

# Manteniendo vivo al FTP

Autor Webmaster

El protocolo de transferencia de archivos &ndash; FTP &ndash; es uno de los servicios basados en TCP/IP más antiguos y utilizados del mundo. A pesar de esto, su futuro está en entredicho, debido básicamente a sus serias limitaciones en cuanto a seguridad y eficiencia en la transferencia de datos. Ya existen soluciones disponibles que brindan las mismas funcionalidades pero con un nivel de protección mayor, como es el caso de SCP, SFTP Y FTPS. Estas nuevas alternativas serán adoptadas progresivamente, de manera que los administradores de sistemas tendremos todavía por varios años que mantener vivo y respirando al venerable FTP tradicional, porque con todo y sus defectos nos sigue siendo muy útil. En este artículo explicaré algunas generalidades relacionadas con la instalación del servicio FTP y advertiré algunas complicaciones que se pueden presentar cuando dicha instalación se hace en un entorno de red moderno, en el que están involucrados cortafuegos y enmascaramiento de direcciones IP.

## MODO DE FUNCIONAMIENTO

El protocolo FTP fue diseñado para la transferencia de archivos entre máquinas remotas, pero además de permitirnos enviar y recibir archivos hace posibles ciertas operaciones en el sistema remoto (crear directorios, borrar archivos, cambiar permisos, etc.). Una sesión FTP típica empieza con un proceso de registro o login, en el que se suministra un nombre de usuario y una contraseña. Una vez que el usuario haya sido autenticado, podrá realizar diversas operaciones relacionadas con la transferencia y administración de archivos. Al ser un protocolo basado en el estándar TELNET, los comandos y respuestas que se intercambian entre el cliente y el servidor son enviados como texto ASCII legible, lo que constituye un importante riesgo de seguridad. Para conectarse a un servidor FTP se necesita un programa cliente, que bien puede ser de línea de comandos o de modo gráfico. Este programa recibe e interpreta los comandos del usuario y los convierte en comandos FTP reales. En este punto es importante entender que una cosa son los comandos aceptados por el cliente y otro los verdaderos comandos que admite el protocolo FTP. Por ejemplo si emitimos el comando PUT manual.doc, este será entendido por nuestro programa cliente como una petición para enviar el archivo local manual.doc al directorio actual del servidor. Tras bambalinas el cliente emite un comando STOR manual.doc que es el que verdaderamente recibe el servidor.

## PARTICULARIDADES DEL PROTOCOLO

FTP es un protocolo sui generis en varios aspectos: En primer lugar, utiliza dos conexiones TCP para su funcionamiento. Estas conexiones se conocen como canal de control y canal de datos. El canal de control es el que se usa para que el cliente y el servidor &ldquo;dialoguen&rdquo;, es decir, por este canal se intercambian comandos y respuestas. Una vez que los participantes se han puesto de acuerdo por el canal de control, pasan a utilizar el canal de datos para realizar a través de él la transferencia real de la información. El hecho de que se deban abrir dos sockets TCP para una operación FTP implica que las transferencias no serán muy eficientes, sobre todo para archivos pequeños. Además, como veremos más adelante, estas dos conexiones implican varios problemas relacionados con la seguridad y la configuración de los equipos de enrutamiento que se ubiquen entre el cliente y el servidor.

## FTP ACTIVO Y PASIVO

Existen dos modos de funcionamiento que pueden usarse para una sesión FTP: activo y pasivo.

## MODO ACTIVO

En el modo activo sucede lo siguiente:

- El cliente inicia una conexión TCP desde un puerto aleatorio (>1024) al puerto en que escucha el servidor (por defecto es el puerto 21).
- Una vez establecido el canal de control, el cliente deberá emitir comandos para registrar al usuario en el sistema remoto. Se suministra entonces un nombre de usuario y contraseña (comandos USER y PASS).
- Una vez autenticado el usuario, el programa cliente puede enviar al servidor comandos relacionados con la transferencia y manipulación de archivos, pero antes de recibir cualquier flujo de datos, deberá emitir el comando PORT w,x,y,z,a,b

Donde w.x.y.z es la dirección IP del cliente, y a,b es la descripción del puerto.

Por ejemplo, si el comando es PORT 200,42,47,44,12,8 Esto significa que el cliente invita al servidor a iniciar una conexión de datos a su dirección IP (200.42.47.44 en este caso) en el puerto  $(12 \times 256) + 8 = 3080$ . El servidor utilizará por su parte el puerto 20 estándar (a menos que se haya configurado de otra forma).

- Una vez establecido el canal de datos y hecho el requerimiento de los mismos (con un comando LIST, STOR, RETR, etc.), se hace la transferencia correspondiente. Al terminar se cierra la conexión.
- La sesión continua hasta que es cerrada por alguna de las dos partes o expira su tiempo de vida. Nótese que para cada transferencia de datos se abrirá un canal diferente, proveniente del servidor (puerto 20 o el que tenga configurado) a un puerto efímero del cliente (>1024).

