



McAfee Web Gateway

Seguridad. Inteligencia conectada. Rendimiento.

McAfee Web Gateway

- Certificación Common Criteria EAL2+ y FIPS 140-2 Level 2.
- Disponible en varios modelos de hardware y como una máquina virtual que admite VMware y Microsoft Hyper-V.
- Integrado con las soluciones de Intel® Security complementarias, incluidas McAfee Advanced Threat Defense y McAfee Threat Intelligence Exchange.
- Calificado como antimalware número uno en un gateway de seguridad web (AV-TEST).

Las organizaciones pueden hacer hoy más cosas que nunca por Internet. La Web actual ofrece al usuario una experiencia dinámica y en tiempo real. Sin embargo, también se ha convertido en un lugar más peligroso, en el que se detectan ataques cada vez más sofisticados. McAfee® Web Gateway es una defensa fundamental a disposición de toda organización que desee protegerse frente a las nuevas amenazas de malware. Mediante este gateway, las organizaciones pueden permitir el acceso, reduciendo al mismo tiempo considerablemente su nivel de riesgo mediante el empleo de una estrategia de seguridad avanzada que combina un eficaz análisis local de intenciones con una protección alojada en la nube, facilitada por McAfee Labs.

Al ritmo que aumentan el uso y la sofisticación de Internet, también es mayor la necesidad de contar con seguridad avanzada para la Web. Incluso los sitios que son aparentemente "seguros" pueden ser objetivo de un ataque de malware.

En el mundo actual, ya no basta con bloquear los virus conocidos o limitar el acceso a los sitios web que se sabe que son maliciosos. Las técnicas reactivas, como los antivirus basados en firmas y el filtrado de URL basado exclusivamente en categorías, aunque necesarias, no bastan para proteger el acceso a las aplicaciones de la nube o combatir los ataques actuales.

Y dado que estas soluciones se centran en contenidos conocidos y en objetos o ejecutables maliciosos, no pueden prevenir los ataques actuales que ocultan código malicioso en el tráfico HTTP o HTTPS aparentemente fiable, ni proporcionar protección frente a las amenazas nuevas y desconocidas. La capacidad para permitir un acceso seguro y diferenciado a las aplicaciones de la nube y bloquear proactivamente las amenazas desconocidas y conocidas es crucial.

Protección total entrante y saliente

McAfee Web Gateway ofrece seguridad integral para todos los aspectos del tráfico de la Web, en una arquitectura de software de dispositivo de alto rendimiento. Para las solicitudes web iniciadas por el usuario, McAfee Web Gateway aplica en primer lugar la directiva de uso de Internet de la empresa. A continuación, para todo el tráfico permitido, utiliza técnicas locales y globales para analizar la naturaleza y la intención de todo el contenido y el código activo que entran en la red a través de las páginas web solicitadas, con el fin de proporcionar protección inmediata frente al malware y otras amenazas ocultas. Y, a diferencia de las técnicas básicas de inspección de paquetes, McAfee Web Gateway puede examinar el tráfico SSL con el fin de ofrecer protección exhaustiva contra código malicioso o aplicaciones de control que se han ocultado mediante técnicas de cifrado.

La protección del tráfico entrante reduce también el riesgo para las organizaciones que albergan sitios web que aceptan cargas de datos o de documentos de fuentes externas. McAfee Web Gateway en modo proxy inverso analiza todo el contenido antes de que se cargue, protegiendo de esta forma tanto el servidor como el contenido.

Para proteger el tráfico saliente, McAfee Web Gateway utiliza la tecnología Intel® Security Data Loss Protection, líder del sector, para analizar el contenido generado por el usuario en todos los protocolos web principales, incluidos HTTP, HTTPS y FTP. Además, protege contra pérdida de información confidencial, sensible o sometida a normativas, que se filtra desde la organización a través de sitios de redes sociales, blogs, wikis o herramientas de productividad online, como el correo, los organizadores y los calendarios basados en la Web. McAfee Web Gateway también evita que los datos no autorizados salgan de la organización a través de equipos infectados por bots que intentan enviar información al atacante o transmitir datos confidenciales.

