

Instalación de ESET NOD32 Antivirus v4.x en Servidores de red

Tutorial



Instalación de ESET NOD32 Antivirus v4.x en Servidores

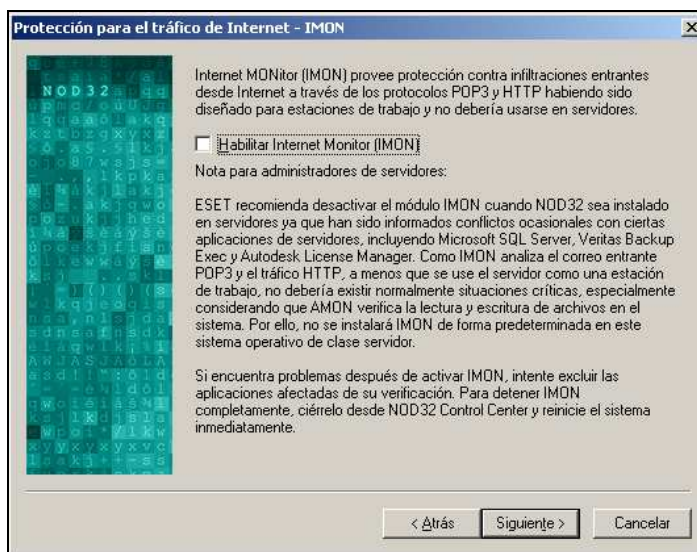
Este documento contiene una serie de recomendaciones y configuraciones para realizar la instalación de ESET NOD32 Antivirus v4.x en un Servidor de Red. También se explicará la implementación de exclusiones de archivos en los distintos tipos de servidores de una red.

NOTA: La implementación de las recomendaciones y las exclusiones descritas en este tutorial dependerán de la estructura de cada red en particular.

1. Recomendaciones

Desactivar el modulo IMON o Protección del tráfico de Internet.

Esta recomendación es advertida por el asistente de instalación de ESET NOD32 Antivirus para Windows 95/98/ME cuando se realiza la instalación del producto en un servidor, informando al administrador del mismo que el modulo **IMON** en ocasiones, genera conflictos con ciertas aplicaciones de servidores, siendo recomendable desactivar dicho modulo.

