HỌC VIỆN KTMM
PHÒNG KT&ĐBCLĐT

ĐỀ THI CHÍNH THỨC
(Đề thi có 10 trang)

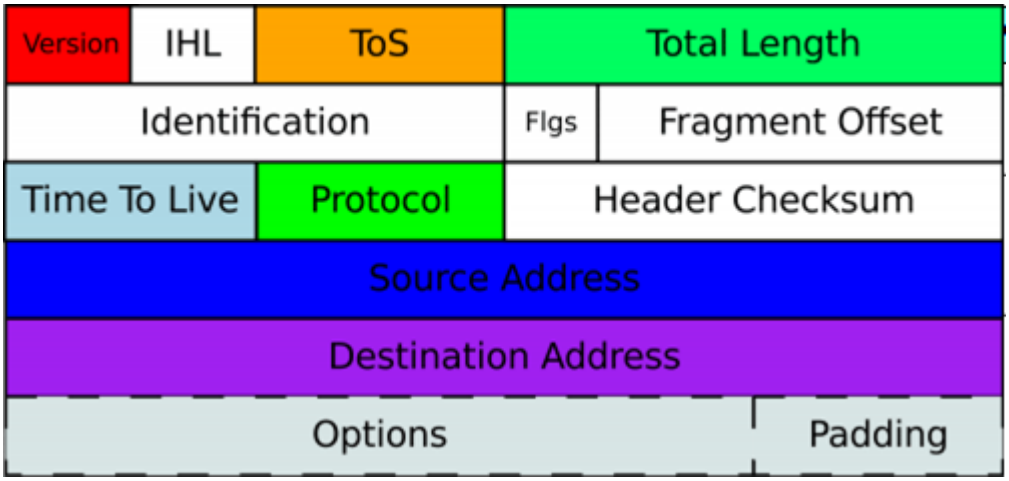
ĐỀ THI MẪU ĐỂ CÔNG BỐ
Môn thi: GIAO THỨC AN TOÀN MẠNG
Thời gian làm bài: 75 phút, không kể thời gian phát đề

Họ, tên thí sinh: .....
Số báo danh: .....

Mã đề thi 308

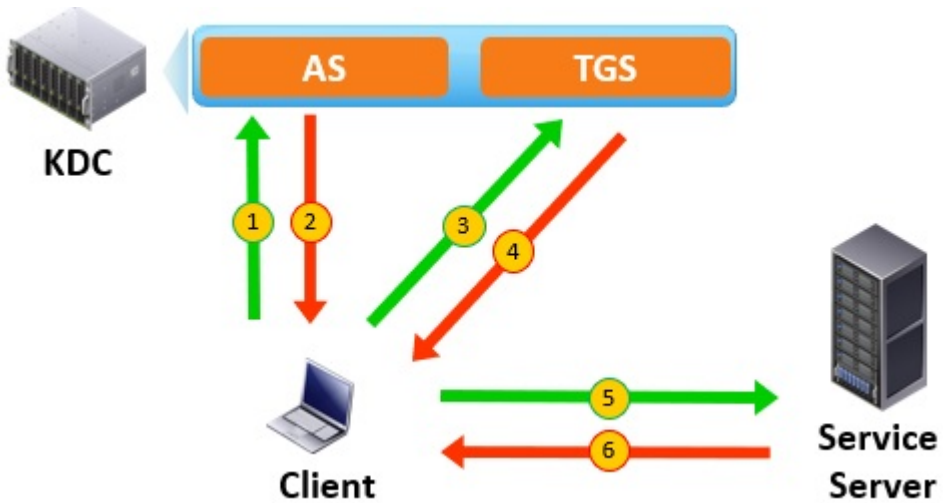
Câu 1. Một giao thức cho phép mail client gửi thư tới mail server, hoạt động trên cổng TCP mặc định là 465. Hãy cho biết tên viết tắt của giao thức.

