به نام خدا

پروتکل FTP

درس کارگاه شبکه‌های کامپیوتری

استاد: سید حامد صالح

دانشجو:

علی مانیان 99110022302012

دانشکده فنی شهید مهاجر اصفهان

نیمسال دوم 1399

فهرست

[آشنائی با پروتکل FTP 2](#_Toc72824220)

[جدول کدهای وضعیت FTP 6](#_Toc72824221)

[نحوه عملکرد پروتکل FTP 9](#_Toc72824222)

[Active Mode 10](#_Toc72824223)

[Passive Mode 11](#_Toc72824224)

[ملاحظات امنیتی 12](#_Toc72824225)

[Passive Mode و یا Active Mode؟ 12](#_Toc72824226)

[پیکربندی فایروال 12](#_Toc72824227)

[یک نکته دیگر دررابطه‌با پروتکل FTP 13](#_Toc72824228)

[منابع 13](#_Toc72824229)

# آشنائی با پروتکل FTP

امروزه از پروتکل‌های متعددی در شبکه‌های کامپیوتری استفاده می‌گردد که صرفاً تعداد اندکی از آنان به‌منظور انتقال داده طراحی و پیاده‌سازی شده‌اند. اینترنت نیز به‌عنوان یک شبکه گسترده از این قاعده مستثنی نبوده و دراین‌رابطه از پروتکل‌های متعددی استفاده می‌شود.

برای بسیاری از کاربران اینترنت همه چیز محدود به وب و پروتکل مرتبط با آن یعنی HTTP است، درصورتی‌که در این عرصه از پروتکل‌های متعدد دیگری نیز استفاده می‌گردد. FTP نمونه‌ای در این زمینه است.

پروتکل FTP چیست؟

تصویر اولیه اینترنت در ذهن بسیاری از کاربران، استفاده از منابع اطلاعاتی و حرکت از سایتی به سایت دیگر است و شاید به همین دلیل باشد که اینترنت در طی سالیان اخیر به‌سرعت رشد و متداول شده است. بسیاری از کارشناسان این عرصه اعتقاد دارند که اینترنت گسترش و عمومیت خود را مدیون سرویس وب می‌باشد.

فرض کنید که سرویس وب را از اینترنت حذف نمایید. برای بسیاری از ما این سؤال مطرح خواهد شد که چه نوع استفاده‌ای را می‌توانیم از اینترنت داشته باشیم؟ در صورت تحقق چنین شرایطی، یکی از عملیاتی که کاربران قادر به انجام آن خواهند بود، دریافت داده، فایل‌های صوتی، تصویری و سایر نمونه فایل‌های دیگر با استفاده از پروتکل FTP (برگرفته از File Transfer Protocol) است.