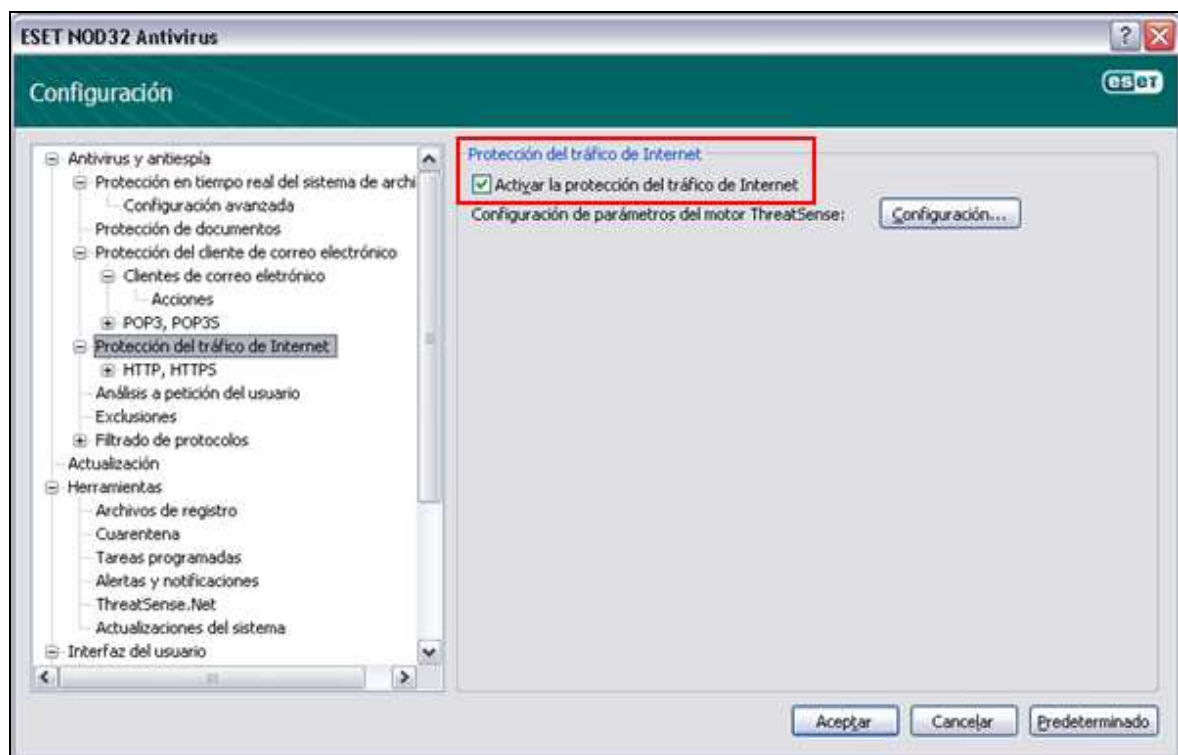


La protección contra infiltraciones desde Internet a través de los protocolos POP3 y HTTP que provee **IMON** esta diseñado para estaciones de trabajo y no debería utilizarse en servidores.

Asimismo el asistente de instalación genera la posibilidad de activar **IMON** dentro de la misma advertencia ya que luego de finalizar la instalación de ESET NOD32 Antivirus para Windows 95/98/ME, si se presentan inconvenientes, existe la posibilidad realizar exclusiones de las aplicaciones afectadas.

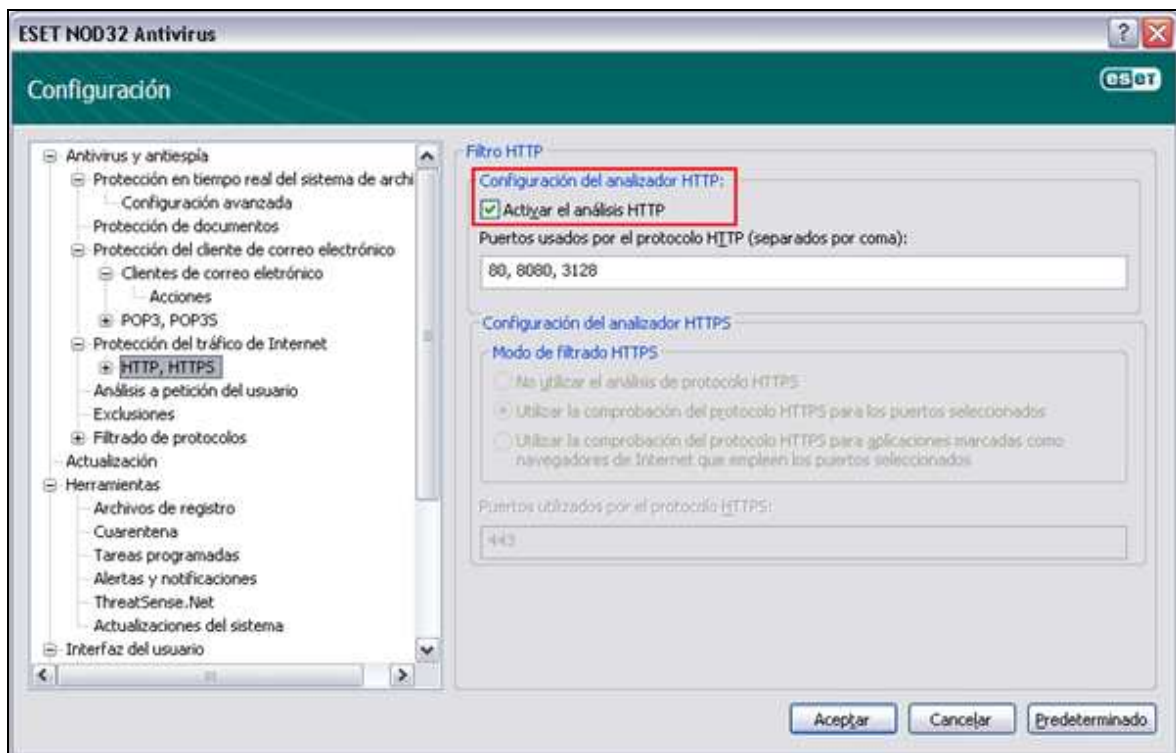
En cuanto a ESET NOD32 Antivirus v4.x instalado en un equipo con sistema operativo y funciones de servidor, es recomendable deshabilitar la opción de **Protección del Tráfico de Internet** y **Análisis HTTP**.

