|  |  |
| --- | --- |
| logomobile.png | BỘ GIÁO DỤC VÀ ĐÀO TẠO  **TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM** |

**BÁO CÁO MÔN HỌC**

**BẢO MẬT THÔNG TIN**

**GIAO THỨC SSL**

Ngành : **CÔNG NGHỆ THÔNG TIN**

Lớp : **18DTHB3**

Sinh viên thực hiện: **HOÀNG VŨ**

MSSV: 1811062571 Lớp: 18DTHB3

**LÊ HOÀNG NAM**

MSSV: 1811061517 Lớp: 18DTHB3

**NGUYỄN QUANG HƯNG**

MSSV: 1811062450 Lớp: 18DTHB3

Giảng viên hướng dẫn : **TỐNG THANH VĂN**

TP. Hồ Chí Minh, 2021

GIAO THỨC SSL

[**Chương 1: Tổng quan về giao thức SSL** 1](#_Toc70551991)

[1. SSL là gì? 1](#_Toc70551992)

[2. Một số định nghĩa, thuật ngữ thường gặp về SSL là gì? 3](#_Toc70551993)

[a. Domain Validation (DV SSL) 3](#_Toc70551994)

[b. Organization Validation (OV SSL) 4](#_Toc70551995)

[c. Extended Validation (EV SSL) 4](#_Toc70551996)

[d. Subject Alternative Names (SANs SSL) 4](#_Toc70551997)

[e. Wildcard SSL Certificate (Wildcard SSL) 4](#_Toc70551998)

[**Chương2:** **Chức năng và hoạt động của SSL** 5](#_Toc70551999)

[1. Chứ năng: 5](#_Toc70552000)

[2. Các trạng thái phiên làm việc và kết nối của SSL 7](#_Toc70552001)

[3. Trình duyệt làm thế nào để kiểm tra một SSL là có thực hay không? 9](#_Toc70552002)

[4. Tại sao nên sử dụng SSL? 10](#_Toc70552003)

[5. Lợi ích khi sử dụng SSL là gì? 10](#_Toc70552004)

[**Chương3: Hướng dẫn cài đặt SSL** 11](#_Toc70552005)

[1. Hướng dẫn cài đặt SSL trên cPanel : 11](#_Toc70552006)

[2. Hướng dẫn cài đặt SSL trên DirectAdmin: 14](#_Toc70552007)

[3. Hướng dẫn cài đặt SSL trên VestaCP: 16](#_Toc70552008)

[4. Hướng dẫn cài đặt SSL với Tomcat: 18](#_Toc70552009)

[5. Hướng dẫn cài đặt Lest’s Encrypt trên máy chủ CentOS với Apache: 20](#_Toc70552010)

[6. Hướng dẫn cài đặt SSL trên máy chủ Ubuntu với Apache2: 23](#_Toc70552011)

[7. Hướng dẫn cài đặt SSL Let’s Encrypt cho trang quản trị VestaCP: 24](#_Toc70552012)

[8. Công cụ kiểm tra SSL đã cài đặt đúng hay chưa: 27](#_Toc70552013)

[**Chương4:** **Kết luận** 28](#_Toc70552014)

# **Chương 1: Tổng quan về giao thức SSL**

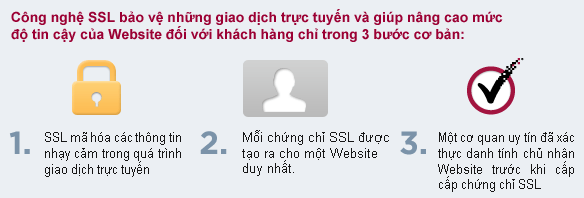
## SSL là gì?

**SSL là viết tắt của từ Secure Sockets Layer. SSL là tiêu chuẩn của công nghệ bảo mật, truyền thông mã hoá giữa máy chủ Web server và trình duyệt**

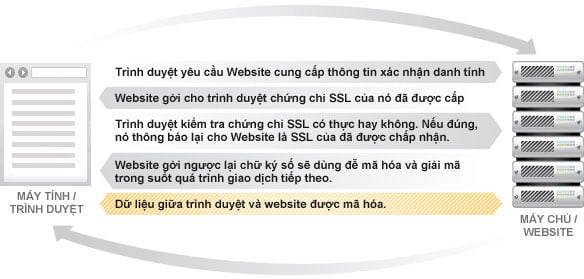
SSL hiện tại cũng là tiêu chuẩn bảo mật cho hàng triệu website trên toàn thế giới, nó bảo vệ dữ liệu truyền đi trên môi trường internet được an toàn.

**SSL** đảm bảo rằng tất cả các dữ liệu được truyền giữa các máy chủ web và các trình duyệt được mang tính riêng tư, tách rời.

Tiêu chuẩn Secure Socket Layer (SSL) – Giao thức an toàn tầng giao vận là một tiêu chuẩn ban đầu do Netscape Communications phát triển ngay sau khi Trung tâm Quốc gia Ứng dụng siêu máy tính (National Center for Supercomputing Applications - NCSA) phát hành Mosaic 1.0, trình duyệt web phổ biến đầu tiên vào năm 1993. Tám tháng sau, vào giữa năm 1994, Netscape Communications đã hoàn thành thiết kế cho SSL phiên bản 1 (SSL 1.0). Phiên bản này chỉ lưu hành nội bộ và chưa bao giờ được công bố ra bên ngoài vì nó đã có một số sai sót. Ví dụ, nó không cung cấp bảo vệ toàn vẹn dữ liệu. Kết hợp với việc sử dụng thuật toán mã hóa dòng RC4 để mã hóa dữ liệu, điều này cho phép một tin tặc thay đổi thông điệp gốc có thể dự đoán được. Ngoài ra, SSL 1.0 không sử dụng số thứ tự, vì vậy nó dễ bị tổn thương để chống lại các cuộc tấn công. Sau đó, các nhà thiết kế của SSL 1.0 thêm số thứ tự và bít kiểm tra, nhưng SSL 1.0 vẫn sử dụng thuật toán kiểm tra lỗi dư thừa theo chu kỳ (Cyclic Redundancy Check - CRC) thay vì sử dụng một hàm băm mã hóa mạnh mẽ. Đến cuối năm 1994, Netscape Communications đã phát triển SSL phiên bản 2 (SSL 2.0) và công bố chính thức vào tháng 2/1995 nhưng chứa nhiều lỗi nghiêm trọng nên dẫn đến phải phát triển SSL phiên bản 3 (SSL 3.0). SSL 3.0 do tổ chức Internet Engineering Task Force (IETF) - Nhóm chuyên trách kỹ thuật Internet công bố vào tháng 11/1996 tại [RFC 6101](http://tools.ietf.org/html/rfc6101) nhưng chỉ ở dạng bản nháp và chưa bao giờ được phát hành chính thức. Các phiên bản tiếp theo của SSL cũng như TLS sẽ dựa trên SSL 3.0 để phát triển.

****

SSL là một chuẩn công nghiệp được sử dụng bởi hàng triệu trang web trong việc bảo vệ các giao dịch trực tuyến với khách hàng của họ.



SSL là một giao thức có phân lớp. Tại mỗi lớp, các thông điệp có thể có các trường như trường độ dài, mô tả và nội dung. SSL có thể phân mảnh gói dữ liệu ban đầu thành nhiều khối dữ liệu nhỏ hơn có thể quản lý, tùy chọn nén dữ liệu, áp dụng một hàm băm Mã xác thực thông điệp (Message Authentication Code - MAC), mã hóa và truyền dữ liệu đi. Dữ liệu nhận về sẽ được giải mã, xác nhận, giải nén và tổng hợp lại, sau đó được chuyển tới các thành phần khác ở mức cao hơn.

Các mục tiêu của SSL 3.0 theo thứ tự ưu tiên là:

+ An ninh mã hóa:

SSL nên được sử dụng để thiết lập một kết nối an toàn giữa hai bên.

+ Khả năng liên thông:

Các nhà phát triển phần mềm độc lập có thể phát triển ứng dụng sử dụng SSL 3.0 có thể trao đổi các tham số mã hóa mà không cần hiểu hết mã nguồn của người khác.

Không phải tất cả các trường hợp có thể kết nối thành công (ngay cả trong cùng lớp ứng dụng). Ví dụ, nếu máy chủ hỗ trợ thiết bị phần cứng cụ thể và máy khách không có quyền truy cập thiết bị phần cứng đó thì kết nối sẽ không thành công.

+ Khả năng mở rộng:

SSL nhằm tạo ra một khung cho phép phương pháp khóa công khai và mã hóa số lượng lớn mới tạo ra có thể kết hợp với nhau khi cần thiết. Điều này cũng sẽ thực hiện hai mục tiêu khác: tránh tạo ra một giao thức mới (rủi ro vì có thể có điểm yếu mới) và tránh phải xây dựng toàn bộ một thư viện bảo mật mới.

+ Hiệu quả tương đối:

Việc mã hóa có xu hướng sử dụng tài nguyên CPU cao, đặc biệt là quá trình trao đổi khóa công khai. Vì lý do này, SSL đã kết hợp một thủ tục lưu trữ bộ nhớ đệm theo phiên tùy chọn để giảm số lượng kết nối cần được thiết lập từ đầu. Ngoài ra, SSL cũng xem xét thực hiện giảm hoạt động mạng.

## Một số định nghĩa, thuật ngữ thường gặp về SSL là gì?

Để hiểu rõ hơn, chúng ta cần phải biết **Certificate Authority (CA)** là gì?

CA là tổ chức phát hành các chứng thực các loại chứng thư số cho người dùng, doanh nghiệp, máy chủ (server), mã code, phần mềm. Nhà cung cấp chứng thực số đóng vai trò là bên thứ ba (được cả hai bên tin tưởng) để hỗ trợ cho quá trình trao đổi thông tin an toàn.