McAfee Web Gateway proporciona la mejor protección del sector

McAfee Web Gateway, que es la solución de seguridad de la Web líder en protección contra malware¹, emplea una modalidad de análisis de intenciones sin firmas patentada, con el motor McAfee Gateway Anti-Malware Engine. El análisis preventivo de intenciones filtra el contenido malicioso, desconocido o zero-day, del tráfico de la Web, en tiempo real. McAfee Web Gateway analiza el contenido activo de una página web, emula y aclara su comportamiento, y prevé su intención. De esta forma, impide que se distribuya malware zero-day a los endpoints, reduciendo enormemente los costos asociados a la limpieza y reparación de los sistemas.

Nosotros combinamos este análisis con el antivirus de Intel Security y las tecnologías de reputación global de McAfee Labs, para bloquear rápidamente el malware conocido y los sitios maliciosos. El uso de varias tecnologías permite a McAfee Web Gateway ofrecer una mayor protección y, al mismo

tiempo, optimizar la seguridad en una única plataforma con tecnologías diferentes, pero complementarias, algo que muchas empresas demandan para sus estrategias de defensa en profundidad.

- **Antivirus de McAfee con reputación de archivos en tiempo real de McAfee Global Threat Intelligence (McAfee GTI):** las funciones de consulta de la reputación de archivos de McAfee GTI basadas en la nube cierran la brecha entre el descubrimiento de los virus y la actualización y protección del sistema.
- **Clasificación web y de reputación de McAfee GTI:** McAfee Web Gateway proporciona una función de filtrado y protección web, mediante la eficaz combinación de filtrado basado en la reputación y filtrado basado en categorías. McAfee GTI crea un perfil de todas las entidades de Internet (sitios web, correo electrónico, direcciones IP) basándose en cientos de atributos diferentes recogidos de las numerosas funciones de recopilación global de datos de los laboratorios McAfee Labs. Seguidamente asigna una puntuación de reputación basada en el riesgo que plantea para la seguridad, permitiendo a los administradores aplicar reglas muy diferenciadas en cuanto a lo que se debe permitir o denegar.
- **Geolocalización:** McAfee Web Gateway incluye geolocalización, por lo que ofrece visibilidad geográfica y administración de directivas basada en el tráfico web y el país de origen del usuario.

Tanto para la clasificación web como para la reputación web, las organizaciones pueden elegir entre búsquedas in situ, en la nube o una combinación de ambas opciones. Las búsquedas en la nube eliminan los intervalos de desprotección entre el momento de detección/cambio y la actualización del sistema, y ofrecen una amplia cobertura con datos de cientos de millones de muestras de malware exclusivas.

Integración con Advanced Threat Defense (ATD)

McAfee Web Gateway se integra con McAfee Advanced Threat Defense—la tecnología avanzada de detección de malware de Intel Security que combina entornos aislados personalizables con análisis detallado de código estático. Advanced Threat Defense, junto a las funciones de análisis en línea del motor Gateway Anti-Malware Engine de McAfee Web Gateway proporcionan la solución más potente disponible para la protección contra amenazas que llegan por Internet.

Intercambio de inteligencia sobre amenazas

En la actualidad, los componentes de la arquitectura de seguridad de muchas organizaciones no se comunican, y no se diseñan para compartir inteligencia sobre amenazas, a pesar de la información que existe en los endpoints, redes, soluciones SIEM, gateways, etc. Si se comparte esta información, se puede aprovechar para mejorar la protección frente a amenazas, la detección de fugas y la corrección eficaz de los sistemas comprometidos. Sin embargo, gracias a McAfee Threat Intelligence Exchange, las soluciones de Intel Security, incluida McAfee Web Gateway, comparten información para llenar estos vacíos. McAfee Web Gateway juega un papel fundamental en este proceso, ya que crea y comparte las reputaciones de nuevos archivos para la detección de malware zero-day descubierto por el motor Gateway Anti-Malware, lo que permite, por ejemplo, proteger los dispositivos endpoint antes de que se distribuyan nuevos DAT. Además, McAfee Web Gateway bloquea más amenazas, gracias a la inteligencia sobre amenazas que proporciona McAfee Threat Intelligence Exchange.

