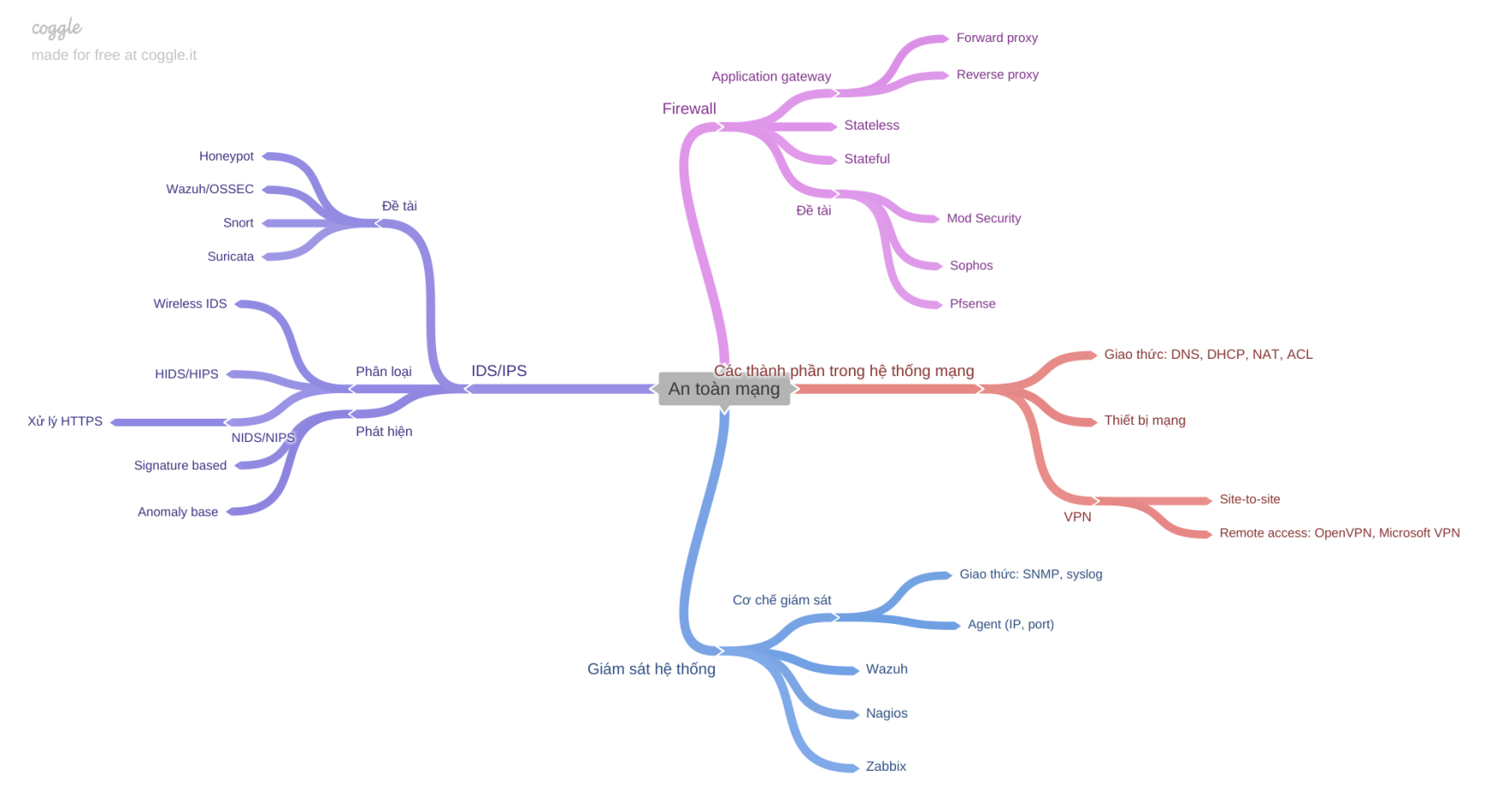
**TỔNG HỢP CHỦ ĐỀ ATM**

Nội dung vấn đáp:  
- Nội dung đề tài của nhóm.  
- Tổng quan, ý nghĩa các đề tài khác.  
- Kiến thức tổng quát từ bài thực hành và các bài tập đã nộp

