

# **PORT MODE --- PASV MODE Y LOS FIREWALLS: LA UTILIDAD DE LO APRENDIDO :)**

---

- \* **¿Por qué me haces estudiar todo este rollo del PORT y PASV MODE?**
  - \* **Hombre, si me preguntas eso mejor te dedicas a otra cosa. Lo que te ha movido a comprar esta revista es la "curiosidad" de "lo desconocido", poder controlar aquello que otros nunca controlarán. Anda, sigue leyendo y lo comprenderás...**
- 

Recuerda que en el artículo anterior propusimos el problema que sufrían algunos Clientes cuando se conectaban a nuestro Servidor FTP. Podían conectarse pero eran incapaces de bajarse archivos. Recordad que este problema podía ser debido a dos motivos:

- **Motivo 1: Que el Cliente esté detrás de un Firewall, por lo que necesitará acceder a nuestro Servidor mediante PASV MODE y, por supuesto, nuestro servidor deberá admitir ese tipo de conexiones.**
- **Motivo 2: Que el Cliente (o el Servidor) esté tras un NAT ("traductor de direcciones de red") , por lo que tendrá que activar la opción NAT en su FlashFXP (o cualquier otro software Cliente FTP que utilice).**

## 1.- Vamos a meternos de lleno en el PASV MODE, la razón de su existencia, su relación con los Firewalls y las posibles vulnerabilidades :). Dejamos el NAT para otro artículo (que se lo merece).

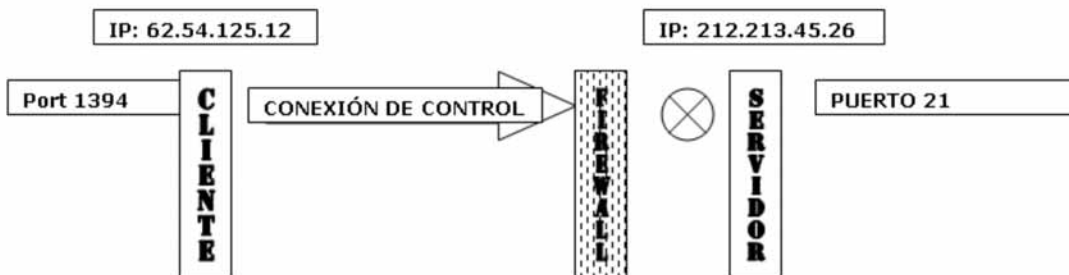
No empezaremos ahora un "curso de Firewall", pero sí dejaremos claros una serie de puntos importantes:

- La misión de un Cortafuegos (Firewall) es impedir las conexiones no "preparadas", es decir, conexiones no esperadas a puertos no esperados.
- Normalmente bloquean por defecto casi todas las conexiones entrantes a la Red que protegen pero son bastante permisivos con las conexiones "salientes" de la red protegida. Esto es muy genérico, pero es así y es muy importante.

La mayoría de ataques llamados "de conexión inversa" se realizan utilizando esta característica de los Firewalls: la permisividad frente a las conexiones salientes. Esto provoca, por ejemplo, poder hacer un telnet inverso y conseguir una Shell del Sistema remoto gracias a que ha sido el "remoto" quien se ha conectado a nosotros. Ya os enseñaré a hacer esto, pero antes hay que estudiar un poco más.

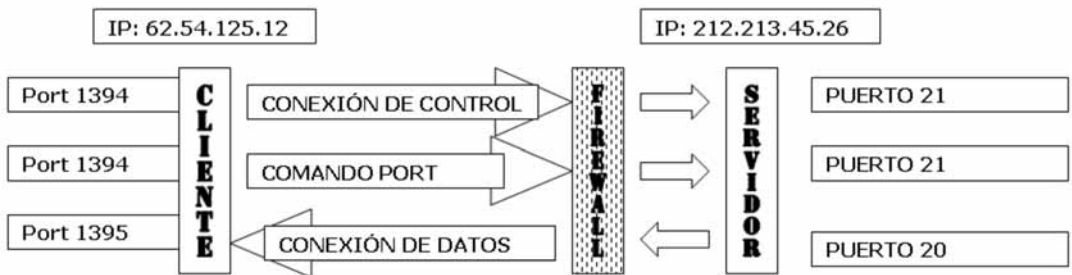
### Ejemplo 1: Un Cliente sin Firewall accediendo en PORT MODE a un Servidor con Firewall que no admite PASV MODE.

Imagina que tienes un Servidor FTP montado en el Puerto 21 y que no admite PASV MODE. Protegiendo tu RED tienes un Firewall que bloquea todas las llamadas entrantes de los Clientes a todos los puertos (incluido el 21) porque no tiene conocimiento (no ha sido configurado) de que ese Servidor puede (y debe) atender llamadas entrantes. El resultado es que ningún Cliente podrá conectarse.



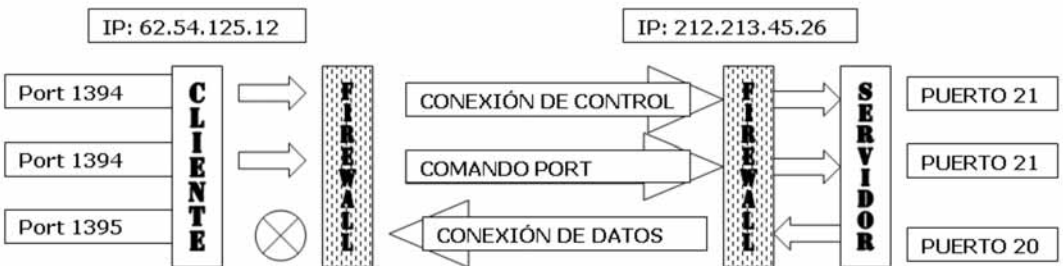
Pero este caso no es muy realista, porque normalmente el Firewall que defiende La RED donde se encuentra el Servidor FTP se configura para admitir conexiones entrantes y salientes para los programas Servidores. Si no, sería imposible ni tan siquiera establecer la Conexión de Control.

