Câu 1: Đâu **KHÔNG** phải khả năng của giao thức SSH đem lại

A Xác thực dữ liệu

B Mã hóa tầng ứng dụng

C. Mã hóa dữ liệu tầng Network

D. Nén dữ liệu

Câu 2: Chế độ Transport của IPSec hoạt động ở tầng nào dưới đây
A. Gateway to gateway

B. Host to gateway

C. Router to router

D. Host to host

Câu 3: Phát biểu **ĐÚNG** về giao thức SSL/TLS

A. CipherSuite do Client quyết định

B. CipherSuite được Client và Server thương lượng trong quá trình bắt tay

C. CipherSuit do Server quyết định

D. Bên nào gửi thông điệp HELLO trước trong quá trình bắt tay thì bên đó quyết định CipherSuite

Câu 4: Bạn được yêu cầu chọn một thuật toán băm để sử dụng trong một giao thức mạng, bạn sẽ chọn thuật toán nào sau đây
A. DES

B. Whirlpool

C. RCA

D. AES

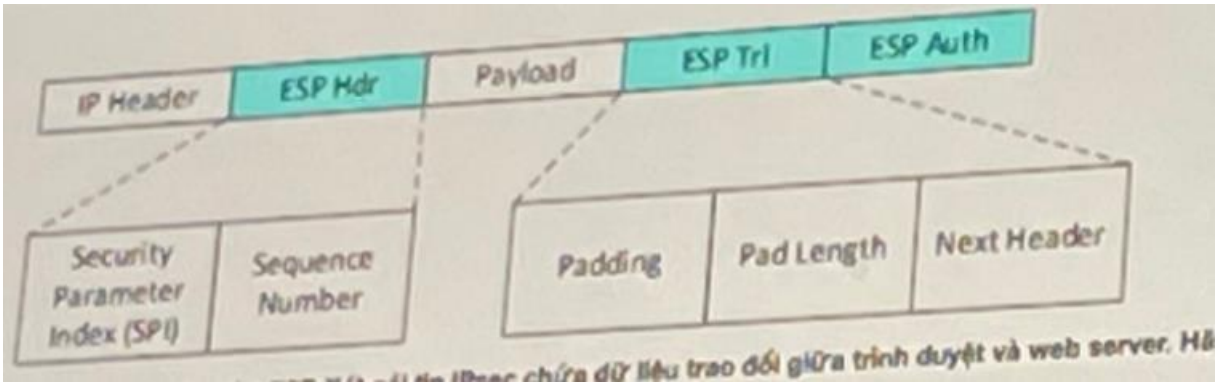
Câu 5: Tấn công hủy xác thực (Deauthentication Attack) vào mạng không dây là loại tấn công nào sau đây
A. Tấn công mật mã

B. Tấn công từ chối dịch vụ

C. Tấn công hạ cấp

D. Tấn công Brute-Force

Câu 6: cho cấu trúc gói tin ESP IPSec như sau:




Giả sử kết nối của IPSec được thiết lập ở chế độ Transport mode, sử dụng giao thức ESP. Xét gói tin IPSec chứa dữ liệu trao đổi giữa trình duyệt và web server. Hãy cho biết giá trị của trường Next Header trong ESP

Đáp án: 6

Câu 7: Trong sơ đồ xác thực sau:
1: Alice -> Bob: “Alice”

2: Bob -> Alice: {Nb}Kp

3. Alice → Bob: Nb

4. Bước kiểm tra tính hợp lí của Nb

Tham số Kp là tham số nào

A. Khóa công khai của Alice

B. Khóa bí mật chia sẻ trước giữa Alice và Bob

C. Khóa công khai của Bob

D. Khóa bí mật của Bob

Câu 8: Đâu là định nghĩa đúng về giao thức an toàn mạng

A. Giao thức an toàn mạng là giao thức mật mã được sử dụng để bảo vệ dữ liệu được truyền trên tầng ứng dụng
B. Giao thức an toàn mạng là giao thức mật mã được sử dụng để bảo vệ dữ liệu lưu trữ trên máy tính

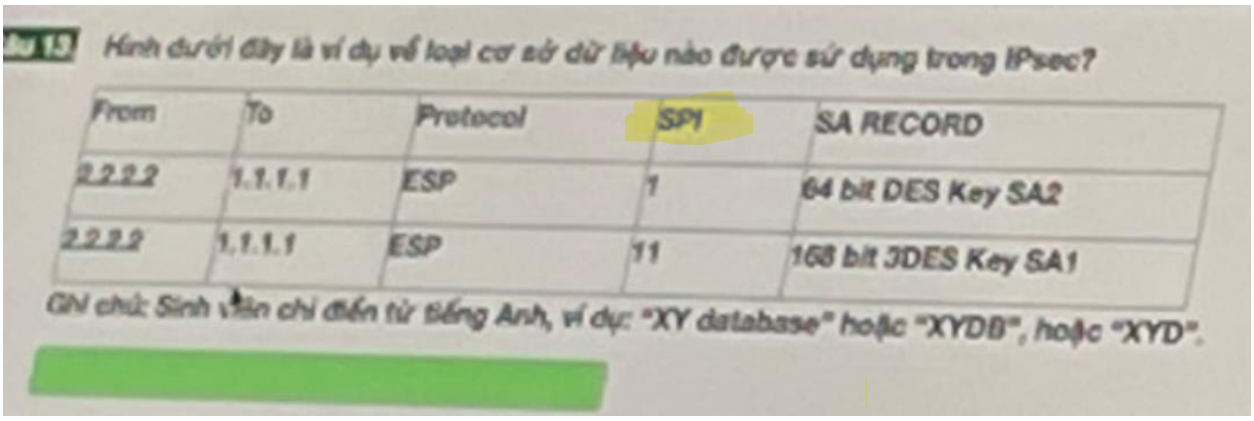
C. Giao thức an toàn mạng là giao thức mật mã được sử dụng để bảo vệ dữ liệu truyền thông giữ các máy tính

D. Giao thức an toàn mạng là giao thức mật mã được sử dụng để bảo vệ dữ liệu trên máy tính và dữ liệu truyền thông

Câu 9: Cho biết cổng mặc định của giao thức TELNET

Đáp án : 23

Câu 10:




Đáp án : SAD

Câu 11: số hiệu của giao thức AH

Đáp án: ~~RFC 2402~~ 51

Câu 12: Độ dài khóa chia sẻ trước trong giao thức WEP là bao nhiêu

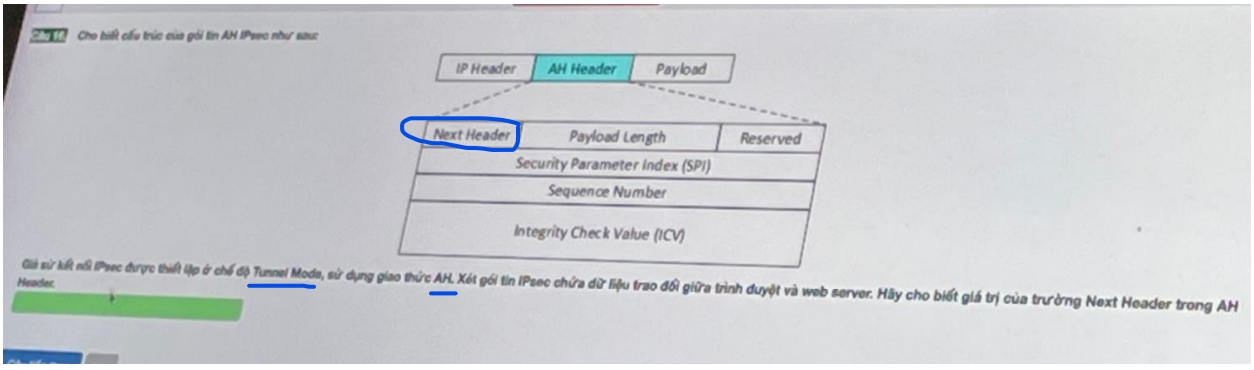
A. 40 hoặc 104 bit

B. 40 hoặc 108 bit

C. 48 hoặc 104 bit

D. 48 hoặc 128 bit

Câu 13:




Đáp án : 4

Câu 14: Phát biểu sai về WPA2

A. WPA2 hỗ trợ xác thực thông điệp bằng AES-CBC-MAC

B. WPA hỗ trợ xác thực bằng giao thức EAP

C. Trong WPA2, khóa giữa AP với các Station khác nhau là khác nhau nên không thể gửi gói tin quảng bá

D. WPA2 bắt buộc hỗ trợ mã hóa bằng AES

Câu 15: Phát biểu **SAI** về PAP

A. PAP là giao thức bắt tay 2 bước

B. Trong PAP, mật khẩu được truyền đi dưới dạng rõ

C. Không thể triển khai xác thực 2 chiều bằng PAP

D. PAP là giao thức xác thực 1 chiều

Câu 16: trong các thành phần sau đây, thành phần nào tiếp nhận yêu cầu truy cập trong mạng VPN

A. VPN client

B. VPN server

C. NAS ( Network Acess Server)

D, Router

Câu 17: Một giao thức liên lạc giữa mail client và mail server hoạt động trên cổng TCP mặc định là 993, tên của giao thức

Đáp án: IMAPS

Câu 18: Đâu không phải giao thức an toàn cho thư điện tử

A. ESMTP

B. POP3S

C. SMTP

D. IMAPS

Câu 19: Phát biểu **ĐÚNG NHẤT** cho đại lượng "nonce" được sử dụng trong các giao thức xác thực