# Pfsence – firewall tích hợp

* PfSense là một ứng dụng có chức năng định tuyến vào tường lửa mạnh và miễn phí, ứng dụng này sẽ cho phép bạn mở rộng mạng của mình mà không bị thỏa hiệp về sự bảo mật. Lọc bởi địa chỉ nguồn và địa chỉ đích, cổng nguồn hoặc cổng đích hay địa chỉ IP. Nó cũng hỗ trợ chính sách định tuyến và có thể hoạt động trong các chế độ bridge hoặc transparent, cho phép bạn chỉ cần đặt pfSense ở giữa các thiết bị mạng mà không cần đòi hỏi việc cấu hình bổ sung. pfSense cung cấp network address translation (NAT) và tính năng chuyển tiếp cổng, tuy nhiên ứng dụng này vẫn còn một số hạn chế với Point-to-Point Tunneling Protocol (PPTP), Generic Routing Encapsulation (GRE) và Session Initiation Protocol (SIP) khi sử dụng NAT.
* Cung cấp các tính năng:
  + Aliases : gom nhóm port, host hoặc netword khác nhau thành 1 để áp dụng chung 1 bộ quy tắc(rules)
  + Firewall rules: Nơi lưu trữ các bộ luật.( có khả năng giới hạn truy cập)
  + NAT: cung cấp tính năng NAT và chuyển tiếp port( hạn chế với PPTP, GRE và SIP).
  + Traffic Shaper: Theo giõi và quản lý traffic( bang thông, hiệu suất, độ trễ)
  + Virtual IPs : Proxy ARP, CARP, và 1 loại khác để thực hiện( chuyển tiếp cổng – NAT, NAT Outbound, NAT 1:1, failover, dịch vụ kết hợp trên router để gắn với IP khác).
  + Filewall Schedules: Cấu hình firewall chạy trong 1 khoảng thời gian nhất định -> lịch làm việc cụ thể hơn

# Captive portal( pfsense) - firewall

**Là 1 dịch vụ của firewall pfsense.**

**Captive portal** là 1 tính năng thuộc dạng flexible, chỉ có trên các thiết bị firewall thương mại lớn, tuy nhiên trên Pfsense tính năng này được cung cấp miễn phí. Tính năng này giúp chuyển hướng trình duyệt của người dùng vào 1 trang web định sẵn, từ đó giúp chúng ta có thể quản lý được người dùng. Tính năng này tiên tiến hơn các kiểu đăng nhập như WPA, WPA2 ở chỗ người dùng sẽ thao tác trực tiếp với 1 trang web (http, https) chứ không phải là bảng đăng nhập khô khan như kiểu authentication WPA, WPA2.

**Dịch vụ Captive Portal của Pfsense có các chức năng sau:**

* **Pass-though MAC:** Các MAC address được cấu hình trong mục này sẽ được bỏ qua, không authentication.
* **Allowed IP address**: Các IP address được cấu hình sẽ không authentication.
* **Users**: Tạo local user để dùng kiểu authentication: local user.
* **File Manager**: Upload trang quản lý của Captive portal lên pfsense.
* **Enable captive portal**: Đánh dấu chọn nếu muốn sử dụng captive portal.
* **Maximum concurrent connections**: Giới hạn các connection trên mối

ip/user/mac.

* **Idle timeout**:Nêu mối ip không còn truy cập mạng trong 1 thời gian xác định thì sẽ ngắt kết nối của ip/user/mac.
* **Hard timeout**: Giới hạn thời gian kết nối của mối ip/users/mac.
* **Logout popup windows**: Xuất hiện 1 popup thông báo cho ip/users/mac.
* **Redirect URL**: Địa chỉ URL mà người dùng sẽ được direct tới sau khi đăng nhập.
* **MAC filtering**: Đánh dấu vào nếu pfsense năm trước router. Bởi vì pfsense quản lý kết nối theo MAC (mặc định). Mà chi dữ liệu qua Router sẽ bị thay đổi mac address nên nếu timeout thì toàn bộ người dùng sẽ mất kết nối
* **Authentication : Có 3 kiểu chứng thực client:**
* **No authentication:** pfSense sẽ điều hướng người dùng tới 1 trang nhất định mà không chứng thực.
* **Local user manager:** pfSense hỗ trợ tạo user để chứng thực.
* **Radius authentication:** Chứng thực bằng radius server (Cần chỉ ra địa chỉ IP của radius, port, …)

