servidor con SharePoint Portal Server. 	<ul style="list-style-type: none"> • Logon único basado en Web • El logon único (SSO) basado en web permite la integración directa con cualquiera de los repositorios soportados por SharePoint (incluyendo soporte nativo para el Directorio Activo de Microsoft®). • Evita la necesidad de introducir las credenciales en múltiples ocasiones para acceder a los documentos • Integración con SharePoint Portal Server <ul style="list-style-type: none"> • Las organizaciones pueden utilizar SharePoint Portal Server como punto de entrada principal a la red. Después de validarse, el usuario se redirige automáticamente a SharePoint Portal Server. • Incorpora los componentes de IAG dentro de la página de inicio de SharePoint Portal Server, tales como el acceso al portal de IAG, acceso a archivos y la barra de herramientas de IAG para mejorar la experiencia del usuario. • Aplicación obligatoria de políticas con lógica positiva <ul style="list-style-type: none"> • El firewall de aplicación solamente admite que las peticiones conocidas, no peligrosas, pasen a los servidores SharePoint, y bloquea los ataques de nivel de aplicación, como el scripting entre sitios diferentes y los desbordamientos de buffer. • Aplicación de políticas específicas de aplicación <ul style="list-style-type: none"> • El entorno de políticas permite liberar o restringir el acceso a la edición de documentos, carga de archivos y descarga basándose en la inspección del extremo de conexión.
<p>Optimizador de Aplicación para Microsoft Exchange Server</p> <p>El Optimizador de Aplicación para Exchange Server permite acceder a una experiencia de usuario transparente mediante el soporte de scripts de login basado en Windows y Logon Único (SSO), eliminando la necesidad de múltiples peticiones de autenticación. Junto con la implementación del módulo Conector Cliente/Servidor, dispone de soporte para acceso al cliente nativo Microsoft Outlook® con plena funcionalidad, igual que si se accediera desde la propia LAN.</p>	<ul style="list-style-type: none"> • Logon Único basado en Web <ul style="list-style-type: none"> • las credenciales de acceso remoto se delegan en directorios nativos y repositorios de correo para garantizar la aplicación de perfiles de usuario y privilegios. • Scripts de logon unificado y basados en Microsoft Windows® para aprovechar la infraestructura existente de políticas y facilitar una configuración rápida. • Seguridad en el punto de conexión <ul style="list-style-type: none"> • Función de eliminación de archivos adjuntos descargados ("Attachment Wiper") • Políticas de visualización de archivos adjuntos basadas en los atributos del punto de conexión y la actividad del Attachment Wiper. • Firewall de nivel de Aplicación <ul style="list-style-type: none"> • Reglas de firewall propias, basadas en lógica positiva configuradas específicamente para Exchange Server e IIS que garantizan el paso exclusivamente de las peticiones válidas a los servidores. • Soporte para múltiples versiones de Outlook Web Access y Outlook mediante una interfaz de usuario intuitiva y guiada mediante asistentes. • Cierre de sesión seguro <ul style="list-style-type: none"> • Automatiza el cierre de sesión y los avisos de sesión inactiva filtrando la actividad de polling.
<p>Optimizador para Microsoft Dynamics</p> <p>El Optimizador de Aplicación para Microsoft CRM 3.0 permite publicar el portal Web de CRM de forma segura, con políticas adaptadas que gestionan las acciones de usuario específicas del entorno CRM y mantienen el nivel de seguridad exigido en la red y en la información</p>	<ul style="list-style-type: none"> • Controles de URL para subida y descarga de documentos • Zonas restringidas – Acceso bloqueado al área de configuración • Control de accesos basado en políticas con Microsoft CRM 3.0 Enhanced Security <ul style="list-style-type: none"> • Deshabilita la impresión • Deshabilita la exportación a Excel® • Permite/denega la subida de archivos adjuntos