A. Nonce là một số được sinh ngẫu nhiên để xác suất lặp lại giá trị vô cùng nhỏ

B. Nonce là một số ngẫu nhiên được sinh ra trong 1 không gian có kích thước lớn để xác xuất lặp lại vô cùng nhỏ

C. Nonce là một đại lượng có giá trị không lặp lại hoặc xác suất lặp lại vô cùng nhỏ

D. Nonce là một giá trị ngẫu nhiên có giá trị không bao giờ lặp lại hoặc xác suất lặp lại vô cùng nhỏ

Câu 20: Phát biểu **ĐÚNG** về giao thức EAP

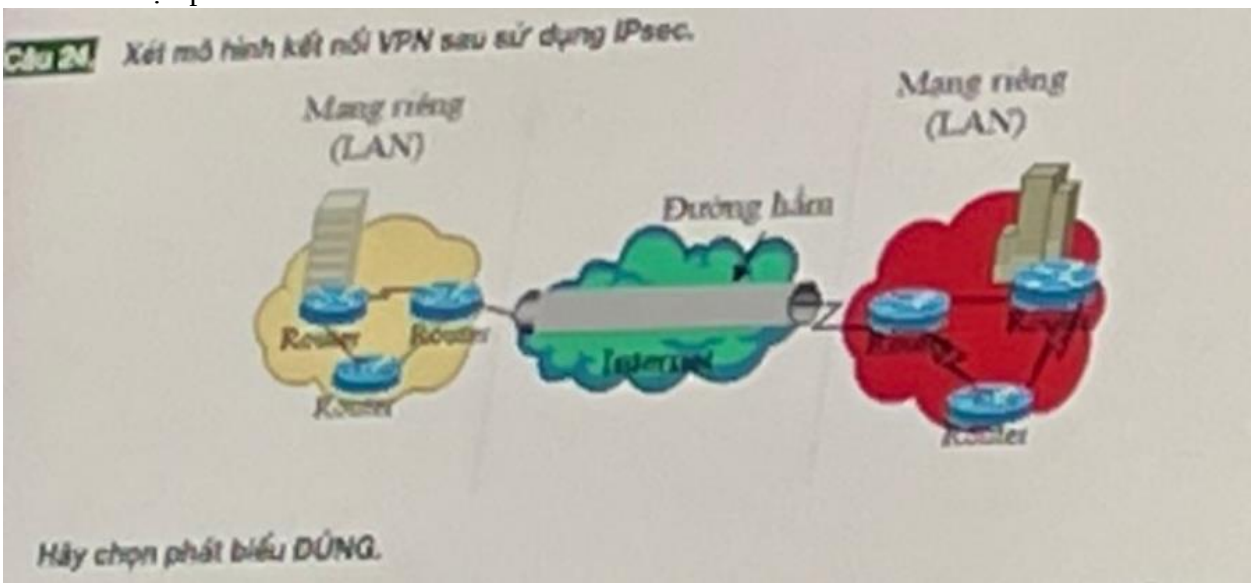
A. EAP là giao thức bắt tay 2 bước

B. EAP truyền mật khẩu dạng rõ

C. EAP là giao thức thách đố-giải đố

D. EAP là giao thức chứa nhiều phương thức xác thực

Câu 21: Chọn phát biểu **ĐÚNG**




A. Các giao thức ở lớp trên của lớp Network trong mô hình TCP/IP phải được cài đặt để hỗ trợ IPSec

B. Các chương trình ứng dụng phải được chỉnh sửa để hỗ trợ IPSec

C. Phải cài đặt thêm phần mềm hỗ trợ ở các site để có thể sử dụng được IPSec

D. Việc triển khai IPSec là hoàn toàn trong suốt với tầng ứng dụng trong mô hình TCP/IP

Câu 22 Đâu không phải thông điệp của giao thức EAP

A. Request

B. Success

C. Acknowlegdement

D. Response

Câu 23: ….. cung cấp dịch vụ an toàn cho tầng giao vận

A. TLS

B. PPP

C. ESP

D. PCP

Câu 24: Mỗi đầu mối IPSec phải duy trì một cơ sở dữ liệu thông tin để biết những gói tin cần được xử lí bằng IPSec, gói tin nào cần được xử lí bằng IP. Hãy cho biết tắt của cơ sở dữ liệu đó

Đáp án: SPD

Câu 25: Trong giao thức an toàn mạng, mật mã đối xứng **KHÔNG** giúp đảm bảo tính chất an toàn nào của thông tin

A. Tính sẵn sàng

B. Tính toàn vẹn

C. Tính bí mật

D. Tính xác thực

Câu 26: Giao thức EAP **KHÔNG** sử dụng trong giao thức WLAN nào

A. WPA

B. WEP

C. TKIP

D. WPA2

Câu 27: Phát biểu **ĐÚNG** về khóa phiên trong SSL/TLS trong trường hợp sử dụng trao đổi khóa RSA

A. Server sinh ra 1 Master Key và gửi cho Client, hai bên sử dụng Master Key để dẫn xuất ra các khóa phiên

B. Client sinh ra một bộ khóa phiên, bao gồm khóa mã hóa, khóa xác thực và gửi cho Server để dùng chung

C. Server sinh ra một bộ khóa phiên, bao gồm khóa mã hóa, khóa xác thực và gửi cho client để dùng chung

D. Client sinh ra một Pre-Master Secret và gửi cho Server, hai bên sử dụng Pre-Master Secret và các giá trị ngẫu nhiên đã gửi cho nhau để tạo ra Master Key, rồi dẫn xuất ra các khóa phiên

Câu 28: Phát biểu **ĐÚNG NHẤT** về SA trong IPSec

A. Một SA được xác định duy nhất bởi địa chỉ của máy tính

B. Một SA được xác định duy nhất bởi SPI kết hợp với giao thức con IPSec

C. Một SA được xác định duy nhất bởi 1 trong 2 cách: bởi địa chỉ máy đích, bởi SPI kết hợp với giao thức con IPSec

D. Một SA được xác định duy nhất bởi SPI

Câu 29: Chọn phát biểu **SAI** về giao thức WEP

A. WEP sử dụng thuật toán kiểm tra toàn vẹn CRC32

B. WEP sử dụng thuật toán mã hóa dữ liệu RC4

C. WEP không chống được tấn công phát lại

D. WEP sử dụng thuật toán mã hóa dữ liệu AES

Câu 30: Điểm **KHÁC BIỆT** giữa WEP và TKIP

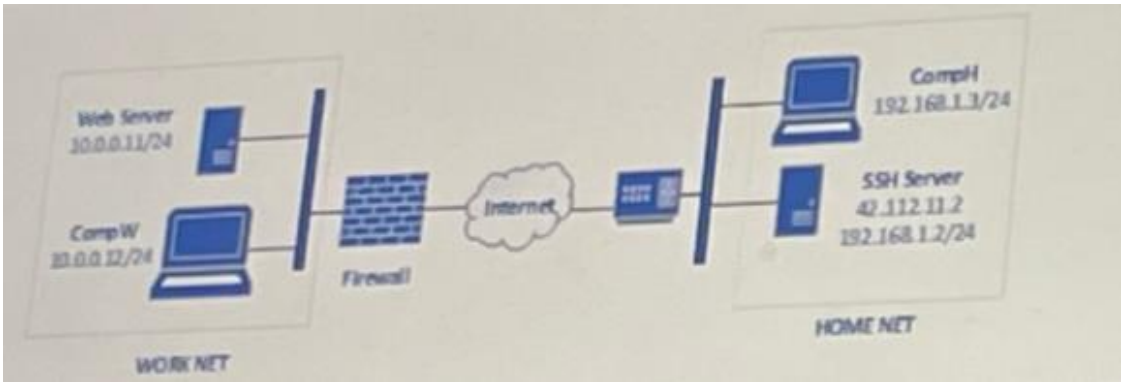
A. WEP sử dụng hàm kiểm tra CRC32, TKIP sử dụng thuật toán Michael-64

B. WEP sử dụng hệ mật DES, TKIP sử dụng AES

C. WEP không hỗ trợ giao thức EAP, TKIP có hỗ trợ EAP

D. WEP không hỗ trợ khóa nhóm, TKIP hỗ trợ khóa nhóm

Câu 31:




Giả sử Firewall không cho kết nối từ Internet đi vào WORK NET nhưng một kỹ sư lại muốn truy cập từ HOME NET tới Web Server để hoàn thành sớm các công việc của mình. Anh ta thiết lập một SSH Server tại HOME NET với một địa chỉ Internet và một địa chỉ cục bộ. Cách làm nào sau đây giúp anh kỹ sư đạt được mục đích

(A) Từ máy CompW thực hiện kết nối tới SSH Server, sử dụng Local Port Forwarding để chuyển kết nối tới 192.168.1.2:80 sang 10.0.0.11:80. Sau đó, từ máy CompH truy cập tới Web Server bằng cách nhập vào trình duyệt địa chỉ http://192.168.1.2.

(B) Từ máy CompW thực hiện kết nối tới SSH Server, sử dụng Remote Port Forwarding để

chuyển kết nối tới 192.168.1.2:80 sang 10.0.0.11:80. Sau đó, từ máy CompH truy cập tới Web Server bằng cách nhập vào trình duyệt địa chỉ http://192.168.1.2.

(C) Từ máy CompW thực hiện kết nối tới SSH Server, sử dụng Local Port Forwarding để chuyển kết nối tới 42.112.11.2:22 sang 10.0.0.11:80. Sau đó, từ máy CompH truy cập tới Web Server bằng cách nhập vào trình duyệt địa chỉ http://42.112.11.2:22.

(D) Từ máy CompW thực hiện kết nối tới SSH Server, sử dụng Remote Port Forwarding để chuyển kết nối tới 42.112.11.2:22 sang 10.0.0.11:80. Sau đó, từ máy CompH truy cập tới Web Server bằng cách nhập vào trình duyệt địa chỉ http://42.112.11.2:22.

