

# Outpost Firewall en las universidades

# Outpost Firewall en las universidades

Introducción	3
Medidas de seguridad	3
Riesgos potenciales	4
Cortafuegos de uso personal	5
Outpost Firewall	5
Beneficios de utilizar Outpost Firewall	6
La última línea de defensa	6
Control del estudiante	6
Personalización	6
Actualizaciones de seguridad y soporte técnico	7

## Outpost Firewall en las universidades

### Introducción

Los establecimientos educativos comparten ciertos riesgos comunes a cualquier organización extendida y con una gran variedad de ordenadores conectados a Internet, pero además, tienen su propia y particular problemática a considerar.

### Medidas de seguridad

En la actualidad, prácticamente todos los establecimientos educacionales se encuentran conectados a Internet.

Esto hace que las transacciones, los intercambios, las comunicaciones y el almacenamiento de información se efectúen más rápidamente.

Sin embargo, Internet hace que sus archivos sean vulnerables a personas malintencionadas y que se oculten a través del planeta.

Por necesidad, las redes locales que integran la organización, usualmente se encuentran conectadas a Internet, lo que hace posible que cualquiera de los ordenadores que la integran sean susceptibles de ser atacados.

Debido a que no se ha inventado todavía el producto que proporcione una protección total, se necesitan varios niveles de defensa para proteger su red y sus ordenadores.

Para muchos establecimientos educacionales, con miles de usuarios utilizando sus ordenadores, fallas en la seguridad pueden causar pérdidas financieras muy altas así como pérdida de derechos de propiedad intelectual.

Tradicionalmente, los administradores de estas redes, utilizan cortafuegos por *hardware* y/o integrados en routers como una única línea de defensa entre sus redes e Internet.

Este tipo de cortafuegos es efectivo a la hora de detectar ataques de nivel básico pero fallan a la hora de bloquear intentos de intrusiones llevadas a cabo por profesionales pagos, acostumbrados a robar secretos industriales y desarrollos intelectuales, así como

tampoco pueden impedir el accionar de individuos malintencionados que gozan infringiendo el mayor daño posible a otras personas e instituciones.

## Riesgos potenciales

Los cortafuegos por *hardware* no son una solución efectiva contra los nuevos ataques debido a que sus algoritmos son simplemente demasiado primitivos.

La principal falla de los cortafuegos por *hardware*, es que no están basados en una aplicación.

Estos cortafuegos no son capaces de analizar las aplicaciones que están conectadas a Internet, simplemente son capaces de detectar el canal que los programas utilizan. Por ejemplo, esto permite que un programa malicioso envíe información confidencial usando el canal habitual del navegador, y esto no será detectado.

Otra falla de los cortafuegos por *hardware*, es que éstos no pueden filtrar el contenido de las páginas de Internet, lo que hace posible que las redes no estén seguras de amenazas provenientes de sitios maliciosos.

Existen pocos cortafuegos por *hardware* que permiten el filtrado de contenidos de páginas de Internet, sin embargo, son muy caros y requieren una administración muy costosa y avanzada.

Independiente de cuantos cortafuegos de *hardware* se estén utilizando, éstos no protegen los ordenadores de una red de las siguientes amenazas:

Amenaza	Riesgo potencial
Troyanos	Acceso remoto total a los ordenadores y redes vulnerables.
Gusanos de correo electrónico	Pérdida de información importante, acceso no autorizado y caída total del sistema.
Configuración incorrecta del sistema	Acceso remoto total a los ordenadores y redes con configuraciones no adecuadas.
Páginas maliciosas en Internet	Pérdida de seguridad y acceso no autorizado a los ficheros del ordenador.
Contenido inapropiado	Gasto innecesario de ancho de banda. Disminución general de la velocidad de acceso.

Otra limitación importante de los cortafuegos corporativos es su inhabilidad para proteger los ordenadores de los estudiantes y docentes cuando estos no están en el establecimiento educacional.