Câu 2. Cho biết cấu trúc của IP Header như sau:



Giả sử kết nối 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 Protocol trong New IP Header.

Câu 3. Cho sơ đồ giao thức Kerberos như sau



1. C→AS: ID_C, ID_{TGS}
2. AS→C: $\{\{ID_C, ID_{TGS}, T_1, L_1, K_{C\_TGS}\}K_{AS\_TGS}, K_{C\_TGS}, T_1, L_1\}K_C$
3. C→TGS: $\{ID_C, ID_{TGS}, T_1, L_1, K_{C\_TGS}\}K_{AS\_TGS}, \{ID_C, T_2\}K_{C\_TGS}, ID_{SS}$
4. TGS→C: $\{\{ID_C, ID_{SS}, T3, L2, K_{C\_SS}\}K_{TGS\_SS}, K_{C\_SS}, T_3\}K_{C\_TGS}$
5. C→SS: $\{ID_C, ID_{SS}, T3, L2, K_{C\_SS}\}K_{TGS\_SS}$, $\{IDC, T_4\}K_{C\_SS}$

6. SS→C: $\{T_4+1\}K_{C\_SS}$

Hãy cho biết đâu là Service Ticket.

A. $ID_C, ID_{SS}, T_3, L_2, K_{C\_SS}$

B. $\{ID_C, ID_{SS}, T_3, L_2, K_{C\_SS}\}K_{TGS\_SS}$

C. $\{ID_C, ID_{TGS}, T_1, L_1, K_{C\_TGS}\}K_{AS\_TGS}$

D. $ID_C, ID_{TGS}, T_1, L_1, K_{C\_TGS}$

Câu 4. Chọn phát biểu đúng về CipherSuite trong giao thức SSL/TLS.

A. CipherSuite xác định thuật toán mật mã, khóa mật mã và thuật toán nén.

B. CipherSuite xác định các thuật toán mã hóa

C. CipherSuite xác định thuật toán mật mã và khóa mật mã

D. CipherSuite xác định thuật toán mật mã và thuật toán nén dữ liệu

Câu 5. Hãy chọn phát biểu ĐÚNG NHẤT về đại lượng "nonce" được sử dụng trong các giao thức xác thực.

A. Nonce là đại lượng để đảm bảo chống tấn công từ chối dịch vụ.

B. Nonce luôn là một số ngẫu nhiên có độ dài 128 bit.

C. Nonce là đại lượng để ddảm bảo tính tươi của thông điệp

D. Nonce chỉ được sinh bởi bên yêu cầu xác thực (Claimant)

Câu 6. 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:
(Ghi chú: Sinh viên ghi tên viết tắt của giao thức, ví dụ: EAP, TLS, TLS 1.2, ...)

Câu 7. Đâu là tên của một giao thức thiết lập khóa?

A. Diffie-Helman (DH)

B. Message Authentication Code (MAC)

C. Authenticated Encryption with Associated Data (AEAD)

D. Cipher Block Chaining (CBC)

Câu 8. Trong các giao thức an toàn mạng, đâu là phát biểu đúng về mật mã khóa đối xứng?

A. Mật mã khóa đối xứng sử dụng hai khóa khác nhau cho mã hóa/giải mã.

B. Mật mã khóa đối xứng có khả năng đảm bảo tính chống chối bỏ

C. Mật mã khóa đối xứng được sử dụng để tạo chứng thư số

D. Mật mã khóa đối xứng có tốc độ mã hóa/giải mã nhanh

Câu 9. Giao thức WEP được định nghĩa trong chuẩn nào sau đây?

A. 802.11 **B**. 802.15 **C**. 802.1x **D**. 802.11i

Câu 10. Trong sơ đồ xác thực sau:

Alice → Bob: "Alice"

Bob → Alice: $\{N_B\}K_P$

Alice → Bob: N_B

Bob: kiểm tra tính hợp lệ của N_B

Tham số K_P là tham số nào?

