**SSL/TLS - Basics**

* SSL viết tắt cho Secure Sockets Layer, được sử dụng để mã hóa các kết nối
* TLS viết tắt cho Transport Layer Security, là phiên bản mới hơn
* Ngày nay, chứng chỉ TLS chủ yếu được sử dụng, nhưng mọi người vẫn gọi là SSL
* Chứng chỉ SSL công khai được cấp bởi Tổ chức phát hành chứng chỉ - Certificate Authorities (CA)
* Comodo, Symantec, GoDaddy, GlobalSign, Digicert, Letsencrypt, etc…
* Chứng chỉ SSL có ngày hết hạn (do bạn thiết lập) và phải được gia hạn

SSL Encryption – How it works

* Bạn có một máy khách và một máy chủ, chúng cần giao tiếp với nhau bằng một kênh an toàn. Chúng cần sử dụng mã hóa SSL.
* Vấn đề là sử dụng mã hóa không đối xứng, là cơ sở của SSL, rất rất đắt (đắt tiền về chu kỳ CPU)
* Mã hóa đối xứng rẻ hơn nhiều, nhưng SSL chỉ dành cho không đối xứng.
* Vì vậy, ý tưởng là “Bắt tay không đối xứng” (asymmetric handshake) được sử dụng để trao đổi một khóa đối xứng ngẫu nhiên cho mỗi khách hàng:  
  **1.Client sends hello, cipher suits & random**: Máy khách nói: Xin chào, đây là bộ quần áo mật mã của tôi và đây là một điều ngẫu nhiên.  
  **2.Server Response with server random & SSL certificate (Public Key)**: Máy chủ phản hồi Được rồi, đây là máy chủ ngẫu nhiên của tôi, và đây là chứng chỉ SSL của tôi.  
  **3.Client verifies SSL certificate**: Máy khách sẽ xác minh tính xác thực của chứng chỉ SSL  
  **4.Master key (symmetric) generated and sent encrypted using the Public Key:** Sau đó nếu nó được tính toán chính xác, máy khách sẽ gửi một khóa đối xứng chính (Master Key) đã được tạo, đồng thời chúng sẽ được mã hóa bằng cách sử dụng Public Key mà nó đã nhận được.  
  **5.Server verifies Client SSL cert (optional)**: Máy chủ xác minh chứng chỉ SSL máy khách. Trong trường hợp máy khách cũng có chứng chỉ SSL, nó sẽ gửi chứng chỉ SSL đó vào lúc này. Vì vậy, có thể có chứng chỉ hai chiều.  
  **6.Master key is decrypted using Private Key**: Master key được giải mã bằng Private Key  
  **7.Secure Symmetric Communication in Place**: Giao tiếp đối xứng an toàn tại chỗ

SSL – Server Name Indication (SNI)

* SNI giải quyết vấn đề tải nhiều chứng chỉ SSL trên một máy chủ web (để server nhiều website)
* Đó là một giao thức mới hơn và yêu cầu máy khách chỉ ra tên máy chủ của máy chủ mục tiêu trong lần bắt tay SSL đầu tiên
* Sau đó, máy chủ sẽ tìm chứng chỉ chính xác hoặc trả về chứng chỉ mặc định
* Lưu ý:  
  \* Chỉ hoạt động với ALB & NLB (newer generation), CloudFront\* Không hoạt động với CLB (older gen)
* Ví dụ, chúng ta có ALB của mình, và nó cần được kết nối với hai target group, được kết nối với các tên máy chủ lưu trữ khác nhau. Cái đầu tiên là [*www.mycorp.com*](http://www.mycorp.com/?fbclid=IwAR3Jjoiuq-bDq8SyWlisXlMHexih7862_v9Bp0Tsd5rMNM7WNMHCQpdW1xA), và cái thứ hai là *Domain1.example.com*
* Chúng ta sẽ tải hai chứng chỉ SSL vào ALB của mình, một chứng chỉ SSL sẽ tương ứng với target group đầu tiên, cái còn lại cho target group thứ hai.
* Một máy khách có khả năng tương thích SNI muốn kết nối với [*www.mycorp.com*](https://l.facebook.com/l.php?u=http%3A%2F%2Fwww.mycorp.com%2F%3Ffbclid%3DIwAR0tXVlW4YLW93-EuZun4pOxzsq0OAeuKC8pc6r5JFvAjTNGdKmuL4wNyIE&h=AT0J_gAp8YXOFVSdpjYAe8Q3pnnx_rndZTN7IYQSzTbLryKLQOJE_wdLL1x3J3SBXGAYAL7oduDkHy2cyxOuoC95FS62HYBoMGPj1QUJYsz5touoZlNxxCweD85oERZCyKTe&__tn__=-UK-R&c%5b0%5d=AT3x73oBx7GkOvcLcneJQ69HOHyjIKsjTrltZ_1oI4Rk5VD81NxiJA1RnNRvhfVOv3uM5YKZFVUG5dJZym459-XqBme1gBdSr1e1DWaPlJFVvPI332aWdO3D7GSvTFVVobLS1qUdKFNr6VXFycKr1uW98qNk). Và ALB, vì nó đã bật SNI, nên sẽ sử dụng đúng SSL, sau đó nó sẽ chuyển hướng đến đúng target group.