Aplicación	Características
<p>Optimizador de Acceso Web para IBM Lotus Domino</p> <p>El Optimizador de Aplicación para el Acceso Web de IBM Lotus Domino (DWA) permite aprovechar al máximo el valor de Domino fuera de la LAN, mantiene la funcionalidad de la aplicación y protege los recursos de red. El Gateway protege la infraestructura interna ocultando el esquema de direccionamiento IP interno y realizando una traducción del contenido interno de Domino sobre la marcha.</p>	<ul style="list-style-type: none"> • Acceso gestionado mediante políticas: dependiendo del perfil del punto de conexión se bloquean las descargas/subidas de documentos. • Selección automática de servidor ("jump application"): Conecta al usuario con el servidor adecuado para las aplicaciones de mensajería en entornos de múltiples servidores, garantizando la transparencia del acceso. • Seguridad en el punto de conexión <ul style="list-style-type: none"> • Eliminador de cache "Attachment Wiper" preconfigurado para la limpieza de contenidos cacheados específicos de Domino. • Impide el envío con archivos adjuntos y los mensajes previos. • Logon único basado en Web: los usuarios pueden redirigirse a dominios independientes según sus niveles de privilegio y derechos de acceso. • Firewall de nivel de aplicación: las reglas de lógica positiva predefinidas permiten la ejecución únicamente de los comandos válidos. • Timeout de inactividad sensible a la aplicación: automatiza los procesos de cierre de sesión y mensajes de inactividad filtrando la actividad de polling normal
<p>Optimizador para IBM Lotus Domino</p> <p>El Optimizador de Aplicación para IBM Lotus Domino establece un entorno de seguridad y gestión del acceso externo basado en Web a todas las aplicaciones de IBM Lotus Domino (incluyendo Domino Web Access).</p>	<ul style="list-style-type: none"> • Conexión transparente para el usuario: en entornos multiservidor, los usuarios se conectan con el servidor adecuado para sus aplicaciones de mensajería mediante una selección transparente del servidor Lotus y una redirección integrada de "Webmail". • Funcionalidad completa para el acceso remoto <ul style="list-style-type: none"> • Se puede utilizar Lotus Sametime desde cualquier punto de acceso, incluso en navegadores sin privilegios, sin necesidad de establecer túneles para el punto de acceso de cliente. • Soporta Domino Offline Services, que permiten leer el correo en modo offline sin disponer de un cliente nativo Lotus completo. • Permite el uso del cliente Lotus estrictamente sobre HTTPS. • Logon Único basado en Web <ul style="list-style-type: none"> • Las credenciales de acceso remoto se delegan en directorios nativos y aplicaciones Lotus para garantizar la aplicación de perfiles y privilegios de usuario. • Soporte para complementos de autenticación y autorización de otros fabricantes. • Seguridad en el punto de conexión <ul style="list-style-type: none"> • Un editor de políticas flexible permite definir controles personalizados para las aplicaciones Lotus, como p.ej. Sametime o Domino Offline Services. • Impide que los usuarios puedan ignorar las reglas de descarga y redirección de contenidos hacia cuentas de correo externas. • Firewall de nivel de aplicación • Reglas de lógica positiva integradas, específicamente diseñadas para Lotus, que garantizan que solamente se pasan al servidor las peticiones válidas.
<p>Optimizador para SAP Enterprise Portal</p> <p>La solución optimizada para SAP ofrece control granular, basado en políticas, sobre aquellas áreas o funcionalidades de las aplicaciones SAP y de SAP Enterprise Portal a las que tiene acceso el usuario, consiguiendo la mejor experiencia de usuario y los máximos niveles de seguridad gracias a funcionalidades como la limpieza de cache personalizada y el timeout de sesión. Con ello se mejora la productividad, se reducen los riesgos para la seguridad y los costes de operación.</p>	<ul style="list-style-type: none"> • Acceso basado en políticas <ul style="list-style-type: none"> • Subida/descarga de documentos basadas en el perfil del punto de conexión. • Control de la edición y borrado de documentos locales basado en el perfil del punto de conexión. • Acceso a iViews concretas: la iView se muestra solo si la aplicación ha sido asignada al usuario. • Acceso restringido a las carpetas personales. • Integración completa con el portal <ul style="list-style-type: none"> • Redirección automática de los usuarios a un portal con políticas definidas de forma independiente y Logon Único seguro • Soporte para aplicaciones SAP, aplicaciones de otros fabricantes (p.ej. email), bases de datos y sistemas antiguos. • Permite el arranque de una única aplicación - el usuario no tiene que validarse por separado en un portal SSL VPN. • Protección completa • Acceso seguro al front-end (cifrado de datos, proxy reverso). • Filtrado de aplicación (restricción de acciones sobre los servidores de back-end, listas blancas). • Comprobación del punto de conexión. • Limpieza de la cache (en el disco local)