## MODO PASIVO

En el modo pasivo sucede lo siguiente:

- El cliente inicia una conexión TCP desde un puerto aleatorio (>1024) al puerto en que escucha el servidor (por defecto es el puerto 21).
- Una vez establecido el canal de control, el cliente deberá emitir comandos para registrar al usuario en el sistema remoto. Se suministra entonces un nombre de usuario y contraseña (comandos USER y PASS).
- Una vez autenticado el usuario, el programa cliente puede enviar al servidor comandos relacionados con la transferencia y manipulación de archivos, pero antes de recibir cualquier flujo de datos, deberá emitir el comando PASV con el que indica al servidor que se va a usar el modo pasivo.
- El servidor responde entonces a la petición enviando la dirección IP en la que va a escuchar y el número de puerto que va a abrir, usando el mismo formato w,x,y,z,a,b que se explicó anteriormente para el modo activo.
- Una vez establecido el canal de datos y hecho el requerimiento de los mismos (comandos LIST, STOR, RETR, etc.), se hace la transferencia correspondiente. Al terminar se cierra la conexión.
- La sesión continua hasta que es cerrada por alguna de las dos partes o expira su tiempo de vida. Nótese que para cada transferencia de datos se abrirá un canal diferente, proveniente del cliente (puerto efímero >1024) a un puerto efímero del servidor.

## LOS PROBLEMAS POR ENFRENTAR

Si los hosts en Internet se comunicaran directamente entre sí, el protocolo FTP funcionaría sin mayores problemas (al menos en lo que a establecer sesiones respecta). Sin embargo, debido a la naturaleza insegura de la red mundial, en la mayoría de los casos existirá al menos un cortafuegos (firewall) entre el cliente y el servidor. Adicionalmente, ante la escasez de direcciones IP públicas, una buena porción de los clientes se conectará desde direcciones IP privadas que luego son enmascaradas (IP masquerading) por el enrutador de salida de la red LAN, lo que también se conoce como NAT varios a uno (many-to-one NAT). Para hacer más complicadas las cosas, en muchos casos el servidor mismo no posee una dirección IP pública propia, sino que se encuentra dentro de una red privada y brinda sus servicios IP al exterior mediante redireccionamiento de puertos (port forwarding).

## PROBLEMAS CON EL FTP ACTIVO

El modo activo es particularmente difícil de implementar por las siguientes razones:

- De la explicación sobre el funcionamiento del modo activo se observa que para el establecimiento del canal de datos el servidor inicia la conexión e intenta abrir un socket a un puerto efímero del cliente (>1024). Si el cliente está detrás de un firewall restrictivo, este tráfico será inmediatamente rechazado. Ahora, como el puerto que abre el cliente para la conexión de datos es esencialmente impredecible, no podemos anticiparnos a dejar un rango específico de puertos abiertos en el firewall perimetral.
- Un alto porcentaje de los clientes del servicio FTP estarán ubicados en una red interna y utilizarán direcciones IP privadas enmascaradas en una única dirección pública (enmascaramiento IP). En este escenario es muy probable que el establecimiento del canal de datos falle, ya que el enrutador de entrada de la red privada desconocerá el host interno al cual va dirigido el tráfico del nuevo socket y simplemente lo descartará.
- Cuando el cliente inicia el modo activo con el comando PORT, indica en los parámetros del comando su dirección IP y puerto en el que escuchará el nuevo socket (canal de datos). Si el cliente tiene una dirección privada y el enrutador de salida carece de la lógica necesaria para entender el protocolo FTP y modificar en concordancia el datagrama que contiene esa dirección, el servidor recibirá una petición para conectarse a una dirección no enrutable por Internet (por ejemplo, 192.168.3.5), con lo que el canal de datos no podrá abrirse.

## PROBLEMAS CON EL FTP PASIVO

Para solucionar en parte los problemas asociados con FTP activo, se agregó un nuevo modo de operación llamado pasivo, en el que tanto el canal de control como el canal de datos son abiertos del lado del cliente. Esto hace posible que los usuarios remotos puedan acceder al servicio en la mayoría de los casos, así estén detrás de dispositivos firewall/NAT, pero en contraposición crea nuevos problemas del lado del servidor:

- De la explicación hecha sobre el funcionamiento del modo pasivo, se observa que el cliente recibe una respuesta al comando PASV, en la que el servidor le indica su dirección IP y el número de puerto al que se puede conectar. Ya que ese número de puerto será no estándar (>1024), las configuraciones por defecto del firewall detrás del cual se encuentra el servidor bloquearán la nueva conexión en la mayoría de los casos. Si el software FTP específico que se usa no permite restringir el rango de puertos en los que se escucharán conexiones de datos, el administrador de la red se verá avocado a dejar un enorme rango de puertos abiertos para que el servicio FTP funcione correctamente.
- Si el servidor FTP tiene una dirección privada y publica sus servicios en Internet mediante redireccionamiento de puertos (port forwarding), la respuesta al comando PASV de los clientes será una dirección IP no enrutable por Internet

(ej: 192.168.2.35). Si el dispositivo de enrutamiento por donde sale el tráfico del servidor no tiene integrado el entendimiento de las conexiones FTP, el cliente recibirá una dirección IP no válida, de tal manera que el canal de datos no llegará a establecerse.