Protección para el tráfico cifrado

Los sofisticados ciberdelincuentes han recurrido al tráfico SSL (HTTPS) como puerta trasera por la que atravesar la barrera de seguridad de la empresa. Es irónico que incluso un protocolo diseñado para proporcionar seguridad deba evaluarse para descubrir si presenta riesgos. McAfee Web Gateway es el primer producto de seguridad que integra completamente la detección de malware, la inspección SSL y la validación con certificados. Ya no es necesario

dirigir el tráfico cifrado a otro buzón para la inspección SSL. McAfee Web Gateway analiza directamente todo el tráfico SSL para garantizar la completa seguridad, integridad y privacidad de las transacciones cifradas.

Prevención de la pérdida de datos

McAfee Web Gateway protege a las organizaciones de las amenazas salientes (como fugas de información confidencial) mediante el análisis de los contenidos que salen de la organización con los principales protocolos web, como SSL. Esto lo convierte en una herramienta eficaz para evitar la pérdida de propiedad intelectual, proteger y documentar el cumplimiento de normativas, y proporcionar datos de análisis forense en caso de incidente. Gracias a la solución McAfee Data Loss Prevention (DLP), McAfee Web Gateway incluye diccionarios de prevención de fuga de datos (DLP) predefinidos y permite crear diccionarios personalizados mediante la correlación de palabras clave, el uso de expresiones regulares o ambos.

Para las organizaciones que emplean almacenamiento basado en la nube, el cifrado de archivos integrado protege los datos que se cargan en sitios para compartir archivos o colaborar, para evitar el acceso no autorizado. Los usuarios no pueden recuperar y ver los datos sin pasar por McAfee Web Gateway.

Protección de los usuarios fuera de la red

Dado que la plantilla cada vez está más distribuida y es más móvil, jamás ha sido tan importante contar con filtrado y protección web durante la transición de la oficina a la calle con el fin de evitar que surjan problemas. McAfee Client Proxy, un agente cliente a prueba de manipulaciones, permite a los usuarios itinerantes autenticar el tráfico y redirigirlo fácilmente a una instalación de Web Gateway in situ, en una DMZ, o al servicio McAfee Web Gateway Cloud Service. Esto permite someter a los usuarios itinerantes o remotos a las directivas de acceso a Internet y a análisis completos de la seguridad, incluso cuando obtienen acceso a Internet a través de portales públicos, como cafeterías, hoteles u otros puntos de acceso Wi-Fi.

McAfee Web Gateway también permite a las empresas extender e implementar sus directivas de seguridad a dispositivos móviles dirigiendo el tráfico web a McAfee Web Gateway. Mediante controles de seguridad y administración de dispositivos estándar, Web Gateway garantiza que los dispositivos móviles estén protegidos con antimalware avanzado y directivas de filtrado web corporativas. Además, extiende la protección a los dispositivos móviles que acceden a los contenidos tradicionalmente disponibles en servidores empresariales internos, como intranets, wikis, servidores Microsoft SharePoint y otras soluciones basadas en la Web. Aunque generalmente esta información no está disponible para determinados dispositivos móviles por razones de seguridad, cuando se despliega como un proxy inverso, McAfee Web Gateway puede permitir el acceso controlado y seguro a estos recursos internos.