Câu 32: Trong một giao thức an toàn mạng ở tầng Network Access của chồng giao thức TCP/IP, để đảm bảo tính bí mật của thông tin truyền đi

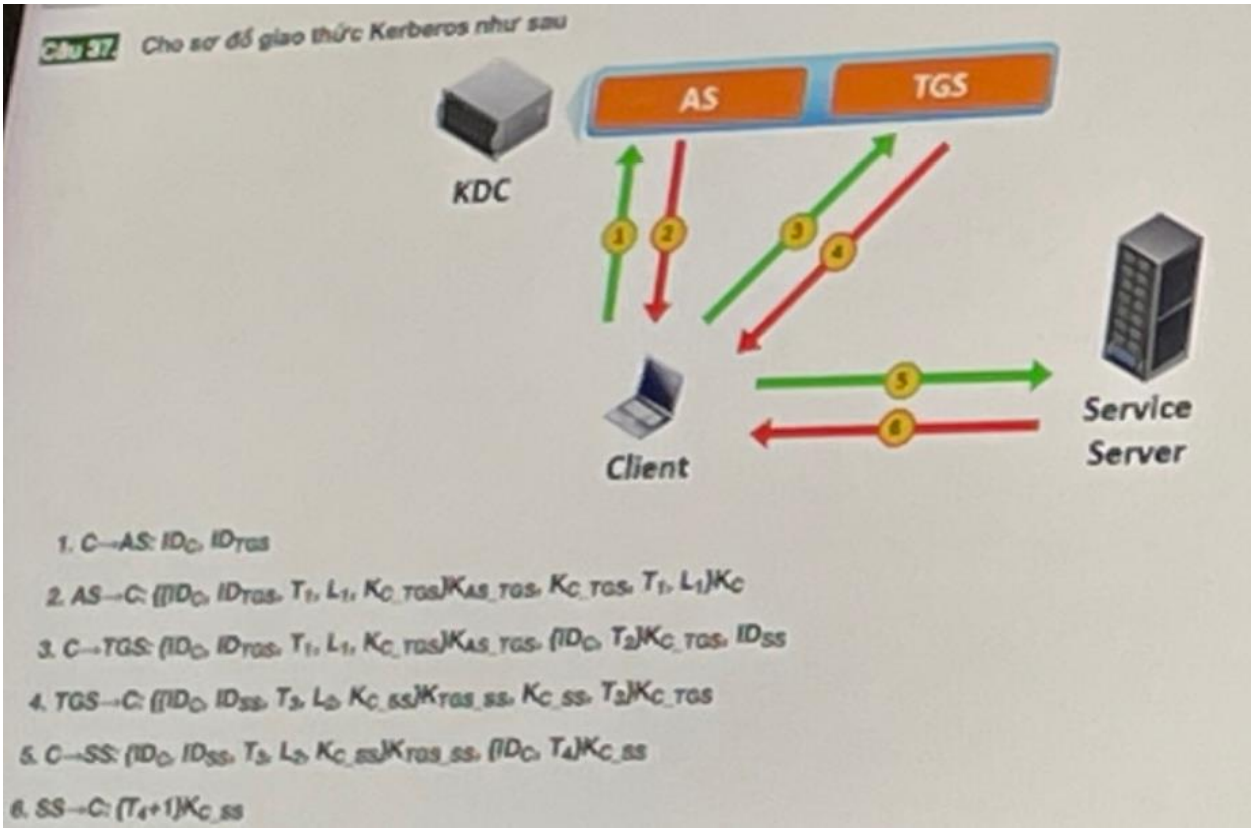
A. Có thể sử dụng chữ kí số

B. có thể sử dụng mật mã công khai

C. cần sử dụng mật mã đối xứng

D. cần sử dụng mật mã khối

Câu 33:




Hãy chọn phát biểu **ĐÚNG NHẤT** về lý do để giao thức Kerberos được coi là có tính chất Single Sign-On.

(A) Vì Client có thể yêu cầu AS cấp đồng thời nhiều vé để xin truy cập tới nhiều Service Server khác nhau.

(B) Vì khi AS cấp cho Client một vé thì Client có thể dùng vé đó để liên hệ với TGS nhiều lần để xin truy cập tới nhiều Service Server khác nhau.

(C) Vì khi TGS cấp cho Client một vé thì Client có thể sử dụng vé đó để truy cập tới nhiều Service Server khác nhau.

(D) Vì Client có thể yêu cầu TGS cấp đồng thời nhiều vé để truy cập tới nhiều Service Server khác nhau.

Câu 34: Đâu là dịch vụ mà giao thức SSH-AUTH cung cấp

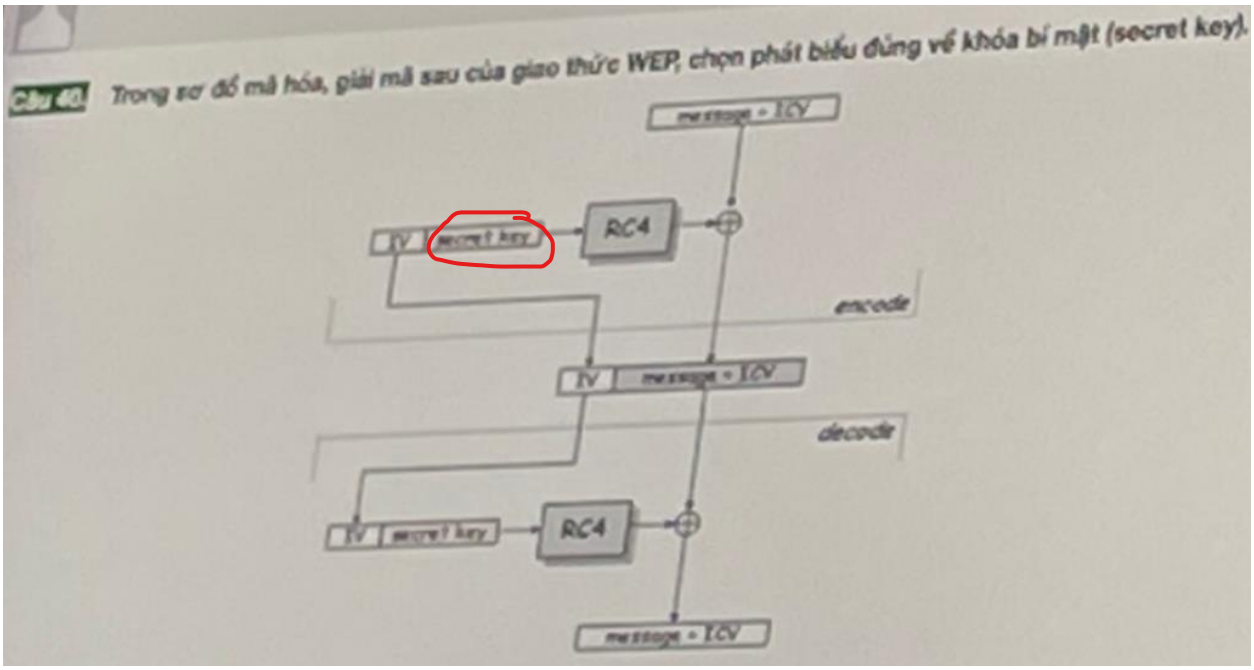
A. Trao đổi các khóa bí mật

B. Xác thực SSH Client

C. Thỏa thuận bộ các tham số mật mã

D. Xác thực SSH Server

Câu 35:



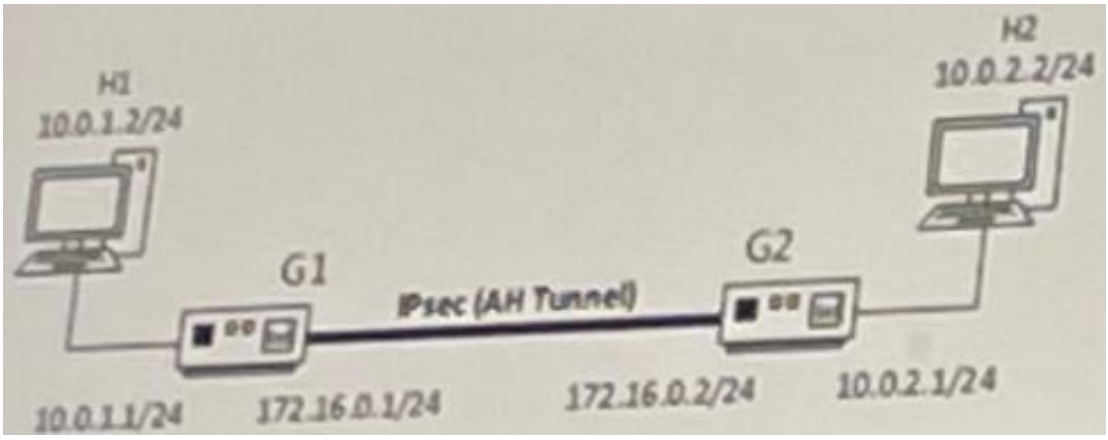

A. Khóa secret key được sinh ra khác nhau cho mỗi gói tin

B. Khóa secret key chỉ đước sinh ra bởi AP

C. Khóa secret key được chia sẻ trước giữa client và AP

D. Khóa secret key chỉ được sinh ra bởi client

Câu 36:




Giữa 2 gateway G1 và G2 ngta thiết lập giao thức IPSec sử dụng giao thức AH ở chế độ Tunnel. Hai gateway này kết nối 2 mạng LAN 10.0.1.0/24 và 10.0.2.0/24 với nhau. Xét một gói tin UDP được gửi từ H1 đến H2. Trong IP Header của gói tin tại G1,trường Protocol có giá trị bằng bao nhiêu
Đáp án: 51