ویژگی‌های پروتکل FTP

* پروتکل FTP، اولین تلاش انجام شده برای ایجاد یک استاندارد به‌منظور مبادله فایل بر روی شبکه‌های مبتنی بر پروتکل TCP/IP است که از اوایل سال 1970 مطرح و مشخصات استاندارد آن طی RFC 959 در اکتبر سال 1985 ارائه گردید.
* پروتکل FTP دارای حداکثر انعطاف لازم و درعین‌حال امکان‌پذیر به‌منظور استفاده در شبکه‌های مختلف باتوجه‌به نوع پروتکل شبکه است.
* پروتکل FTP از مدل سرویس‌گیرنده - سرویس‌دهنده تبعیت می نمایت. برخلاف HTTP که یک حاکم مطلق در عرصه مرورگرهای وب و سرویس دهندگان وب است، نمی‌توان ادعای مشابهی را دررابطه‌با پروتکل FTP داشت و هم‌اینک مجموعه‌ای گسترده از سرویس‌گیرندگان و سرویس دهندگان FTP وجود دارت.
* برای ارسال فایل با استفاده از پروتکل FTP به یک سرویس‌گیرنده FTP نیاز می‌باشد. ویندوز دارای یک برنامه سرویس‌گیرنده FTP از قبل تعبیه شده می‌باشد ولی دارای محدودیت‌های مختص به خود می‌باشد. دراین‌رابطه نرم‌افزارهای متعددی تاکنون طراحی و پیاده‌سازی شده است:
* WS FTP Professional، FTP Explorer و Smart FTP نمونه‌هایی در این زمینه می‌باشند.
* پروتکل FTP را می‌توان به‌عنوان یک سیستم پرس‌وجو نیز تلقی نمود چراکه سرویس‌گیرندگان و سرویس دهندگان گفتگوی لازم به‌منظور تأیید یکدیگر و ارسال فایل را انجام می‌دهند. علاوه بر این، پروتکل فوق مشخص می‌نماید که سرویس‌گیرنده و سرویس‌دهنده، داده را بر روی کانال گفتگو ارسال نمی‌نماید. در مقابل، سرویس‌گیرنده و سرویس‌دهنده در خصوص نحوه ارسال فایل‌ها بر روی اتصالات مجزا و جداگانه (یک اتصال برای هر ارسال داده) با یکدیگر گفتگو خواهند کرد نمایش لیست فایل‌های موجود در یک دایرکتوری نیز به‌عنوان یک ارسال فایل تلقی می‌گردد ت.
* پروتکل FTP امکان استفاده از سیستم فایل را مشابه پوسته یونیکس و یا خط دستور ویندوز در اختیار کاربران قرار می دهت.
* سرویس‌گیرنده در ابتدا یک پیام را برای سرویس‌دهنده ارسال و سرویس‌دهنده نیز به آن پاسخ خواهد داد و در ادامه ارتباط غیرفعال می‌گردد. وضعیت فوق با سایر پروتکل‌هایی که به‌صورت تراکنشی کار می‌کنند، متفاوت می‌باشد نظیر پروتکل HTTP. برنامه‌های سرویس‌گیرنده زمانی قادر به شبیه‌سازی یک محیط تراکنشی می‌باشند که از مسائلی که قرار است در آینده محقق شوند، آگاهی داشته باشند. در واقع، پروتکل FTP یک دنباله stateful از یک و یا چندین تراکنش است.
* سرویس‌گیرندگان، مسئولیت ایجاد و مقداردهی اولیه درخواست‌ها را برعهده دارند که با استفاده از دستورات اولیه FTP انجام می‌گردد. دستورات فوق، عموماً سه و یا چهار حرفی می‌باشند (مثلاً برای تغییر دایرکتوری از دستور CWD استفاده می‌شود). سرویس‌دهنده نیز بر اساس یک فرمت استاندارد به سرویس‌گیرندگان پاسخ خواهد داد سه رقم که به دنبال آن از space استفاده شده است به همراه یک متن تشریحی. سرویس‌گیرندگان می‌بایست صرفاً به کد عددی نتیجه استناد نمایند چراکه متن تشریحی تغییرپذیر بوده و در عمل برای اشکال‌زدایی مفید است برای کاربران حرفه‌ای ت.
* پروتکل FTP دارای امکانات حمایتی لازم برای ارسال داده با نوع‌های مختلف می‌باشد. دو فرمت متداول، اسکی برای متن (سرویس‌گیرنده با ارسال دستور TYPE A ،‌موضوع را به اطلاع سرویس‌دهنده می‌رساند) و image برای داده‌های باینری است توسط TYPE I مشخص می‌گردد. ارسال داده با فرمت اسکی در مواردی که ماشین سرویس‌دهنده و ماشین سرویس‌گیرنده از استانداردهای متفاوتی برای متن استفاده می‌نمایند، مفید بوده و یک سرویس‌گیرنده می‌تواند پس از دریافت داده آن را به فرمت موردنظر خود ترجمه و استفاده نمایت. مثلاً در نسخه‌های ویندوز از یک دنباله carriage return و linefeed برای نشان‌دادن انتهای خط استفاده می‌گردد درصورتی‌که در سیستم‌های مبتنی بر یونیکس صرفاً از یک linefeed استفاده می شوت. برای ارسال هر نوع داده که به ترجمه نیاز نداشته باشد، می‌توان از ارسال باینری استفاده نمود.
