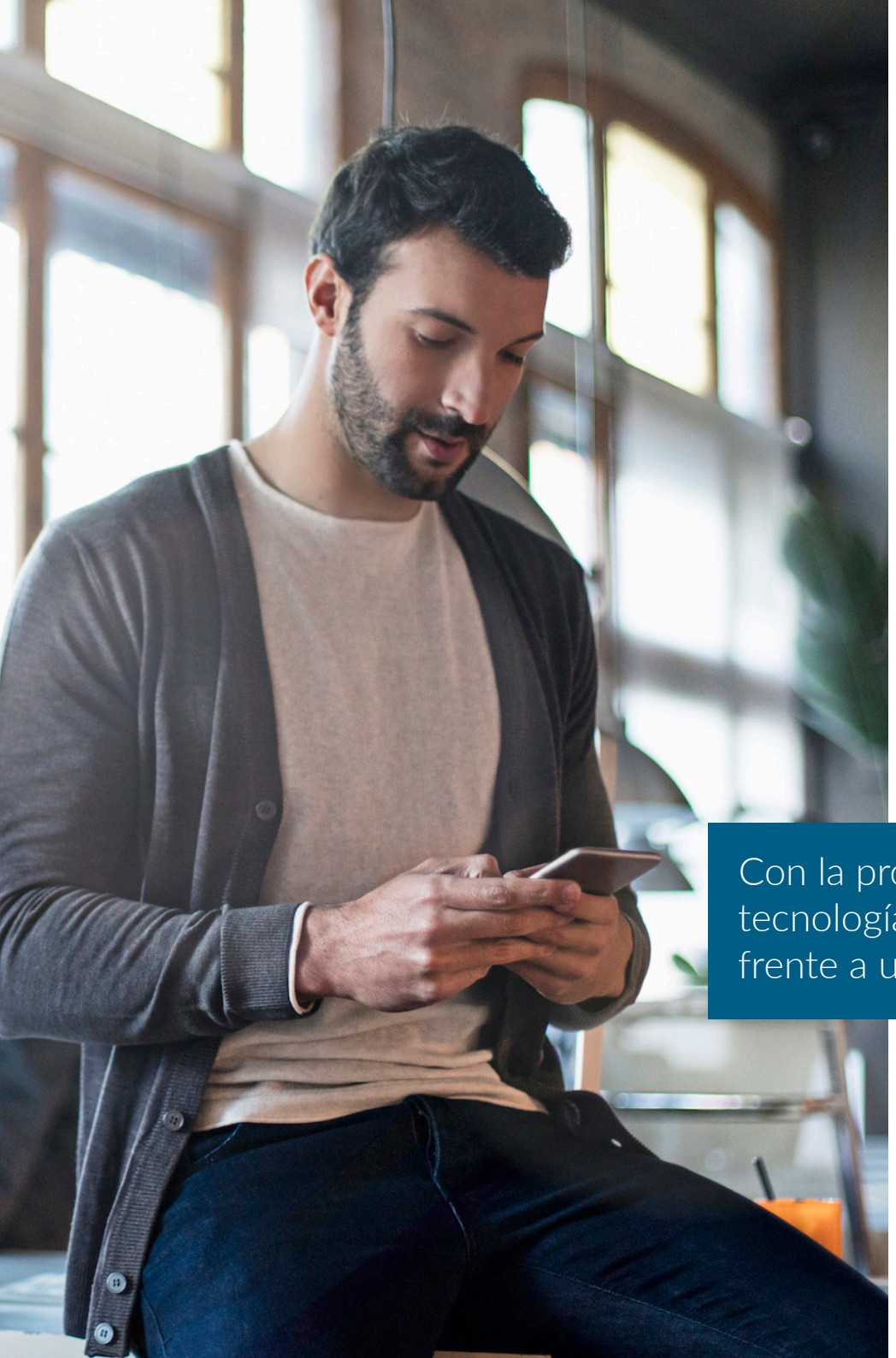
11 FUNCIONES IMPRESCINDIBLES QUE DEBERÍA TENER SU CORTAFUEGOS

Además de bloquear las amenazas a la red, proteja, gestione y controle el tráfico de las aplicaciones