Câu 37: Đâu là đặc điểm **ĐÚNG** của các giao thức WPA ở chế độ Enterprise

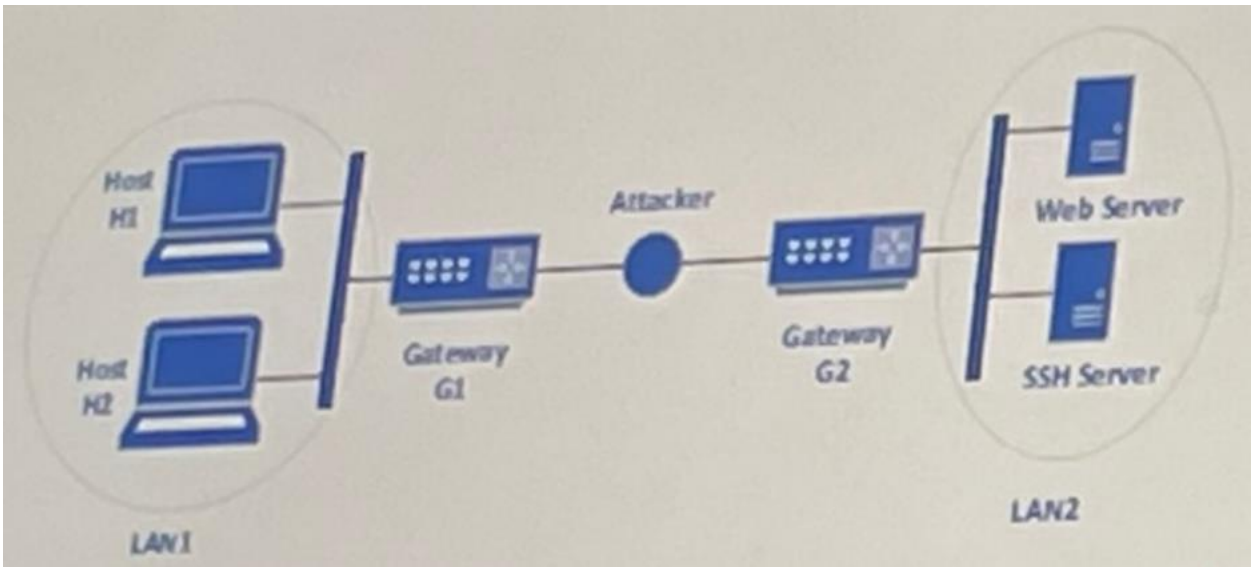
A. Không yêu cầu máy chủ xác thực

B. Yêu cầu một máy chủ xác thực

C. Không sử dụng giao thức TKIP

D. Sử dụng xác thực mở

Câu 38:



Cho biết giữa G1 và G2 đã thiết lập IPSec ở chế độ Tunnel, sử dụng giao thức con ESP để kết nối LAN1 và LAN2. Giả sử giao thức IPSec an toàn. Chọn phát biểu **ĐÚNG**

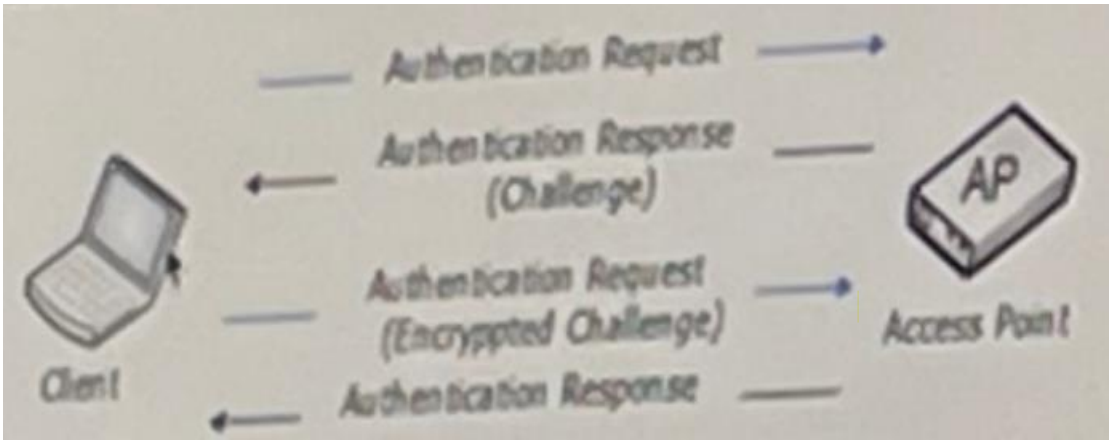
A. Dữ liệu trao đổi giữa các H1 và Web server được đảm bảo tuyệt đối

B. Attacker vẫn có thể phân biệt được máy nguồn và máy đích đối với mọi kết nối từ LAN1 đến LAN2

C. Attacker vẫn có thể phân biệt được kết nối từ LAN1 tới Web Server và kết nối từ LAN1 đến SSH Server

D. Attacker không thể phân biệt được H1 hay H2 đang giao tiếp với Web Server

Câu 39:




Sơ đồ sau mô tả phương pháp xác thực nào được sử dụng trong WLAN

A. Xác thực dựa trên địa chỉ MAC

B. Xác thực mở rộng EAP

C. Xác thực dựa trên khóa chia sẻ trước

D. Xác thực mở

Câu 40: Trong giao thức WEP, tên viết tắt của thuật toán mã được sử dụng để mã hóa dữ liệu giữa Access Point và các máy trạm là

Đáp án: RC4

Câu 41: Tấn công nào sau đây **KHÔNG** phải tấn công chủ động

A. Tấn công nghe lén

B. Tấn công từ chối dịch vụ

C. Tấn công giả mạo

D. Tấn công phát lại

Câu 42. Mạng Extranet VPN thường được sử dụng để

(A) Kết nối các khách hàng và đối tác tới mạng Intranet trung tâm.

(B) Kết nối các văn phòng chi nhánh với nhau

(C) Kết nối các văn phòng chi nhánh với mạng Inttranet trung tâm

(D) Kết nối chỉ trong một chi nhánh

Câu 43. Cho sơ đồ giao thức Needham-Schroeder như sau.

1. Alice → Sandy: Alice, Bob
2. Sandy → Alice: {TS, L, K, Bob, {TS, L, K, Alice}KBS}KAS
3. Alice → Bob: {TS, L, K, Alice}KBS, {Alice, TA}K
4. Bob → Alice: {TA+1}K

Hãy chọn phát biểu đúng.

(A) Có thể coi bước 1 và 2 là pha cấp vé {TS, L, K, Alice}KBS cho Alice. Alice có thể sử dụng vé này bao nhiêu lần tùy ý (bước 3 và 4); giá trị KBS trong vé là để Alice biết vé này chỉ để liên lạc với Bob.

(B) Có thể coi bước 1 và 2 là pha cấp vé {TS, L, K, Alice}KBS cho Alice. Vé này có thời hạn sử dụng được xác định bởi TS và L. Trong thời hạn đó, Alice có thể liên lạc với Bob (bước 3 và 4) số lần tùy ý.

(C) Có thể coi bước 1 và 2 là pha cấp vé {TS, L, K, Alice}KBS cho Alice. Thời hạn bắt đầu có hiệu lực của vé được xác định bởi TS, Alice có thể liên lạc với Bob (bước 3 và 4) L lần, sau đó thì phải xin cấp vé mới.

(D) Có thể coi bước 1 và 2 là pha cấp vé {TS, L, K, Alice}KBS cho Alice. Alice có thể sử dụng vé này bao nhiêu lần tùy ý (bước 3 và 4); giá trị TS trong vé là để Alice biết vé này được cấp bởi Sandy.

Câu 44. Chọn phát biểu **ĐÚNG** về giao thức an toàn mạng.

(A) Giao thức an toàn mạng là giao thức được thiết kế để đảm bảo an toàn cho các giao thức mạng không có tính năng an toàn.

(B) Giao thức an toàn mạng có thể nằm ở bất kỳ tầng nào của chồng giao thức TCP/IP.

(C) Một giao thức an toàn mạng sẽ đảm bảo tính bí mật và toàn vẹn cho thông tin được truyền qua nó.

(D) Một giao thức an toàn mạng sẽ đảm bảo cả ba tính chất bí mật, toàn vẹn và khả dụng cho thông tin được truyền qua nó

Câu 45. Trong các thành phần sau, thành phần nào có thể đóng vai trò Authenticator?

(A) Supplicant

(B) User

(C) Gateway

(D) NAS (Network Access Server)

Câu 46. Sau khi kết thúc giao thức SSH-TRANS, giữa SSH Server và SSH Client
(A) thỏa thuận được 2 khóa phiên đối xứng. Trong đó 1 khóa được sử dụng để mã hóa thông điệp, 1 khóa được sử dụng để xác thực thông điệp giữa Server và Client.
(B) thỏa thuận được 2 khóa phiên đối xứng. Trong đó 1 khóa được sử dụng để mã hóa và xác thực thông điệp từ Server tới Client, 1 khóa được sử dụng để mã hóa và xác thực thông điệp từ Client tới Server.
(C) thỏa thuận được 4 khóa phiên đối xứng. Trong đó 2 khóa được sử dụng để mã hóa và xác thực thông điệp từ Server tới Client, 2 khóa được sử dụng để mã hóa và xác thực thông điệp từ Client đến Server.
(D) thỏa thuận được 1 khóa phiên đối xứng để mã hóa và xác thực thông điệp trao đổi sau đó giữa Server và Client.

Câu 47. Giao thức WEP là viết tắt của cụm từ nào sau đây?
(A) Wired Equivalent Private
|(B) Wired Equivalence Private
(C) Wired Equivalence Privacy
(D) Wired Equivalent Privacy

Câu 48. Vào năm 2003, khi chuẩn IEEE 802.11i còn chưa được chính thức ban hành, Wi-Fi Alliance đã đưa ra một giao thức an toàn dựa trên một phần của IEEE 802.11i để áp dụng trong các thiết bị Wi-Fi. Tên viết tắt của giao thức an toàn đó là:

Đáp án: WPA

Câu 49. Bạn được yêu cầu chọn một thuật toán mật mã khóa công khai để sử dụng trong một giao thức mạng, bạn sẽ chọn thuật toán nào sau đây?

(A) Triple-DES

(B) RSA

(C) ECB

(D) SHA

Câu 50.Chọn phát biểu đúng về hoạt động của giao thức SSL Handshake?

(A) Trong SSL Handshake, Client bắt buộc gửi Certificate sang cho Server

(B) Trong SSL Handshake, Server không bắt buộc phải Certificate của mình sang Client, Client bắt buộc gửi Certificate sang cho Server

(C) Trong SSL Handshake, Server không bắt buộc phải Certificate của mình sang Client

(D) Trong SSL Handshake, Server bắt buộc phải gửi Certificate của mình sang Client, Client không bắt buộc gửi Certificate sang cho Server

Câu 51. Xét mô hình kết nối sau.


Biết rằng trình duyệt trên Web Client truy cập tới Web Server qua giao thức HTTPS. Hãy chọn phát biểu **ĐÚNG NHẤT**.

(A) Cả trình duyệt trên Web Client và phần mềm máy chủ web trên Web Server phải được lập trình để hỗ trợ SSL/TLS.