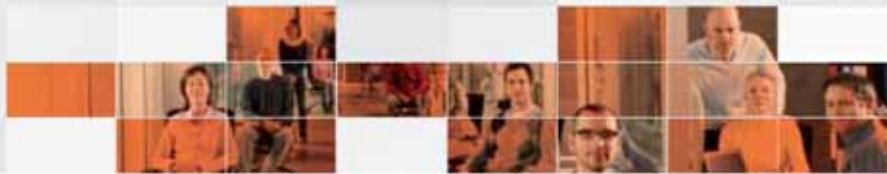


Aplicación	Características	
<p>Optimizador de Acceso para dispositivos móviles</p> <p>La solución de Intelligent Application Gateway para acceso desde dispositivos móviles establece un front-end seguro para los servidores Exchange, permite el cifrado de datos y logon único para la funcionalidad de correo "push" de Microsoft ActiveSync®. El Optimizador además establece una infraestructura de alta seguridad para ActiveSync, un micro-portal de infraestructura con autenticación bifactorial y procedimientos de inicio y cierre de sesión específicos para dispositivos móviles, así como filtrado de URLs y comandos de aplicación.</p>	<ul style="list-style-type: none"> • Micro-portal de acceso para dispositivos móviles: <ul style="list-style-type: none"> • El Gateway implementa un portal exclusivo para el acceso desde dispositivos móviles que permite separar el tráfico inalámbrico de la actividad de acceso remoto basada en Internet. • Páginas de inicio y cierre de sesión del micro-portal totalmente personalizables. • Logon único para aplicaciones de movilidad: el logon único basado en Web automatiza la sincronización con ActiveSync, sin necesidad de más pasos de autenticación como ocurre en otras implementaciones de VPN sobre SSL. • Separación completa de redes: <ul style="list-style-type: none"> • El Gateway determina el tráfico de la DMZ evitando la necesidad de disponer de conexión directa entre el dispositivo móvil y el servidor Exchange Server. • Aplica de forma rigurosa los procesos de autenticación y autorización. • Protección de nivel de aplicación: <ul style="list-style-type: none"> • Reglas de lógica positiva configuradas específicamente para Outlook Web Access, orientadas a garantizar que únicamente se pasan las peticiones válidas a los servidores. • Permite definir zonas restringidas para dispositivos móviles. 	
<p>Otras aplicaciones soportadas por el producto</p> <p>IAG dispone de soporte integrado y personalizado para más de 40 aplicaciones y servicios distintos, con lo que puede ofrecer una de las experiencias de acceso más completas disponibles hoy día. Sus políticas preconfiguradas, sus controles de seguridad específicos de cada aplicación y su soporte para un elevado número de protocolos permiten un acceso seguro y sencillo de los usuarios a las infraestructuras de IT más importantes de la empresa sin esfuerzo adicional.</p>	<p>Soluciones disponibles en paquetes</p> <ul style="list-style-type: none"> • Windows Terminal Services / cliente Web • IBM Host-On-Demand • IBM WebSphere Portal 5.2 • Lotus Domino Webmail • Lotus Domino Offline Services • Lotus Sametime • PeopleSoft • SAP Enterprise Portal • Citrix Program Neighborhood • Citrix NFuse FR2/FR3 (SecureGateway) • Citrix Presentation Server • Citrix Secure Access Manager • NetManage Rumba Web-to-Host 	<p>Soporte genérico para aplicaciones</p> <ul style="list-style-type: none"> • Aplicaciones Carbon de Apple Macintosh OS X • Aplicaciones basadas en Web o con funciones integradas de navegación Web • Aplicaciones cliente/servidor (RDP, RPC, etc.) • Aplicaciones compatibles con HTTP proxy (p.ej. Microsoft Live Communications Server) • Aplicaciones basadas en SOCKS • HAT (Host Address Translation) mejorado • Mapeo de unidades de disco locales, Acceso a archivos basado en Web • FTP • Telnet
<p>Application Optimizer Toolkit</p> <p>El Application Optimizer Toolkit permite personalizar políticas para otras aplicaciones, para aplicaciones existentes cliente/servidor y para modificar en profundidad los Optimizadores disponibles a fin de adaptarlos a las necesidades concretas de una organización.</p>	<ul style="list-style-type: none"> • Permite ampliar los Optimizadores disponibles para, a partir de configuraciones estándar, cubrir necesidades específicas de la empresa y crear nuevas políticas y controles de contenido para aplicaciones desarrolladas internamente. • IAG incorpora sofisticadas funciones de edición de políticas que permiten a los administradores definir puntos de comprobación complejos, como puede ser la verificación de si se han aplicado las actualizaciones antivirus en la última semana. El Advanced Policy Editor permite definir políticas utilizando operaciones booleanas y nuevas variables, evitando con ello el complicado e intensivo trabajo manual que exige la gestión de políticas en los equipos SSL-VPN de la competencia. 	