* اتخاذ تصمیم دررابطه‌با نوع ارسال فایل‌ها در اختیار سرویس‌گیرنده است برخلاف HTTP که می‌تواند به سرویس‌گیرنده نوع داده ارسالی را اطلاع دهد ت. معمولاً سرویس‌گیرندگان ارسال باینری را انتخاب می‌نمایند و پس از دریافت فایل، ترجمه لازم را انجام خواهند داد. ارسال باینری ذاتاً دارای کارایی بیشتری است چراکه سرویس‌دهنده و سرویس‌گیرنده نیازی به انجام تراکنش‌های on the fly نخواهند داشت. ارسال اسکی گزینه پیش‌فرض انتخابی توسط پروتکل FTP است و در صورت نیاز به ارسال باینری، سرویس‌گیرنده می‌بایست این موضوع را از سرویس‌دهنده درخواست نمایت.
* یک اتصال پروتکل TCP/IP (نسخه شماره چهار) شامل دو نقطه مجزا می‌باشد که هر نقطه از یک آدرس IP و یک شماره پورت استفاده می نمایت. برقراری ارتباط بین یک سرویس‌گیرنده و یک سرویس‌دهنده منوط به وجود چهار عنصر اطلاعاتی است: آدرس سرویس‌دهنده،‌پورت سرویس‌دهنده، آدرس سرویس‌گیرنده و پورت سرویس گیره. در زمان برقراری یک ارتباط، سرویس‌گیرنده از یک شماره پورت استفاده می نمایت. این شماره پورت می‌تواند متناسب با نوع عملکرد برنامه سرویس‌گیرنده به‌صورت اختیاری و یا اجباری باشد. مثلاً برخی برنامه‌های سرویس‌گیرنده به‌منظور ارتباط با سرویس‌دهنده، نیازمند استفاده از یک شماره پورت خاص می‌باشند نظیر برنامه‌های سرویس‌گیرنده وب و یا مرورگرهای وب که از پورت شماره 80 به‌منظور ارتباط با سرویس‌دهنده وب استفاده می‌نماید. در مواردی که الزامی در خصوص شماره پورت وجود ندارد از یک شماره پورت موقتی و یا ephemeral استفاده می‌گردد. این نوع پورت‌ها موقتی بوده و توسط IP stack ماشین مربوطه به متقاضیان نسبت‌داده‌شده و پس از خاتمه ارتباط، پورت آزاد می‌گردد. باتوجه‌به این‌که اکثر IP Stacks بلافاصله از پورت موقت آزاد شده استفاده نخواهند کرد (تا زمانی که تمام pool تکمیل نشده باشد) ،درصورتی‌که سرویس‌گیرنده مجدداً درخواست برقراری یک ارتباط را نماید، یک شماره پورت موقتی دیگر به وی تخصیص داده می شوت.
* پروتکل FTP منحصراً از پروتکل TCP استفاده می‌نماید هرگز از پروتکل UDP استفاده نمی‌شود. معمولاً پروتکل‌های لایه Application (باتوجه‌به مدل مرجع OSI) از یکی از پروتکل‌های TCP و یا UDP استفاده می‌نمایند به جزء پروتکل DNS ت. پروتکل FTP نیز از برخی جهات شرایط خاص خود را دارد و برای انجام وظایف محوله از دو پورت استفاده می نمایت. این پروتکل معمولاً از پورت شماره 20 برای ارسال داده و از پورت 21 برای گوش‌دادن به فرمان‌ها استفاده می نمایت. توجه داشته باشید که برای ارسال داده همواره از پورت 20 استفاده نمی‌گردد و ممکن است در برخی موارد از پورت‌های دیگر استفاده شوت.
* اکثر سرویس دهندگان FTP از روش خاصی برای رمزنگاری اطلاعات استفاده نمی‌نمایند و در زمان login سرویس‌گیرنده به سرویس‌دهنده، اطلاعات مربوط به نام و رمز عبور کاربر به‌صورت متن معمولی در شبکه ارسال می‌گردد. افرادی که دارای یک Packet sniffer بین سرویس‌گیرنده و سرویس‌دهنده می‌باشند، می‌توانند به‌سادگی اقدام به سرقت نام و رمز عبور نماید. علاوه بر سرقت رمزهای عبور، مهاجمان می‌توانند تمامی مکالمات بر روی اتصالات FTP را شنود و محتویات داده‌های ارسالی را مشاهده نماید. پیشنهادهای متعددی به‌منظور ایمن‌سازی سرویس‌دهنده FTP مطرح می‌گردد ولی تا زمانی که رمزنگاری و امکانات حفاظتی در سطح لایه پروتکل IP اعمال نگردد (مثلاً رمزنگاری توسط IPsecs) ، نمی‌بایست از FTP استفاده گردد خصوصاً اگر بر روی شبکه اطلاعات مهم و حیاتی ارسال و یا دریافت می‌گردد.
* همانند بسیاری از پروتکل‌های لایه Application ، پروتکل FTP دارای کدهای وضعیت خطا مختص به خود می‌باشد (همانند HTTP) که اطلاعات لازم در خصوص وضعیت ارتباط ایجاد شده و یا درخواستی را ارائه می نمایت. زمانی که یک درخواست (GET , PUT) برای یک سرویس‌دهنده FTP ارسال می‌گردد، سرویس‌دهنده پاسخ خود را به‌صورت یک‌رشته اعلام می نمایت. اولین خط این رشته معمولاً شامل نام سرویس‌دهنده و نسخه نرم‌افزار FTP است. در ادامه می‌توان دستورات GET و یا PUT را برای سرویس‌دهنده ارسال نمود. سرویس‌دهنده با ارائه یک پیام وضعیت به درخواست سرویس‌گیرندگان پاسخ می‌دهد. کدهای وضعیت برگردانده شده را می‌توان در پنج گروه متفاوت تقسیم نمود:

کدهای 1xx : پاسخ اولیه

کدهای 2xx : درخواست بدون خطا اجرا گردید.

کدهای 3xx : به اطلاعات بیش‌تری نیاز است.

کدهای 4xx : یک خطا موقت ایجاد شده است.

کدهای 5xx : یک خطا دائمی ایجاد شده است.

# جدول کدهای وضعیت FTP

|  |  |
| --- | --- |
| کدهای وضعیت سری 100 | |
| 110 | Restart reply |
| 120 | Service ready in x minutes |
| 125 | Connection currently open, transfer starting |
| 150 | File status okay, about to open data |
| کدهای وضعیت سری 200 | |
| 200 | Command okay |
| 202 | Command not implemented, superfluous at this site |
| 211 | System status/help reply |
| 212 | Directory status |
| 213 | File status |
| 214 | System Help message |
| 215 | NAME system type |
| 220 | Service ready for next user. |
| 221 | Service closing control connection. Logged off where appropriate |
| 225 | Data connection open; no transfer in progress. |
| 226 | Closing data connection. Requested action successful |
| 227 | Entering Passive Mode |
| 230 | User logged in, continue |
| 250 | Requested file action okay, completed |
| 257 | "PATHNAME" created. |
| کدهای وضعیت سری 300 | |
| 331 | User name okay, need password. |
| 332 | Need account for login |
| 350 | Requested file action pending further information. |
| کدهای وضعیت سری 400 | |
| 421 | Service not available, closing control connection. |
| 425 | Can't open data connection |
| 426 | Connection closed; transfer aborted. |
| 450 | Requested file action not taken. File not available - busy etc ... |
| 451 | Request aborted: error on server in processing. |
| 452 | Requested action not taken. Insufficient resources on system |
| کدهای وضعیت سری 500 | |
| 500 | Syntax error, command unrecognized |
| 501 | Syntax error in parameters or arguments. |
| 502 | Command not implemented. |
| 503 | Bad sequence of commands |
| 504 | Command not implemented for that parameter. |
| 530 | Not logged in. |
| 532 | Need account for storing files |
| 550 | Requested action not taken. File unavailable |
| 552 | Requested file action aborted. Exceeded storage allocation |
| 553 | Requested action not taken. File name not allowed |
| مفهوم برخی از کدهای متداول | |
| 226 | دستور بدون هیچ‌گونه خطائی اجرا گردید. |
| 230 | زمانی این کد نمایش داده می‌شود که یک سرویس‌گیرنده رمز عبور خود را به‌درستی درج و عملیات login با موفقیت انجام شده باشد. |
| 231 | کد فوق نشان‌دهنده دریافت  username  ارسالی سرویس‌گیرنده توسط سرویس‌دهنده می‌باشد و تأییدی است بر اعلام وصول Username (نه صحت آن). |
| 501 | دستور تایپ شده دارای خطا گرامری است و می‌بایست مجدداً" دستور تایپ گردد. |
| 530 | عملیات login با موفقیت انجام نشده است. ممکن است Username و یا رمز عبور اشتباه باشد. |
| 550 | فایل مشخص شده در دستور تایپ شده نامعتبر است. |