(B) Trình duyệt trên Web Client phải được lập trình để hỗ trợ SSL/TLS

(C) Phần mềm máy chủ web trên Web Server phải được lập trình để hỗ trợ SSL/TLS.

(D) SSL/TLS là trong suốt đối với tầng ứng dụng (Application) trong chồng giao thức TCP/IP nên trình duyệt và phần mềm máy chủ web không cần phải biết về sự tồn tại của SSL/TLS.

Câu 52. Một giao thức liên lạc giữa mail client và mail server, hoạt động trên cổng TCP mặc định là 143. Hãy cho biết tên viết tắt của giao thức.

Đáp án: IMAP

Câu 53. Mô tả nào sau đây **KHÔNG ĐÚNG** về giao thức WEP?

(A) Không có khóa phiên nào được thiết lập trong suốt quá trình xác thực

(B) Không có bảo vệ chống tấn công phát lại

(C) Hỗ trợ xác thực hai chiều

(D) Cùng một khóa chia sẻ giống nhau được dùng cho cả mã hóa và xác thực

Câu 54.Chọn phát biểu đúng về giao thức PAP (Password Authentication Protocol).

(A) PAP là giao thức bắt tay 3 bước

(B) Trong giao thức PAP, mật khẩu được mã hóa trước khi truyền đi

(C) PAP là giao thức xác thực 2 chiều

(D) PAP là giao thức bắt tay 2 bước

Câu 55. Trong một giao thức an toàn mạng ở tầng Liên mạng (Internet) của chồng giao thức TCP/IP

(A) có thể sử dụng kết hợp, nhưng không nên sử dụng kết hợp ký số và mã hóa vì sẽ làm giảm đáng kể hiệu năng của hệ thống.

(B) cần phải sử dụng kết hợp mã hóa và ký số nếu muốn đảm bảo đồng thời tính bí mật và tính xác thực cho thông tin.

(C) có thể sử dụng kết hợp mã hóa và ký số để đảm bảo tính bí mật và xác thực cho thông tin.

(D) luôn phải có sự kết hợp mã hóa và ký số để đảm bảo tính bí mật và xác thực cho thông tin.

Câu 56.Trong một giao thức an toàn mạng, chứng thư số khóa công khai được sử dụng để

(A) kiểm tra chữ ký số của chủ thể được nêu danh trong chứng thư.

(B) trao đổi khóa phiên với chủ thể được nêu danh trong chứng thư.

(C) xác nhận một khóa công khai thuộc về chủ thể được nêu danh trong chứng thư.

(D) mã hóa thông tin gửi cho chủ thể được nêu danh trong chứng thư.

Câu 57.Chọn phát biểu ĐÚNG NHẤT về mã hóa dữ liệu tầng ứng dụng trong giao thức SSL/TLS.

(A) Việc mã hóa dữ liệu luôn là bắt buộc.

(B) Việc mã hóa dữ liệu luôn được thực hiện bằng mật mã đối xứng.

(C) Việc mã hóa dữ liệu bằng mật mã đối xứng hay mật mã khóa công khai là do CipherSuite quyết định.

(D) Việc mã hóa dữ liệu luôn được thực hiện bằng mật mã khóa công khai, sử dụng chứng thư số X.509.

Câu 58. Hãy chọn phát biểu ĐÚNG NHẤT về đại lượng “nonce” được sử dụng trong các giao thức xác thực.

(A) Nonce luôn được sinh ra bởi bên yêu cầu xác thực (Claimant)

(B) Nonce có thể được sinh bởi bên xác thực (Verifier) hoặc bên yêu cầu xác thực (Claimant) thùy thuộc vào sự thỏa thuận giữa hai bên trong pha đầu tiên của giao thức xác thực.

(C) Nonce được sinh bởi bên xác thực (Verifier) nếu bên xác thực khởi xướng phiên liên lạc, được sinh bởi bên yêu cầu xác thực (Claimant) nếu bên yêu cầu xác thực khởi xướng phiên liên lạc.

(D) Nonce luôn được sinh ra bởi bên xác thực (Verifier)

Câu 60.Chọn phát biểu đúng về giao thức CHAP

(A) Trong giao thức CHAP, mật khẩu được truyền dưới dạng rõ

(B) CHAP là giao thức bắt tay 3 bước

(C) CHAP là giao thức bắt tay 2 bước

(D) Giao thức CHAP sử dụng cả nonce và timesamp

Câu 61.Tổ hợp an toàn (SA) trong IPsec tương ứng với cụm từ nào sau đây?

(A) Secured Association

(B) Security Association

(C) Security Associated

(D) Secured Associating

Câu 62. SSH là viết tắt của?

(A) Secure Server

(B) Secure Shell

(C) Security Shell

(D) Secure Socket

Câu 63. Tại sao mã xác thực thông báo (MAC) có thể xác thực được nguồn gốc của dữ liệu?

(A) Vì trong MAC có chứa một giá trị bí mật được chia sẻ trước giữa người gửi và người nhận.

(B) Vì MAC có khả năng chống tấn công phát lại (replay attack)

(C) Vì trong MAC có chứa định danh của cả người gửi và người nhận.

(D) Vì trong MAC có sử dụng hàm băm.

Câu 64. Giao thức SSL cung cấp dịch vụ nào sau đây?

(A) Tính bí mật

(B) Tính toàn vẹn

(C) Nén dữ liệu

(D) Cả ba đáp án trên

Câu 64. Giao thức xác thực nào sau đây sử dụng trung tâm phân phối khóa (KDC- Key Distribution Center)

(A) CHAP.

(B) EAP

(C) PAP

(D) Kerberos

Câu 65.Hãy chọn phát biểu ĐÚNG NHẤT về đại lượng "timestamp" được sử dụng trong các giao thức xác thực.

(A) Giá trị của timestamp do bên xác thực (Verifier) quyết định.

(B) Giá trị của timestamp được các bên (bên xác thực và bên yêu cầu xác thực) thống nhất trước khi tiến hành xác thực.

(C) Giá trị của timestamp do bên yêu cầu xác thực (Claimant) quyết định.

(D) Giá trị của timestamp được mỗi bên (bên xác thực và bên yêu cầu xác thực) tự xác định khi cần.

Câu 66.Trong các giao thức an toàn mạng, mật mã đối xứng có thể được sử dụng để đảm bảo tính chất an toàn nào của thông tin?

(A) Tính bí mật.

(B) Tính toàn vẹn.

(C) Tính xác thực.

(D) Cả 3 tính chất trên.

Câu 67. Phương án nào sau đây không phải là phương pháp xác thực được sử dụng trong WLAN?

(A) Xác thực dựa trên địa chỉ MAC

(B) Xác thực dựa trên khóa chia sẻ trước

(C) Xác thực dựa trên địa chỉ IP

(D) Xác thực mở rộng EAP

Câu 68.Chọn phát biểu SAI về giao thức EAP

(A) Trong giao thức EAP mật khẩu được truyền đi dưới dạng rõ.

(B) EAP là giao thức xác thực khả mở rộng.

(C) EAP là giao thức xác thực 1 chiều.

(D) EAP là giao thức sử dụng nhiều phương thức xác thực khác nhau.

Câu 69. Phát biểu nào dưới đây là đúng?

(A) Các giao thức SSL, TLS, SSH là những giao thức hoạt động ở cả tầng giao vận và tầng mạng.

(B) POP, IMAP, DHCP, SNMP là những giao thức hoạt động ở tầng ứng dụng.

(C) TCP, ICMP, SSL và HTTP là những giao thức hoạt động ở tầng giao vận.

(D) ARP, PPP, IP là giao thức hoạt động ở tầng liên kết dữ liệu.

Câu 70: Xác thực là

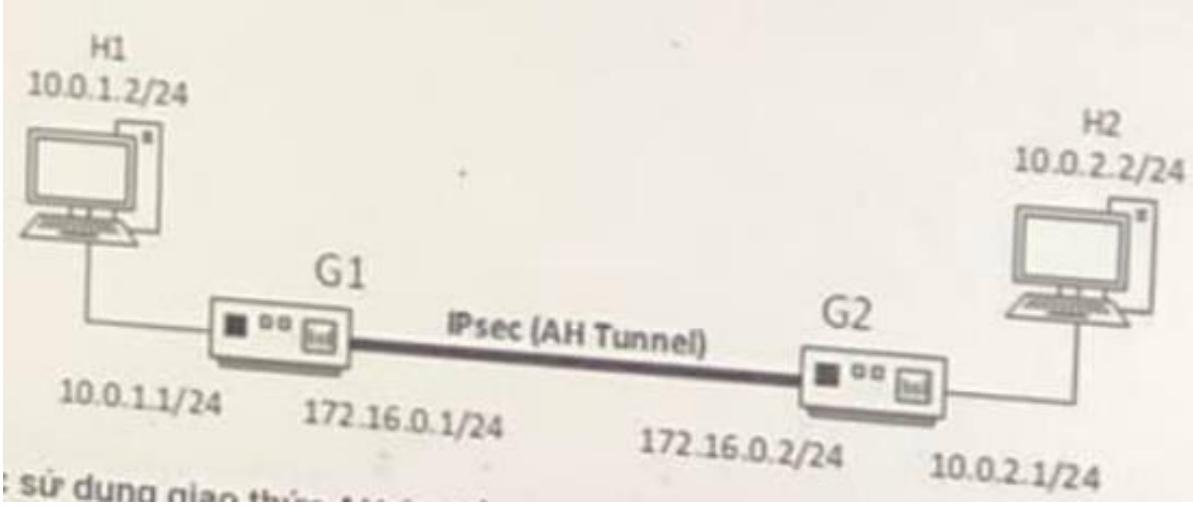
A. xác nhận sự thật về một thuộc tính của một chủ thể hoặc một đối tượng

B. xác nhận sự thật một thuộc tính của một người dùng (nếu là xác thực thể) hoặc một thông điệp (nếu là xác thực nguồn gốc thông điệp)

C. kiểm tra và xác nhận tính sống của một chủ thể hoặc tính tươi của 1 đối tượng

D. kiểm tra và xác nhận tính chân thực của một định danh người dùng (nếu là xác thực thực thể) hoặc tính đúng đắn của nguồn gốc một thông điệp (nếu là xác thực thông điệp)

Câu 71: Cho mô hình mạng dưới đây




Giữa hai gateway G1 và G2, người ta thiết lập giao thức IPsec sử dụng giao thức AH ở chế độ tunnel. Hai gateway này kết nối với hai mạng LAN 10.0.1.0/24 và 10.0.2.0/24 với nhau. Xét một gói tin UDP được gửi từ H1 đến H2. Trong IP Header của gói tin IP tại H1, các giá trị Source IP và Destination IP và Protocol là gì ?