Escalabilidad	
Usuarios	Cada gateway soporta un número ilimitado de usuarios.
Alta Disponibilidad	Escala de forma lineal hasta configuraciones de alta disponibilidad de 64 nodos
Gestión y administración	
Flexibilidad	Configuraciones integradas de software para las aplicaciones corporativas más comunes, y facilidades para la personalización, incluyendo la definición de perfiles de autenticación, autorización y nivel de cumplimiento de directivas en el punto de conexión, y portales Web sensibles a contexto. Soporta conjuntos de reglas de lógica positiva y adaptación de filtros para URLs, así como la capacidad de desarrollar reglas para aplicaciones propietarias o a medida.
Portal SSL VPN	Un punto único de acceso para las aplicaciones, que soporta múltiples puntos de acceso con diferentes configuraciones de políticas, p.ej. para una extranet de partners y portales de empleados, todo en el mismo gateway.
Informes y logs	<p>Dispone de monitorización, registro de actividad y generación de informes para la gestión y seguimiento de nivel corporativo (vistas de sistema, seguridad del usuario y sesión):</p> <ul style="list-style-type: none"> • El Monitor de Eventos permite una monitorización completa por usuario, aplicación y periodo de tiempo. • El Registro de Eventos Integrado recopila información de uso del sistema y actividad de los usuarios y envía alertas ante la aparición de eventos de seguridad a una consola de administración. • La Herramienta de Consulta de Eventos dispone de plantillas de consulta preconfiguradas y funcionalidad completa de elaboración de informes
Entorno completo de gestión de políticas	<p>Las configuraciones de acceso a las aplicaciones y seguridad en el punto de conexión están diseñadas para garantizar el mínimo esfuerzo en la integración y reducir al máximo los costes de gestión en el futuro.</p> <ul style="list-style-type: none"> • Con el Intelligent Application Toolkit se pueden definir conjuntos de reglas en lógica positiva y filtros de URLs para complementar las configuraciones de los Optimizadores y desarrollar políticas para aplicaciones propietarias o a medida. • La Plantilla de Aplicación Inteligente (Intelligent Application Template) ofrece un entorno para la creación de un Optimizador de Aplicación válido para aplicaciones Web genéricas y también para aplicaciones corporativas complejas que incorporan componentes, web-parts y objetos
Políticas de Acceso	
Validación de nivel de cumplimiento de directivas en el punto de conexión	Las políticas aplicables al punto de conexión permiten definir controles de nivel de cumplimiento con las directivas de seguridad corporativas de acuerdo con variables propias que incluyen la presencia de un software de seguridad concreto y componentes específicos de IAG como el Eliminador de Archivos Adjuntos ("Attachment Wiper"). Soporta la definición de reglas complejas con verificaciones de seguridad basadas en operaciones booleanas.
Experiencia del usuario final	<ul style="list-style-type: none"> • Ofrece un portal VPN basado en SSL y páginas de inicio de sesión que facilitan la configuración y reducen el esfuerzo administrativo posterior • Permite la personalización total del portal y páginas de inicio de sesión para replicar la intranet existente • No necesita seguir las pautas de una plantilla de portal de un fabricante concreto.
Gestión integrada de la Autoridad de Certificación	Dispone de una autoridad de certificación integrada, en el caso de que el administrador prefiera no utilizar una autoridad de certificación externa. Permite a los usuarios disponer de un certificado de punto de conexión de confianza para una máquina concreta a petición.