# نحوه عملکرد پروتکل FTP

FTP ، یک پروتکل ارسال فایل است که با استفاده از آن سرویس‌گیرندگان می‌توانند به سرویس دهندگان متصل و صرف‌نظر از نوع سرویس‌دهنده اقدام به دریافت و یا ارسال فایل نمایند. پروتکل FTP به‌منظور ارائه خدمات خود از دو حالت متفاوت استفاده می‌نماید: Active Mode و Passive Mode. مهم‌ترین تفاوت بین روش‌های فوق جایگاه سرویس‌دهنده و یا سرویس‌گیرنده در ایجاد و خاتمه یک ارتباط است.

همان گونه که در بخش اول اشاره گردید، یک اتصال پروتکل TCP/IP (نسخه شماره چهار) شامل دو نقطه مجزا می‌باشد که هر نقطه از یک آدرس IP و یک شماره پورت استفاده می‌نماید. برقراری ارتباط بین یک سرویس‌گیرنده و یک سرویس‌دهنده منوط به وجود چهار عنصر اطلاعاتی است: آدرس سرویس‌دهنده،‌پورت سرویس‌دهنده، آدرس سرویس‌گیرنده و پورت سرویس‌گیرنده. در زمان برقراری یک ارتباط، سرویس‌گیرنده از یک شماره پورت استفاده می‌نماید. این شماره پورت می‌تواند متناسب با نوع عملکرد برنامه سرویس‌گیرنده به‌صورت اختیاری و یا اجباری باشد. مثلاً" برخی برنامه‌های سرویس‌گیرنده به‌منظور ارتباط با سرویس‌دهنده، نیازمند استفاده از یک شماره پورت خاص می‌باشند (نظیر برنامه‌های سرویس‌گیرنده وب و یا مرورگرهای وب که از پورت شماره 80 به‌منظور ارتباط با سرویس‌دهنده وب استفاده می‌نماید). در مواردی که الزامی در خصوص شماره پورت وجود ندارد از یک شماره پورت موقتی و یا ephemeral استفاده می‌گردد. این نوع پورت‌ها موقتی بوده و توسط IP stack ماشین مربوطه به متقاضیان نسبت‌داده‌شده و پس از خاتمه ارتباط، پورت آزاد می‌گردد. باتوجه‌به این‌که اکثر IP Stacks بلافاصله از پورت موقت آزاد شده استفاده نخواهند کرد (تا زمانی که تمام pool تکمیل نشده باشد) ،درصورتی‌که سرویس‌گیرنده مجدداً" درخواست برقراری یک ارتباط را نماید، یک شماره پورت موقتی دیگر به وی تخصیص داده می‌شود.

پس از این مقدمه، در ادامه به بررسی هر یک از روش‌های Active و Passive در پروتکل FTP خواهیم پرداخت.