SSL – Man in the Middle Attacks

Tấn công man-in-the-middle xảy ra khi ai đó ở giữa hai máy tính (máy khách và máy chủ từ xa) và có khả năng nghe trộm hoặc thậm chí chặn liên lạc giữa hai máy và đánh cắp thông tin nhạy cảm. Các cuộc tấn công man-in-the-middle là một vấn đề bảo mật nghiêm trọng.

SSL – Man in the Middle Attack: Cách để phòng tránh?

* Không sử dụng HTTP, thay vào đó sử dụng HTTPS (đồng nghĩa với việc sử dụng SSL/TLS certificates)
* Sử dụng DNS có DNSSEC

\* Khi máy chủ DNS bị tấn công, hoặc máy chủ vi phạm bản quyền có thể giả mạo phản hồi DNS, nó có thể gửi request của bạn đến máy chủ mục tiêu sai.\* Có thể bảo vệ domain của bạn bằng cách định cấu hình DNSSEC\* Amazon Route 53 hỗ trợ DNSSEC để đăng ký domain.\* Route 53 hỗ trợ DNSSEC cho dịch vụ DNS kể từ tháng 12 năm 2020 (sử dụng KMS)\* Bạn cũng có thể chạy một máy chủ DNS tùy chỉnh trên Amazon EC2 chẳng hạn (Bind là phổ biến nhất, ngoài ra còn có dnsmasq, KnotDNS, PowerDNS).

AWS Certificate Manager - ACM

* ACM có thể hoạt động như một tổ chức phát hành chứng chỉ công cộng hoặc tổ chức phát hành chứng chỉ tư nhân (Certificate Authority - CA)
* Private CA: Các ứng dụng cần tin tưởng CA riêng của bạn
* Public CA: Trình duyệt tin cậy một danh sách các nhà cung cấp, có thể tin tưởng các nhà cung cấp khác
* Với ACM, chúng ta có thể tạo hoặc nhập (import) các chứng chỉ
* Nếu ACM tạo chứng chỉ, chứng chỉ có thể tự động gia hạn. Nếu chứng chỉ được nhập, người dùng có trách nhiệm gia hạn.
* ACM chỉ có thể triển khai chứng chỉ cho các dịch vụ được hỗ trợ (các dịch vụ trong AWS được tích hợp với ACM)
* Không phải tất cả các dịch vụ đều được hỗ trợ, về cơ bản chỉ CloudFront và ALB được hỗ trợ. Ví dụ: EC2 không được hỗ trợ
* ACM là một dịch vụ khu vực (regional). Để sử dụng chứng chỉ cho ALB ở ap-northeast-1, chứng chỉ phải nằm ở ACM trên ap-northeast-1
* Chứng chỉ không được rời khỏi khu vực chúng được tạo hoặc nhập vào
* Đối với các dịch vụ toàn cầu (Global Services), vd như CloudFront, chứng chỉ bắt buộc phải được lưu ở **us-east-1**