Intelligent Application Gateway 2007



Ventajas de una Solución Integrada

La elección de un método de acceso debe venir justificada tanto por las necesidades de la empresa como por los niveles de seguridad. El objetivo de Microsoft es ofrecer una solución de amplio espectro que pueda adaptarse fácilmente a una gran variedad de escenarios de implantación y utilización.

Despliegue	ISA Server (2006) independiente	Intelligent Application Gateway 2007
Redes de oficinas	<ul style="list-style-type: none"> Gateway para conectividad y seguridad entre sitios remotos 	<ul style="list-style-type: none"> Facilitado por ISA Server
Protección del acceso a Internet	<ul style="list-style-type: none"> Control del acceso al Datacenter desde Internet, cache Web con un firewall completo de nivel de red. 	<ul style="list-style-type: none"> Facilitado por ISA Server
Acceso remoto seguro	Control de Accesos	
	<ul style="list-style-type: none"> Acceso publicado, seguro y pre-autenticado a ciertas aplicaciones Web (Exchange Server, SharePoint Server) 	<ul style="list-style-type: none"> Acceso diferenciado y gestionado mediante políticas a casi todas las aplicaciones y recursos de red, servidores o datos. VPN flexible basada en SSL para el acceso inteligente a las aplicaciones desde cualquier sitio y dispositivo. Granularidad en las políticas de acceso y seguridad, incluyendo controles internos para las aplicaciones. Experiencia de portal Web personalizable y basada en la identidad del usuario
	Protección de activos	
	<ul style="list-style-type: none"> Protección de red perimetral mediante inspección interna de los paquetes de datos Protección de las aplicaciones gracias a filtros avanzados y métodos de validación 	<ul style="list-style-type: none"> Inspección de contenidos en profundidad y filtrado con validación de entrada, y controles granulares de subidas y descargas de contenidos Firewall adaptable para aplicaciones Web, que aplica de forma estricta filtros específicos para cada aplicación, para protegerlas frente al riesgo de PCs y redes no gestionadas Integración con la infraestructura corporativa, garantizando la integridad y seguridad de los recursos de red y aplicaciones Gran capacidad de monitorización y registro para un mejor cumplimiento de normativas registrando la actividad de los usuarios y el uso de la información
Salvaguarda de la información		
<ul style="list-style-type: none"> Conectividad de red VPN con protocolo IPSec integrada en el motor del firewall para habilitar el acceso de PCs gestionado. 	<ul style="list-style-type: none"> Acceso total a la red basado en navegador de Internet Gestión potente de la seguridad en el extremo de conexión y métodos de verificación que garantizan el cumplimiento con las normativas de seguridad y el control de sesión. Control más granular del acceso de los usuarios a recursos Web y no basados en Web Cumplimiento de las directivas corporativas de uso de la información mediante limpieza en el lado del cliente. 	



Módulos de conectividad

Conector Cliente/Servidor

El Conector Cliente/Servidor permite establecer un acceso seguro a las aplicaciones cliente/servidor críticas para la empresa, como son Microsoft Exchange, el cliente nativo de Lotus Notes, Citrix, Microsoft Terminal Services, FTP y Telnet y facilita extraordinariamente la configuración para cualquier otra aplicación cliente/servidor gracias a una herramienta de definición de aplicación genérica.

Modos de Tunneling

- **Redirección de Puertos:** el componente de cliente escucha en una dirección local y puertos concretos, y hace que la aplicación envíe el tráfico TCP a esta dirección en lugar de hacia la dirección IP real del servidor de la aplicación. El cliente SSL VPN encapsula el tráfico interceptado dentro de SSL y lo envía al gateway. Este modo funciona perfectamente para aplicaciones que utilizan puertos TCP estáticos, o con aplicaciones compatibles con proxy HTTP o SOCKS.
- **Redirección de Sockets:** el componente de cliente se conecta a la interfaz de Microsoft Winsock Service Provider. Utiliza las interfaces LSP/NSP (Windows Layered Service Provider/Name Space Provider) y permite un manejo del socket a bajo nivel. La interfaz NSP se utiliza para resolver los nombres internos de servidores, garantizando que se accederá a través del túnel. Es totalmente compatible con todas las aplicaciones Winsock – TCP y puertos dinámicos.