# Zabbix – giám sát

**Zabbix** là công cụ giám sát hệ thống. Zabbix giúp các doanh nghiệp quản lí hệ thống mạng cũng như thông tin trong các hệ thống mạng một cách toàn diện. Đặc biệt, công cụ này còn giúp ích không chỉ giúp ích đối với các doanh nghiệp trong quản lí mạng nội bộ mà nó còn góp phần to  
lớn trong việc ***quản lí hệ thống mạng*** của các công ty làm về lĩnh vực truyền thông, các dịch vụ công nghệ thông tin.  
Đây là một hệ thống giám sát được phát triển nhiều tính năng vượt trội trong việc giám sát thông tin kể cả thông tin khách hàng cung cấp. Bằng các giải quyết thông minh và linh hoạt Zabbix sẽ báo cáo các sự cố và ***gửi về cho máy chủ hoặc quản trị viên bằng email, sms, OTT app***. Không chỉ vậy, công cụ hỗ trợ giám sát nào còn ***cung cấp và báo cáo một cách  
chính xác những thông tin đã thu thập được***.

Zabbix giám sát các thiết bị **qua Zabbix agent hoặc qua các giao**

**thức SNMP**… Các Agent (thiết bị mạng hay server được cài đặt snmp hay

zabbix agent) **sẽ gửi các event liên quan đến thiết bị mạng, máy chủ tới**

**Zabbix server**, Zabbix server làm n**hiệm vụ phân tích số liệu thu thập**

**được và dựa vào các trigger do người quản trị hệ thống thiết lập mà quyết định đưa ra các cảnh báo theo mức độ khác nhau (Critical, warning, hoặc infomation…)** Hình thức cảnh báo là gửi SMS, email….

**Các chức năng của Zabbix** rất linh hoạt, nó có thể được cấu hình để  
**theo dõi, giám sát thiết bị mạng, máy chủ** theo cách ta muốn. Nó cũng có  
một cơ chế để **tự động phản ứng với các vấn đề, và một hệ thống cảnh báo mạnh**. Tất cả điều này được dựa trên một hệ thống định nghĩa các đối tượng rõ ràng.  
***− Khả năng giám sá***t: Zabbix có cấu hình tập trung, các thông tin giám  
sát được tập trung vào một cơ sở dữ liệu. Zabbix có khả năng sử dụng các proxy với số lượng không giới hạn, số nút đó có thể lên tới hàng ngàn.  
***− Khả năng mở rộng***: Các thí nghiệm cho thấy nó có khả năng xử lý quản trị tới 100.000 thiết bị và máy chủ. Số lượng thông tin, dịch vụ giám sát có thể lên tới 1.000.000  
***− Hỗ trợ giám sát thời gian thực***: Zabbix có thể cảnh báo ngay tới  
người quản trị viên khi hệ thống được giám sát có sự cố gì thông qua  
mail, SMS… Hơn nữa Zabbix còn có hồ sơ về các thông tin giám sát  
***− Khả năng hiển thị kết quả*** bằng đồ thị, biểu đồ giúp người dùng có  
thể dễ dàng giám sát.  
− Khả năng ***nhập và xuất*** cơ sở dữ liệu thông qua XML.  
− ***Khả năng tự động phát hiện***: Người dùng có thể tạo ra các luật dựa  
trên nó Zabbix có thể tự động phát hiện ra các địa chỉ IP, các dịch vụ  
hoặc các thiết bị SNMP để thực hiện việc giám sát.  
− ***Tính linh*** ***hoạt:*** Zabbix hỗ trợ cả IPv4 và IPv6, các Zabbix agent có  
khả năng cài đặt trên nhiều nền tảng khác nhau.  
− Khả năng giám sát các thiết bị không hỗ trợ cài đặt Zabbix agent:  
Zabbix có khảnăng giám sát các thiết bị hỗ trợ IPMI, SNMP v1,2,3,4.  
− ***Khả năng bảo mật***: Zabbix hỗ trợ người dùng một các linh hoạt, nó  
cung cấp khảnăng chứng thực của địa chỉ IP.  
***− Quản trị các chức năng***: Ta có thể chạy lệnh ping, traceroute trên  
một chuỗi các máy chủ, các thiết bị được quản trị.

# Suricata – ids/ips

Suricata là một hệ thống **phát hiện xâm nhập** dựa trên **mã nguồn mở**.

Suricata là công cụ IDS/**IPS dựa trên luật để theo dõi lưu lượng mạng và  
cung cấp cảnh báo** đến người quản trị hệ thống khi có sự kiện đáng ngờ xảy  
ra. Nó được thiết kế để tương thích với các thành phần an ninh mạng hiện  
có. Bản phát hành đầu tiên chạy trên nền tảng linux 2.6 có hỗ trợ nội tuyến  
(inline) và cấu hình giám sát lưu lượng thụ động có khả năng xử lý lưu  
lượng lên đến gigabit. Suricata là công cụ IDS/IPS miễn phí trong khi nó  
vẫn cung cấp những lựa chọn khả năng mở rộng cho các kiến trúc an ninh  
mạng phức tạp nhất.