## Active Mode

Active Mode ، روش سنتی ارتباط بین یک سرویس‌گیرنده FTP و یک سرویس‌دهنده می‌باشد که عملکرد آن بر اساس فرایند زیر است:

سرویس‌گیرنده یک ارتباط با پورت 21 سرویس‌دهنده FTP برقرار می‌نماید. پورت 21 ، پورتی است که سرویس‌دهنده به آن گوش فرامی‌دهد تا از صدور فرمان‌ها آگاه و آنان را به ترتیب پاسخ دهد. سرویس‌گیرنده برای برقراری ارتباط با سرویس‌دهنده از یک پورت تصادفی و موقتی (بزرگ‌تر از 1024) استفاده می‌نماید (پورت x).

سرویس‌گیرنده شماره پورت لازم برای ارتباط سرویس‌دهنده با خود را از طریق صدور دستور PORT N+1 به وی اطلاع می‌دهد (پورت x+1)

سرویس‌دهنده یک ارتباط را از طریق پورت 20 خود با پورت مشخص شده سرویس‌گیرنده (پورت x+1) برقرار می‌نماید.

|  |  |
| --- | --- |
| لطفاً" به من از طریق پورت 1931  بر روی آدرس  IP: 192.168.1.2  متصل و سپس داده را ارسال نمایید. | سرویس‌گیرنده |
| تأیید دستور | سرویس‌دهنده |

در فرایند فوق، ارتباط توسط سرویس‌گیرنده آغاز و پاسخ به آن توسط سرویس‌دهنده و از طریق پورت x+1 که توسط سرویس‌گیرنده مشخص شده است، انجام می‌شود. درصورتی‌که سرویس‌گیرنده از سیستم‌ها و دستگاه‌های امنیتی خاصی نظیر فایروال استفاده کرده باشد، می‌بایست تمهیدات لازم به‌منظور ارتباط کامپیوترهای میزبان راه دور به سرویس‌گیرنده پیش‌بینی تا آنان بتوانند به هر پورت بالاتر از 1024 سرویس‌گیرنده دستیابی داشته باشند. بدین منظور لازم است که پورت‌های اشاره شده بر روی ماشین سرویس‌گیرنده open باشند. این موضوع می‌تواند تهدیدات و چالش‌های امنیتی متعددی را برای سرویس‌گیرندگان به دنبال داشته باشد.

## Passive Mode

در Passive Mode که به آن " مدیریت و یا اداره سرویس‌گیرندگان FTP" نیز گفته می‌شود از فرایند زیر استفاده می‌گردد:

* سرویس‌گیرنده دو پورت را فعال می‌نماید (پورت x و x+1)
* ارتباط اولیه از طریق پورت x سرویس‌گیرنده با پورت 21 سرویس‌دهنده آغاز می‌گردد.
* سرویس‌دهنده یک پورت را فعال (Y) و به سرویس‌گیرنده شماره پورت را اعلام می‌نماید.
* در ادامه سرویس‌گیرنده یک اتصال از طریق پورت x+1 با پورت y سرویس‌دهنده برقرار می‌نماید.

|  |  |
| --- | --- |
| لطفاً به من بگوئید که از کجا می‌توانم داده را دریافت نمایم | سرویس‌گیرنده |
| با من از طریق پورت 4023  بر روی آدرس  IP: 192.168.1.25 ارتباط برقرار نمایید. | سرویس‌دهنده |

در فرایند فوق، سرویس‌گیرنده دارای نقش محوری است و فایروال موجود بر روی سرویس‌گیرنده می‌تواند درخواست‌های دریافتی غیرمجاز به پورت‌های بالاتر از 1024 را به‌منظور افزایش امنیت بلاک نمایند. درصورتی‌که بر روی کامپیوترهای سرویس‌دهنده نیز فایروال نصب شده باشد، می‌بایست پیکربندی لازم به‌منظور استفاده از پورت‌های بالاتر از 1024 بر روی آن انجام و آنان open گردند. باز نمودن پورت‌های فوق بر روی سرویس‌دهنده می‌تواند چالش‌های امنیتی خاصی را برای سرویس‌دهنده به دنبال داشته باشد.