Máxima flexibilidad con McAfee Web Gateway

McAfee Web Gateway incluye un potente motor basado en reglas que proporciona flexibilidad y control de las directivas. Para agilizar la creación de directivas, McAfee Web Gateway ofrece una extensa biblioteca de reglas predefinidas con acciones comunes de directivas. Las organizaciones pueden elegir varias reglas y modificarlas con facilidad, así como compartir sus propias reglas a través de una comunidad online. Para una administración avanzada, la exclusiva combinación de criterios de reglas basadas en el contexto y listas compartidas abre la puerta a infinitas posibilidades para solucionar problemas y optimizar la seguridad de la Web. El seguimiento interactivo de las reglas simplifica su depuración.

McAfee Web Gateway extiende el control a las aplicaciones en la nube, permitiendo ejercer un control diferenciado, basado en proxy, del uso de las aplicaciones web. Las empresas pueden aplicar más de 1600 controles a aplicaciones en la nube, para activar o desactivar funcionalidades específicas según convenga, así como controlar quién utiliza una aplicación web y cómo. ¿Desea permitir el acceso a Dropbox pero no autorizar las cargas? Es posible.

La flexibilidad y el control también se extienden a la autenticación y el acceso de usuarios. McAfee Web Gateway admite un buen número de métodos de autenticación, incluidos NTLM, RADIUS, AD/LDAP, eDirectory, autenticación de cookies, Kerberos o una base de datos de usuarios local. El motor de autenticación de McAfee Web Gateway permite a los administradores implementar reglas flexibles, así como utilizar varios métodos de autenticación. Por ejemplo, McAfee Web Gateway puede intentar autenticar de forma transparente a un usuario y, en función del resultado, solicitarle las credenciales, utilizar otro método de autenticación, aplicar una directiva restrictiva o simplemente denegarle el acceso.

McAfee Web Gateway Identity, un complemento opcional, incluye conectores de inicio de sesión único (SSO) para cientos de aplicaciones populares alojadas en la nube. McAfee Web Gateway Identity permite mejorar la seguridad y reducir las llamadas a asistencia por temas relacionados con las contraseñas, mediante una plataforma de lanzamiento de inicio de sesión único (SSO) que permite a los usuarios acceder a las aplicaciones en la nube autorizadas, con un solo clic. La compatibilidad con conectores HTTP POST y SAML (Security Assertion Markup Language) ofrece cobertura para una amplia gama de aplicaciones. Los conectores permiten a los administradores crear y cancelar cuentas de usuario en determinadas aplicaciones de software como servicio (SaaS).

McAfee Web Gateway extiende también el control de acceso al contenido transmitido a través de la función proxy de transmisión nativa, lo que ahorra ancho de banda y reduce la latencia. Pueden establecerse controles de ancho de banda adicionales para aplicar mínimos, máximos y establecer prioridades para determinados tipos de tráfico, lo que permite a las empresas optimizar el uso del ancho de banda del que disponen.

Agilidad para la infraestructura y el rendimiento con McAfee Web Gateway

McAfee Web Gateway es un proxy de alto rendimiento y de categoría empresarial, que se ofrece dentro de una familia de modelos de dispositivos que integran alta

disponibilidad, compatibilidad con máquinas virtualizadas y despliegue híbrido con el servicio **McAfee Web Gateway Cloud Service**. McAfee Web Gateway proporciona flexibilidad de despliegue y rendimiento, junto con la capacidad de ampliación para dar soporte con facilidad a cientos de miles de usuarios en un único entorno.

Además, se pueden combinar las opciones de despliegue. Por ejemplo, puede dirigir todo el tráfico web al dispositivo in situ para los usuarios conectados a la red, y dirigir al servicio en la nube a todos los usuarios no conectados a la red, para eliminar el costo de transmitir el tráfico a través de líneas MPLS o VPN. La sincronización automatizada de directivas y la generación de informes para despliegues in situ y en la nube híbridos facilitan la administración, garantizan una implementación coherente de las directivas y simplifican la generación de informes, la supervisión y la investigación.