A. 172.16.0.1, 172.16.0.2 và 6

B. 10.0.1.2, 172. 16.0.2 và 6

C. 172.16.0.1, 172.16.0.2 và 17

D. 10.0.1.2, 10.0.2.2 và 17

Câu 72: Vào năm 2004, khi chuẩn IEEE 802.11i được chính thức ban hành, Wi-Fi Alliance đã đưa ra một giao thức an toàn hỗ trợ đầy đủ tất cả các thành phần bắt buộc của chuẩn này để áp dụng trong các thiết bị Wi-Fi. Tên viết tắt của giao thức an toàn đó là:

Đáp án: WPA2

Câu 73: Chọn phát biểu đúng về vai trò của hàm băm (không khóa và có khóa) trong giao thức an toàn mạng

A. Hàm băm có thể được sử dụng để đảm bảo tính xác thực và tính khả dụng của thông tin

B. Hàm băm có thể được sử dụng để đảm bảo tính toàn vẹn và bí mật thông tin truyền đi

C. Hàm băm có thể được sử dụng để đảm bảo tính xác thực và bí mật thông tin truyền đi

D. Hàm băm có thể được sử dụng để đảm bảo tính xác thực thông tin và xác thực thực thể

Câu 74: Đâu là 1 điểm khác biệt giữa WEP và TKIP

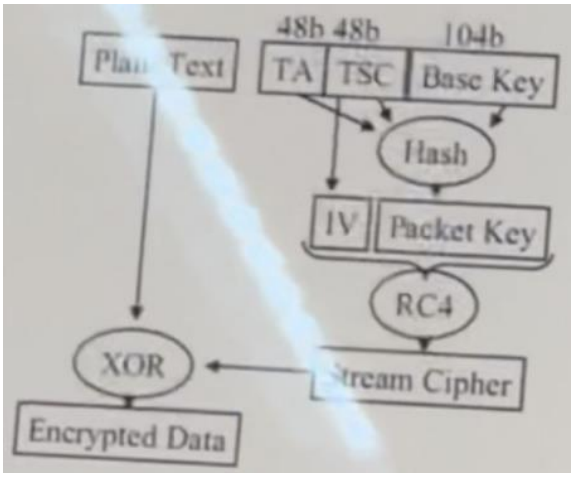
A. WEP sử dụng IV ngẫu nhiên, TKIP sử dụng IV tất định

B. WEP chỉ hỗ trợ xác thực bằng mật khẩu, TKIP hỗ trợ nhiều phương thức xác thực khác nhau

C. WEP không hỗ trợ khóa nhóm, TKIP hỗ trợ khóa nhóm

D. WEP sử dụng DES, TKIP sử dụng AES

Câu 75: Sơ đồ mã hóa nào sau đây mô tả về giao thức nào được sử dụng trong WLAN



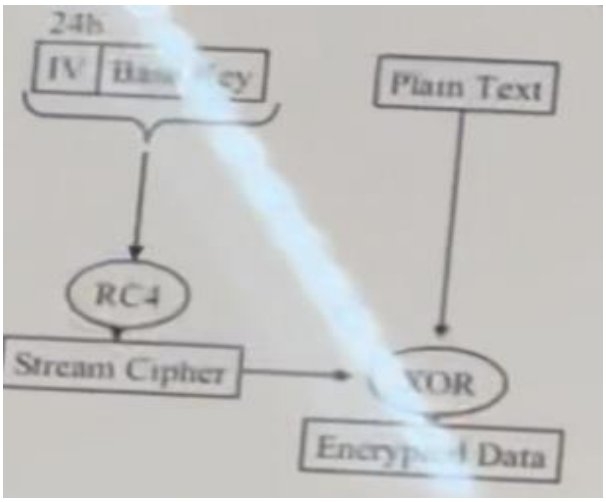

A. TKIP

B. WPA2

C. WEP

D. WPA

Câu 76: Sơ đồ mã hóa nào sau đây mô tả về giao thức WLAN nào




A. WPA

B. WEP

C. WPA2

D. TKIP

Câu 77: Chọn phát biểu ĐÚNG NHẤT về giao thức an toàn mạng

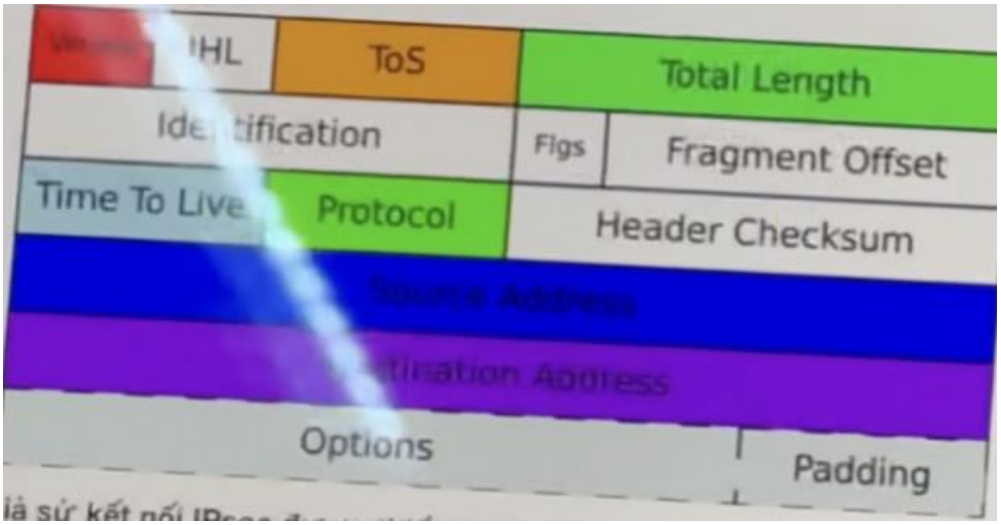
A. Trong chồng giao thức TCP/IP, khi áp dụng triển khai các cơ chế an toàn bằng cách thay đổi giao thức ở tầng Liên mạng (Internet) hoặc/và tầng Truy cập mạng (Network Access) thì dữ liệu của tầng ứng dụng có thể được bảo vệ mà không chỉnh sửa phần mềm ứng dụng

B. Trong chồng giao thức TCP/IP, khi áp dụng triển khai các cơ chế an toàn bằng cách thay đổi giao thức ở tầng Giao vận (Transport) hoặc/và tầng Liên mạng (Internet) thì dữ liệu của tầng ứng dụng có thể được bảo vệ mà không chỉnh sửa phần mềm ứng dụng

C. Trong chồng giao thức TCP/IP, khi áp dụng triển khai các cơ chế an toàn bằng cách thay đổi giao thức ở tầng Giao vận (Transport) thì dữ liệu của tầng ứng dụng có thể được bảo vệ mà không chỉnh sửa phần mềm ứng dụng

D. . Trong chồng giao thức TCP/IP, khi áp dụng triển khai các cơ chế an toàn bằng cách thay đổi giao thức ở tầng Liên mạng (Internet) thì dữ liệu của tầng ứng dụng có thể được bảo vệ mà không chỉnh sửa phần mềm ứng dụng

Câu 78: Cho cấu trúc của IP Header như sau



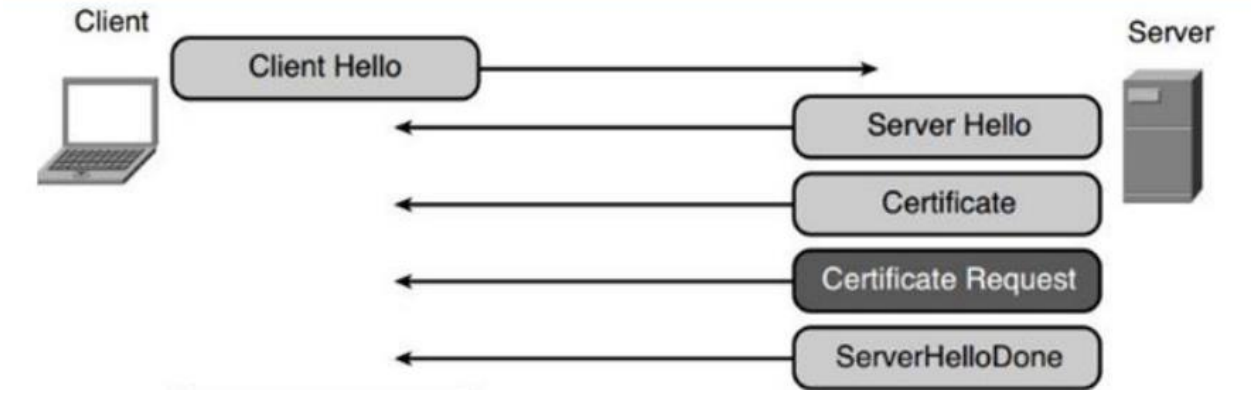

Giả sử kết nối Ipsec được thiết lập ở chế độ Transport Mode, sử dụng giao thức AH. Xét gói tin IPSec chứa dữ liệu trao đổi giữa trình duyệt và web server. Hãy cho biết giá trị của trường Protocol trong IPHeader ngoài cùng

Đáp án: 51

Câu 79: Hãy cho biết số hiệu cổng TCP mặc định của SMTPS

Đáp án: 465

Câu 80: Trong các bước của giao thức SSL Handshake, khi nhận được Certificate của Server, Client sẽ xác thực được gì