Para realizar esto, se debe dirigir a **Configuración, Mostrar Opciones Avanzadas de Configuración**, donde se encontrará la opción **Protección del Tráfico de Internet**, como se ve en la siguiente imagen.



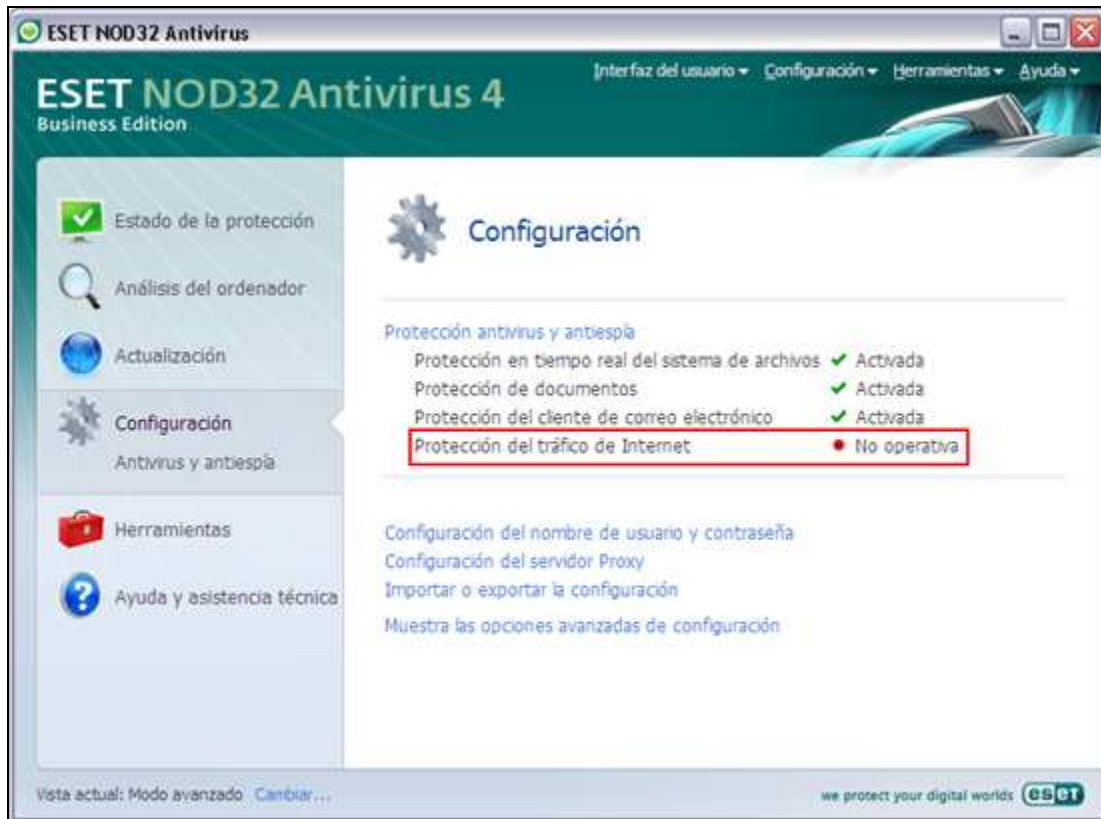
Se debe desmarcar la opción **Activar la protección del tráfico de Internet**. Luego en la siguiente sección del menú lateral llamada **HTTP**, se encuentran las configuraciones del **Filtro HTTP**.

Donde se debe desmarcar la opción **Activar el análisis de HTTP** como se muestra en la imagen, luego se debe aceptar las modificaciones.



Con estas acciones, desmarcar la **Protección del tráfico de Internet** y el **Análisis de HTTP** en ESET NOD32 Antivirus v4.x, se está realizando la misma función que en el caso de la desactivación del módulo **IMON** como se ha visto anteriormente en la instalación de ESET NOD32 Antivirus para Windows 95/98/ME.

Luego de aceptar los cambios, el producto informará al usuario que la **Protección del tráfico de Internet** se encuentra **No operativa**.