## FTP Y EL MODELO OSI

Si observamos con detenimiento, el protocolo de transferencia de archivos rompe con el esquema normal del modelo OSI para interconexión de sistemas abiertos. Dentro del campo de datos de los datagramas IP, los comandos y respuestas del protocolo (PORT, PASV), que corresponden a la capa de aplicación, incluyen información sobre direcciones IP y puertos, que corresponde a la capa de red del modelo de OSI. Esto obliga a que los dispositivos de enrutamiento modernos realicen SPI stateful packet inspection (inspección completa del paquete), operación que permite detectar tráfico correspondiente al protocolo FTP y realizar al vuelo las modificaciones pertinentes en los datagramas de control para que los canales de datos de dicho protocolo puedan establecerse exitosamente.

## SOLUCIONES PARA LOS PROBLEMAS

Aunque las soluciones para el establecimiento de las conexiones FTP son diferentes dependiendo del escenario, en términos generales podemos decir que el modo recomendado es el PASIVO. La razón de esto es sencilla de entender: Con el modo activo dejamos los problemas en el lado del cliente, quien muchas veces no tiene ni el conocimiento técnico ni la asesoría para detectar problemas o modificar configuraciones. En el modo pasivo en cambio centralizamos los problemas en el lado del servidor, sobre el cual si tenemos control completo. Recordemos que al fin y al cabo estamos brindando un servicio, por lo que trataremos de garantizar que el mayor número posible de usuarios pueda conectarse sin tener que realizar modificaciones especiales en sus equipos o configuraciones. Hay que en cuenta también que muchos clientes FTP, incluyendo los navegadores más populares, usan el modo pasivo por defecto, por lo que es definitivamente la mejor opción.

## SOLUCIONES PARA EL MODO ACTIVO

Una vez entendidas las complicaciones del modo activo con respecto al establecimiento de sesiones FTP, podemos plantear estas posibles soluciones:

- Si los clientes enmascaran sus direcciones IP privadas mediante NAT, se requiere un enrutador o cortafuegos del lado del usuario que haga revisión completa de paquetes y detecte las conexiones correspondientes al protocolo FTP. Entonces el enrutador abrirá dinámicamente los puertos de entrada según los parámetros establecidos previamente por el canal de datos y redireccionará las peticiones entrantes al cliente correcto.
- Un enrutador conciente del protocolo FTP como el descrito en el punto anterior, se encargará también de modificar la dirección IP y el puerto que el cliente suministra con el comando PORT, para que coincidan con la dirección IP pública que sirve de máscara y el puerto que se usará para el mapeo interno.

## SOLUCIONES PARA EL MODO PASIVO

Con el modo pasivo desaparecen las complicaciones del lado cliente, pero se abren nuevos retos para el administrador del lado servidor. Estas son algunas posibles soluciones:

- Para reducir los riesgos de seguridad que se generarían si se deja abierto en el firewall perimetral un número arbitrario de puertos, conviene instalar un software de servidor FTP que permita definir un rango de puertos específico para el modo pasivo. Productos reconocidos, como vsftpd o PureFTP se pueden configurar para usar un rango delimitado de puertos. Dicho rango deberá ser lo más estrecho posible e irse ampliando en la medida que el número de conexiones simultáneas al servicio así lo requiera. Si el servidor es accedido mediante port forwarding, se deberá redireccionar en el enrutador de entrada el mismo rango de puertos configurado en el servidor.

- Si el router/firewall perimetral de la red del servidor tiene la capacidad de detectar las conexiones FTP, mantendrá el rango de puertos asignados al modo pasivo en estado cerrado y solo los abrirá dinámicamente cuando detecte que en un canal de control se ha negociado la apertura de un nuevo socket proveniente del mismo cliente que solicitó el modo pasivo.

- En el caso de que el enrutador o cortafuegos del lado del servidor que esté enmascarando direcciones privadas pero no tenga conocimiento del protocolo FTP, se puede usar una característica de ciertos paquetes FTP por la cual el servidor no responde al comando PASV con su dirección IP verdadera (la privada) sino con la dirección que se le configure, misma que deberá coincidir con la dirección pública que sirve de máscara.

## PALABRAS FINALES

Como hemos visto en este artículo, lograr que un servicio FTP funcione sin problemas puede ser complicado cuando existen routers/firewalls entre el cliente y el servidor. Con el paso del tiempo los dispositivos de enrutamiento, es decir, enrutadores, cortafuegos y balanceadores de carga, tienden a incorporar de fábrica las capacidades para manejar sin problemas las conexiones FTP. Mientras eso pasa, los administradores de red deberán estar al tanto de los problemas potenciales que se pueden presentar e implementar la mejor solución posible para cada situación en particular.

Autor: Ing. Javier Eraso

Abril de 2007

-----

CIBERNAT ofrece servicios especializados en el área de tecnología informática, incluyendo la instalación y configuración de servidores HTTP, FTP, SSH, Correo entrante y saliente, DNS, bases de datos, etc.