

Lista de funciones

NetOp Desktop Firewall

Servidor de seguridad basado en el controlador de mini-puertos NDIS y el controlador TDI: todos los algoritmos de filtrado se implementan en el controlador (como un controlador NDIS). Esto significa que el servidor de seguridad está siempre funcionando; es decir, el usuario goza de una protección máxima incluso si la propia aplicación del servidor de seguridad no está activa. Con ello se garantiza el bloqueo de todo el tráfico de red, con la consiguiente eliminación de cualquier riesgo en caso de producirse algún vacío de seguridad durante el inicio del sistema.

Sistema de perfiles con reglas de detección automática de red: esta prestación cambia automáticamente la configuración del servidor de seguridad cuando se trabaja en una red distinta: incluso si dos o más redes utilizan el mismo rango de direcciones IP.

Comprobación de los componentes seguros y protección ante procesos de piratería: mediante la verificación del checksum, el servidor de seguridad comprueba la integridad de la aplicación que intenta establecer comunicación. En caso de haber sido modificado, se envía un aviso. El seguimiento de los procesos parentales de la aplicación permite al servidor de seguridad detectar si otra aplicación intenta ejecutar una aplicación cuya confianza ya haya sido comprobada y, de ser así, denegar el acceso a la red, incluso a la aplicación de confianza.

Denegación de la ejecución de procesos desconocidos: esta función protege el sistema de amenazas desconocidas configurando el servidor de seguridad para que evite la ejecución y comunicación de procesos desconocidos.

Bloqueo bidireccional de puertos y protocolos: abre únicamente los puertos y protocolos necesarios (en sentido entrante o saliente, o en ambos) para mejorar la seguridad.

Control bidireccional de las redes de confianza: garantiza la comunicación de las aplicaciones únicamente a través de redes de confianza, nunca mediante redes externas.

Control bidireccional de las redes prohibidas: impide la comunicación con redes determinadas. Las reglas del servidor de seguridad se activan en cuanto el sistema operativo detecta una conexión de red. Estas reglas protegen el equipo ante cualquier amenaza que se origine en la red.

Puertos cerrados: oculta la presencia del equipo para evitar ataques y la detección de los puertos. Incluso herramientas como Nmap, que identifican los sistemas y explotan las vulnerabilidades conocidas de los sistemas operativos, son incapaces de detectar el ordenador.

Registro de sucesos avanzado y visualización de paquetes en tiempo real: las estadísticas en directo de Network Matrix ofrecen una visión gráfica completa de la actividad de la red en tiempo real. Permite ajustar el tráfico de la consola para obtener una vista a tamaño completo del tráfico y así mejorar la capacidad de realizar ajustes en tiempo real en las políticas de seguridad.

Comunicación encriptada: la comunicación encriptada con el servidor NetOp Policy Server y las bases de datos de sistema locales garantizan la seguridad ante paquetes de código malicioso que intentan atacar la configuración del servidor de seguridad.

Contraseña de mantenimiento: la protección mediante contraseña permite que los usuarios o administradores bloqueen componentes del servidor de seguridad para evitar configuraciones no deseadas del producto. Si es preciso, cuando se utiliza esta prestación junto con el servidor NetOp Policy Server, se puede conseguir que el usuario no pueda desconectarse manualmente del servidor si no proporciona la contraseña correcta.

Compatibilidad con tecnologías gigabit e inalámbricas: el producto ofrece compatibilidad plena con las últimas tecnologías de comunicación.

Carga del sistema reducida: garantiza la protección del equipo sin que los usuarios perciban una disminución del rendimiento.

Instalación con MSI: la instalación de NetOp Desktop Firewall se lleva a cabo con Microsoft Windows Installer y puede ejecutarse bien interactivamente bien en modo silencioso para realizar instalaciones en masa. La activación del servidor de seguridad puede posponerse hasta el próximo reinicio planificado a fin de no interrumpir la actividad de los usuarios.

NetOp Policy Server

Consola de NetOp Policy Server: se trata de la interfaz de usuario principal desde la que los administradores pueden gestionar un servidor maestro para que controle las asignaciones de las políticas de seguridad para cada uno de los servidores NetOp Desktop Firewall. La consola puede iniciarse desde cualquier plataforma compatible.

Servidor maestro: este módulo mantiene la configuración maestra e interactúa con cada uno de los servidores NetOp Desktop Firewall a través de uno o más servidores de replicación. La instalación inicial instala tanto el servidor maestro como el de replicación en un mismo equipo.