McAfee Web Gateway ofrece numerosas opciones de implementación, desde el modo proxy explícito a los modos de puente y enrutador transparentes, para garantizar la compatibilidad con la arquitectura de su red.

Compatible con numerosas normas de integración, McAfee Web Gateway está diseñado para trabajar en el entorno específico de su organización. Sea cual sea el protocolo utilizado, WCCP (Web Cache Communication Protocol), ICAP/ICAPS (Internet Content Adaptation Protocol), WebSocket o SOCKS, McAfee Web Gateway se comunica con eficacia con todos los demás dispositivos de la red y los dispositivos de seguridad.

Además, McAfee Web Gateway ofrece compatibilidad con IPv6 para ayudar a las grandes organizaciones y organismos estatales a cumplir con las normativas. McAfee Web Gateway salva la distancia entre las redes IPv4 internas e IPv6 externas y aplica al tráfico todas las características y funciones de seguridad e infraestructura disponibles.

Plataforma unificada para el futuro

McAfee Web Gateway combina e integra numerosas protecciones que de otro modo requerirían varios productos independientes. El filtrado de URL, antivirus, antimalware zero-day, análisis SSL, prevención de pérdida de datos y la administración central están unificados en una arquitectura de software de dispositivo. La administración de despliegues está unificada en todos los formatos, de manera que puede ampliarse una directiva a dispositivos in situ, clústeres de dispositivos, dispositivos virtuales y servicios en la nube, desde una sola consola de administración.

Gestión de riesgos de seguridad y generación de informes

McAfee Web Gateway es compatible con la conocida y respetada plataforma de administración de la seguridad, McAfee ePolicy Orchestrator® (McAfee ePO™), como fuente única de todos los informes de seguridad.

El software McAfee ePO permite la generación de informes de seguridad web detallados mediante la extensión McAfee Content Security Reporter. McAfee Content Security Reporter proporciona información y herramientas de análisis forense para saber de qué forma utiliza su organización la Web, identificar las instancias de aplicaciones desconocidas o falsas, las denominadas "shadow IT", cumplir las normativas, identificar tendencias, aislar problemas y personalizar su configuración de filtrado con el fin de implementar sus directivas de uso de Internet. McAfee Content Security Reporter ofrece un servidor de informes externo e independiente diseñado para descargar del servidor de McAfee ePO las tareas de procesamiento y almacenamiento de datos que consumen muchos recursos, lo que le permite satisfacer las necesidades de informes incluso de las multinacionales más grandes.

Licencias

Para disponer de la máxima flexibilidad de despliegue y asegurar su inversión en el futuro, Intel Security ofrece todas las funciones de McAfee Web Gateway y el servicio McAfee Web Gateway Cloud Service en una única suite: **McAfee Web Protection**. Puede realizar el despliegue in situ, en la nube, o ambos para una mayor flexibilidad y la mayor disponibilidad. Usted elige. Todas las opciones le permitirán disfrutar de la galardonada protección antimalware y filtrado web completo de Intel Security.

El hardware de McAfee Web Gateway se vende por separado.



McAfee. Part of Intel Security.

6205 Blue Lagoon Drive
Suite 600
Miami, Florida 33126
U.S.A.
www.intelsecurity.com

1. En pruebas realizadas por AV-TEST, McAfee Web Gateway detectó el 94,5 % del malware de tipo zero-day, el 99,8 % de los archivos PE para Windows 32 maliciosos y el 98,63 % de archivos no PE. "McAfee Web Gateway Security Appliance Test", (prueba de McAfee Web Gateway Security Appliance), AV-TEST GmbH.

Intel y los logotipos de Intel y McAfee, ePolicy Orchestrator y McAfee ePO son marcas comerciales de Intel Corporation o McAfee, Inc. en EE. UU. y/o en otros países. Los demás nombres y marcas pueden ser reclamados como propiedad de otros. Copyright © 2016 Intel Corporation. 1758_0916
SEPTIEMBRE DE 2016