A. Khóa bí mật của Bob

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

C. Khóa công khai của Alice

D. Khóa công khai của Bob

Câu 11. Đâu là một điểm khác biệt giữa WEP và TKIP?

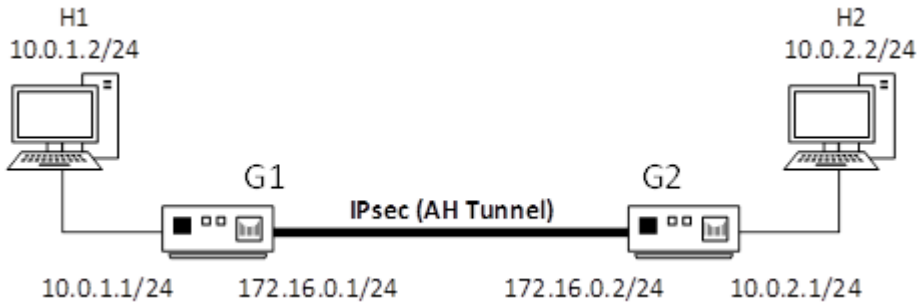
A. WEP không hỗ trợ giao thức xác thực EAP, còn TKIP có hỗ trợ EAP.

B. WEP sử dụng hàm kiểm tra CRC32, còn TKIP sử dụng hàm băm MD5.

C. WEP sử dụng hệ mật DES, còn TKIP sử dụng hệ mật AES.

D. WEP không thực hiện dẫn xuất khóa, còn TKIP thực hiện dẫn xuất khóa cho từng gói tin.

Câu 12. 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 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. Trường Next Header trong AH Header của gói tin IP tại G1 có giá trị bằng bao nhiêu?

Câu 13. Trong gói tin ServerHello của giao thức SSL Handshake, giá trị ngẫu nhiên (Random) mà Server gửi cho Client gồm bao nhiêu byte?

A. 32 **B**. 30 **C**. 28 **D**. 4

Câu 14. Tại sao mã xác thực thông báo (MAC) có thể xác thực được nguồn gốc của dữ liệu?

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

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

C. Vì trong MAC có sử dụng hàm băm.

D. Vì trong MAC có chứa định danh của cả người gửi và người nhận.

Câu 15. 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. Trình duyệt trên Web Client phải được lập trình để hỗ trợ SSL/TLS

B. 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.

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

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

Câu 16. Thứ tự thực hiện các giao thức con trong SSH là:

A. SSH-TRANS, SSH-AUTH, SSH-CONN

B. SSH-AUTH, SSH-TRANS, SSH-CONN

C. SSH-CONN, SSH-TRANS, SSH-AUTH

D. SSH-TRANS, SSH-CONN, SSH-AUTH

Câu 17. Chức năng AAA trong RADIUS có nghĩa là gì?

A. Authentication, Accounting, Auditing

B. Authentication, Authorization, Availability

C. Authentication, Authorization, Accounting

D. Authentication, Authority, Auditing

Câu 18. Câu 1. Hình dưới đây là ví dụ về loại cơ sở dữ liệu nào được sử dụng trong IPsec?