Esto quedaría así:



### Ejemplo 2: Un Cliente con Firewall accediendo en PORT MODE a un Servidor con Firewall que no admite PASV MODE.

Mírate el gráfico y lo comentamos después:



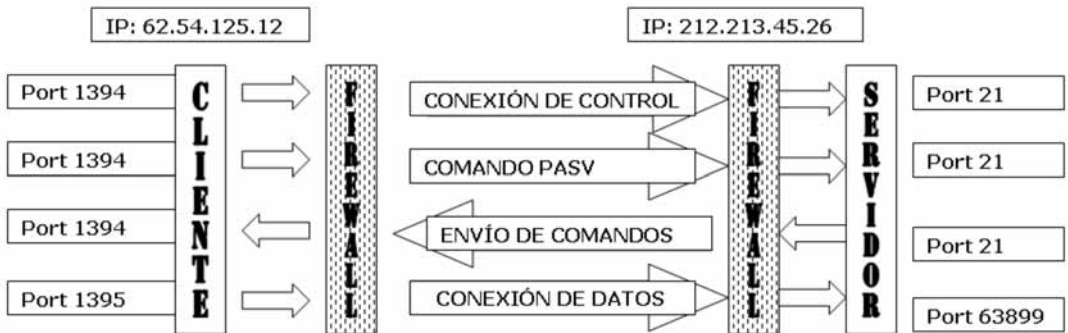
¿Qué ha ocurrido? ¿Por qué no le llega la conexión de Datos? Pues porque como ya hemos avisado, el Firewall del cliente detiene la conexión entrante.

La solución sería decirle al Cliente (que utiliza por ejemplo el FlashFXP) que configure su Firewall para que deje pasar (actuar) a su Software Cliente (el FlashFXP) como un Servidor, es decir, que le de todo tipo de permisos. Buffffffff, eso no es bueno cara a la seguridad ¿verdad? Pues bien, para eso existe el modo PASV Ahora veremos eso en el ejemplo 4.

**Ejemplo 3: Un Cliente con Firewall accediendo en PASV MODE a un Servidor con Firewall que no admite PASV MODE.**

**No tiene sentido explicar esta posibilidad, porque si el Servidor FTP no admite PASV MODE simplemente la conexión no se realizará con éxito.**

**Ejemplo 4: Un Cliente con Firewall accediendo en PASV MODE a un Servidor con Firewall que admite PASV MODE.**



Ahora acabamos de descubrir el motivo de la existencia del PASV MODE Podemos ver como es el Cliente quien establece la Conexión de Datos, respetando la seguridad del Firewall que impide las conexiones entrantes Ahora no hay ni una sola conexión entrante al Cliente

Alguien podría decirme que SI existe una conexión entrante, esa flecha donde pone envío de comandos. Pero recordad que esos comandos se transmiten por una Conexión de Control ya creada anteriormente por el Cliente ¿vale? Recuerda que la conexión, una vez creada permanece hasta que el Cliente cierra su FlashFXP y que en una relación Cliente FTP con Servidor FTP solo existen dos conexiones (la de Control y la de Datos).

Queda claro entonces que las dos conexiones (Control y Datos) han sido establecidas por el Cliente, respetando entonces la máxima de cualquier Firewall: Defender la RED de Conexiones Entrantes

## 2.- Muy bien, te has quedado a gusto... ¿y ahora que?

Cuando te explique como saltarte algunos tipos de Firewalls que protegen Servidores FTP en modo PASV ya me lo agradecerás, ya .

Un ejemplo: Existe un error de implementación del cortafuegos FireWall-1 de la empresa Check Point. Este permite a una máquina con servidor FTP protegida tras este cortafuegos, ser vulnerable a todo tipo de accesos.

FireWall-1 es lo que se denomina un "stateful packet firewall" (cortafuegos de paquetes, con estado). Este tipo de cortafuegos abren y cierran ventanas de comunicación observando el tráfico en tiempo real, de forma dinámica. El FW-1 acepta comandos "PASV" por parte de sus usuarios, para permitir que estos atraviesen su propio cortafuegos (lógico ¿no?, si no no podrían transferirse los archivos, objetivo de tener un Servidor FTP)... PERO!!! ... el problema con FW-1 es la forma que tiene de detectar la apertura de puertos en el servidor FTP que protege: sencillamente busca la cadena 227 al principio de cada paquete que envía el servidor FTP (227 es la respuesta al comando PASV ) ... Y ... existen otros casos en que se puede encontrar un 227 al principio de un paquete, por ejemplo forzando la fragmentación de una respuesta del servidor FTP empleando técnicas de modulación de MTU (Maximum Transfer Unit - Unidad Máxima de Transferencia) y MSS (Maximum Segment Size - Tamaño Máximo de Segmento).

Claro, claro, ahora ya quieres empezar asaltando máquinas que están protegidas por Firewalls y ser el mejor Hacker de la Red... deja de soñar, todo llegará Lo verdaderamente importante es que ahora ya posees conocimientos que te permitirán comprender conceptos mucho mas avanzados, ahora podrás emprender la lectura y práctica de futuros ejercicios, pero aun falta bastante para que puedas empezar a gatear. Seguro que este párrafo se te ha atragantado con términos como MTU, MSS, detección de apertura dinámica, cortafuegos de paquete con estado... je,je, no esperarías otra cosa ¿verdad? No desesperes, todo será explicado en su momento.