

## ImproveNet: Breve reseña



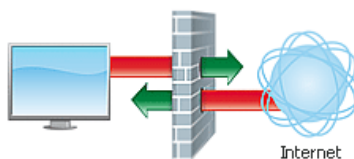
ImproveNet fue incorporado en una versión anterior de Outpost Firewall Pro, con la finalidad de ahorrar tiempo a los usuarios, y proveer seguridad adicional recogiendo, aprobando y redistribuyendo conjuntos de reglas habitualmente utilizados entre los usuarios de Outpost.

En Outpost 4.0, ImproveNet recolecta información acerca del modo en que los programas interactúan a nivel local en el ordenador. Estas reglas locales nuevas se actualizan automáticamente para los suscriptores de ImproveNet, y se utilizan para diferenciar las actividades seguras, de las riesgosas.

Este acercamiento brinda un nuevo nivel de seguridad sobre los procesos locales.

### ImproveNet 3.5

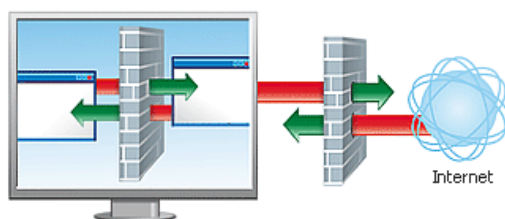
Las reglas que reciben los usuarios suscriptos a ImproveNet, afectan tanto al tráfico de datos interno y externo, como a las conexiones.



### ImproveNet 4.0

Con ImproveNet 4.0, los usuarios reciben un nivel de protección de última generación.

Además de las características anteriormente incluidas, las interacciones entre las aplicaciones están bajo el control de las reglas de seguridad, que se distribuyen a los suscriptores de ImproveNet.



### A mayor cantidad de amenazas, mayor complejidad del cortafuegos

El rápido crecimiento del uso de Internet, demostrado por la creciente cantidad de usuarios conectados, el aumento de la velocidad de conexión, y la diseminación de servicios y plataformas basados en la Web, trajo aparejados algunos inconvenientes.

Delincuentes informáticos (*hackers*) y otros desarrolladores de programas maliciosos han creado un territorio fértil para los ataques basados en Internet, apuntando a datos confidenciales, el rendimiento de los ordenadores, y la integridad de las redes corporativas.

Las vulnerabilidades no reparadas y la ausencia de actualizaciones de seguridad tempranas, contribuyen a incrementar los problemas de seguridad.

Los programas cortafuegos brindan una protección confiable contra los ataques delictivos, pues crean una coraza virtual sobre el ordenador anfitrión. De este modo, previenen el establecimiento de comunicaciones maliciosas desde y hacia la máquina, protegiéndolo contra ataques piratas.

Los programas antivirus (en su mayoría) actúan por reacción, detectando y eliminando virus del ordenador. En cambio, un cortafuegos está diseñado para ser proactivo, y prevenir que el virus llegue al ordenador monitorizando constantemente todo tipo de actividad en las conexiones, y descartando paquetes de datos no adecuados.

Debido a su relativa complejidad y sofisticación, los cortafuegos pueden necesitar cierto grado de conocimientos técnicos de parte del usuario, para ser configurados de tal manera que provean el máximo nivel de seguridad. Mientras que el funcionamiento de un antivirus es más lineal, ya que en la mayoría de las implementaciones conocidas, para un producto que no tenga un desarrollo tecnológico elevado, la protección consiste en que el usuario toma un archivo y lo analiza con dicho antivirus. mientras que los cortafuegos necesitan el ingreso de información de parte del usuario para poder discriminar qué tipos de accesos a Internet o a la red serán permitidos.

Los usuarios novatos son los más afectados por las solicitudes de información de los cortafuegos, porque no tienen la experiencia suficiente para saber qué responde (¿cómo podrían saber si es normal que el programa "iexplore.exe" solicite acceso a Internet a través del puerto 80 de un protocolo HTTP?) Después de ver unas pocas preguntas de este estilo, seguramente el novato abandone el uso del cortafuegos, o sencillamente permitirá la conexión sin deliberación alguna. Obviamente, ninguna de estas opciones es una buena solución.

El problema se extiende a todos los usuarios, no sólo a los novatos, debido a la cantidad de aplicaciones que requiere acceso a Internet actualmente. Como resultado, aún los usuarios experimentados pueden terminar con un sistema mal configurado y comprometer la seguridad del mismo. Tanto si se debe a la falta de tiempo para investigar los parámetros de acceso correctos, como si se debe sólo a la falta de información disponible, los usuarios necesitan ayuda para configurar su cortafuegos eficientemente, sin interferir con las actividades en línea.

Agnitum reconoció la necesidad de brindar a los usuarios una manera confiable y sencilla de configurar correctamente el cortafuegos, sin dejar de proveer el máximo nivel de seguridad. El resultado fue el desarrollo de **ImproveNet**, un sistema que automatiza la configuración del cortafuegos de acuerdo al juicio de nuestros expertos en seguridad, y que permite la distribución de dichas configuraciones a todos los usuarios participantes.