Trong bài viết này, chúng tôi đơn cử **Global Sign** – một trong những doanh nghiệp đầu tiên trên thế giới được công nhận là nhà cung cấp dịch vụ chứng thực chữ ký số công cộng cung cấp tất cả các loại chứng thư, gói chứng thư, giải pháp chứng thư số cho các ngành tài chính – ngân hàng, y tế, giáo dục và các lĩnh vực kinh doanh khác.

* Chứng thư tiêu chuẩn toàn cầu.
* Tương thích với 99% các trình duyệt.
* Cung cấp bởi một trong những CA uy tín nhất thế giới.
* Định hướng doanh nghiệp với tất cả các dòng sản phẩm SSL.
* Tiết kiệm cho doanh nghiệp với lựa chọn Wildcard, SAN.

### Domain Validation (DV SSL)

Chứng thư số SSL chứng thực cho Domain Name – Website. Khi 1 Website sử dụng DV SSL thì sẽ được xác thực tên domain, website đã được mã hoá an toàn khi trao đổi dữ liệu.

### Organization Validation (OV SSL)

Chứng thư số SSL chứng thực cho Website và xác thực doanh nghiệp đang sở hữu website đó .

### Extended Validation (EV SSL)

Cho khách hàng của bạn thấy Website đang sử dụng chứng thư SSL có độ bảo mật cao nhất và được rà soát pháp lý kỹ càng.

### Subject Alternative Names (SANs SSL)

Nhiều tên miền hợp nhất trong 1 chứng thư số:

* Một chứng thư số SSL tiêu chuẩn chỉ bảo mật cho duy nhất một tên miền đã được kiểm định. Lựa chọn thêm SANs chỉ với chứng thư duy nhất bảo đảm cho nhiều tên miền con. SANs mang lại sự linh hoạt cho người sử dụng, dễ dàng hơn trong việc cài đặt, sử dụng và quản lý chứng thư số SSL. Ngoài ra, SANs có tính bảo mật cao hơn Wildcard SSL, đáp ứng chính xác yêu cầu an toàn đối với máy chủ và làm giảm tổng chi phí triển khai SSL tới tất cả các tên miền và máy chủ cần thiết.
* Chứng thư số SSL SANs có thể tích hợp với tất cả các loại chứng thư số SSL của GlobalSign bao gồm: *Chứng thực tên miền (DV SSL)*, *Chứng thực tổ chức doanh nghiệp (OV SSL)* và *Chứng thực mở rộng cao cấp (EV SSL)*.

### Wildcard SSL Certificate (Wildcard SSL)

Sản phẩm lý tưởng dành cho các cổng thương mại điện tử. Mỗi e-store là một sub-domain và được chia sẻ trên một hoặc nhiều địa chỉ IP. Khi đó, để triển khai giải pháp bảo bảo mật giao dịch trực tuyến (đặt hàng, thanh toán, đăng ký & đăng nhập tài khoản,…) bằng SSL, chúng ta có thể dùng duy nhất một chứng chỉ số Wildcard cho tên miền chính của website và tất cả sub-domain.

**Chương2: Chức năng và hoạt động của SSL**

* 1. **Chứ năng:**

SSL là một giao thức theo mô hình khách/chủ (client/server) cung cấp các dịch vụ bảo mật cơ bản trong việc kết nối ngang hàng sau đây:

• Các dịch vụ xác thực;

• Các dịch vụ kết nối bảo mật;

• Các dịch vụ kết nối toàn vẹn (không phục hồi).

SSL cung cấp dịch vụ kết nối an ninh có ba đặc tính cơ bản:

- Kết nối bí mật. Mã hóa được sử dụng sau khi thiết lập kết nối để xác định một khóa bí mật. Mã hóa đối xứng được sử dụng để mã hóa dữ liệu (ví dụ các tiêu chuẩn mã hóa: Data Encryption Standard - DES, 3DES – Triple Data Encryption Standard, RC4).

- Định danh của điểm kết nối có thể được xác thực bằng cách sử dụng mã hóa bất đối xứng hoặc khóa công khai (ví dụ như Rivest-Shamir-Adleman - RSA, Digital Signature Standard - DSS).

- Kết nối đáng tin cậy. Thông điệp vận chuyển thông báo bao gồm kiểm tra tính toàn vẹn thông điệp sử dụng một MAC, hàm băm an toàn được sử dụng để tính toán MAC ví dụ SHA, MD5.

Mặc dù thực tế giao thức SSL sử dụng mật mã khóa công khai nhưng nó không cung cấp dịch vụ chống chối bỏ, không chống chối bỏ cho bằng chứng về nguồn gốc cũng như không chống chối bỏ cho bằng chứng đã truyền tin. Điều này trái ngược hẳn với giao thức an toàn truyền siêu văn bản (Secure Hypertext Transfer Protocol, S-HTTP) và ký số ngôn ngữ đánh dấu mở rộng (Extensible Markup Language Signature- XML Signature). Như tên gọi của nó, giao thức SSL định hướng theo cửa giao tiếp mạng, có nghĩa là tất cả hoặc không có dữ liệu gửi hoặc nhận nào được mã hóa bảo vệ từ một cửa giao tiếp mạng theo cùng một cách.

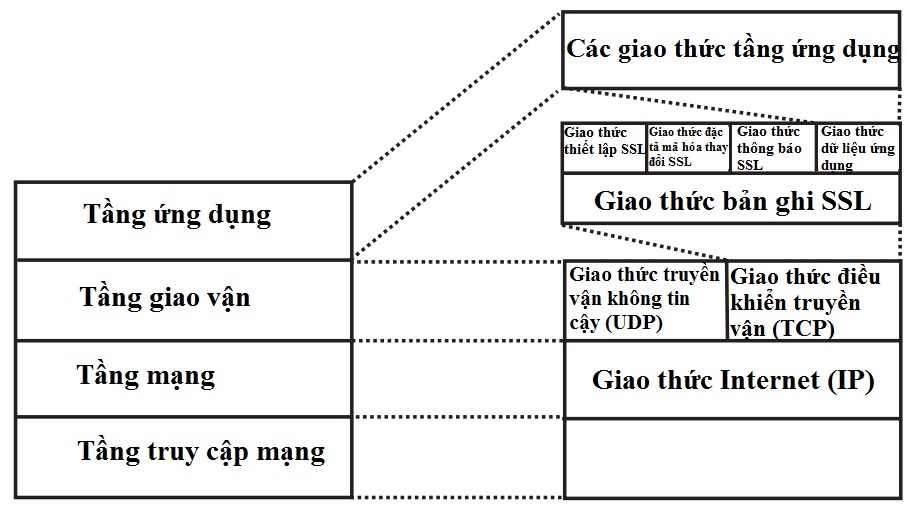
SSL được xem như một tầng trung gian tốt nhất giữa tầng giao vận và tầng ứng dụng trong mô hình TCP/IP. SSL có hai chức năng chính sau:

- Thứ nhất là thiết lập một kênh kết nối an toàn giữa các điểm giao tiếp (ví dụ, xác thực và bảo mật).

- Thứ hai, SSL sử dụng kết nối này để truyền tải dữ liệu của giao thức ở tầng cao hơn từ nơi gửi đến nơi nhận một cách an toàn. Do đó, nó chia dữ liệu thành các phần nhỏ hơn và xử lý từng phần dữ liệu đã chia đó, mỗi phần có thể được nén, xác thực với một MAC, mã hóa, thêm vào trước với một tiêu đề và được truyền đến nơi nhận. Mỗi phần dữ liệu được xử lý và chuẩn bị theo cách này được gọi là một bản ghi SSL.

- Về phía người nhận, các bản ghi SSL phải được giải mã, xác nhận (sử dụng MAC của mình), giải nén, và tập hợp lại, trước khi dữ liệu có thể được gửi đến các tầng cao hơn tương ứng, thường là tầng ứng dụng.

Vị trí của giao thức SSL được minh họa trong Hình 1. Nó bao gồm hai lớp con và một số giao thức thành phần:



***Hình 1: Quan hệ giữa SSL và các giao thức***

(Nguồn: *SSL and TLS: Theory and Practice*, Rolf Oppliger)

- Lớp thấp hơn gọi là Lớp bản ghi (Record Layer), bao gồm Giao thức bản ghi SSL (SSL Record Protocol), nằm trên tầng giao vận, một số giao thức trong tầng giao vận như Giao thức điều khiển truyền vận (TCP),

Giao thức truyền vận không tin cậy (UDP).

- Lớp cao hơn gọi là Lớp thiết lập (Handshake Layer) nằm trên lớp chứa Giao thức bản ghi SSL bao gồm bốn giao thức:

• Giao thức thiết lập SSL (SSL Handshake Protocol) là giao thức cốt lõi của SSL, nó cho phép các điểm giao tiếp xác thực lẫn nhau và thoả thuận cách thức mã hóa và phương pháp nén. Cách thức mã hóa được sử dụng để mã hóa bảo vệ dữ liệu về tính xác thực, tính toàn vẹn và tính bí mật, trong khi đó phương pháp nén là tùy chọn để nén dữ liệu.

• Giao thức đặc tả mã hóa thay đổi SSL (SSL Change Cipher Spec Protocol) cho phép các điểm giao tiếp thông báo thay đổi cách thức mã hóa. Trong khi Giao thức thiết lập SSL được sử dụng để thỏa thuận các tham số bảo mật, thì Giao thức đặc tả mã hóa thay đổi SSL được sử dụng để đặt các tham số vào đúng vị trí và làm chúng hoạt động có hiệu quả.

• Giao thức cảnh báo SSL (SSL Alert Protocol) cho phép các điểm giao tiếp báo hiệu các vấn đề có thể xảy ra và trao đổi thông điệp cảnh báo tương ứng.

• Giao thức dữ liệu ứng dụng SSL (SSL Application Data Protocol) được sử dụng cho chức năng thứ hai của SSL đề cập ở trên (ví dụ truyền tải an toàn của dữ liệu ứng dụng). Giao thức này là thành phần hoạt động chính thực tế của SSL: nó lấy dữ liệu từ tầng cao hơn, thường là tầng ứng dụng và chuyển cho Giao thức bản ghi SSL để bảo vệ mã hóa và bảo đảm an toàn việc truyền dẫn.