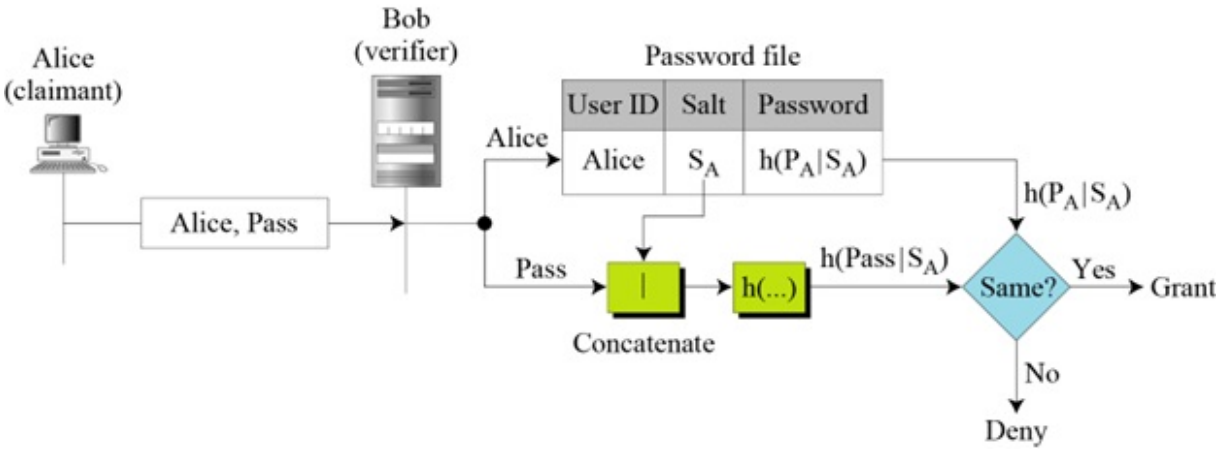
From	To	Protocol	Port	Policy
1.1.1.1	2.2.2.2	TCP	1000	ESP with 3DES
1.1.1.1	2.2.2.2	*	*	ESP with DES

Ghi chú: Sinh viên chỉ điền từ tiếng Anh, ví dụ: “XY database” hoặc “XYDB”, hoặc “XYD”.

Câu 19. Hãy cho biết số hiệu cổng TCP mặc định của giao thức TELNET (chỉ ghi phần số).

Câu 20. Cho sơ đồ giao thức xác thực bằng mật khẩu sau đây.

P_A: Alice's password
S_A: Alice's salt
Pass: Password sent by claimant



Hãy cho biết ý nghĩa của việc sử dụng "Salt" trong sơ đồ trên.

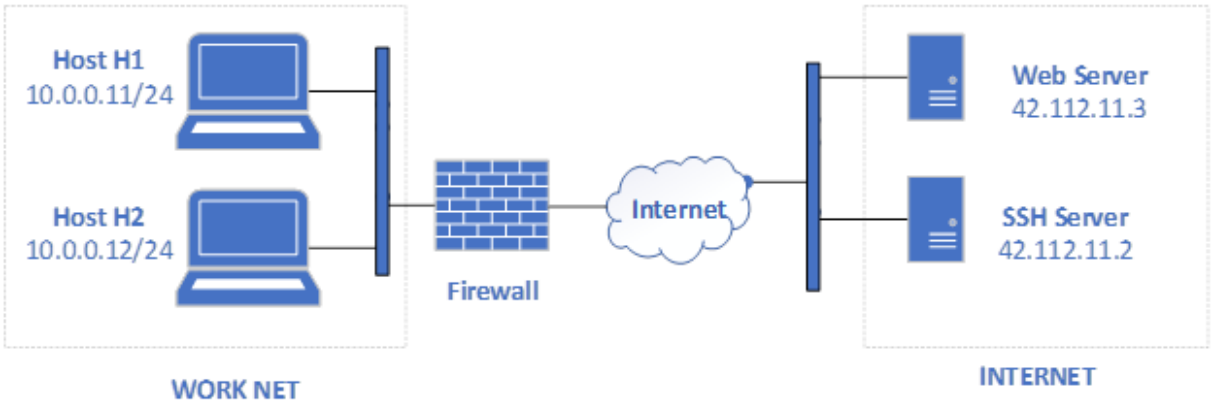
A. Chống lại các tấn công sử dụng bảng giá trị băm

B. Đóng vai trò như là một khóa mật mã để sử dụng khi băm (hash) mật khẩu của Alice.

C. Để làm tăng tính ngẫu nhiên cho mật khẩu của người dùng, bởi người dùng có xu hướng chọn mật khẩu dễ nhớ.

D. Chống lại tấn công từ điển khi thông tin về Alice trong "Password file" bị lộ.

Câu 21. Xét mô hình mạng sau đây



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. Từ máy H1 có thể thiết lập kết nối tới SSH Server, sử dụng Local Port Forwarding để chuyển tiếp kết nối tới localhost:1234 sang 42.112.11.3:80. Khi đó, mọi người dùng tại WORK NET có thể truy cập tới Web Server bằng cách nhập vào trình duyệt địa chỉ http://10.0.0.11:1234.