Suricata là phần mềm mã nguồn mở: Suricata được phát hành dưới giấy  
phép GNU/GPL điều này có nghĩa là **bất cứ ai cũng có thể sử dụng** Suricata một cách miễn phí dù đó là doanh nghiệp hay người dùng cá nhân. Ngoài ra vì là phần mềm mã nguồn mở nên Suricata có một cộng đồng người sử dụng lớn, sẵn sàng hỗ trợ nếu có bất cứ thắc mắc gì.

Là một công cụ đa luồng, suricata **cung cấp tăng tốc độ và hiệu quả trong  
việc phân tích lưu lượng mạng.** Ngoài việc **tăng hiệu quả phần cứng** (với  
phần cứng và card mạng giới hạn), công cụ này được xây dựng để **tận dụng  
khả năng xử lý cao được cung cấp bởi chip CPU đa lõ**i mới nhất.  
Suricata làm việc như thế nào, tập tin cấu hình ở đâu, các luật như thế nào  
người quản trị đều có thể biết và cấu hình theo ý mình được. Kể cả việc tạo  
ra các luật mới.  
Luật của Suricata thường xuyên được cập nhật: Các luật của Suricata  
thường xuyên được bổ sung và cập nhật các hình thức xâm nhập mới

# Mod security - firewall

Mod security là **một tường lửa open-source được tích hợp vào các web server** như apache, IIS, Nginx ...nhằm bảo vệ các ứng dụng web khỏi các cuộc tấn công web phổ biến. Nó đóng vai trò như một tường lửa để ngăn chặn các dữ liệu độc hại đi vào web server.

Mod Security có các chức năng  
• Request filtering: sang lọc và ktra các request tới webserver trc khi chuyển chúng tới các module khác

• Anti-evasion techniques: chuẩn hóa

• Understanding of the HTTP protocol: hiểu http

• POST payload analysis: sang lọc dưa trên post request

• Audit logging: ghi lại log request

• HTTPS filtering: phân tích https

• Compressed content filtering: phân tích hậu xử lý request data.

# Open vpn:

OpenVPN là một phần mềm **mạng riêng ảo** mã nguồn mở dành cho việc tạo các đường ống (**tunnel**) **điểm-tới-điểm** được mã hóa giữa các máy chủ..  
OpenVPN cho phép các máy đồng đẳng **xác thực lẫn nhau** bằng một **khóa bí mật** được chia sẻ từ trước, chứng chỉ mã công khai (**public key certificate**), hoặc tên người dùng/mật khẩu. Nó có nhiều tính năng bảo mật và kiểm soát. Nó không phải một mạng riêng ảo web, và không tương thích với IPsec hay các gói VPN khác. Toàn bộ phần mềm gồm **có một file nhị phân cho cả các kết nối client và server, một file cấu hình không bắt buộc, và một hoặc nhiều file khóa** tùy theo phương thức xác thực được sử dụng.

# Wazuh – giám sát – ids/isp(wazuh/ossec)

Wazuh là 1 project mã nguồn mở dùng cho việc bảo vệ an ninh. Được xây dựng từ các thành phần: OSSEC HIDS, OpenSCAP và Elastic Stack.

**OSSEC HIDS**: host-based Intrusion Detection System (HIDS) được dùng cho việc **phát hiện xâm nhập, hiển thị và giám sát**. Nó dựa vào 1 multi-platform agent cho việc đẩy dữ liệu hệ thống (log message, file hash và phát hiện bất thường) tới 1 máy quản lý trung tâm, nơi sẽ phân tích và xử lý, dựa trên các cảnh báo an ninh. Các agent truyền event data event data tới máy quản lý trung tâm thông qua kênh được bảo mật và xác thực. OSSEC HIDS cung cấp syslog server trung tâm và hệ thống giám sát không cần agent, cung cấp việc giám sát tới các event và thay đổi trên các thiết bị không cài được agent như firewall, switch, router, access point, thiết bị mạng....