## 2. Các trạng thái phiên làm việc và kết nối của SSL

- Một phiên làm việc của SSL có trạng thái. Đây là nhiệm vụ của Giao thức thiết lập SSL để điều phối các trạng thái của máy khách và máy chủ, do đó cho phép giao thức quản lý cơ chế làm việc của mỗi máy để hoạt động thống nhất mặc dù hành động không diễn ra đồng thời.

- Có hai trạng thái làm việc, một là trạng thái hoạt động hiện tại (trong quá trình thiết lập giao thức), hai là trạng thái chờ. Bên cạnh đó, cũng phân biệt các trạng thái đọc và ghi để duy trì cơ chế làm việc. Khi máy khách hay máy chủ nhận một thông báo đặc tả thay đổi mã hóa, nó sao chép trạng thái chờ đọc vào trạng thái đọc hiện tại. Khi máy khách hay máy chủ gửi một thông báo đặc tả thay đổi mã hóa, nó sao chép trạng thái chờ ghi vào trạng thái ghi hiện tại. Khi quá trình thỏa thuận thiết lập hoàn thành, máy khách và máy chủ trao đổi các thông điệp đặc tả thay đổi mã hóa và bắt đầu giao tiếp bằng cách sử dụng những đặc tả mã hóa đã thỏa thuận trước đó.

- Một phiên làm việc SSL có thể bao gồm nhiều kết nối an toàn, bên cạnh đó, các bên tham gia có thể có nhiều phiên làm việc khác nhau đồng thời.

- Một trạng thái phiên làm việc bao gồm các tham số sau đây:

• Định danh phiên làm việc (*session identifier*): Là một byte bất kỳ có thứ tự được chọn bởi máy chủ để xác định một trạng thái phiên làm việc đang hoạt động hoặc có thể khôi phục lại trạng thái phiên làm việc hiện tại.

• Chứng thư của thành phần tham gia (*peer certificate)*: X509.v3, chứng thư của thành phần tham gia, tham số này có thể bỏ trống.

• Phương pháp nén (*compression method*): Thuật toán sử dụng để nén dữ liệu trước khi mã hóa.

• Đặc tả mã hóa (*cipher spec*): Xác định thuật toán mã hóa dữ liệu lớn (ví dụ như DES..) và một thuật toán MAC (ví dụ MD5 hay SHA). Nó cũng định nghĩa các thuộc tính mã hóa, ví dụ kích thước băm (*hash\_size*).

• Mã bí mật chính (*master secret*): Một thông điệp bí mật có kích thước 48 byte được chia sẻ giữa máy khách và máy chủ.

• Có thể khôi phục (*is resumable*): Một chỉ báo phiên làm việc có thể được sử dụng để khởi tạo các kết nối mới.

- Trạng thái kết nối bao gồm các thành phần sau:

• Số thứ tự máy chủ và máy khách ngẫu nhiên (*server and client random*): Là một byte sắp thứ tự được chọn bởi máy chủ và máy khách trong từng phiên làm việc.

• Máy chủ ghi mã MAC bí mật (*server write MAC secret*): Mã bí mật được máy chủ ghi ra trong quá trình thực hiện MAC.

• Máy khách ghi mã MAC bí mật (*client write MAC secret*): Mã bí mật được máy khách ghi ra trong quá trình thực hiện MAC.

• Khóa máy chủ ghi (*server write key*): Khóa mã được sử dụng để mã hóa dữ liệu bởi máy chủ và giải mã của máy khách.

• Khóa máy khách ghi (*client write key*): Khóa mã được sử dụng để mã hóa dữ liệu bởi máy khách và giải mã của máy chủ.

• Các véc-tơ khởi tạo (*initialization vectors*): Khi một khối mã hóa trong mô hình mã hóa theo khối (Cipher Block Chaining - CBC) được sử dụng, một véc-tơ khởi tạo được sinh ra cho từng khóa. Trường này đầu tiên được khởi tạo bởi Giao thức thiết lập SSL, sau đó khối mã hóa cuối cùng từ mỗi bản ghi được lưu trữ để sử dụng cho bản ghi tiếp theo.

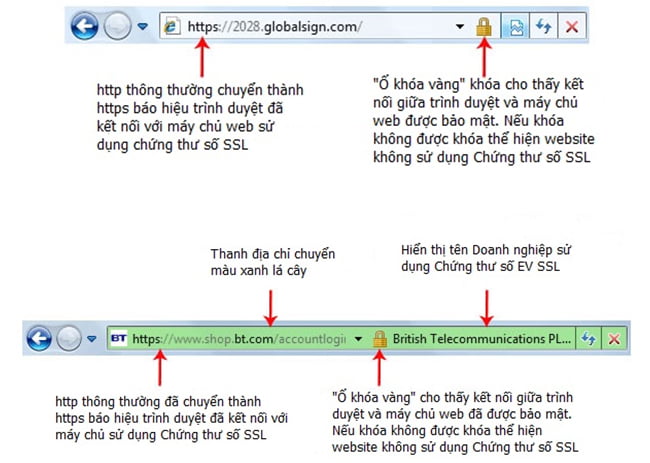
• Số thứ tự (*sequence numbers*): Mỗi bên tham gia trong phiên làm việc quản lý những số thứ tự riêng biệt để truyền và nhận thông điệp trong mỗi kết nối. Khi một bên gửi hoặc nhận một thông điệp đặc tả mã hóa thay đổi, số thứ tự tương ứng được đặt bằng 0. Các số thứ tự có dạng số nguyên và giá trị không được vượt quá 264 – 1.

## Trình duyệt làm thế nào để kiểm tra một SSL là có thực hay không?

Khi Website gởi cho trình duyệt một chứng chỉ SSL, Trình duyệt sẽ gởi chứng chỉ này đến một máy chủ lưu trữ các chứng chỉ số đã được phê duyệt. Các máy chủ này được thành lập bởi những công ty uy tín như GlobalSign, [VeriSign](http://www.verisign.com/).

Về mặt kỹ thuật, SSL sử dụng mã hóa công khai. Kỹ thuật này giúp cho Website và Trình duyệt tự thỏa thuận (bước 4 ở hình trên) một bộ khóa sẽ dùng trong suốt quá trình trao đổi thông tin sau đó.

Bộ khóa sẽ thay đổi theo mỗi trong lần giao dịch kế tiếp, một người khác sẽ không thể giải mã ngay cả khi có được dữ liệu của máy chủ lưu trữ chứng chỉ số nói trên.

Khi Website gởi cho trình duyệt một chứng chỉ SSL, Trình duyệt sẽ gởi chứng chỉ này đến một máy chủ lưu trữ các chứng chỉ số đã được phê duyệt.

## Tại sao nên sử dụng SSL?

SSL được phát triển cho phép trao đổi riêng tư trên mạng Internet, cho phép các ứng dụng khách/chủ giao tiếp an toàn, ngăn ngừa tấn công, bóc tách dữ liệu hay phá hủy thông điệp trái phép như an toàn truyền siêu văn bản, an toàn trao đổi thư điện tử… Trong [Thông tư số 01/2011/TT-BTTTT](http://mic.gov.vn/vbqppl/Lists/Vn%20bn%20QPPL/DispForm.aspx?ID=7734) ngày 04/01/2011 của Bộ trưởng Bộ Thông tin và Truyền thông Công bố Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước quy định **Bắt buộc áp dụng** tiêu chuẩn SSL phiên bản 3.0 và được xếp vào nhóm **Tiêu chuẩn về an toàn thông tin**.

Khi bạn [đăng ký tên miền](https://www.matbao.net/ten-mien/dang-ky-ten-mien.html) để sử dụng các dịch vụ website, email v.v… luôn có những lỗ hổng bảo mật cho hacker tấn công, **SSL** bảo vệ website và khách hàng của bạn.

* **An toàn dữ liệu:** dữ liệu không bị thay đổi bởi hacker.
* **Bảo mật dữ liệu:** dữ liệu được mã hóa và chỉ người nhận đích thực mới có thể giải mã.
* **Chống chối bỏ:** đối tượng thực hiện gửi dữ liệu không thể phủ nhận dữ liệu của mình.

Tiêu chuẩn xác thực – SSL chỉ được cung cấp bởi các đơn vị cấp phát chứng thư (CA) có uy tín trên toàn thế giới sau khi đã thực hiện xác minh thông tin về chủ thể đăng ký rất kỹ càng mang lại mức độ tin cậy cao cho người dùng Internet và tạo nên giá trị cho các website, doanh nghiệp cung cấp dịch vụ.

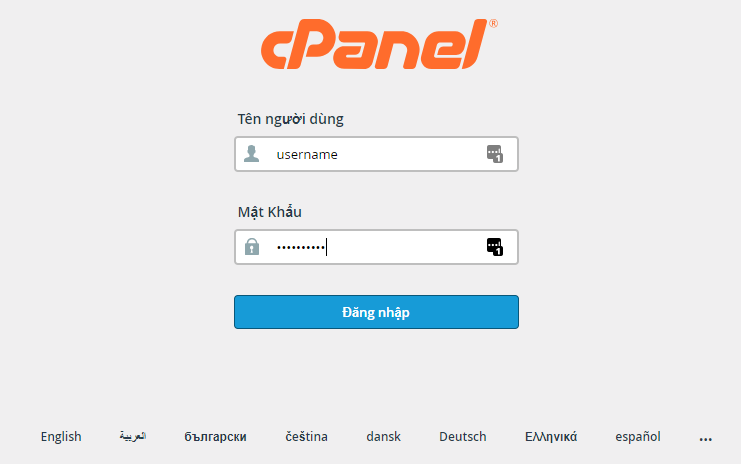
## Lợi ích khi sử dụng SSL là gì?