B. Từ mỗi máy tại WORK NET thiết lập kết nối tới SSH Server, sử dụng Local Port Forwarding để chuyển tiếp kết nối tới localhost:1234 sang 42.112.11.3:80; sau đó có thể kết nối tới Web Server bằng cách nhập vào trình duyệt địa

chỉ http://localhost:1234.

C. Từ máy H1 có thể thiết lập kết nối tới SSH Server, sử dụng Remote Port Forwarding để chuyển tiếp kết nối tới localhost:1234 sang 42.112.11.3:80. Khi đó, mọi người dùng tại WORK NET có thể truy cập tới Web Server bằng cách nhập vào trình duyệt địa chỉ http://10.0.0.11:1234.

D. Từ mỗi máy tại WORK NET thiết lập kết nối tới SSH Server, sử dụng Remote Port Forwarding để chuyển tiếp kết nối tới localhost:1234 sang 42.112.11.3:80; sau đó có thể kết nối tới Web Server bằng cách nhập vào trình duyệt địa chỉ http://localhost:1234.

Câu 22. Đâu KHÔNG phải khả năng mà giao thức SSH đem lại?

A. Mã hóa dữ liệu tầng Network

B. Mã hóa dữ liệu tầng ứng dụng

C. Xác thực dữ liệu

D. Nén dữ liệu

Câu 23. Chọn phát biểu đúng về giao thức EAP

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

B. EAP không thể triển khai xác thực 2 chiều.

C. EAP là giao thức bắt tay 3 bước.

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

Câu 24. Giao thức con IPsec nào mà ở chế độ Tunnel có khả năng đảm bảo tính xác thực cho toàn bộ gói tin IPsec?

A. ESP

B. Không có giao thức con nào như thế.

C. AH

D. Cả AH và ESP.

Câu 25. Người ta phân biệt hai loại Security Association (SA) khi nói về IPsec là:

A. SA dài hạn và SA ngắn hạn.

B. AH SA và ESP SA.

C. IPsec SA và IKE SA.

D. SA mã hóa và SA xác thực.

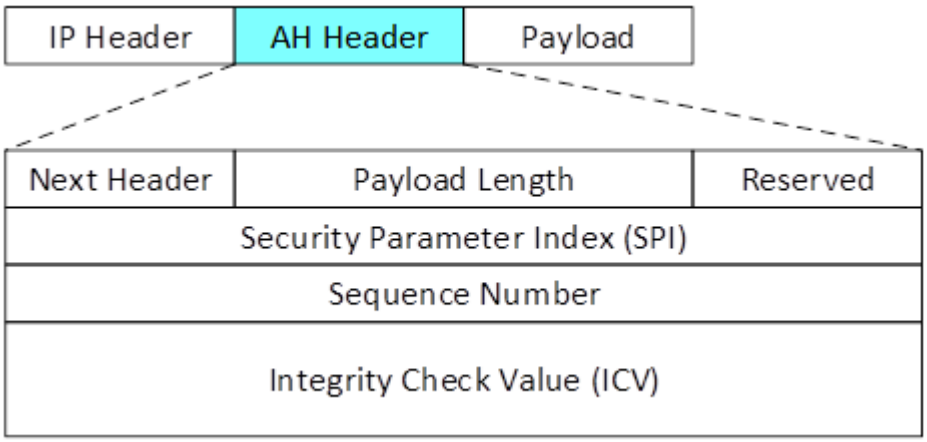
Câu 26. Giao thức nào sau đây KHÔNG phải giao thức VPN?