Servidores de replicación: estos servidores se organizan en un clúster a fin de permitir la redundancia, la distribución de la carga, la interacción con los servidores NetOp Desktop Firewall y el registro de dichas interacciones. Los servidores de replicación interactúan de forma regular con su servidor maestro para recibir las actualizaciones de las políticas de seguridad y devolver los registros de interacción de su NetOp Desktop Firewall para que se almacenen en el servidor maestro. Cada servidor de replicación puede dar servicio a varios miles de servidores de seguridad.

Administración de los servidores: podrá aprobar, eliminar o mover los servidores de replicación y controlar su estado en tiempo real.

Gestión de los administradores: cada servidor maestro dispone de un administrador. Puede definir y gestionar varios administradores auxiliares que le permitirán distribuir la carga de trabajo entre los administradores locales.

Administración de las políticas de seguridad: la consola de NetOp Policy Server controla la configuración de los programas, puertos, protocolos, redes de confianza y redes prohibidas. También controla los perfiles y las reglas de perfiles de cada política de seguridad. Ofrece la posibilidad de aprobar o denegar los programas nuevos que los usuarios intentan iniciar para cada política de seguridad. Esta función puede activarse en los servidores NetOp Desktop Firewall en cuestión de segundos.

Administración centralizada: puede definir las políticas de seguridad y asignarlas a los grupos de seguridad de Microsoft Active Directory para agilizar la administración. El servidor de políticas NetOp Policy Server también puede mantener grupos independientes para equipos que no formen parte de un directorio Microsoft Active Directory.

Interrupción de todo el acceso a Internet: en caso de desencadenarse una epidemia de virus u otras situaciones peligrosas, el administrador de NetOp Policy Server puede evitar la ejecución del proceso ilegal en cuestión en todos los equipos. También tiene capacidad para bloquear el acceso a Internet de toda la empresa o de un grupo de seguridad específico hasta que se resuelva la situación.

Estadísticas avanzadas y registros: el servidor NetOp Policy Server registra las solicitudes de programas confirmados y sin confirmar, de los inicios de sesión y de las sincronizaciones. Esta información puede mostrarse gráficamente para controlar la carga y el rendimiento del servidor o en forma de lista. De esta forma podrá buscar, por ejemplo, equipos que estén intentando iniciar archivos con contenido malicioso.

Requisitos técnicos	Cliente	Servidor de políticas
Equipo	Procesador Intel Pentium a 233 MHz o superior, o compatible 100%	Procesador Intel Pentium a 233 MHz o superior, o compatible 100%
Memoria	Requisitos del sistema operativo más 32 MB de memoria RAM adicionales	Requisitos del sistema operativo más 32 MB de memoria RAM adicionales (se recomiendan 64 MB)
Vídeo	Cualquier adaptador para gráficos VGA compatible 100% con Windows	Cualquier adaptador para gráficos VGA compatible 100% con Windows
Espacio en disco duro	10 MB libres de espacio en disco	10 MB libres de espacio en disco
Plataforma	Windows XP Professional Windows XP Home Edition Windows 2000 Professional	Windows Server 2003 Standard, Web Edition, Enterprise Edition Windows XP Professional Windows 2000 Server, Advanced Server Windows 2000 Professional
Comunicaciones	Un adaptador de red o módem como mínimo TCP/IP: Winsock 2 o compatible Acceso a Internet (para el registro inicial del producto)	Un adaptador de red como mínimo TCP/IP: Winsock 2 o compatible Acceso a Internet (para el registro inicial del producto)

NetOp® Desktop Firewall

www.netop.com

El primer servidor de seguridad para ordenadores de escritorio del mundo basado en controladores que ofrece un control centralizado de los equipos portátiles de la empresa

- Control total de los programas y los servicios
- Arquitectura de filtrado dinámico de paquetes
- Aplicación activa de las políticas de seguridad corporativas
- Un complemento imprescindible para los servidores de seguridad perimetrales



Un solo equipo portátil infectado puede poner en peligro toda la red...





Supervise y controle todos los programas y servicios que se ejecutan en los equipos portátiles conectados a la red... incluso desde fuera.

La verdad es que la mayoría de los servidores de seguridad personales se limitan a controlar el tráfico de entrada y salida de los equipos, pero no los procesos que ejecutan. Una vez que se ha infectado un equipo, el servidor de seguridad carece de utilidad. Por su parte, los servidores de seguridad perimetrales se han diseñado únicamente para proteger los equipos corporativos de los datos maliciosos que provienen de Internet. Este enfoque resulta adecuado siempre y cuando los equipos portátiles se utilicen sólo en la oficina. Ahora, gracias a NetOp Desktop Firewall, podrá obtener lo mejor de ambos mundos en un único paquete de administración centralizada. Pero eso no es todo...