Durante las vacaciones de verano, los docentes, estudiantes y empleados en general, suelen viajar y necesitar conectarse a Internet utilizando ordenadores públicos o personales, desde hoteles, lugares de reunión o desde su propia casa y esto incrementa fuertemente los riesgos potenciales descritos o cualquier otro tipo de ataque.

### **Cortafuegos de uso personal**

Afortunadamente, se creó otra línea de defensa para proteger los ordenadores de sofisticados y modernos ataques.

El cortafuegos de uso personal, es un programa que puede ser constantemente actualizado y mejorado para protegerlo de las últimas amenazas y que resulta más efectivo y confiable que el cortafuegos por *hardware*.

Los cortafuegos de uso personal son instalados en cada ordenador de la universidad, protegiéndolos de ataques provenientes del interior o el exterior, sin importar que conexión se utilice para Internet.

Este dúo (cortafuegos de uso personal + cortafuegos por *hardware*) hacen que una red de área local se convierta en una fortaleza impenetrable.

### **Outpost Personal Firewall**

Outpost es, para muchos evaluadores independientes, el cortafuegos bajo Windows más completo y avanzado del mundo.

De hecho, Outpost defiende su ordenador de cualquier amenaza de Internet.

Con Outpost usted tendrá seguridad, privacidad, control y facilidad de uso.

Outpost fue diseñado para usuarios finales, sin embargo, es tan poderoso, que muchas corporaciones y otros tipos de organizaciones lo utilizan para proteger sus redes.

## Beneficios de utilizar Outpost Firewall en entornos de área local:

### La última línea de defensa

Outpost no sólo protege su ordenador de todas las amenazas de Internet, sino que también, por diseño, de amenazas desconocidas.

Independientemente de si el ordenador está conectado o no a una red local, Outpost protege cualquier ordenador inmediatamente después de instalado.

Outpost es muy fácil de usar y no requiere ningún conocimiento específico para comenzar a utilizarlo.

Outpost Firewall Pro puede trabajar también en modo oculto y de esta forma, nadie puede modificar los parámetros de configuración al desconocer su ejecución, además que es posible proteger, por contraseña, sus parámetros de funcionamiento impidiendo cambios no autorizados.

### Control del estudiante

Uno de los mayores problemas es que los estudiantes gastan su tiempo visitando páginas con contenidos para adultos, jugando en línea o participando en sitios de conversación y encuentro (*Chat*).

Es oneroso, indeseable y virtualmente imposible espiar los hábitos de cada estudiante.

Utilizando Outpost no sólo es posible controlar los sitios que los estudiantes visiten, sino que además no posee ningún costo adicional y es perfecta y éticamente aceptable.

Con Outpost protegiendo su red local, los estudiantes no se pueden tentar en distraerse de sus estudios navegando por sitios inapropiados.

### Personalización

Agnitum Outpost Firewall es el primer cortafuegos personal que soporta complementos (*Plug-Ins*).

Esto permite que desarrolladores independientes puedan implementar esta revolucionaria tecnología para muy fácilmente expandir y mejorar las prestaciones de Outpost Firewall.

Con esta tecnología cada organización puede desarrollar sus propios complementos para ajustar con gran precisión, el funcionamiento de Outpost Firewall a sus particulares necesidades y entorno de trabajo.

Outpost Firewall le permite obtener flexibilidad y capacidades ilimitadas.

Outpost Firewall se ajusta a las necesidades de cada organización.

### **Actualizaciones de seguridad y soporte técnico**

Gracias a las actualizaciones automáticas de Outpost, usted puede estar seguro de contar siempre con la más actualizada protección contra las últimas amenazas y peligros.

Nuestros desarrolladores continuamente investigan para elevar la protección que ofrece Outpost Firewall y que usted mantenga el altísimo nivel de seguridad que sólo Outpost Firewall Pro puede ofrecerle.

Las actualizaciones de Outpost están completamente automatizadas y pueden ejecutarse también manualmente con una sola pulsación del ratón.

Frente a cualquier dificultad no contemplada, usted cuenta con diversas modalidades de soporte técnico detalladas en nuestra página de soporte:

<http://www.outpost-es.com/support/> .



Traducción y adaptación al español:  
Ontinet.com, S.L.