A. MPLS **B**. SSTP **C**. L2F **D**. PPP

Câu 27. Bạn được yêu cầu chọn một chế độ để mã khối hoạt động như một hệ mã dòng sử dụng trong một giao thức mạng, bạn sẽ chọn đáp án nào sau đây?

A. ECB **B**. CBC **C**. OFB **D**. CTS

Câu 28. Cho biết cấu trúc của gói tin AH IPsec 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 Next Header trong AH Header.

Câu 29. Đâu KHÔNG phải là một dịch vụ an toàn mạng?

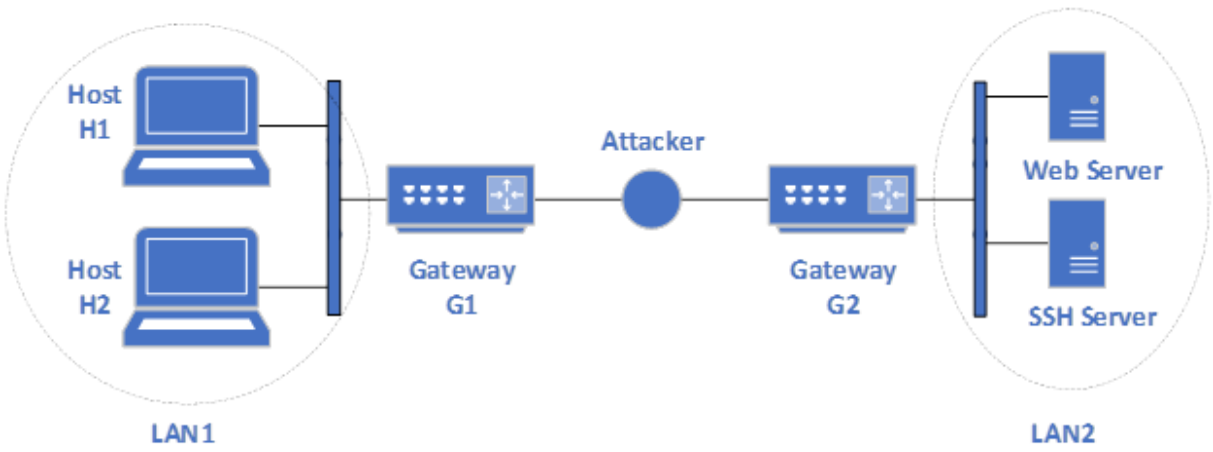
A. Xác thực **B**. Định danh **C**. Toàn vẹn **D**. Chống chối bỏ

Câu 30. Tấn công hủy xác thực (deauthentication attack) vào mạng không dây là loại tấn công nào sau đây?

A. Tấn công Brute-force **B**. Tấn công mật mã

C. Tấn công hạ cấp **D**. Tấn công từ chối dịch vụ

Câu 31. Xét mô hình kết nối sau:



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. Hãy chọn phát biểu đúng.

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

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

C. Dữ liệu trao đổi giữa các H1 và Web Server được đảm bảo bí mật tuyệt đối.

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

Câu 32. Độ dài của giá trị IV được sử dụng trong giao thức WPA là bao nhiêu?

A. 24 bit **B**. 128 bit **C**. 56 bit **D**. 48 bit

Câu 33. Trong IPsec, những thông tin nào có thể đồng thời có trong một Security Association?

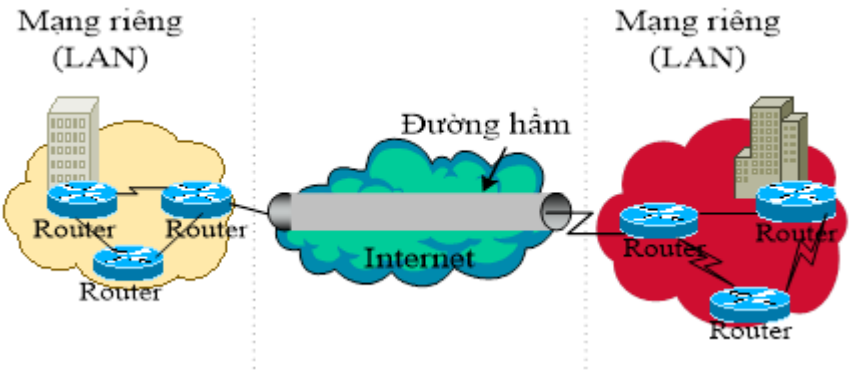
A. Thuật toán mã hóa, thuật toán xác thực dữ liệu, giao thức trao đổi khóa.