SONICWALL®

Índice

SONICWALL®



El papel del cortafuegos crece

Los cortafuegos tradicionales de inspección dinámica de paquetes se centran en bloquear las amenazas a la capa de red evaluando los puertos y los protocolos utilizados por el tráfico de la capa de red. Los cortafuegos de última generación (NGFW) profundizan en la inspección de paquetes, analizando toda la carga de estos para ofrecer funciones avanzadas de prevención de intrusiones, antimalware, filtración de contenidos y antispam. Muchas de las aplicaciones que se distribuyen en la web lo hacen a través de puertos comunes y protocolos HTTP o HTTPS. En la práctica, esto hace que los cortafuegos tradicionales sean incapaces de ver estas aplicaciones y no puedan dar prioridad al tráfico productivo y seguro frente al tráfico improductivo y potencialmente poco seguro. Los cortafuegos de última generación ofrecen información sobre las propias aplicaciones, algo fundamental para los profesionales de las redes.

Con la proliferación de la informática en la nube y las tecnologías de la web 2.0, los cortafuegos han de hacer frente a un nuevo desafío: el control de aplicaciones.

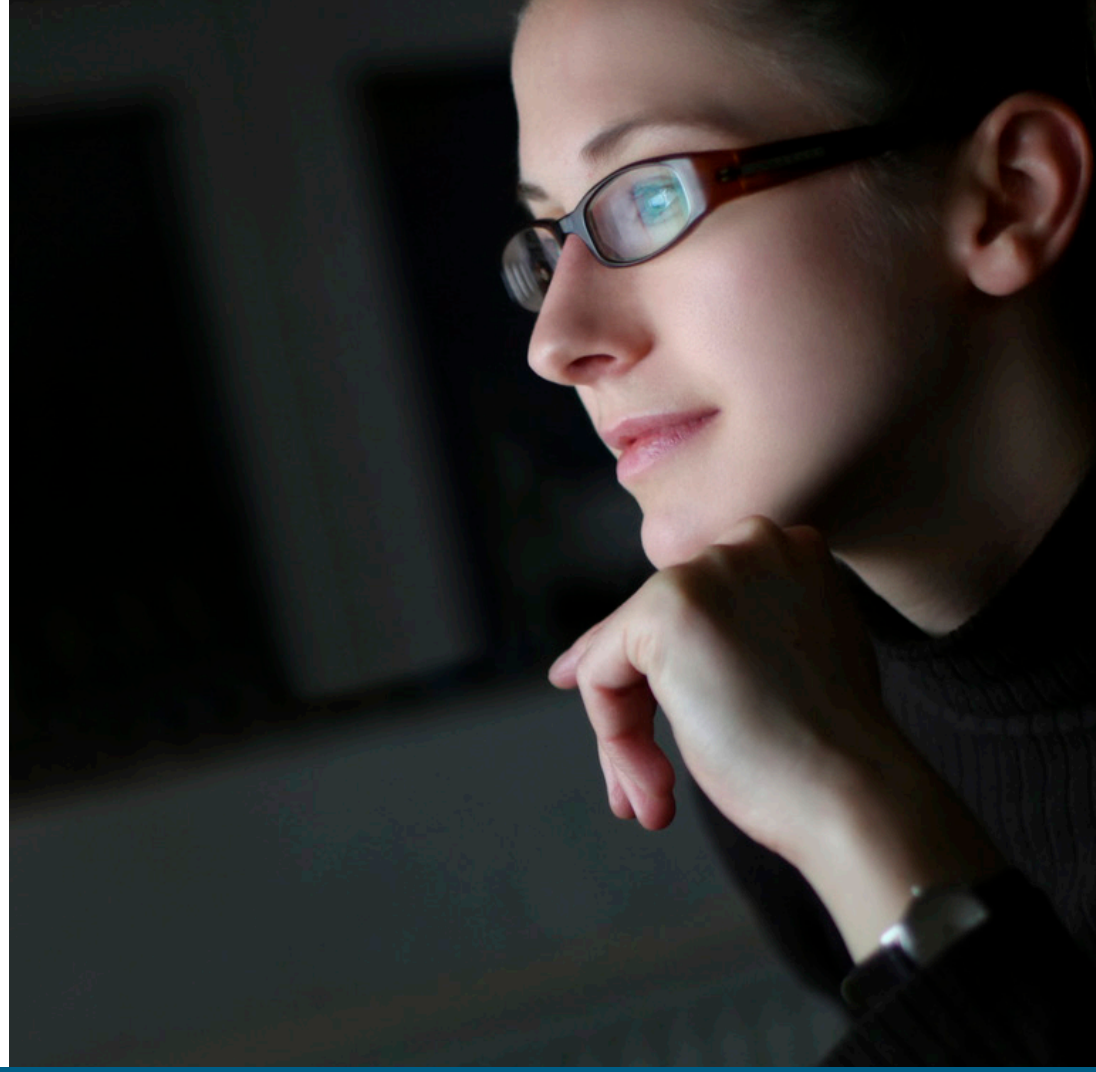
SONICWALL®

What does SonicWall Application Intelligence and Control do?