متأسفانه تمامی سرویس‌گیرندگان FTP از Passive Mode حمایت نمی‌نمایند. اگر یک سرویس‌گیرنده بتواند به یک سرویس‌دهنده login نماید ولی قادر به ارسال داده بر روی آن نباشد، نشان‌دهنده این موضوع است که فایروال و یا Gateway برای استفاده از Passive Mode به‌درستی پیکربندی نشده است.

# ملاحظات امنیتی

درصورتی‌که فایروال‌های موجود بر روی کامپیوترهای سرویس‌گیرنده به‌درستی پیکربندی نگردند، آنان نمی‌توانند از Active Mode استفاده نمایند. در Passive Mode استحکام سیستم امنیتی در سمت سرویس‌دهنده و توسط فایروال مربوطه انجام خواهد شد؛ بنابراین لازم است به سرویس‌دهنده اجازه داده شود که به اتصالات هر پورت بالاتر از 1024 پاسخ دهد. ترافیک فوق، معمولاً" توسط فایروال سرویس‌دهنده بلاک می‌گردد. در چنین شرایطی امکان استفاده از Passive Mode وجود نخواهد داشت.

## Passive Mode و یا Active Mode؟

باتوجه‌به مستندات درج شده در RFC 1579 ، استفاده از Passive Mode به دلایل متعددی به Active Mode ترجیح داده می‌شود:

* تعداد سرویس دهندگان موجود بر روی اینترنت به‌مراتب کمتر از سرویس‌گیرندگان می‌باشد.
* با استفاده از امکانات موجود می‌توان سرویس دهندگان را پیکربندی تا بتوانند از مجموعه پورت‌های محدود و تعریف شده‌ای با درنظرگرفتن مسائل امنیتی، استفاده نمایند.

## پیکربندی فایروال

جدول زیر پیکربندی فایروال در Active Mode و Passive Mode را نشان می‌دهد.

|  |  |
| --- | --- |
| Active Mode | |
| Server Inbound | from any client port > 1024 to port 21 on the server |
| Server Outbound | from port 20 on the client on any port > 1024 |
| Client Inbound | ports 20 from the server to any port > 1024 on client |
| Client Outbound | from any port > 1024 to port 21 on the server |
| Passive Mode | |
| Server Inbound | port 21 and any port > 1024 from client/anywhere, from any port > 1024 |
| Server Outbound | port 21 and any port > 1024 to client/anywhere, to any port > 1024 |
| Client Inbound | Return traffic, any port > 1024 from server using any port > 1024 |

# یک نکته دیگر دررابطه‌با پروتکل FTP

درصورتی‌که در زمان دریافت یک فایل با استفاده از پروتکل FTP مشکلات خاصی ایجاد که منجر به قطع ارتباط با سرویس‌دهنده FTP گردد، سرویس‌گیرنده می‌تواند با مشخص‌کردن یک offset از فایل دریافتی به سرویس‌دهنده اعلام نماید که عملیات ارسال را از جایی که ارتباط قطع شده است، ادامه دهد (سرویس‌گیرنده از محلی شروع به دریافت فایل می‌نماید که ارتباط غیرفعال شده بود). استفاده از ویژگی فوق به امکانات سرویس‌دهنده FTP بستگی دارد.

# منابع

<https://dmacourse.com/blog/what-is-ftp/>

<https://blog.iranserver.com/ftp-file-transfer-protocol/>

<https://7learn.com/network-and-hardware/ftp>

<https://blog.faradars.org/ftp-%D8%B3%D8%B1%D9%88%D8%B1/>

<https://www.zoomit.ir/howto/135379-what-is-ftp-and-how-do-i-use-it/>

<https://fa.wikipedia.org/wiki/%D9%BE%D8%B1%D9%88%D8%AA%DA%A9%D9%84_%D8%A7%D9%86%D8%AA%D9%82%D8%A7%D9%84_%D9%81%D8%A7%DB%8C%D9%84>

پایان