# اجزای پروتکل SSL

❖ پروتکل SSL دارای دو زیرپروتکل تحت عناوین زیر می باشد:

1. SSL Record Protocol : که نوع قالب بندی داده های ارسالی را تعیین می‌کند.
2. SSL Handshake Protocol : که براساس قالب تعیین شده در پروتکل قبلی، مقدمات ارسال داده ها میان سرویس دهنده و سرویس گیرنده را فراهم می‌سازد.

# مزایای بخش بندی پروتکل SSL به دو زیر پروتکل

1. در ابتدای کار و طی مراحل اولیه ارتباط دست تکانی (Handshake) هویت سرویس دهنده برای سرویس گیرنده مشخص می گردد.

2. در همان ابتدای شروع مبادلات، سرویس دهنده و گیرنده بر سر نوع الگوریتم رمزنگاری تبادلی توافق می کنند.

# به دو زیر پروتکل SSLمزایای بخش بندی پروتکل

3. در صورت لزوم، هویت سرویس گیرنده نیز برای سرویس دهنده احراز می گردد.
4. در صورت استفاده از تکنیک های رمزنگاری مبتنی بر کلید عمومی، می‌توانند کلیدهای اشتراکی مخفی را ایجاد نمایند.
5. ارتباطات رمزنگاری می شود.

# پروتکل HTTPS

- در حال حاضر بسیاری از وب سایت ها علاوه بر پروتکل معمول HTTP از SSL نیز حمایت می کننـد و بـرای دسترسـی امن به اطلاعات وب‌سایت های مذکور می توان از HTTPS استفاده کرد.

- پروتکل HTTP-S همان Secure HTTP است و از پروتکل SSL برای انتقال اطلاعات استفاده می‌کند.

# پروتکل HTTPS

در موارد زیر از پروتکل Https استفاده می‌شود:

- بانک ها
- فروشگاه های الکترونیکی
- Mail Serverها
- و کلیه سایت هایی با اطلاعات مهم و محرمانه کار می‌کنند.

# پروتکل HTTPS

- قابل ذکر است که پروتکلHTTP به صورت پیش فرض از پورت ۸۰ استفاده می کند در حالی کـه پروتکـل HTTPS بـه صورت پیش فرض از پورت ۴۴۳ استفاده می کند. به عبارت دیگر این دو پروتکل دو مجرای ارتباطی کاملاً مجزا دارند.

- تبدیل کدها (رمزگذاری و رمز گشایی) در مبدا و مقصد زمانی را به خود اختصاص می‌دهند. بنـابراین سـرعت HTTPS از HTTP کمتر است.

# پروتکل HTTPS

- وبسایت‌هایی که از پروتکل امن SSL جهت رمزگذاری داده‌ها استفاده می‌کنند، از طریق پروتکل (HTTPS) به جای حالت عادی و غیر امن آن یعنی HTTP با سرویس گیرنده‌ها ارتباط برقرار می‌کنند.

- در مرورگرها، اینگونه وبسایت‌ها معمولاً با علامت قفل سبز (به معنای ارتباط امن سالم) نشان داده می‌شوند.

## ❖ مشخصه های مهم یک فایروال

1. توانایی ثبت و اخطار
2. بازدید حجم بالایی از بسته های اطلاعات
3. سادگی پیکربندی
4. امنیت و افزونگی فایروال

# انواع فایروال

- . فایروالهای سطح مدار (Circuit-Level)
- 2. فایروالهای پروکسی سرور
- فیلترهای Nosstateful packet
- فیلترهای Stateful Packet
- فایروالهای شخصی

## ❖ موقعیت یابی برای فایروال

موقعیت و محل نصب از لحاظ توپولوژیکی

قابلیت دسترسی و نواحی امنیتی

مسیریابی نامتقارن

فایروال‌های لایه‌ای