B. Thuật toán mã hóa, thuật toán xác thực dữ liệu, địa chỉ IP của 2 đầu mối của kết nối IPsec.

C. Thuật toán mã hóa, thuật toán xác thực dữ liệu, giao thức xác thực thực thể.

D. Thuật toán mã hóa, thuật toán xác thực dữ liệu, khóa để mã hóa và/hoặc xác thực dữ liệu.

Câu 34. Xét mô hình kết nối VPN sau sử dụng IPsec.



Hãy chọn phát biểu ĐÚNG.

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

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

C. Các chương trình ứng dụng phải được chỉnh sửa để hỗ trợ Ipsec.

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

Câu 35. Chọn phát biểu SAI về giao thức WEP?

A. WEP sử dụng phương pháp xác thực dựa trên khóa chia sẻ trước

B. WEP sử dụng giá trị IV dài 24 bit

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

D. WEP sử dụng thuật toán kiểm tra toàn vẹn Michael-64

Câu 36. Trong một giao thức an toàn mạng ở tầng Liên mạng (Internet) của chồng giao thức TCP/IP

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

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

C. 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.

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

Câu 37. Có một giao thức an toàn cho mạng không dây WLAN trong đó sử dụng RC4 để mã hóa, CRC32 để xác thực thông điệp. Tên viết tắt của giao thức này là:
(Ghi chú: Sinh viên ghi tên viết tắt của giao thức, ví dụ: EAP, TLS, TLS 1.2, ...)

Câu 38. Chọn phát biểu SAI về WPA2.

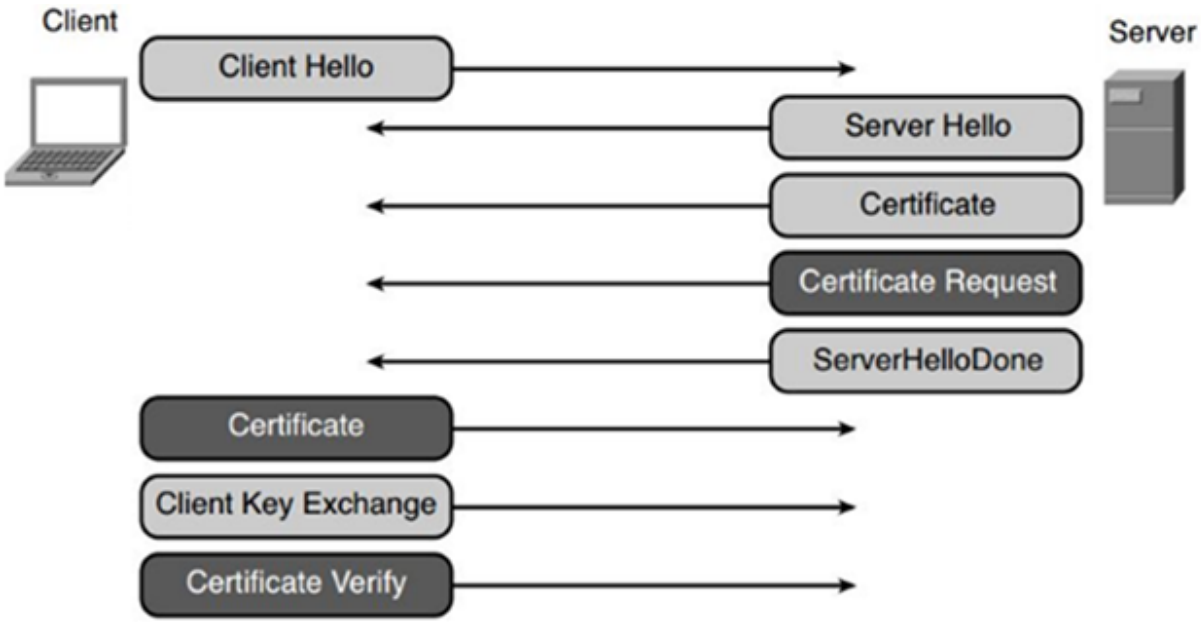
A. WPA2 sử dụng thuật toán mã hóa AES ở chế độ CCM.