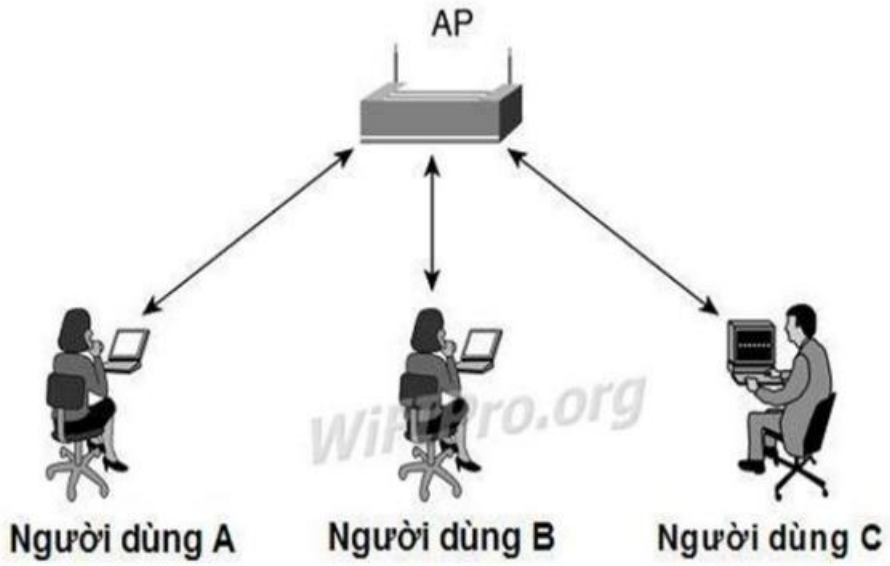

A. Xác thực được khóa bí mật của Server

B. Xác thực được định danh của Server

C. Xác thực được khóa công khai của Server

D. Xác thực được Server

Câu 81: Sơ đồ sau đây mô tả mạng WLAN nào




A. Ad-hoc

B. CSS

C. BSS

D. ESS mô hình ESS: có nhiu AP

Câu 82: Bạn được yêu cầu chọn 1 thuật toán mã dòng để sử dụng trong một giao thức mạng, bạn sẽ chọn thuật toán nào

A. IDEA

B. Triple-DES

C. RC4

D. AES

Câu 83: chọn phát biểu đúng về 802.1x

A. 802.1x là chuẩn được sử dụng cho tầng Internet

B. 802.1x là chuẩn được sử dụng chỉ cho mạng có dây

C. 802.1x là chuẩn được sử dụng cho mạng có dây và không dây

D. 802.1x là chuẩn được sử dụng chỉ cho mạng không dây

Câu 84: Những giao thức nào dưới đây sử dụng mã hóa để bảo mật dữ liệu đường truyền

A. SSH, SCP, FTPS

B. SCP, DNS, SSH

C. SSH, SCP, Telnet

D. HTTPS, FTP, SSH

Câu 85: Đâu KHÔNG phải một loại VPN

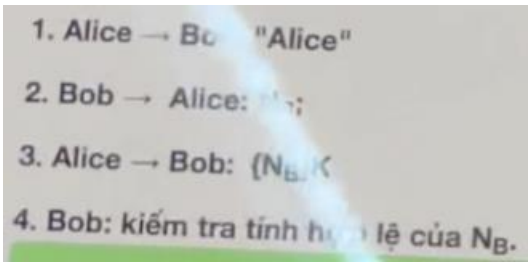
A. Trusted VPN, MPLS VPN

B. Hybrid VPN

C. Secure VPN

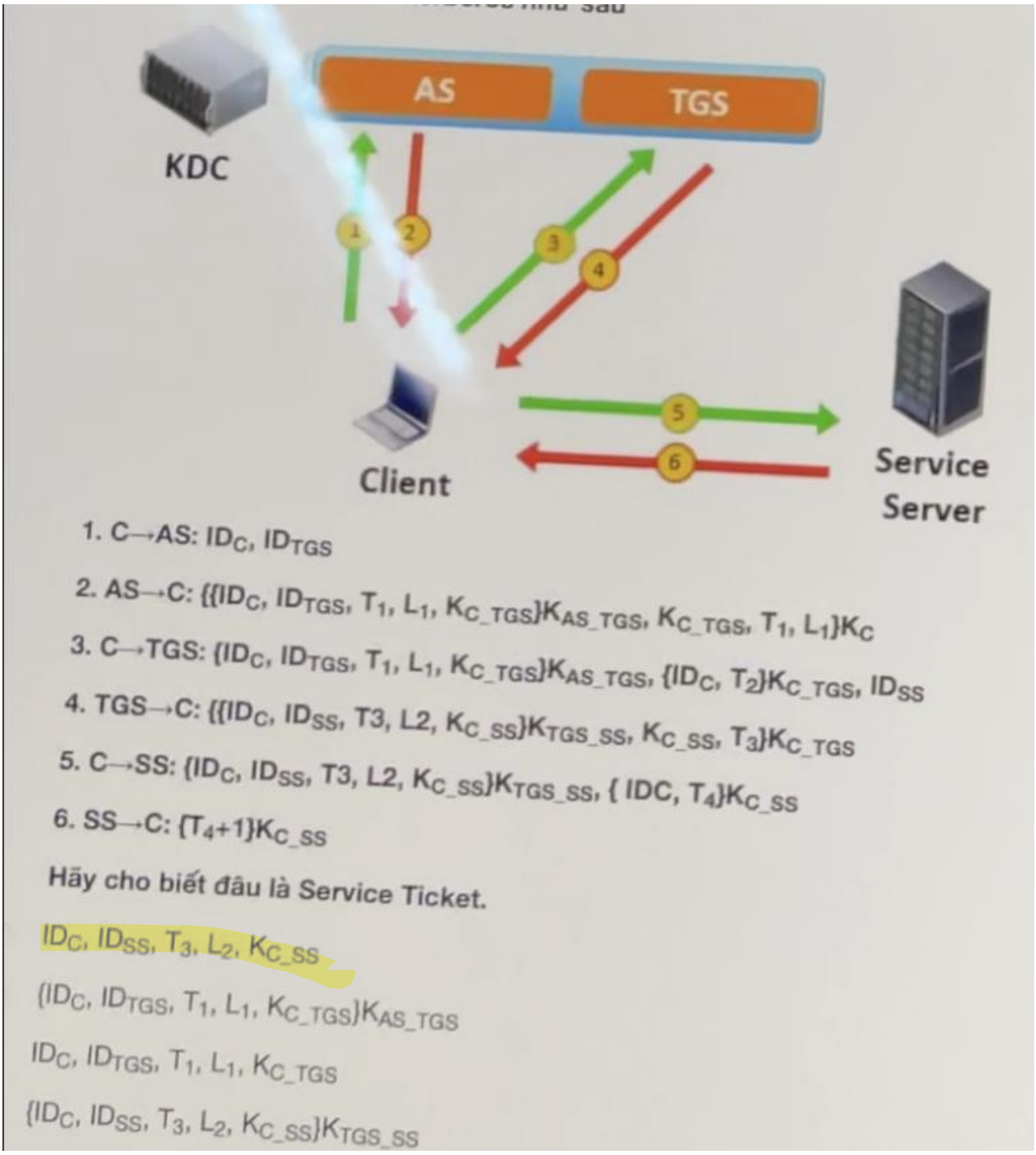
D. Nested VPN

Câu 85: Trong sơ đồ xác thực sau: Alice và Bob phải chia sẻ trước với nhau tham số nào




Đáp án: K

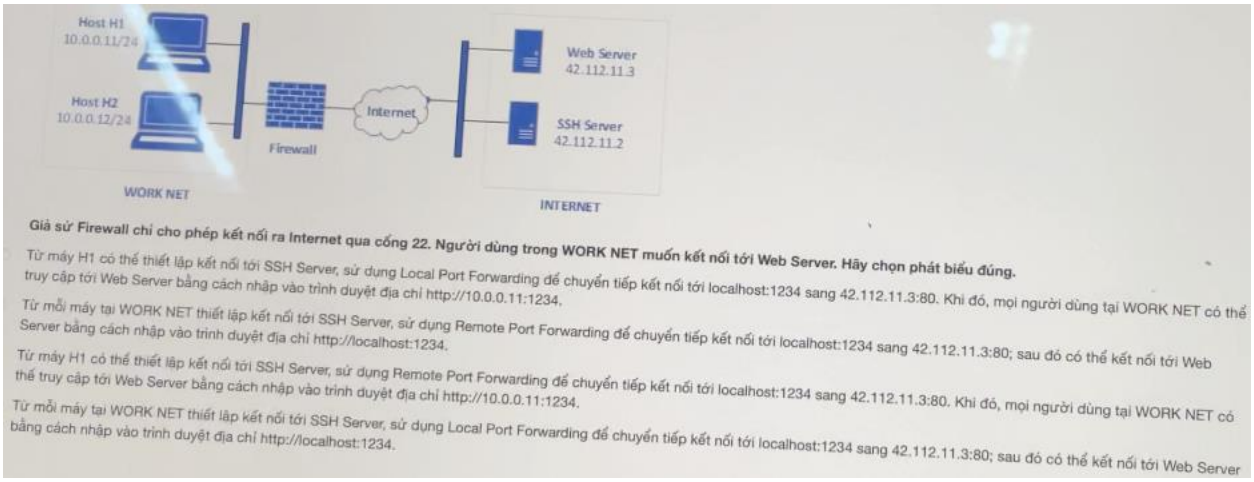
Câu 86: cho sơ đồ giao thức Kerberos như sau:




Hãy cho biết đâu là Service Ticket

Đáp án: IDc, IDss, T3, L2, Kc_ss

Câu 87: Xét mô hình mạng sau:




Giả sử Firewall chỉ cho phép kết nối ra Internet qua cổng 22. Người dùng trong WORK NET muốn kết nối tới Web Server. Hãy chọn phát biểu đúng A
Đáp án: Từ mỗi máy tại WORK NET thiết lập kết nối tới SSH Server, sử dụng Local Port Fortwarding để chuyển tiếp kết nối tới localhost:1234 sang 42.112.11.3:80, sau đó có thể kết nối tới WebServer bằng cách nhập vào trình duyệt có địa chỉ http://localhost:1234

Câu 88: số hiệu của giao thức ESP

Đáp án: RFC 2406 50

Câu 89: Xét mô hình kết nối sau:


Biết rằng một kết nối Ipsec ở chế độ Transport đã được thiết lập giữa 2 máy Web Client và Web Server. Hãy chọn phát biểu ĐÚNG NHẤT

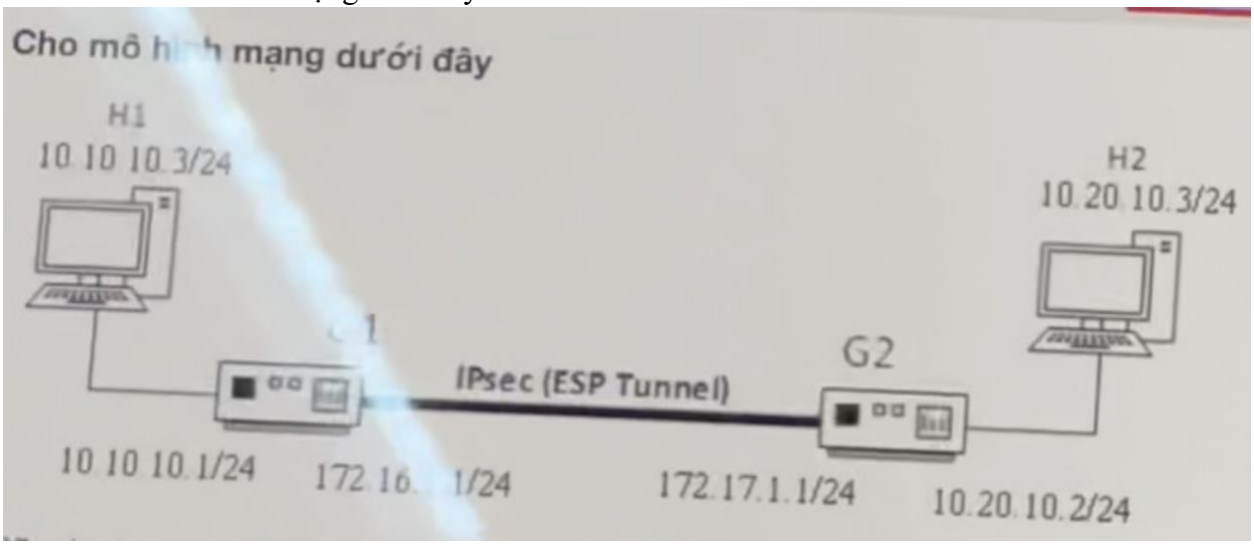
A. IPSec là trong suốt đối với tầng ứng dụng (Application) trong chồng giao thức TCP/IP nên trình duyệt và phần mềm máy chủ web không cần phải biết về sự tồn tại của IPSec

B. Cả trình duyệt trên web client và phần mềm máy chủ web trên web server phải được lập trình để hỗ trợ IPsec

C. Phần mềm máy chủ web trên web server phải được lập trình để hỗ trợ IPsec

D. Trình duyệt trên web client phải được lập trình để hỗ trợ IPsec

Câu 90: Cho mô hình mạng dưới đây:




Giữa 2 gateway G1 và G2, người ta thiết lập giao thức IPSec sử dụng ESP ở chế độ Tunnel. Hai gateway này kết nối với hai mạng LAN 10.10.10.0/24 và 10.20.10.0/24 với nhau. Xét một gói tin TCP được gửi từ H1 đến H2. Trong IP Header của gói tin IP tại H1, giá trị Soucre IP và Destination IP và Protocol là gì

A. 10.10.10.3, 172.17.1.1 và 1

B. 10.10.10.3, 10.20.10.3 và 6

C. 172.16.1.1, 10.20.10.3 và 1

D. 172.16.1.1. 172. 17.1.1 và 17

Câu 91: Chọn phát biểu đúng nhất về SA trong IPSec

A. Khi xử lý gói tin đi, một SA được xác định duy nhất bởi giá trị SPI, khi xử lí gói tin đến, một SA được xác định duy nhất bởi địa chỉ máy đích kết hợp với giao thức con IPSec cai nay phai la dia chi dich

B. Khi xử lý gói tin đi, một SA được xác định duy nhất bởi địa chỉ máy nguồn kết hợp với giao thức con IPSec, khi xử lí gói tin đến, một SA được xác định duy nhất bởi giá trị SPI

C. Khi xử lý gói tin đi, một SA được xác định duy nhất bởi địa chỉ máy nguồn kết hợp với giao thức con IPSec, khi xử lí gói tin đến, một SA được xác định duy nhất bởi giá trị SPI

D. Khi xử lý gói tin đi, một SA được xác định duy nhất bởi giá trị SPI, khi xử lí gói tin đến, một SA được xác định duy nhất bởi địa chỉ máy nguồn kết hợp với giao thức con IPSec

Câu 92: Đâu KHÔNG phải dịch vụ mà giao thức SSH-TRANS cung cấp

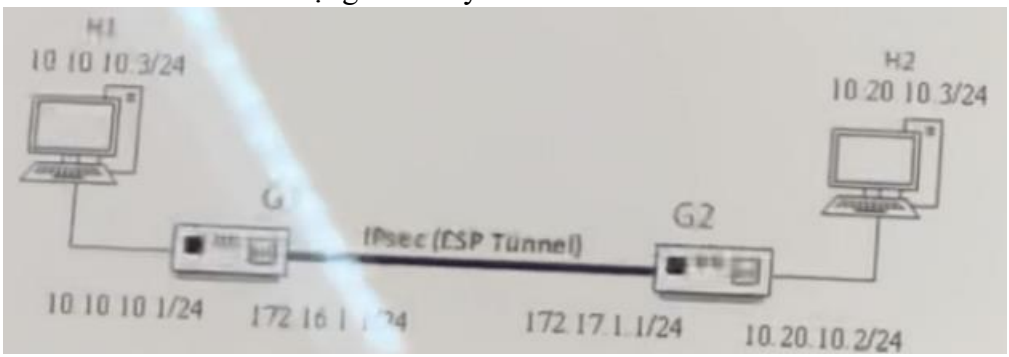
A. Nén dữ liệu

B. Xác thực SSH client

C. Xác thực SSH Server

D. Mã hóa dữ liệu

Câu 93: Cho mô hình mạng dưới đây




Giữa 2 gateway G1 và G2 ngta thiết lập giao thức IPSec sử dụng giao thức ESP ở chế độ Tunnel. Hai gateway này kết nối 2 mạng LAN 10.0.1.0/24 và 10.20.10.0/24 với nhau. Xét một gói tin TCP được gửi từ H1 đến H2. Trong IP Header của gói tin tại G1,trường Protocol có giá trị bằng bao nhiêu

Đáp án: 50

Câu 94: Chọn phát biểu ĐÚNG về CipherSuite trong giao thức SSL/TLS

A. Các phiên SSL/TLS mới hơn hỗ trợ các CipherSuite mà các phiên bản cũ hơn hỗ trợ

B. CipherSuite xác định thuật toán xác thực dữ liệu và khóa xác thực

C. Mỗi CipherSuite được hiển thị bởi một số nguyên 4 bit

D. CipherSuite xác định các thuật toán xác thực dữ liệu

Câu 95: Chọn phát biểu đúng về giao thức EAP

A. EAP không thể triển khai xác thực 2 chiều

B. EAP là giao thức xác thực sử dụng nonce và timestamp

C. EAP là giao thức bắt tay 3 bước

D. EAP là giao thức sử dụng nhiều phương thức xác thực khác nhau

Câu 96: Số hiệu cổng TCP mặc định của giao thức SSH

Đáp án : 22

Câu 97: Chọn mô tả ĐÚNG về MIME

A. MIME là một chuẩn Internet cho phép trao đổi các kiểu file dữ liệu khác nhau thông qua các thông điệp thư điện tử

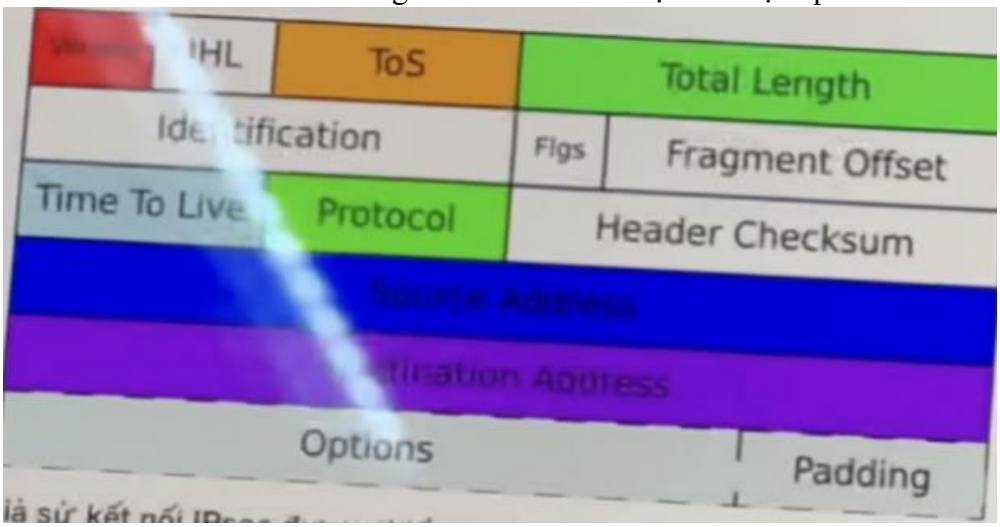
B. MIME cung cấp các giao thức truyền/nhận để định danh người gửi/nhận thông điệp

C. MIME cung cấp các giao thức truyền/nhận thư cơ chế xác thực dựa trên hàm băm và base64

D. MIME cung cấp các giao thức truyền/nhận thư để mã hóa các thông điệp

Câu 98: Giao thức con nào của IPSec có thể bảo vệ xác thực và toàn vẹn cho toàn bộ gói tin IP
Đáp án: AH

Câu 99: Cho biết cấu trúc của gói tin IP sau khi được bảo vệ kép bởi AH và ESP như sau




Đây là gói tin được bảo vệ bằng IPSec ở chế độ nào
Đáp án : Transport