De esta manera el producto libera las conexiones al servidor de la red por parte de las estaciones de trabajo, los cuales si mantienen activado el modulo **IMON** o **Protección del trafico de Internet** en sus productos.

Desactivar **IMON** o la **Protección del tráfico de Internet** en un servidor de red, no debería presentar normalmente situaciones críticas, especialmente considerando que **AMON** o la **Protección en tiempo real del sistema de archivos** verifica la lectura y escritura de archivos en el sistema.

2. Exclusiones

A continuación se mostrará una lista de archivos y directorios recomendados para su exclusión. Cabe aclarar que estas exclusiones varían dependiendo de la estructura de la red y de cada caso en particular.

NOTA: X corresponde a la unidad del sistema.

2.1. Servidor Exchange

- Base de datos = X:\ Archivos de Programa \Exchsrvr\Mdbdata (verificar ubicación)
- Archivos MTA = X:\ Archivos de Programa \Exchsrvr\Mtadata
- Archivos .log = X:\ Archivos de Programa \Exchsrvr\server_name.log
- SMTP Mailroot = X:\ Archivos de Programa \Exchsrvr\Mailroot
- X:\ Archivos de Programa \Exchsrvr\Conndata
- Servicio de replica del sitio = X:\ Archivos de Programa \Exchsrvr\srsdata

2.2. IIS exclusiones relacionadas

- IIS System Files = X:\WINDOWS\system32\inetsrv
- IIS Carpeta de compresión = X:\WINDOWS\IIS Temporary Compressed Files

2.3. Controlador de Dominio

- Active Directory = X:\WINDOWS\NTDS
- SYSVOL X:\WINDOWS\SYSVOL
- Base de datos NTFRS = X:\WINDOWS\ntfrs

2.4. Servicios de Windows SharePoint

- Carpeta temporal de SharePoint = X:\windows\temp\Frontpagetempdir

2.5. Servicios de Data Bases

- Base de datos DHCP = X:\WINDOWS\system32\dhcp
- Base de datos WINS = X:\WINDOWS\system32\wins
- X:\Archivos de Programa\Microsoft SQL Server\MSSQL\$SBSMONITORING\Data
- X:\ Archivos de Programa \Microsoft SQL Server\MSSQL\$SHAREPOINT\Data
- X:\ Archivos de Programa \Microsoft SQL Server\MSSQL\Data

2.6. Exclusiones Adicionales

- Removable Storage Database (utilizado por SBS Backup) = X:\Windows\System32\ntmsdata
- SBS POP3 connector Failed Mail = X:\ Archivos de Programa \Microsoft Windows *Small Business* Server\Networking\POP3\Failed Mail
- SBS POP3 connector Incoming Mail = X:\ Archivos de Programa \Microsoft Windows *Small Business* Server\Networking\POP3\Incoming Mail
- Windows Update Store = X:\WINDOWS\SoftwareDistribution\DataStore
- X:\urlcache
- X:\pagefile.sys

2.7. SBS Exclusiones Autorizadas

- Archivo - %windir%\system32\licstr.cpa
- Carpeta - %windir%\windows\system32\lfs

NOTA: Ejecute el asistente de Licencias y genere un backup en otro directorio.

2.9. Terminal de Servicios (Exclusiones Autorizadas)

- X:\WINDOWS\System32\LServer:
 - edb.log y edb.chk
 - res1.log y res2.log
 - TLSLic.edb
 - temp.edb

2.10. Per 822158

- Base de Datos de Windows Update:
%windir%\SoftwareDistribution\Datastore\datastore.edb
- Archivos de transacción diarios: %windir%\SoftwareDistribution\Datastore\Logs\edb*.log
- Res1.log y Res2.log
- Edb.chk y Tmp.edb

2.11. Per 815623

- Excluir:
 - %systemroot%\sysvol
 - %systemroot%\sysvol\domain\DO_NOT_REMOVE_NtFrs_Preinstall_Directory
 - %systemroot%\sysvol\staging
 - %systemroot%\sysvol\staging areas
 - %systemroot%\sysvol\sysvol
- Analizar:
 - %systemroot%\sysvol\domain
 - %systemroot%\sysvol\domain\Policies
 - %systemroot%\sysvol\domain\Scripts