* Xác thực website, giao dịch.
* Nâng cao hình ảnh, thương hiệu và uy tín doanh nghiệp.
* Bảo mật các giao dịch giữa khách hàng và doanh nghiệp, các dịch vụ truy nhập hệ thống.
* Bảo mật webmail và các ứng dụng như Outlook Web Access, Exchange, và Office Communication Server.
* Bảo mật các ứng dụng ảo hó như Citrix Delivery Platform hoặc các ứng dụng điện toán đám mây.
* Bảo mật dịch vụ FTP.
* Bảo mật truy cập control panel.
* Bảo mật các dịch vụ truyền dữ liệu trong mạng nội bộ, file sharing, extranet.
* Bảo mật VPN Access Servers, Citrix Access Gateway …
* Website không được xác thực và bảo mật sẽ luôn ẩn chứa nguy cơ bị xâm nhập dữ liệu, dẫn đến hậu quả khách hàng không tin tưởng sử dụng dịch vụ.

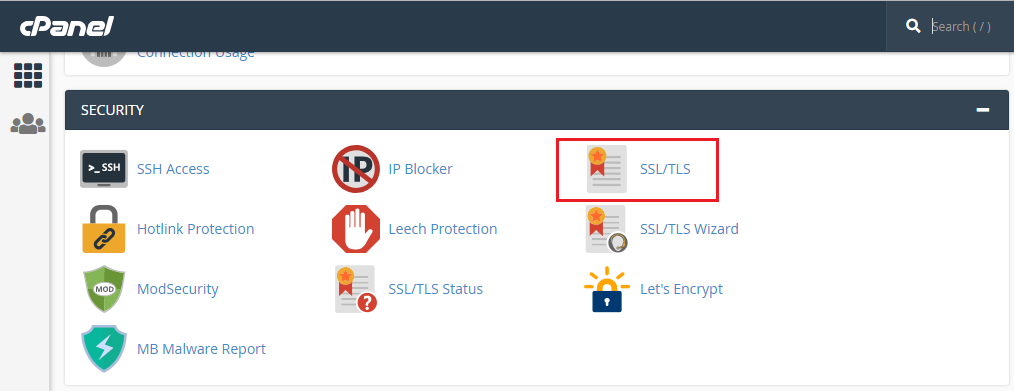
# **Chương3: Hướng dẫn cài đặt SSL**

## 1. [Hướng dẫn cài đặt SSL trên cPanel](https://wiki.matbao.net/kb/huong-dan-cai-dat-ssl-tren-cpanel/):

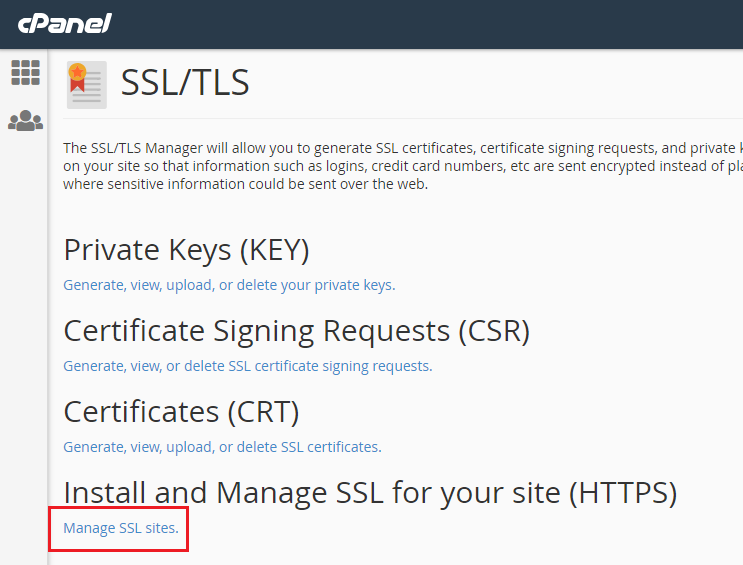
Đầu tiên, cần đăng nhập vào **cPanel** theo thông tin quản trị Cloud Hosting mà Mắt Bão đã cung cấp.



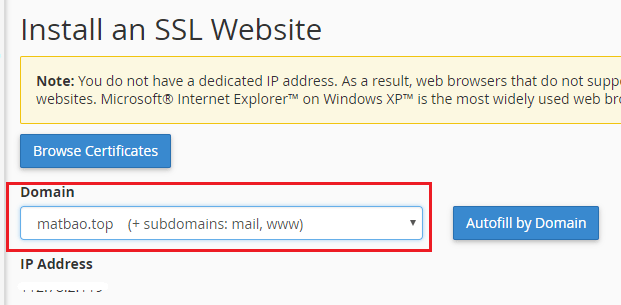
Tiếp theo, bạn nhấp chọn vào mục **SSL/TLS**trong trình đơn**SECURITY**



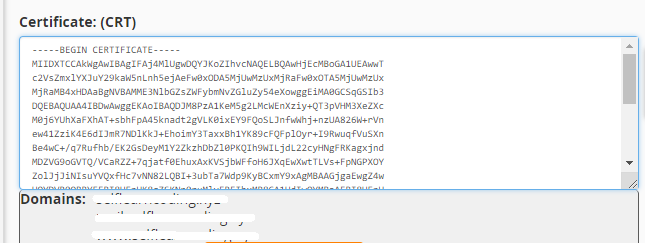
Trong giao diện chính SSL/TLS, bạn nhấp chọn vào mục **Manage SSL sites**

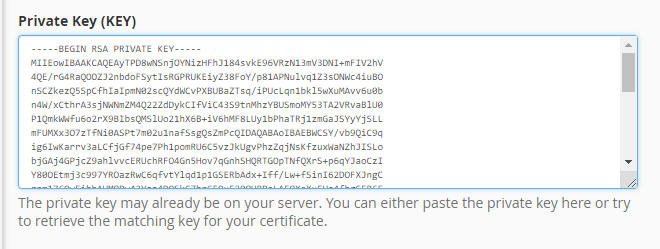


Trong giao diện **Manage SSL Hosts**, bạn chọn tên miền cần cài đặt chứng chỉ SSL

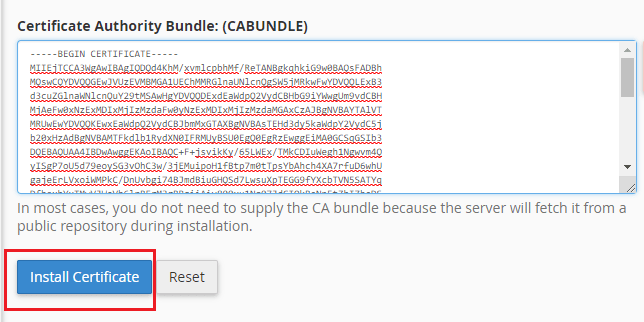


Ngay phía bên dưới, bạn copy và dán chính xác nội dung file CRT, Private Key và CA lần lượt vào 3 ô trống **Certificate: (CRT)**, **Private Key (KEY)**, **Certificate Authority Bundle (CABUNDLE)** tương ứng.





Cuối cùng bạn nhấp chọn **Install Certificate** để hệ thống khởi động tiến trình cài đặt chứng chỉ SSL.



Quá trình cài đặt SSL thành công. Sau ít phút bạn có thể kiểm tra lại thông tin chứng chỉ SSL tại trang:

https://managed.matbao.com/tool/ssl/sslchecker/

## [Hướng dẫn cài đặt SSL trên DirectAdmin](https://wiki.matbao.net/kb/huong-dan-cai-dat-ssl-tren-directadmin/):

Để cài đặt SSL bạn cần phải đăng ký dịch vụ chứng chỉ số tại Mắt Bão hoặc tại nhà cung cấp dịch vụ khác. Để hiểu hơn về chứng chỉ SSL, cách tạo mã CSR và đăng kí SSL bạn có thể tham khảo các bài viết sau:

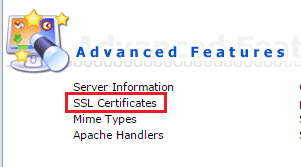
* [Hiểu về chứng chỉ SSL](https://wiki.matbao.net/kb/tong-quan-ve-ssl/)
* [Những lưu ý khi đăng ký sử dụng chứng thư SSL](https://wiki.matbao.net/kb/nhung-luu-y-khi-dang-ky-su-dung-chung-thu-ssl/)
* [Tạo mã CSR (Certificate Signing Request) và Private Key](https://tool.matbao.support/Tools/SSLCsrGenerator)

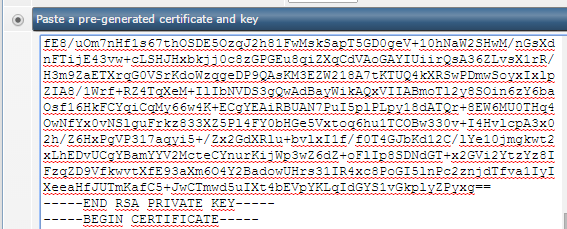
Bài viết này Mắt Bão hướng dẫn cài đặt chứng chỉ số trên DirectAdmin với quyền quản trị cao nhất. Với quyền thấp hơn bạn có thể liên hệ với hỗ trợ kỹ thuật để yêu cầu xử lý một số bước ở quyền quản trị.

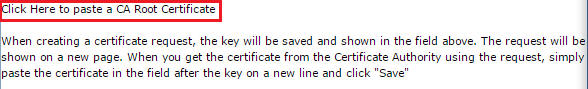
Truy cập SSH vào VPS bằng quyền root.