**OpenSCAP** là 1 OVAL (Open Vulnerability Assesment Language) và XCCDF (Extensible Configuration Checklist Description Format) được dùng để **kiểm tra cấu hình hệ thống và phát hiện các ứng dụng dễ bị tấn công**. Nó được biết đến như là một công cụ được thiết kế để kiểm tra việc tuân thủ an ninh của hệ thống sử dụng các tiêu chuẩn an ninh dùng cho môi trường doanh nghiệp

**ELK Stack** Sử dụng cho việc **thu thập, phân tihcs, index, store, search và hiển thị dữ liệu log.**

# Wireless ids

# NagiOS – giám sát

Nagios là một phần mềm mã nguồn mở hỗ trợ giám sát hoạt động của các thiết bị và các dịch vụ trong mạng. Nagios giúp giám sát hoạt động một số thiết bị trung tâm trong mạng như Server, Switch, Router,... Đồng thời kết hợp với bộ phận phát  
cảnh báo qua giao diện Web và âm thanh (Audio) phát cảnh báo trong trường hợp một thiết bị n gưng hoạt động hoặc một dịch vụ mạng ngưng hoạt động.

Nagios giám sát các thiết bị mạng thông qua các giao thức  
SNMP, … để theo dõi trạng thái hoạt động của các thiết bị.  
Đồng thời, Nagios còn cho phép thiết lập cơ chế giám sát hoạt  
động của các dịch vụ mạng. Các dịch vụ phổ biến được giám  
sát như: HTTP, FTP, SMTP, POP3,

Nagios gồm 5 chức năng:  
•Cảnh báo: Nagios gửi cảnh báo khi có thành phần cơ sở hạ tầng  
bất ổn định và phục hồi, cung cấp cho các quản trị viên thông  
báo của các sự kiện quan trọng. Cảnh báo có thể được gửi qua  
email, SMS, hay tùy chỉnh.

•Ứng phó: Nhân viên CNTT có thể xác nhận cảnh báo và bắt  
đầu giải quyết sự cố ngưng hoạt động và kiểm tra hệ thống cảnh  
báo ngay lập tức. Cảnh báo có thể được gia tăng cho các nhóm  
khác nhau nếu thông báo không xác nhận một cách kịp thời.  
•Báo cáo: Báo cáo cung cấp một hồ sơ lịch sử của sự cố ngưng  
hoạt động, sự kiện, thông báo, và phản ứng cảnh báo để xem  
xét. Sẵn có các báo cáo giúp đảm bảo SLAs của người dùng  
đang được đáp ứng.  
•Bảo trì: Dự kiến thời gian ngừng làm việc ngăn cản các cảnh  
báo tỏng quá trình bảo trì theo lịch trình và nâng cấp.

•Kế hoạch: Lập lịch đồ thị và báo cáo xu hướng và công suất  
cho phép người dùng cách định sự cần thiết nâng cấp cơ sở hạ  
tầng trước khi xảy ra sự cố

# Owasp honeypot –

OWASP Honeypot là một phần mềm mã nguồn mở viết bằng ngôn ngữ Python,  
được thiết kế để tạo honeypot bằng cách sử dụng docker container.  
•Honeypot là một hệ thống gắn liền với mạng được thiết kế giả dạng các tài sản có  
giá trị cao như servers hoặc một lỗ hổng mạng.  
•Docker Container là một gói phần mềm độc lập, có thể thực thi, bao gồm các ứng  
dụng và phần phụ thuộc của chúng

OWASP Honeypot thu hút, đánh lạc hướng tấn công của tin tặc, ngăn không cho  
chúng tấn công hệ thống thật.

Nó phát hiện, giám sát, thu thập dữ liệu hoạt động của tin tặc để người quản trị  
phân tích những mối đe dọa và giải quyết mọi điểm yếu của hệ thống

# HTTPS :

HTTPS (viết tắt của Hypertext Transfer Protocol Secure) là sự kết hợp giữa HTTP và giao thức bảo mật SSL (Secure Socket Layer ) hay TLS (Transport Layer Security ) cho phép trao đổi thông tin một cách bảo mật trên Internet bằng cách mã hóa chúng với các biểu hiện sau:

Confidentiality: sử dụng phương thức encryption để đảm bảo rằng các thông điệp được trao đổi giữa client và server không bị kẻ thứ ba đọc được.

Integrity: sử dụng phương thức hashing để cả client và server đều có thể tin tưởng rằng thông điệp mà chúng nhận được có không bị mất mát hay chỉnh sửa.