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

C. WPA2 sử dụng giải pháp xác thực dựa trên 802.1x/EAP.

D. WPA2 sử dụng thuật toán kiểm tra toàn vẹn Michael-64

Câu 39. Trong các bước sau của giao thức SSL Handshake, khi nhận được thông điệp Certificate Verify của Client, Server sẽ xác thực Client bằng gì?



A. Khóa bí mật của Client

B. Chứng thư số của Server

C. Giá trị Pre-Master Key mà Client sinh ra

D. Chứng thư số của Client

Câu 40. Chọn mô tả đúng về chuẩn MIME?

A. MIME cung cấp các giao thức truyền/nhận thư cơ chế xác thực dựa trên hàm băm và base 64.

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

C. MIME là một chuẩn Internet cho phép trao đổi các kiểu file dữ liệu ở nhiều định dạng khác nhau thông qua các thông điệp thư điện tử.

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

Câu 41. Xác thực là

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

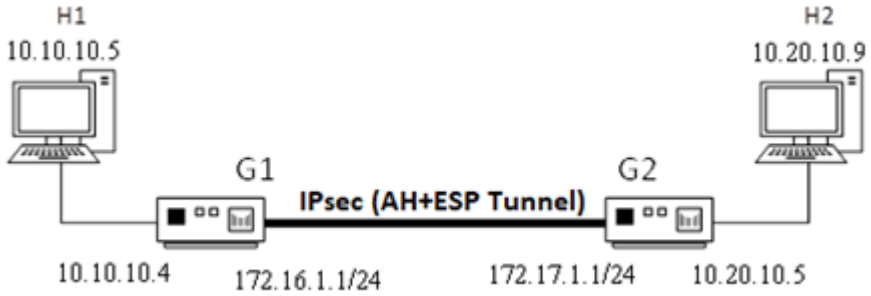
B.

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).

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

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

Câu 42. Cho sơ đồ mạng như sau:



Giữa hai gateway G1 và G2, người ta thiết lập giao thức IPsec sử dụng giao thức AH và ESP ở trên độ Tunnel. Hai gateway này kết nối hai mạng LAN 10.10.10.0/24 và 10.20.10.0/24 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. 10.10.10.5, 172.17.1.1 và 6

B. 172.16.1.1, 172.17.1.1 và 17

C. 10.10.10.5, 10.20.10.9 và 17

D. 172.16.1.1, 172.17.1.1 và 6

Câu 43. Hãy cho biết số hiệu của giao thức ESP

Câu 44. Sơ đồ sau mô tả phương pháp xác thực nào được sử dụng trong WLAN?

A. Xác thực mở rộng EAP

B. Xác thực dựa trên địa chỉ MAC

C. Xác thực dựa trên khóa chia sẻ trước

D. Xác thực mở

Câu 45. Chọn phát biểu SAI về giao thức SSH

A. Trong SSH luôn luôn yêu cầu xác thực 2 chiều.

B. SSH Server có thể được xác thực bằng mật khẩu hoặc khóa công khai.

C. Ở phía Client, SSH hỗ trợ xác thực từng người dùng hoặc xác thực máy trạm.

D. SSH Client có thể được xác thực bằng mật khẩu hoặc khóa công khai.

---------- *Hết* ----------