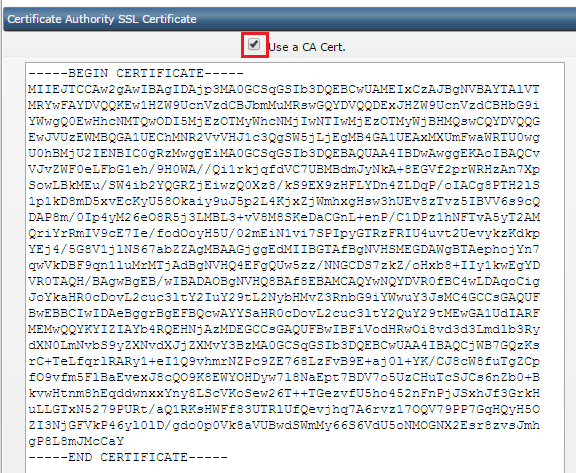
Thêm **enable\_ssl\_sni=1** vào directadmin.conf bằng lệnh:  
# vi /usr/local/directadmin/conf/directadmin.conf

Restart lại dịch vụ DirectAdmin và Apache  
# service directadmin restart  
# service httpd restart  
**Lưu ý: Bước 2 và bước 3 thuộc quyền quản trị hệ thống.**

Đăng nhập trang quản trị DirectAdmin quyền user. Tại mục **Andvanced Features** nhấn chọn **SSL Certificates.  
**

Tích chọn ‘**Paste a pre-generated certificate and key**‘, sau đó copy và dán nội dung file certificate và key vào, chọn ‘**Save**‘  


Trở lại ‘**SSL Certificates**‘ và chọn ‘**Click Here to paste a CA Root Certificate**‘  


Copy và dán nội dung file CA vào và tích chọn ‘**Use a CA Cert**‘, sau đó chọn ‘**Save**‘  


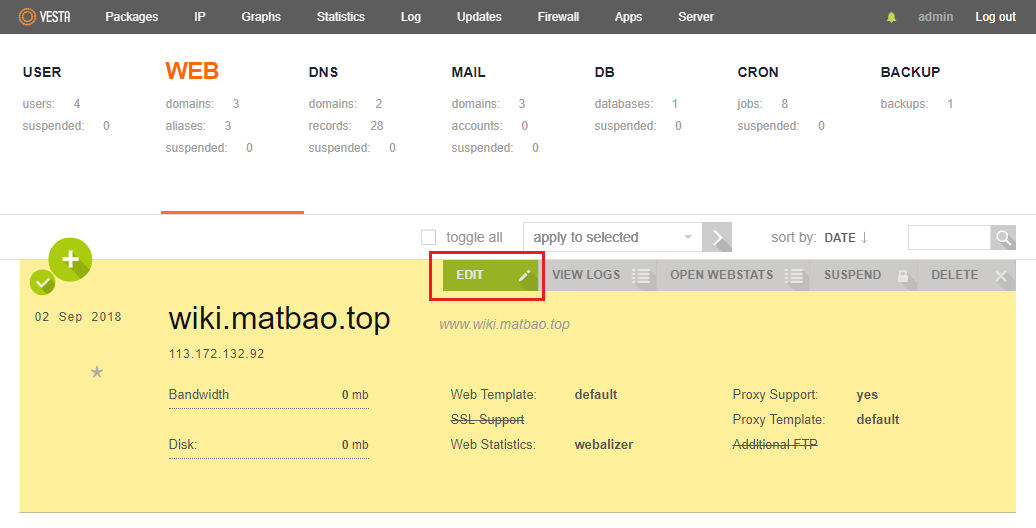
Quá trình cài đặt SSL thành công. Sau ít phút bạn có thể kiểm tra lại việc cài đặt tại trang: <http://managed.matbao.com/tool/ssl/sslchecker/>

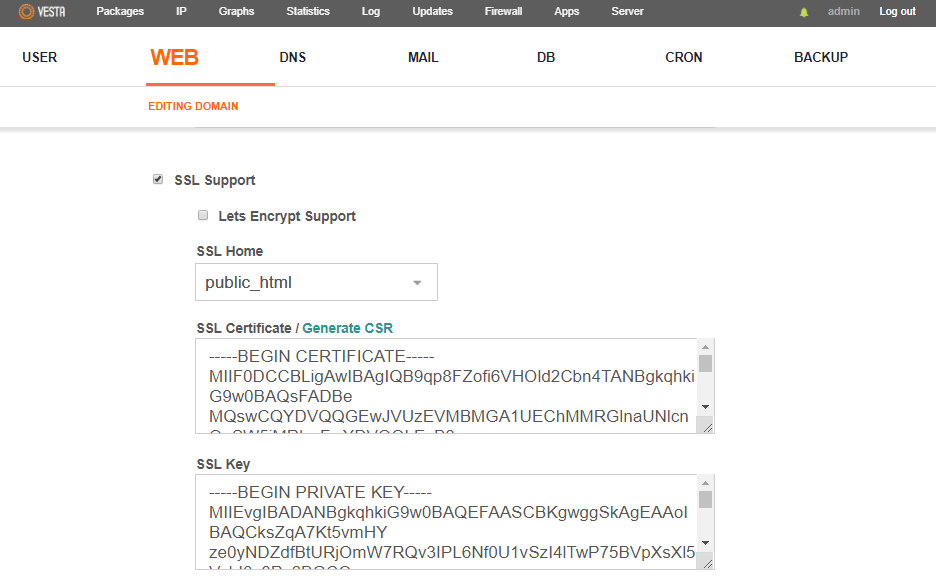
## [Hướng dẫn cài đặt SSL trên VestaCP](https://wiki.matbao.net/kb/huong-dan-cai-dat-ssl-tren-vestacp/):

Để cài đặt chứng chỉ SSL trên VestaCP, bạn thực hiện như sau:

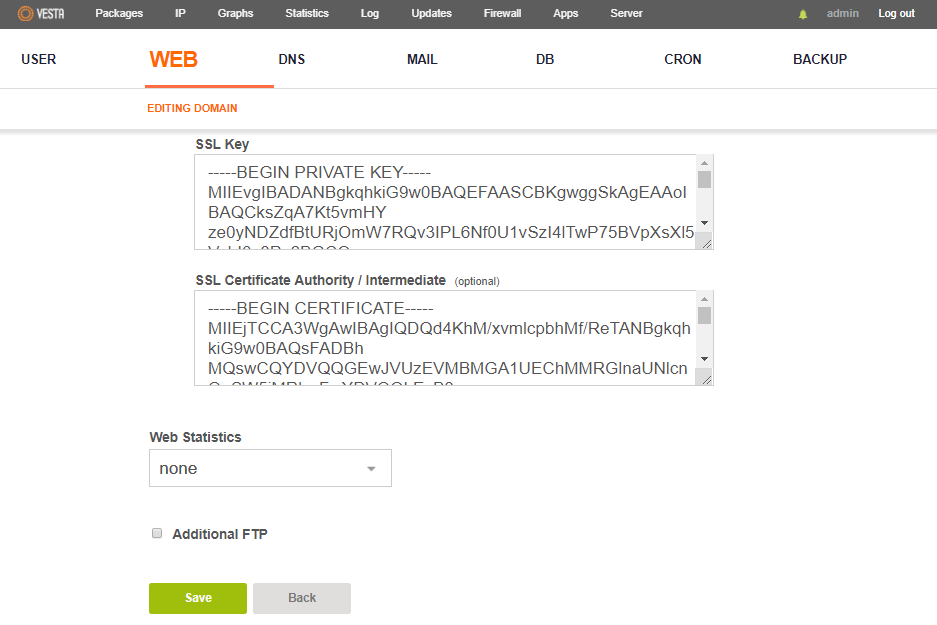
Đầu tiên, bạn đăng nhập vào trang quản trị VestaCP bằng user có website cần cài đặt chứng chỉ SSL bởi đường dẫn: https://IP-của-bạn:8083

Tiếp theo, bạn nhấp chọn vào mục **WEB**, chọn tên miền website cần cài đặt và nhấp chon **Edit**



Trong giao diện thiết lập cấu hình, bạn check vào tùy chọn **SSL Support**, sau đó copy và dán chính xác nội dung file CRT, Private Key và CA lần lượt vào 3 ô trống **SSL Certificate / Generate CSR**, **SSL Key**, **SSL Certificate Authority / Intermedia****te** tương ứng.

Cuối cùng bạn nhấp chọn **Save** để lưu lại các thiết lập.



Quá trình cài đặt SSL thành công. Sau ít phút bạn có thể kiểm tra lại thông tin chứng chỉ SSL tại trang:

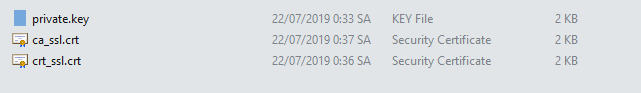
https://managed.matbao.com/tool/ssl/sslchecker/

## [Hướng dẫn cài đặt SSL với Tomcat](https://wiki.matbao.net/kb/huong-dan-cai-dat-ssl-voi-tomcat/):

**Bước 1**: Xác định các file cài đặt SSL.

Để cài đặt SSL, cần phải có các file cài đặt cần thiết như sau:

* Private Key, file này được tạo ra lúc bạn tạo thành công file CSR (Certificate Signing Request).
* File CRT Certificate.
* CA chain file.



**Bước 2**: Xuất các file định PEM thành file Pfx để cài đặt lên server

Để xuất các file cài đặt SSL dạng PEM thành Pfx, bạn có thể sử dụng lệnh sau:

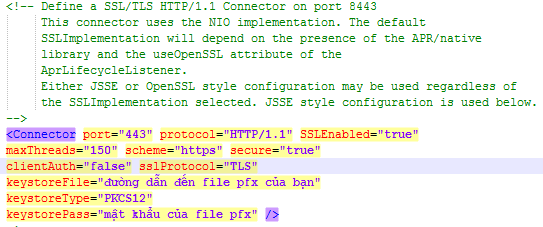
openssl pkcs12 -export -out {tên file pfx}.pfx -inkey privateKey.key -in certificate.crt -certfile CACert.crt

Lưu ý: Trên Linux đã có sẵn OpenSSL chỉ cần thực hiện lệnh là xuất thành công, trên Windows chưa có nên sẽ phải cài đặt.