Los cortafuegos SonicWall le permiten identificar y controlar todas las aplicaciones que se utilizan en su red. Este control adicional mejora el cumplimiento normativo y la prevención de las pérdidas de datos, ya que identifica las aplicaciones en función de sus firmas únicas en lugar de los puertos o protocolos. Esto se consigue visualizando el tráfico de las aplicaciones para determinar los patrones de uso y, a continuación, creando directivas pormenorizadas para las aplicaciones, los usuarios o incluso los grupos de usuarios, además de la hora del día y otras variables, lo que permite un control flexible que puede adaptarse a cualquier necesidad de red.

¿Cómo funciona SonicWall Application Intelligence and Control (Información y Control sobre las Aplicaciones de SonicWall)?

Con ayuda de una amplia base de datos de firmas de aplicaciones que crece constantemente y se actualiza de forma automática, SonicWall identifica las aplicaciones en función de su «ADN», en lugar de atributos menos indicativos, como el puerto de origen, el puerto de destino o el tipo de protocolo. Por ejemplo, puede permitir la llegada de mensajería instantánea, pero bloquear la transferencia de archivos, o permitir el acceso a Facebook, pero bloquear el acceso a juegos basados en esta red social. Estos controles también están disponibles para el tráfico cifrado TLS/SSL, que debe inspeccionarse igual que las conexiones no cifradas. Además, usted puede visualizar fácilmente los resultados de los controles, lo que le permitirá ajustar el uso de las aplicaciones y optimizar el ancho de banda de la red.



Categorías de control de aplicaciones, aplicaciones individuales y funciones específicas dentro de las aplicaciones.

La visualización de aplicaciones le permite «ver» qué navegadores se utilizan antes de crear la directiva.

1.ª función imprescindible:

Controlar las aplicaciones que se permiten en la red

Usted quiere asegurarse de que todos sus empleados utilizan la última versión de Internet Explorer. Su misión consiste en asegurarse de que todos los empleados que accedan a IE9 o IE10 sean redirigidos automáticamente al sitio de descarga de IE11 y no puedan acceder a ningún otro sitio web. Estas son algunas de las posibles soluciones:

- Comprobar físicamente todos los sistemas cada día para ver qué versión del navegador web se utiliza
- Escribir un *script* personalizado para comprobar automáticamente las versiones del navegador
- Establecer una directiva con ayuda de SonicWall Application Intelligence and Control (Información y Control sobre las Aplicaciones de SonicWall) y dejar de preocuparse

Crear una directiva para que los usuarios de IE9 o IE10 sean redirigidos a la página de descarga del navegador IE más reciente y para que el acceso a internet con IE9 o IE10 quede bloqueado

1. El motor de inspección profunda de paquetes (DPI) busca al agente de usuario = IE 9.0 o al agente de usuario = IE 10.0 en el encabezado HTTP
2. La directiva redirige a los usuarios de IE9 o IE10 al sitio de descarga de IE11 y bloquea el acceso a otros sitios web desde IE9 o IE10

SONICWALL®

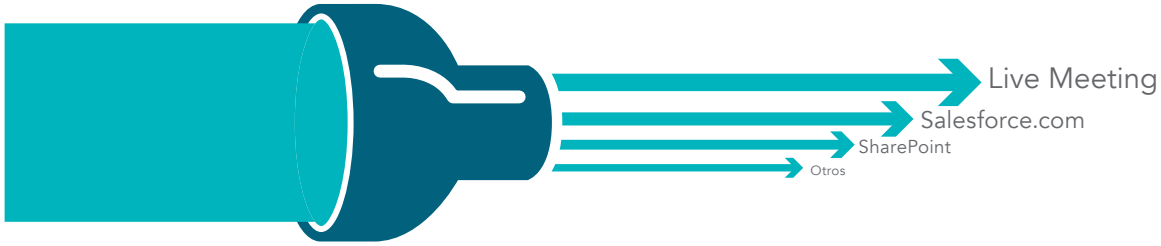
2.ª función imprescindible:

Gestionar el ancho de banda para aplicaciones críticas

Muchas aplicaciones críticas, como Live Meeting, Salesforce.com® y SharePoint®, se basan en la nube o se ejecutan en redes geográficamente dispersas. Garantizar que estas aplicaciones tengan prioridad sobre la navegación improductiva mejora la productividad de la empresa.