Control completo a partir de controladores que aísla los equipos portátiles infectados

NetOp Desktop Firewall es un cliente basado realmente en controladores cuyo objetivo es efectuar un filtrado de paquetes sofisticado que evite que los datos no deseados o peligrosos se introduzcan en el equipo o salgan del mismo. Además, gracias al control de los procesos garantiza que sólo los programas aprobados puedan cargarse o establecer comunicaciones en la red. Por último, dado que NetOp evita que se ejecuten los procesos desconocidos, el sistema está siempre a punto ante ataques nuevos y desconocidos.

Gestión y aplicación activa de las políticas de seguridad

Los estudios de IDC demuestran que más de la mitad de las infracciones de seguridad tienen su origen en los equipos situados dentro del servidor de seguridad perimetral. Ahora, gracias a NetOp Desktop Firewall, los usuarios ya no podrán anular las políticas de seguridad aplicadas a su equipo. La administración centralizada permite introducir cambios en las políticas de forma inmediata y aplicarlos con rigor. Sin excepciones. Siempre.

Le resulta familiar?



El hotel. La habitación con acceso de banda ancha. Comprueba el correo electrónico. Decide navegar un poco por Internet para entretenerse. Y desde el primer clic su equipo queda expuesto a gusanos y troyanos.



Puntos de acceso puntual. Recuerde cuando trabaja en entornos sin protección, sea un café o un aeropuerto. Es decir, cualquier usuario de la red puede emprender un ataque directo contra su equipo.



Su casa. Los niños traen a casa un CD de la escuela. O decide descargar un archivo adjunto de correo electrónico que le envía un amigo. Aunque conozca la fuente, ¿puede estar seguro de que no conlleva riesgos?

No se preocupe!

NetOp Desktop Firewall no sólo mantiene la seguridad de su equipo cuando está de viaje, sino que garantiza que los programas maliciosos que haya descargado no puedan "escapar" al regresar a la oficina.

Gracias a NetOp Desktop Firewall, el equipo portátil trabaja en modo oculto, lo que lo hace invisible a los demás. El servidor sólo permite paquetes salientes de determinados programas, puertos y protocolos.

Gracias al reconocimiento de los distintos perfiles de seguridad según la ubicación, el servidor NetOp Desktop Firewall le permite hacer lo que quiera cuando está en casa, pero cambia a un nivel seguridad más elevado cuando está en el trabajo a fin de proteger a los compañeros y la empresa.

El sistema NetOp Desktop Firewall consta de dos módulos: el cliente, que se instala en todos los portátiles de la red, y el servidor NetOp Policy Server, que administra los niveles de seguridad tanto corporativos como individuales.

Cliente de NetOp Desktop Firewall

Control de los procesos: esta función de NetOp Desktop Firewall es una herramienta de extremada eficacia que permite administrar todos los procesos que se ejecutan en el sistema. Mediante el control de los procesos podrá definir reglas para cualquier aplicación específica. Podrá evitar la ejecución de aplicaciones, permitir la comunicación, permitir la comunicación sólo con una red de confianza o evitar todas las comunicaciones.

Filtrado de paquetes: la arquitectura de filtrado de paquetes dinámico de NetOp Desktop Firewall actúa al nivel de red a fin de controlar las direcciones IP, los puertos y los protocolos. El filtrado de paquetes dinámico supervisa el estado de las conexiones y recopila la información en una tabla de estado. Es decir, las decisiones del filtrado se basan tanto en reglas de filtrado de paquetes estático como en el contexto establecido por los paquetes anteriores que han pasado por el servidor de seguridad. Como medida de seguridad adicional ante la detección de puertos, NetOp Desktop Firewall los cierra todos hasta que se solicita la conexión con uno concreto.

NetOp Policy Server

Control de NetOp Desktop Firewall: el servidor NetOp Policy Server asigna una política de seguridad a un servidor NetOp Desktop Firewall que haya iniciado sesión mediante la especificación en tiempo real de la configuración para los programas, puertos, protocolos, redes de confianza, reglas para redes prohibidas, perfiles y reglas de perfiles. También se encarga de registrar la información recibida de cada uno de los servidores NetOp Desktop Firewall.

Administración: el servidor NetOp Policy Server es compatible con Microsoft Active Directory, lo que permite aplicar políticas de seguridad a los equipos miembros de los grupos de seguridad de Active Directory. Gracias a esta prestación es posible administrar la seguridad de la infraestructura mediante la herramienta habitual de los administradores: Usuarios y equipos de Active Directory. Para la tolerancia de errores y la distribución de la carga, NetOp Policy Server se ha implementado con un servidor maestro y varios servidores de replicación que garantizan una disponibilidad máxima del sistema.