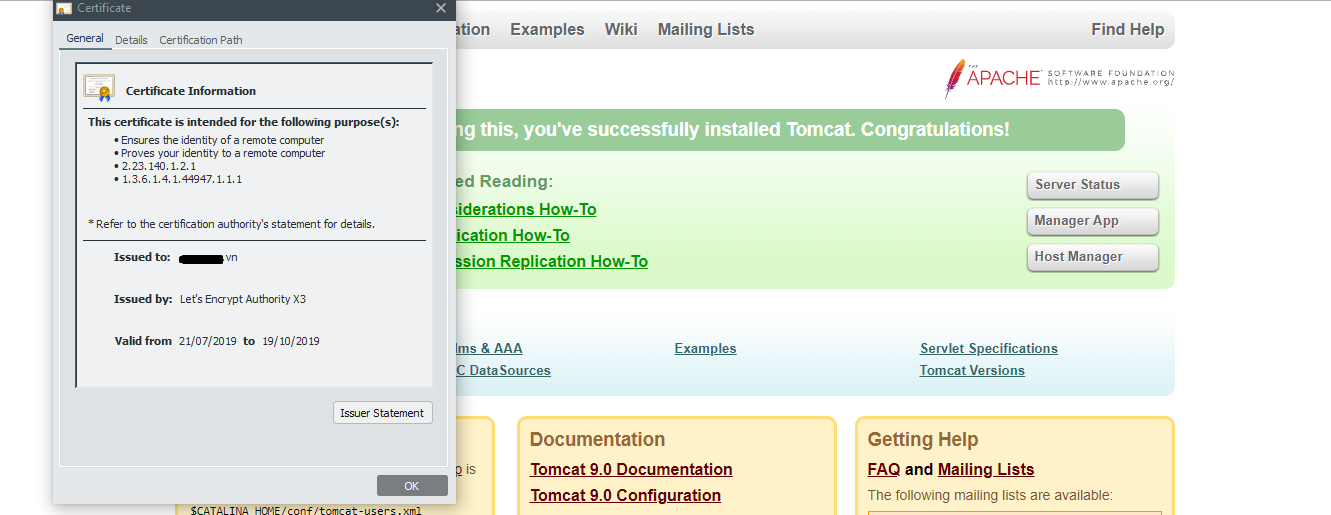
**Bước 3**: Tìm đến file confing của Tomcat để cấu hình SSL cho Webserver.

Bạn tìm đến đường dẫn sau conf/server.xml đây là file cấu hình cho Webserver tomcat. Tìm đến dòng “Define a SSL/TLS HTTP/1.1 Connector on port …” Sau đó thêm đoạn cấu hình bên dưới sau đó lưu lại và restart Tomcat.

<Connector port=”443″ protocol=”HTTP/1.1″ SSLEnabled=”true”  
maxThreads=”150″ scheme=”https” secure=”true”  
clientAuth=”false” sslProtocol=”TLS”  
keystoreFile=”đường dẫn đến file pfx của bạn”  
keystoreType=”PKCS12″  
keystorePass=”mật khẩu của file pfx” />



Sau khi hoàn tất restart Tomcat bạn thử truy cập lại website để kiểm tra. Kết quả như ảnh

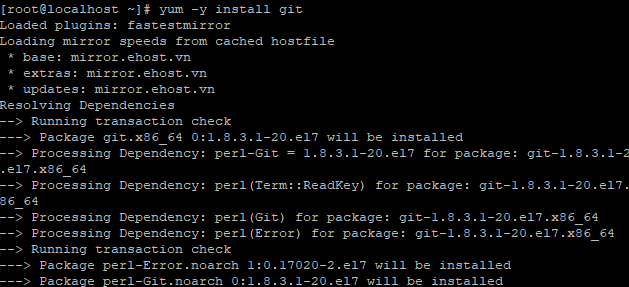


## [Hướng dẫn cài đặt Lest’s Encrypt trên máy chủ CentOS với Apache](https://wiki.matbao.net/kb/huong-dan-cai-dat-ssl-tren-may-chu-centos-voi-apache/):

Hầu hết các trình duyệt phiên bản mới đều đã bắt buộc các website khi truy cập phải có https phía trước do đó nhiều người dùng sẽ gặp rắc rối khi website của họ bị báo lỗi không bảo mật do chưa có SSL. Các dịch vụ SSL tính phí hiện có chi phí khá cao và chưa chắc đem lại hiệu quả cho website do đó một tổ chức đã đứng ra và thiết lập SSL miễn phí để mọi người đều có thể sử dụng. Bài viết này nhằm mục đích hướng dẫn cài đặt SSL miễn phí lên máy chủ linux có cấu hình apache chạy Virtual Host.

Đầu tiên chúng ta phải cài đặt github

**yum -y install git**



Cài github xong chúng ta sẽ clone mã nguồn của Let’s Encrypt về thư mục **/opt/letsencrypt**:

**git clone https://github.com/letsencrypt/letsencrypt /opt/letsencrypt**

https://wiki.matbao.net/wp-content/uploads/2018/12/ssl4-e1545464879995.png

Cập nhật phiên bản mới nhất của Let’s Ecncrypt

**cd /opt/letsencrypt && git pull**

https://wiki.matbao.net/wp-content/uploads/2018/12/ssl5-e1545464953635.png

Tạm thời tắt webservice vì quá trình cài đặt sẽ cần cổng **80** và **443**

**service httpd stop**

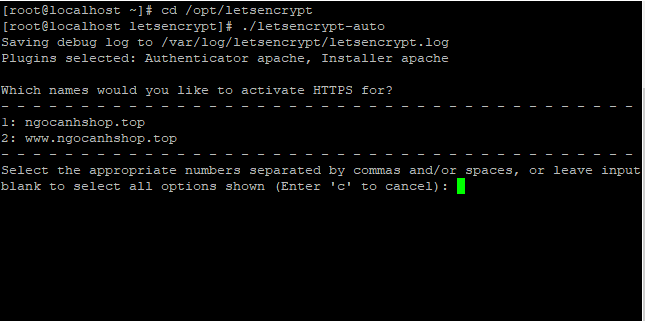
https://wiki.matbao.net/wp-content/uploads/2018/12/ssl6-e1545465044941.png

Bắt đầu cài đặt

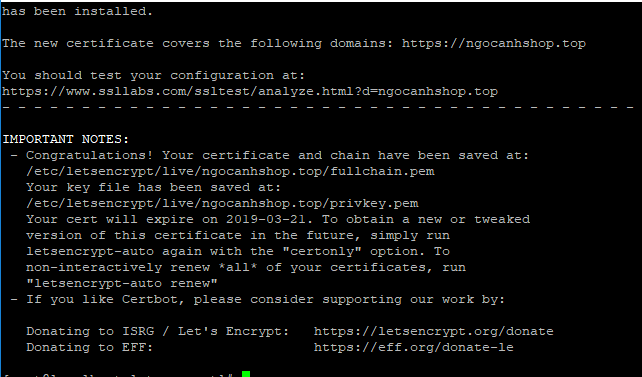
**cd /opt/letsencrypt**  
**./letsencrypt-auto**

Trong quá trình cài đặt, chúng ta sẽ được hỏi email trong trường hợp cần lấy lại SSL và đồng ý một số điều khoản và điều kiện. Về sau để cài đặt SSL cho các tên miền khác, bạn chỉ cần vào thư mục **/opt/letsencrypt** và chạy câu lệnh **./letsencrypt-auto** là các tên miền cần cài đặt sẽ được hiện ra

Khi cài đặt hoàn tất Let’s Encrypt sẽ liệt kê ra các tên miền có sẵn trên máy chủ



Chọn số ứng với tên miền cần cài đặt SSL và hệ thống sẽ tự động sinh ra các tập tin CRT và private key để cài đặt SSL theo đường dẫn cung cấp sẵn



Lưu ý chúng ta phải cài đặt mod SSL cho apache

**yum install mod\_ssl -y**

Tạo một thư mục chứa SSL và sao chép các tập tin CRT và key này vào đường dẫn chứa các chứng thư ví dụ như tạo một thư mục ssl theo đường dẫn**/etc/httpd**

**mkdir /etc/httpd/ssl**

Sau đó sao chép chứng thư được cung cấp

**cp /etc/letencrypt/live/domain/CRT.pem /etc/httpd/ssl/domain.pem**

**cp /etc/letencrypt/live/domain/privatekey.pem /etc/httpd/ssl/domain.key**

Mở tập tin **ssl.conf** theo đường dẫn **/etc/httpd/conf.d/ssl.conf** và thêm khối sau vào cuối tập tin (lưu ý thay đổi các giá trị cho phù hợp với tên miền của bạn)

**<VirtualHost \*:443>**  
**DocumentRoot “/var/www/html/domain.com/”**  
**ServerName domain.com:443**  
**SSLEngine on**  
**SSLCertificateFile /etc/httpd/ssl/domain.pem**  
**SSLCertificateKeyFile /etc/httpd/ssl/domain.key**  
**CustomLog logs/ssl\_request\_log**  
**“%t %h %{SSL\_PROTOCOL}x %{SSL\_CIPHER}x ”%r” %b”**  
**</VirtualHost>**

Đóng và save sau đó restart dịch vụ **httpd** rồi truy cập thử vào website với giao thức https

Để gia hạn dịch vụ SSL các bạn đánh dòng sau:

**/opt/letsencrypt/letsencrypt-auto renew –pre-hook “service httpd stop” –post-hook “service httpd start”**

## [Hướng dẫn cài đặt SSL trên máy chủ Ubuntu với Apache2](https://wiki.matbao.net/kb/huong-dan-cai-dat-ssl-tren-may-chu-ubuntu-voi-apache2/):

**Bước 1: Sao chép tệp Chứng chỉ lên máy chủ của bạn.**

Tải về chứng chỉ Trung Gian [Intermediate (nhacungcap.crt)] và SSL của bạn (ten\_mien\_cua\_ban.crt) từ matbao.net, sau đó tải lên máy chủ của bạn. Phân quyền Chỉ Đọc cho tài khoản ROOT.

**Bước 2: Tìm tệp cấu hình Apache để chỉnh sửa**

Tệp cấu hình Apache cho website của bạn thường được tìm thấy tại địa chỉ **/etc/apache2/sites-enabled/ten\_mien\_cua\_ban**. nếu không thể tìm thấy tại vị trí này, bạn cần chạy lệnh **sudo a2ensite ten\_mien\_cua\_ban**.