Crear una directiva para dar prioridad de ancho de banda a la aplicación Live Meeting

1. El motor de inspección profunda de paquetes busca la firma o el nombre de la aplicación
2. Asigne una prioridad de ancho de banda superior a la aplicación Live Meeting



La prioridad de la aplicación puede basarse en la fecha (un ejemplo sería la prioridad de las aplicaciones de ventas al finalizar un trimestre).

SONICWALL®

3.ª función imprescindible:

Bloquear las aplicaciones de punto a punto

Las aplicaciones de punto a punto (P2P) improductivas, como BitTorrent, suelen utilizarse para descargar versiones sin licencia de elementos protegidos por derechos de autor, y pueden consumir mucho ancho de banda o transmitir malware. Sin embargo, la creación de nuevas aplicaciones P2P o la introducción de cambios sencillos (p. ej., números de versión) en las aplicaciones P2P existentes son constantes, por lo que bloquear manualmente una aplicación P2P concreta resulta difícil.

SonicWall actualiza continuamente la información sobre aplicaciones y la base de datos de control para añadir nuevas aplicaciones P2P en cuanto están disponibles. Ahora puede crear una sola directiva que le permita bloquear todas las aplicaciones P2P en el futuro.

Crear una directiva para bloquear el uso de aplicaciones P2P

1. El motor de inspección profunda de paquetes emplea firmas de aplicaciones P2P predefinidas procedentes de la lista de firmas de aplicaciones
2. Elija las aplicaciones P2P de la lista de firmas predefinidas
3. Aplique la directiva a todos los usuarios
4. Bloquee las aplicaciones P2P mediante restricciones basadas en el ancho de banda y en el tiempo

Lista de firmas de aplicaciones

BitTorrent-6.1
BitTorrent-6.0.3
BitTorrent-6.0.2
BitTorrent-6.0.1
... y cientos más

+

Lista de firmas de aplicaciones

Se reciben y aplican las actualizaciones de SonicWall

=

Lista de firmas de aplicaciones

BitTorrent-6.1.1
BitTorrent-6.1
BitTorrent-6.0.3
BitTorrent-6.0.2
... y cientos más

Los resultados

- Usted puede gestionar y controlar las aplicaciones P2P
- Usted no tiene que dedicar su tiempo a actualizar las reglas de firmas de los IPS rules

4.ª función imprescindible:

Bloquear los componentes improductivos de las aplicaciones

Las aplicaciones de redes sociales como Facebook, Instagram y YouTube se han convertido en nuevos canales de comunicación para individuos particulares y empresas. Aunque bloquear todas las aplicaciones de redes sociales puede ser contraproducente, es muy posible que desee controlar su uso en el trabajo.

Por ejemplo, tal vez quiera que el personal de marketing pueda actualizar la página de Facebook de la empresa, pero no permitir que jueguen a juegos de Facebook como Texas HoldEm Poker o Candy Crush Saga. Con información y control sobre las aplicaciones, usted puede crear una directiva que permita el acceso a Facebook, pero bloquee los juegos.

Crear una directiva que permita el acceso a Facebook, pero bloquee los juegos de Facebook

1. Seleccione «Todos» los usuarios
2. Seleccione la categoría «Aplicaciones de juegos de Facebook»
3. Cree una sola regla para «bloquear» el acceso a los juegos de Facebook para todos los usuarios

También puede permitir que se chatee pero bloquear la transferencia de archivos a través del chat.