Authenticity: sử dụng digital certificate để giúp client có thể tin tưởng rằng server/website mà họ đang truy cập thực sự là server/website mà họ mong muốn vào, chứ không phải bị giả mạo.

muốn áp dụng HTTPS thì trong quá trình cấu hình Webserver, bạn phải có một SSL certificate( có thể tự tạo(không có tín authenticity) hoặc mua từ một Trusted Root CA). Một số thông tin quan trọng được chứa trong SSL certificate:

- Thông tin về chủ sở hữu của certificate (có thể là tổ chức, tên cá nhân hoặc tên miền của website).  
- Thông tin và digital signature của CA mà cấp certificate này.  
- Khoảng thời gian mà certificate còn hiệu lực.  
- Public key của website. Còn private key không có trong certificate mà được lưu trữ trên chính server và - tuyệt đối không được để lộ cho bất cứ client nào.  
- Một số thông tin phụ khác như: loại SSL certificate, các thuật toán dùng để encryption và hashing, chiều dài (tính bằng bit) của key, cơ chế trao đổi key (như RSA, DSA). v.v…

Quá trình giao tiếp:

1. Client gửi request cho một secure page (có URL bắt đầu với https://)

2. Server gửi lại cho client certificate của nó.

3. Client (web browser) tiến hành xác thực certificate này bằng cách kiểm tra (verify) tính hợp lệ của chữ ký số của CA được kèm theo certificate.

Giả sử certificate đã được xác thực và còn hạn sử dụng hoặc client vẫn cố tình truy cập mặc dù Web browser đã cảnh báo rằng không thể tin cậy được certificate này (do là dạng self-signed SSL certificate hoặc certificate hết hiệu lực, thông tin trong certificate không đúng) thì mới xảy ra bước 4 sau.

4. Client tự tạo ra ngẫu nhiên một symmetric encryption key (hay session key), rồi sử dụng public key (lấy trong certificate) để mã hóa session key này và gửi về cho server.

5. Server sử dụng private key (tương ứng với public key trong certificate ở trên) để giải mã ra session key ở trên.

6. Sau đó, cả server và client đều sử dụng session key đó để mã hóa/giải mã các thông điệp trong suốt phiên truyền thông.

Và tất nhiên, các session key sẽ được tạo ra ngẫu nhiên và khác nhau trong mỗi phiên làm việc với server. Ngoài encryption thì cơ chế hashing sẽ được sử dụng để đảm bảo tính Integrity cho các thông điệp được trao đổi.

**HTTPS proxy:**

Các proxy HTTPS đảm bảo giao tiếp với bảo mật end-to-end sử dụng đường hầm(tunnel).

* Trong luồng này, máy khách gửi một yêu cầu đặc biệt tới proxy bằng động từ CONNECT.
* Proxy xây dựng một tunnel (đường hầm ) kết nối với máy chủ được yêu cầu bằng TCP .
* Kết nối được thiết lập, Server gửi về một reponse đến máy khách thông báo kết nối thành công. Bắt đầu quá trình trao đổi dữ liệu.

# DoS/DDoS:

**Dos**

Denial-of-Service (DoS) là một cuộc tấn công nhằm tắt máy hoặc ngắt kết nối, khiến người dùng ngừng truy cập. Các cuộc tấn công DoS thường hoạt động bằng cách áp đảo hoặc làm quá tải mục tiêu với các request cho đến khi không thể xử lý, dẫn đến từ chối dịch vụ cho người dùng. Trong cả hai trường hợp, DoS đều tước quyền sử dụng dịch vụ hoặc tài nguyên hợp pháp của người dùng. Một cuộc tấn công DoS được đặc trưng bằng cách sử dụng một máy tính duy nhất để khởi động cuộc tấn công.

Có hai phương pháp tấn công DoS: Flooding attack hoặc crashing attack.

**DDOS**

Một cuộc tấn côn DDoS xảy ra khi nhiều máy đang hoạt động cùng nhau để tấn công một mục tiêu. Những kẻ tấn công DDoS thường tận dụng việc sử dụng botnet. Một nhóm các thiết bị kết nối internet bị tấn công để thực hiện các cuộc tấn công quy mô lớn. Kẻ tấn công lợi dụng các lỗ hổng bảo mật hoặc điểm yếu của thiết bị để kiểm soát nhiều thiết bị sử dụng phần mềm. Khi đã kiểm soát, kẻ tấn công có thể ra lệnh cho botnet của họ tiến hành DDoS trên mục tiêu. Trong trường hợp này, các thiết bị bị nhiễm cũng là nạn nhân của vụ tấn công.