Nếu bạn mở tệp bằng trình chỉnh sửa văn bản, bạn sẽ có thể tìm các đoạn chứa cài đặt Apache.

* **Xác định khối SSL để cấu hình**Nếu bạn cần truy cập trang web của mình thông qua cả kết nối an toàn (https) và không an toàn (http), bạn sẽ cần 2 tệp tin tại **/etc/apache2/sites-enabled/**. Một cho cổng 80 và một cho cổng 443. Cấu hình như miêu tả ở bước 2.2. Nếu bạn chỉ cần trang web của bạn được truy cập an toàn, hãy định cấu hình máy chủ ảo hiện tại cho SSL như được mô tả trong bước 2.2.
* **Cấu hình khối .**

<VirtualHost IPServer:443>

DocumentRoot /var/www/

SSLEngine on

SSLCertificateFile /path/to/ten\_mien\_cua\_ban.crt

SSLCertificateKeyFile /path/to/private.key

SSLCertificateChainFile /path/to/chung\_chi\_trung\_gian.crt

</VirtualHost>

*Nếu chỉ thị SSLCertificateChainFile không hoạt động, thay bằng chỉ thị SSLCACertificateFile.*

**Bước 3: Kiểm thử cấu hình Apache trước khi khởi động lại**

Bước quan trọng, vì Apache sẽ không khởi động lại được khi cú pháp trong tệp cấu hình bị sai

apachectl configtest

**Bước 4: Khởi động lại Apache**

apachectl stop

apachectl start

## [Hướng dẫn cài đặt SSL Let’s Encrypt cho trang quản trị VestaCP](https://wiki.matbao.net/kb/huong-dan-cai-dat-ssl-lets-encrypt-cho-trang-quan-tri-vestacp/):

Để cài đặt SSL Let’s Encrypt cho trang quản trị VestaCP, bạn cần login vào server thông qua SSH với quyền root và chạy lệnh

# yum install -y git

# cd /opt/

# git clone https://github.com/letsencrypt/letsencrypt

# cd letsencrypt/

Ở trên mình lưu Let’s Encrypt ở thư mục **/opt/letsencrypt** nên sau này cần chạy lệnh letsencrypt thì nhớ cd vào thư mục này.

Bây giờ chúng ta tạm tắt NGINX và Apache.

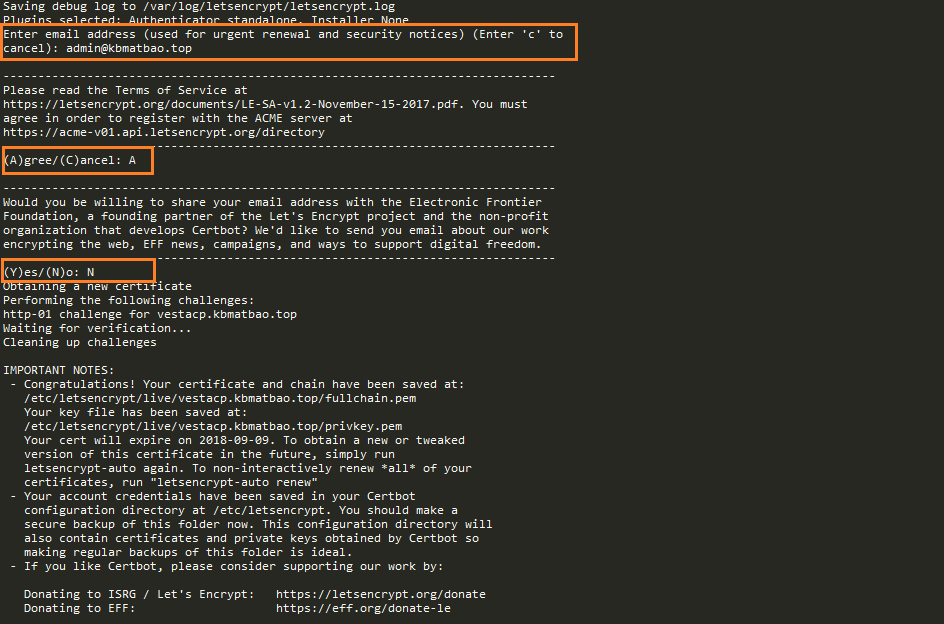
# service nginx stop

# service httpd stop

Và tạo chứng chỉ SSL từ Let’s Encrypt cho hostname của mình, trong bài mình dùng hostname là *vestacp.kbmatbao.top*, nhớ thay lại thành hostname của bạn

# ./letsencrypt-auto certonly --standalone -d vestacp.kbmatbao.top

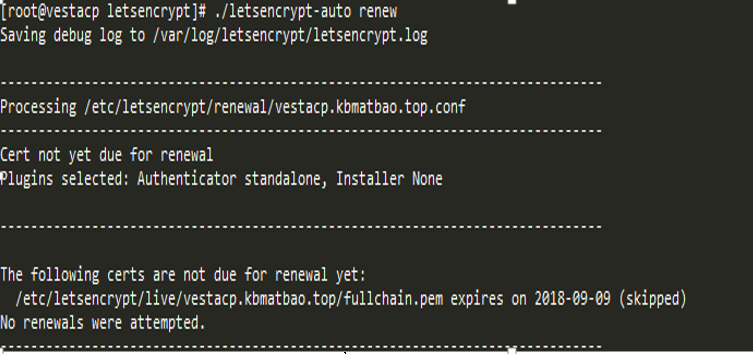
Trong lúc cài, nó sẽ hỏi bạn điền email (email để khôi phục chứng chỉ nếu bị mất) và đồng ý điều khoản sử dụng. Chọn *Angree* và Enter.



Bật tính năng tự động gia hạn chứng chỉ vì mặc định Let’s Encrypt sẽ hết hạn chứng chỉ trong 3 tháng

# cd /opt/letsencrypt

# ./letsencrypt-auto renew



Khi tạo xong chứng chỉ của bạn sẽ nằm ở thư mục ***/etc/letsencrypt/live/vestacp.kbmatbao.top*** bao gồm ***cert.pem****,****privkey.pem***

Bước cuối cùng là tạo một cái symbolic link các tập tin chứng chỉ này thay thế chi 2 tập tin chứng chỉ tự tạo của VestaCP tại thư mục **/usr/local/vesta/ssl**

# rm -rf /usr/local/vesta/ssl/certificate.crt

# ln -s /etc/letsencrypt/live/vestacp.kbmatbao.top/cert.pem /usr/local/vesta/ssl/certificate.crt

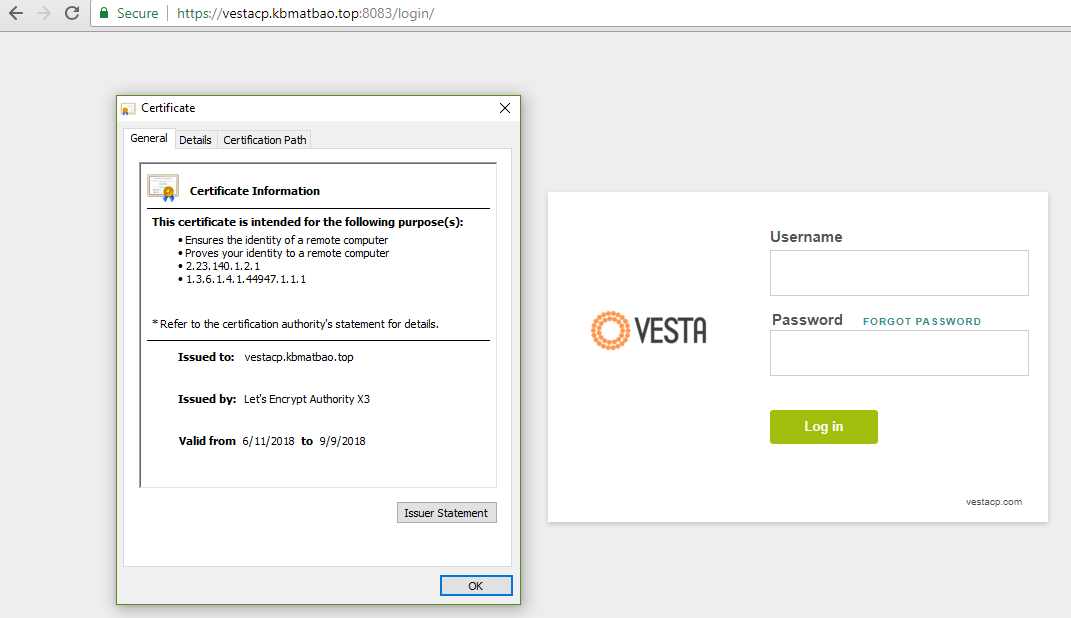
# rm -rf /usr/local/vesta/ssl/certificate.key

# ln -s /etc/letsencrypt/live/vestacp.kbmatbao.top/privkey.pem /usr/local/vesta/ssl/certificate.key

Cuối cùng là khởi động lại VestaCP

# service vesta restart

Bây giờ hãy thử truy cập vào trang quản trị VestaCP bằng hostname nhé. Ví dụ:*vestacp.kbmatbao.top:8083* và bạn đã có chứng chỉ SSL hợp lệ