5.ª función imprescindible:

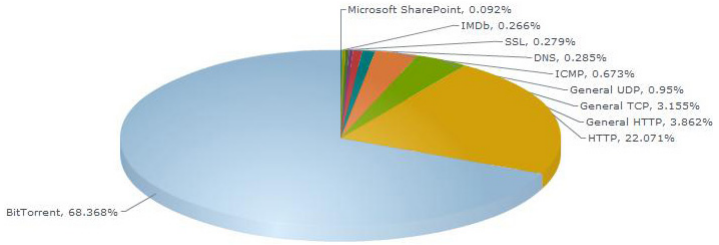
Visualizar el tráfico de sus aplicaciones

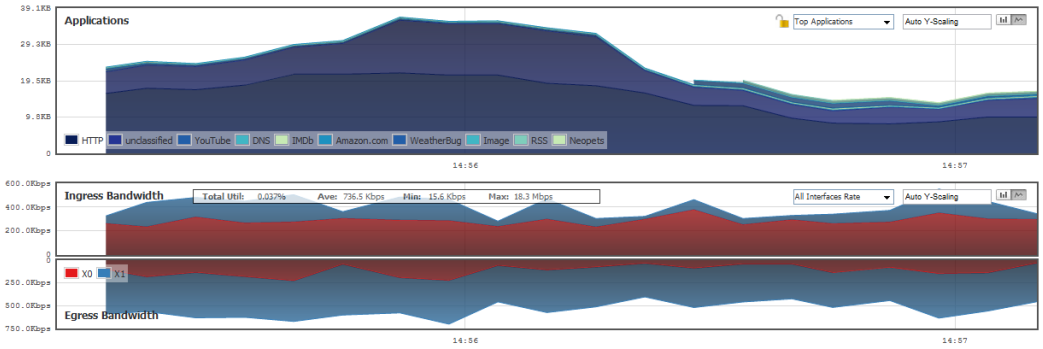
¿Qué sucede en mi red? ¿Quién está consumiendo mi ancho de banda? ¿Por qué va tan lenta mi red? ¿Se ha planteado alguna vez estas preguntas? Para darles respuesta podría utilizar una combinación de herramientas independientes, pero esto le llevaría mucho tiempo y solo le daría información una vez ocurridos los hechos. La visualización en tiempo real del tráfico de las aplicaciones de SonicWall le permite responder a estas preguntas al instante, diagnosticar rápidamente los problemas, detectar usos inadecuados de la red, crear directivas adecuadas y comprobar de inmediato la eficacia de dichas directivas.

Ver todo el tráfico en tiempo real iniciando sesión en Application Flow Monitor (Monitor de Flujo de Aplicaciones)

1. Consulte los gráficos en tiempo real de todo el tráfico de las aplicaciones
2. Consulte los gráficos en tiempo real del ancho de banda de entrada y salida
3. Consulte los gráficos en tiempo real de los sitios web visitados y de la actividad del usuario
4. Cree un filtro propio que le proporcione la información más relevante

La visualización proporciona a los administradores información instantánea sobre los flujos de tráfico de la red.





SONICWALL®

6.ª función imprescindible:

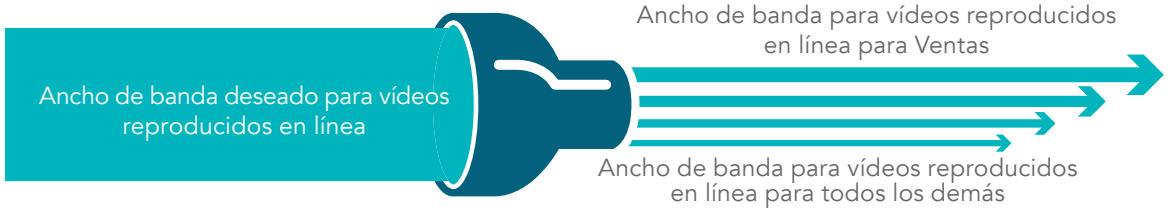
Gestionar el ancho de banda de un grupo de usuarios

¿Qué puede hacer si su director ejecutivo se queja de que los vídeos de noticias de negocios que quiere ver cada mañana se entrecortan y no se reproducen correctamente? Tras indagar un poco, llega a la conclusión de que el motivo es una directiva de administración del ancho de banda que usted implementó a nivel empresarial para los vídeos reproducidos en línea. Antes tendría que reducir las restricciones de ancho de banda para todos, pero ahora hay una solución mejor: la gestión del ancho de banda basada en grupos.

Crear una directiva para excluir al equipo directivo de la administración de ancho de banda para los vídeos reproducidos en línea

1. Elija el grupo directivo importado del servidor LDAP
2. El motor de inspección profunda de paquetes emplea firmas de aplicaciones de vídeos en línea predefinidas procedentes de la lista de firmas de aplicaciones
3. Aplique la restricción de ancho de banda al tráfico que presente ese encabezado

Muchas empresas han descubierto que los empleados están más contentos si se les permite disfrutar de un acceso completo a internet, aunque el ancho de banda para visitar sitios improductivos sea reducido.