Conector de Red

El Conector de Red permite instalar, ejecutar y gestionar conexiones remotas para facilitar un acceso completo de nivel de red a los usuarios sobre una conexión virtual, transparente y protegida, con los mismos niveles de funcionalidad que tendrían si estuviesen conectados en su misma red corporativa.

- El Módulo de Conector de Red da a los usuarios externos una dirección IP local igual que si estuviesen en la LAN, permitiéndoles el acceso a los servidores corporativos y a sistemas complejos como archivos compartidos y bases de datos internas sobre una conexión segura de nivel de red (carpetas compartidas).
- El Módulo Conector de Red puede establecer túneles para prácticamente cualquier protocolo basado en IP, incluyendo soporte para Voz sobre IP (VoIP).
- El Conector de Red puede implementar una conexión directa a servidores departamentales basándose en la identidad del usuario, en vez de establecer una conexión totalmente abierta de nivel de red para todos los usuarios a través del gateway directamente hacia la LAN, lo que mejora sensiblemente el nivel de seguridad.
- Los administradores pueden, opcionalmente, lanzar la conexión inmediatamente después de la validación del usuario mediante un script predefinido, realizar una comprobación de nivel de seguridad del cliente o, a petición del usuario pulsando en el icono del Conector de Red en la página del portal, después de ser autorizado.

Lo mejor de ambos mundos

IAG 2007 se integra con ISA Server 2006 en un equipo unificado y consolidado para la defensa de la red perimetral, la gestión de los accesos remotos y la protección del nivel de aplicación sobre conexiones SSL e IPsec. Con ello las empresas disponen de más alternativas para resolver sus necesidades de acceso remoto. La integración de VPN sobre SSL dentro de la infraestructura actual de Microsoft soporta el acceso a aplicaciones y servicios, tanto de Microsoft como de otros fabricantes, todo ello utilizando un solo equipo.

Los equipos IAG 2007 ofrecen un nuevo diseño, optimizado y económico, que permite reducir el coste total de propiedad y elimina la necesidad de implementar múltiples dispositivos de fabricantes distintos para cada uno de los métodos de acceso. Su grupo de IT corporativo puede disponer de una solución consolidada de seguridad en un único equipo de hardware, flexible y fácil de instalar.

Seguridad para la red perimetral

ISA Server, en combinación con el Intelligent Application Gateway, resuelve la necesidad de aislamiento de las redes y pleno control del tráfico y contenidos en ambas direcciones, y añade una serie de funcionalidades de seguridad perimetral esenciales para hacer frente a la gran cantidad de amenazas que proceden de Internet.

El equipo consolidado supone una solución flexible, basada en software, con una elevada capacidad de respuesta, necesaria para garantizar un óptimo rendimiento, mantenimiento y escalabilidad, además de una solución completa de seguridad. La integración del filtrado de paquetes a nivel de contenidos, filtrado de circuitos y filtros de nivel de aplicación, junto con la función de proxy Web y la seguridad del punto de conexión dentro de un mismo dispositivo pone en manos de los administradores un amplio abanico de opciones para gestionar mediante políticas configurables el acceso a las aplicaciones y recursos de la red

ISA Server es capaz de filtrar el tráfico, superando las soluciones puramente mecánicas, y ofrece tres tipos de funcionalidad de firewall: filtrado de paquetes (también conocido como capa de circuito), inspección de contenidos (stateful), y filtrado de nivel de aplicación. La capacidad de aplicar filtros basados en reglas a todo el tráfico que atraviesa la barrera de la red corporativa hace posible que esta solución combinada detenga directamente amenazas como gusanos o malware que pueden introducir usuarios no autenticados.

Microsoft
**Internet Security &
Acceleration Server 2006**

Más información sobre Intelligent Application Gateway 2007, en el sitio Web <http://www.microsoft.es/forefront/edge/default.aspx>.

Esta hoja de producto se publica con fines informativos exclusivamente. MICROSOFT NO OFRECE GARANTIAS, EXPRESAS O IMPLÍCITAS, EN ESTE RESUMEN.

© 2007 Microsoft Corporation. Todos los derechos reservados