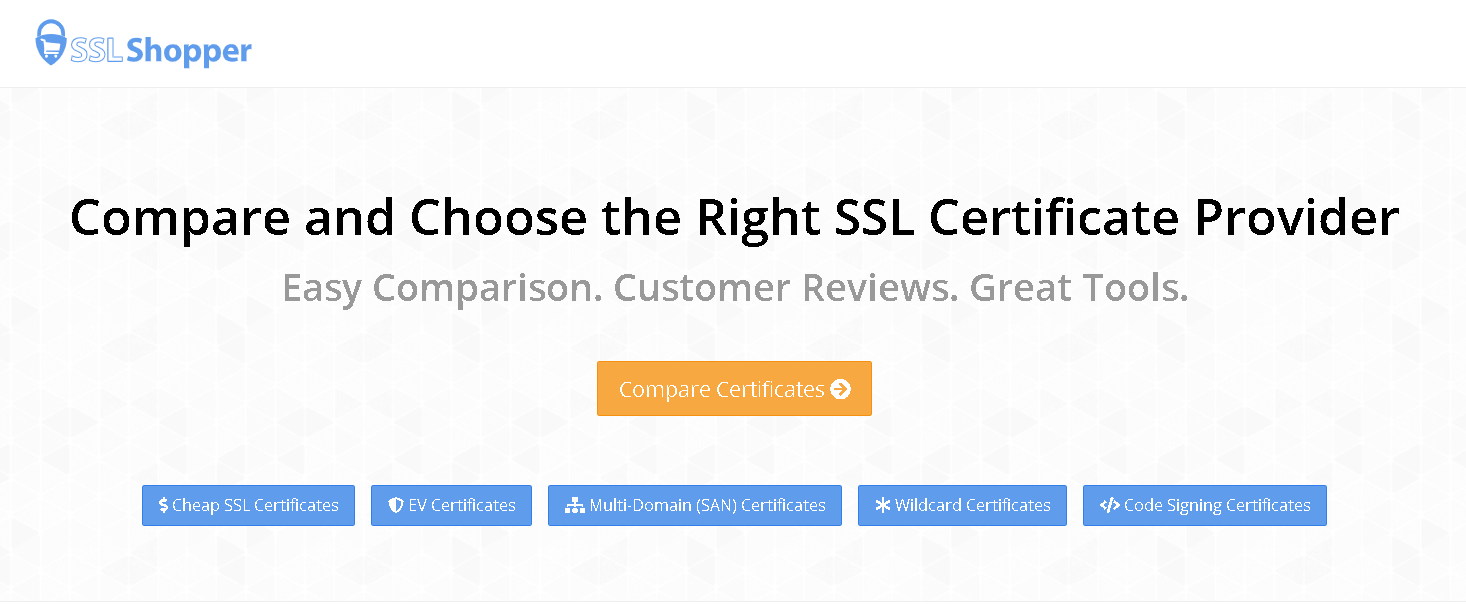
## ****Công cụ kiểm tra SSL đã cài đặt đúng hay chưa:****

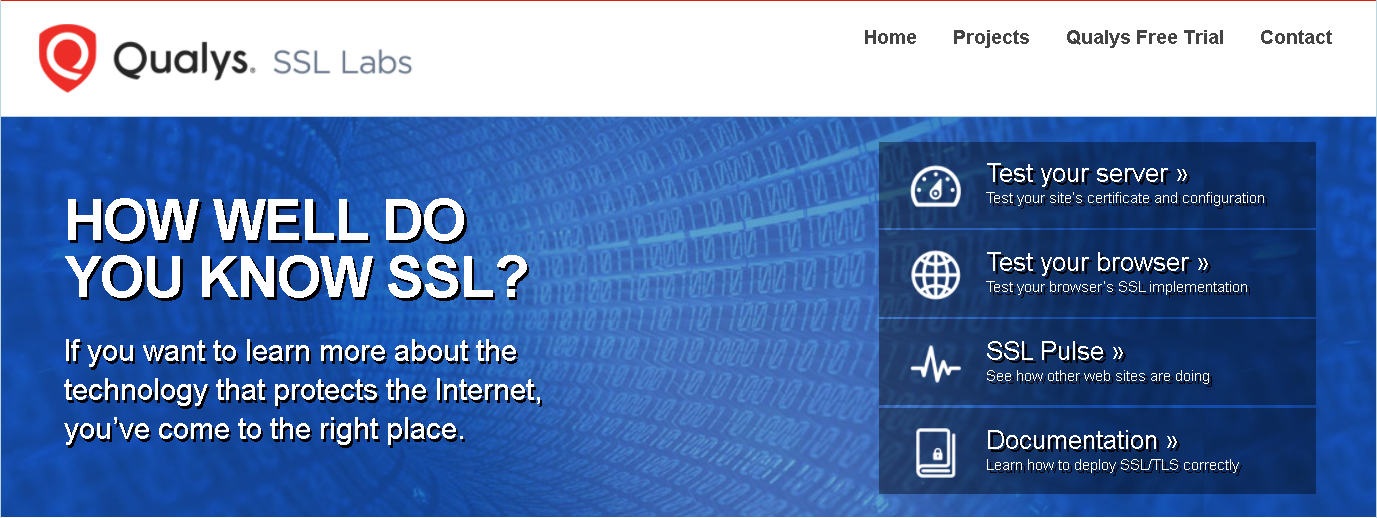
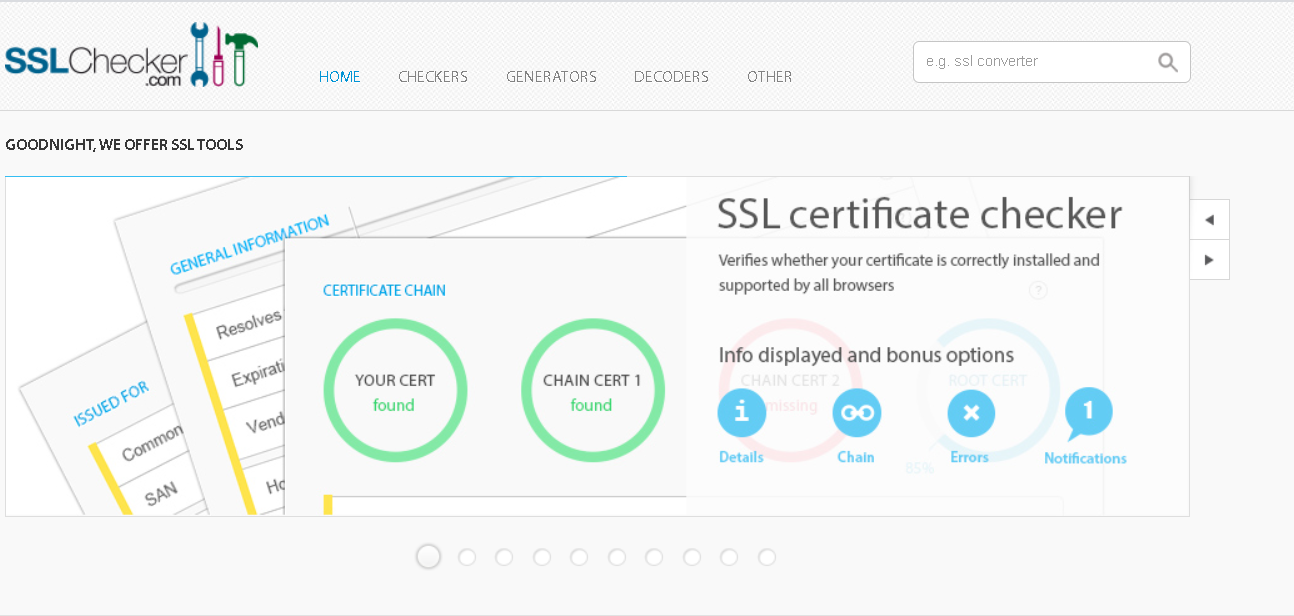
**kiểm tra SSL** đã được cài đặt đúng hay chưa, có tin cậy với các trình duyệt hay không.

Các công cụ này cũng cung cấp các thông tin: Tên miền sử dụng SSL, loại và thời hạn còn lại của SSL, SSL đã được cài đặt đầy đủ và chính xác các mã CA hay không.

Chỉ cần nhập tên miền đang sử dụng SSL vào và nhấn nút kiểm tra.

* [sslshopper.com](https://www.sslshopper.com/ssl-checker.html)



* [ssllabs.com](https://www.ssllabs.com/ssltest/)
* [sslchecker.com](https://www.sslchecker.com/sslchecker)

# **Chương4: Kết luận**

Vào năm 2014 thì google đã chưng thức thay đổi thuật toán và ưu tiên xếp hạng những website sử dụng SSL certificate trước và sao đó thì google thường xuyên nhấn mạnh **tầm quan trọng của SSL trong SEO**.  
  
Hiện nay trong hầu hết các trường hợp thì SSL sẽ tạo ra sự khác biệt nhỏ về các vấn đề tối ưu hóa công cụ tìm kiếm - SEO, và việc cài đặt chứng chỉ SSL vào một website của có chứng chỉ nào thì sẽ có hiệu quả thấp hơn so với việc tạo ra một vài content mạnh cũng như số lượng link chất lượng đổ vè đó. Nhưng bạn cũng không nên xem thường tầm quan trọng của SSL nhé.  
  
Việc cài đặt chứng chỉ SLL là 1 trong những bước tối ưu hóa website trong SEO, ngoài ra công việc này còn giúp khách hàng cảm thấy yên tâm hơn, thời gian onsite cũng lâu hơn bởi tất cả các vấn đề về bảo mật đều được website này cài đặt tốt nhất, cho nên đây chính là lý do khiến google đánh giá cao website đã cài đặt chứng chỉ SSL.

Nếu như bạn đang sử dụng website với source code là wordpress thì việc cài đặt SSL/TLS vô cùng dễ dàng bởi nền tảng này đã cung cấp sẵn các plugin như **Really Simple SSL** hay **SSL Insecure Content Fixer**. Nhưng bạn cũng cần phải mua chứng chỉ SSL từ các nhà cung cấp chứng chỉ SLL. Ngoài ra nếu mới đầu bạn mua domain, hosting thì hầu như các nhà cung cấp đó đều cung cấp sẵn SSL rồi, việc còn lại của bạn là chỉ cần cài vào 2 plugin ở trên mà thôi.  
  
Khi đó bạn chỉ cần **đăng nhập vào wordpress**, sau đó chuyển tới mục **setting**-> **General**, sau đó kéo tới mục**Wordpress Address(URL)**  và **Site Address(URL)**. Khi đó bạn chỉ cần đổi từ **HTTP**thành **HTTPS**, sau đó **Save**lại, và kiểm tra xem website của bạn đã có SSL hay chưa.