SONICWALL

7.ª función imprescindible:

Bloquear los ataques de *ransomware* y las violaciones de datos

La seguridad de la red debe ser un aspecto prioritario para cualquier administrador de TI. La capacidad de bloquear ataques como el *ransomware* y las violaciones de datos que se producen a través del malware y los intentos de intrusión libera a la organización de grandes riesgos y ahorra recursos que pueden estar malgastándose. Los servicios de seguridad de SonicWall, que se basan en la arquitectura de última generación de SonicWall, de alto rendimiento y latencia ultrabaja, son capaces de bloquear el acceso a la red de millones de amenazas conocidas y desconocidas antes de que se conviertan en un peligro para su compañía. SonicWall Capture amplía la capacidad de prevención de amenazas del cortafuegos mediante la detección y la prevención de ataques desconocidos y de día cero a través de un servicio de entornos aislados multimotores basados en la nube.

Bloquee los ataques y las intrusiones de *malware* antes de que lleguen a su red.

SONICWALL®

8.ª función imprescindible:

Identificar las conexiones por país

¿Una conexión a una IP de un país extranjero realizada desde su oficina o una sucursal de su empresa es una conexión inofensiva de alguien que está navegando por internet o se trata de un ataque *botnet*? Puede utilizar la identificación del tráfico por países de GeoIP para identificar y controlar el tráfico de red que entra o sale de países específicos con el fin de protegerse frente a ataques de orígenes conocidos o presuntos de actividades amenazantes, o para investigar el tráfico sospechoso que se origina en la red.

Ver las conexiones por país o crear filtros específicos para un país

1. Compruebe qué aplicaciones se conectan a direcciones IP de otros países
2. Vea qué usuarios y equipos se conectan a direcciones IP de otros países
3. Cree filtros para restringir el tráfico de los países que desee aplicando listas de exclusión

Una vez que conozca la respuesta a la pregunta, podrá hablar con el usuario, inspeccionar el equipo que tenga la dirección IP infractora o habilitar una función de captura de paquetes en el cortafuegos para analizar exactamente lo que ocurre con esa conexión. Gracias a la identificación de tráfico por países de SonicWall GeoIP, podrá determinar y abordar problemas que de otro modo desconocería.

9.ª función imprescindible:

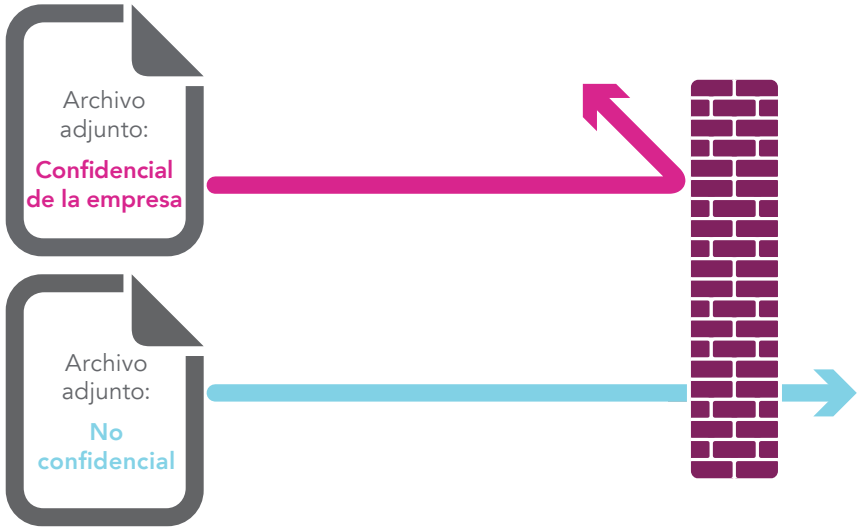
Evitar la filtración de datos por correo electrónico

En algunas empresas, el correo electrónico saliente no pasa por el sistema de seguridad de correo electrónico o dicho sistema no comprueba el contenido de los archivos adjuntos. En cualquier caso, es fácil que los archivos adjuntos «confidenciales de la empresa» puedan salir de la compañía. Dado que el tráfico de red saliente pasa por su cortafuegos, usted puede detectar y bloquear estos «datos en movimiento».

