FTP

¿Qué es?

El protocolo FTP es una de los primeros protocolos desarrollados para la arquitectura TCP/IP. FTP es un protocolo del nivel de aplicación. Permite establecer una conexión cliente/servidor para transferir archivos del servidor al cliente (descarga) o del cliente al servidor (subida). Las conexiones FTP se establecen sobre conexiones TCP de nivel de transporte.

FUNCIONES PRINCIPALES DE FTP

* Transferencia de archivos entre un cliente y un servidor
* Autenticación de usuarios para acceder al servidor y administrar archivos
* Gestión de archivos y directorios en el servidor remoto.

CÓMO FUNCIONA FTP

* **Cliente-Servidor:** Para transferir archivos. Los clientes FTP inician la conexión para transferir archivos, mientras que los servidores FTP esperan conexiones entrantes
* **Dos canales:** uno de comando para control y otro de datos para transferencia de archivos.

FTP: ACTIVOS Y PASIVOS

|  |  |
| --- | --- |
| Ventajas modo activo | Desventajas modo activo |
| Permite conexiones entrantes y salientes | Requiere puertos adicionales abiertos en el firewall |
| Adecuado para transferencias grandes y de alto volumen | Puede tener problemas con direcciones IP dinámicas |

TIPOS DE TRANSFERENCIA DE FTP

* **Modo activo:** Permite a un servidor FTP iniciar una conexión de datos con el cliente. Requiere que el cliente esté escuchando en un puerto especificado.
* **Modo pasivo:** El cliente inicia la conexión de datos con el servidor. Adecuado para clientes detrás de Firewalls o NAT.
* **Modo Estandarizado:** Utiliza los puertos 20 y 21 para control y transferencia de datos.

CARACTERÍSTICAS DE SEGURIDAD DE FTP

* FTP utiliza un protocolo no seguro, lo que significa que los datos se transmiten en texto claro y son vulnerables a intercepciones.
* No incorpora mecanismos de cifrado ni autenticación robusta por defecto, lo que lo hace vulnerable a ataques de suplantación y escucha.
* Aunque puede implementarse sobre SSL\/TLS (FTPS), carece de funciones avanzadas de seguridad como FTPS.

FTP vs. HTTP

|  |  |
| --- | --- |
| Ventajas de FTP | Ventajas de HTTP |
| FTP es más eficiente para transferir archivos grandes | HTTP es más sencillo de usar para transferir archivos pequeños o páginas web |
| FTP permite la transferencia de archivos sin interrupciones por pérdida de conexión | HTTP no requiere software adicional para la mayoría de las tareas de transferencia de archivos. |
| FTP admite la transferencia de archivos binarios y de texto | HTTP es el protocolo estándar para el acceso a recursos en la World Wide Web |

FTP vs SFTP

|  |  |
| --- | --- |
| FTP | SFTP |
| No es seguro: las contraseñas se envían en texto plano | Altamente seguro: todas las comunicaciones están cifradas |
| Utiliza el puerto 21 por defecto | Utiliza el puerto 22 por defecto |
| Menor protección de datos durante la transferencia | Mayor protección de datos durante la transferencia |

FTP vs FTPS

|  |  |
| --- | --- |
| FTP | FTPS |
| Permite transferencia sin cifrado | Todas las transferencias se cifran para mayor seguridad |
| Menos seguro para transferir datos sensibles | Adecuado para datos sensibles y confidenciales |

CLIENTE FTP

|  |  |  |
| --- | --- | --- |
| Ventajas | Usos comunes | Recomendaciones |
| Permite a los usuarios transferir archivos a y desde un servidor. Ofrece alta velocidad en la transferencia de archivos grandes. | Ampliamente utilizado por desarrolladores web para cargar archivos al servidor. Empleado en entornos de trabajo para compartir documentos. | Utilizar clientes FTP seguros que soporten cifrado. Configurar permisos de usuario adecuados para garantizar la seguridad |

SERVIDOR FTP

|  |  |  |
| --- | --- | --- |
| Funciones principales | Requisitos del sistema | Seguridad y configuración |
| Permite a los usuarios cargar, descargar, renombrar y eliminar archivos en el servidor FTP | Se necesita un sistema informático, generalmente un servidor, con conexión a Internet y un software de servidor FTP instalado | Es crucial configurar adecuadamente los permisos y la seguridad del servidor FTP para proteger la integridad de los datos |

COMANDOS DE FTP

**USER:** Permite especificar el nombre de usuario para iniciar una sesión FTP

**PASS:** Se utiliza para proporcionar la contraseña del usuario especificado.

**PWD (Print Working Directory):** Muestra el directorio de trabajo actual en el servidor remoto

**QUIT:** Cierra la sesión FTP y sale del programa cliente FTP

CÓDIGOS DE RESPUESTA DE FTP

|  |  |
| --- | --- |
| Código primer dígito | Descripción |
| 1XX | Respuesta preliminar positiva. Se ha iniciado la acción requerida y se debe esperar otra respuesta antes de enviar otro comando |
| 2XX | Respuesta de finalización positiva. Comando completado de forma satisfactoria |
| 3XX | Respuesta intermedia positiva. La orden se ha aceptado, pero falta información para completarla. El cliente debe enviar otro comando que incluya dicha información. |
| 4XX | Respuesta de finalización negativa transitoria. Comando descartado de forma temporal |
| 5XX | Respuesta de finalización negativa permanente. Comando descartado permanentemente. |

CÓMO CONFIGURAR FTP EN LINUX

1. Instalarlo “sudo apt-get install vsftpd”
2. Archivos de configuración /etc/vsftpd/ y /etc/ftpusers
3. Iniciarlo “sudo systemctl start vsftpd” o “sudo systemctl restart vsftpd”
4. Configurar reglas de cortafuegos, puertos 20 y 21.

RESOLUCIÓN DE PROBLEMAS COMUNES DE FTP

**Problema de conexión:** Verificar la configuración del cortafuegos y del enrutador para permitir conexiones FTP.

**Problema de autenticación:** Revisar nombre de usuario y contraseña. Permisos de acceso

**Problema de transferencia de archivos:** Verificar permisos de escritura y el espacio disponible del disco.

**Problema de seguridad:** Si hay vulnerabilidades, usar SFTP o FTPS

MEJORES PRÁCTICAS CON FTP

* Utilizar FTP en entornos seguros y no críticos. Evitar enviar datos sensibles a través de FTP sin cifrado.
* Usar contraseñas fuertes y actualizar regularmente las credenciales de acceso
* Hacer copias de seguridad regularmente y verificar la integridad de los datos transferidos.

ALTERNATIVAS A FTP

|  |  |  |
| --- | --- | --- |
| SFTP | FTPS | OTRAS ALTERNATIVAS |
| Alternativa segura que utiliza SSH para cifrar los datos de transferencia | Utiliza SSL/TLS para cifrar los transferencias de datos, más seguro. | WebDAV o SCP |

CONCLUSIÓN

* FTP se sigue usando por su simplicidad y eficiencia en la transferencia de archivos
* Tiene limitaciones en términos de seguridad y cifrado
* Considerar alternativas más seguras como SFTP o FTPS.