Cree una directiva para bloquear los archivos adjuntos de correo electrónico que contengan la marca de agua «confidencial de la empresa»

El motor de inspección profunda de paquetes buscará:

1. Contenido del correo electrónico = «Confidencial de la empresa» y
2. Contenido del correo electrónico = «Propiedad de la empresa» y
3. Contenido del correo electrónico = «Propiedad privada», etc.



SONICWALL®

10.ª función imprescindible:

Evitar la filtración de datos por correo web

Supongamos que su actual protección *antispam* puede detectar y bloquear un correo electrónico saliente normal que contiene información «confidencial de la empresa». Pero ¿qué sucede si un empleado utiliza un servicio de correo web, como Yahoo® o Gmail®, para enviar información «confidencial de la empresa»?

Crear una directiva para bloquear los adjuntos «confidenciales de la empresa» en el tráfico web

1. El motor de inspección profunda de paquetes busca la marca «confidencial de la empresa» en los archivos transferidos a través de http o https.
2. Bloquee el mensaje y notifique al remitente que el mensaje contiene información «confidencial de la empresa».

ADELANTE

De: usuariobueno@su_empresa.com

Para: usuariobueno@socio.com

Asunto: Aprobación de la ficha de control horario de Luis

Apruebo las horas recogidas en su ficha de control de esta semana. Juan

ALTO

De: usuariomalo@su_empresa.com

Para: usuariomalo@lacompetencia.com

Asunto: Hoja de ruta del diseño

Esta es la hoja de ruta

09 de ene. – Versión 7.0

Este es un documento **confidencial de la empresa**

También se puede aplicar a contenido transmitido por FTP.

11.ª función imprescindible:

Gestionar el ancho de banda para la transmisión de audio y vídeo en línea

En ocasiones, el acceso a los vídeos de sitios como YouTube.com es útil, pero a menudo se abusa de ellos. Bloquear estos sitios puede dar resultado, pero es preferible limitar el ancho de banda total asignado a los vídeos reproducidos en línea, independientemente de su procedencia. Lo mismo sucede con sitios de transmisión de audio en línea, como las emisoras de radio y los servicios de reproducción de música tipo Spotify y Apple Music. Este tráfico no tiene por qué venir de sitios conocidos; también puede estar alojado en blogs. Así, el objetivo es identificar este tráfico por lo que es, más que por su origen. En este sentido, la inspección profunda de paquetes es excelente.

Crear una directiva para limitar la reproducción de audio y vídeo en línea mediante una lista de firmas predefinida

1. Seleccione Transmisión de vídeo en línea y Transmisión de audio en línea como categorías de aplicaciones
2. Defina el ancho de banda que desea asignar a estas categorías de aplicaciones (p. ej., un 10 %)
3. Cree una regla por la que la transmisión de vídeo y audio en línea consuma como máximo un 10 % del ancho de banda disponible (excluyendo si lo desea a departamentos específicos, como los de formación)
4. Si lo estima conveniente, puede programar la regla de modo que sea efectiva durante el horario laboral habitual, pero no durante el almuerzo o después de las 18:00
5. Confirme la eficacia de su nueva directiva visualizando en tiempo real lo que ocurre desde Application Flow Monitor (Monitor de Flujo de Aplicaciones)

SONICWALL®

Cuando combinamos todas estas funciones

Plataforma de alto rendimiento
+ Inspección profunda de paquetes
+ Prevención de intrusiones
+ Inteligencia, control y visualización de aplicaciones

Cortafuegos de última generación de SonicWall

Seguridad, rendimiento y control

SONICWALL®

Acerca de nosotros

SonicWall lleva más de 27 años combatiendo el crimen cibernético y defendiendo a pequeñas y medianas empresas así como a grandes compañías de todo el mundo. Gracias a nuestra combinación de productos y partners, hemos logrado una solución automatizada de prevención y detección de amenazas en tiempo real, ajustada a las necesidades concretas de más de 500.000 organizaciones en más de 215 países y territorios, para que pueda hacer negocios con total tranquilidad. Si desea más información, visite www.sonicwall.com o síganos en Twitter, LinkedIn, Facebook e Instagram.

Si tiene alguna pregunta relativa al posible uso de este material, póngase en contacto con:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035 (Estados Unidos)

Encontrará más información en nuestro sitio web.
www.sonicwall.com

Ebook-11CoolThings-Firewall-US-VG-MKTG5084

SONICWALL