**Đề thi mẫu**

* + - * 1. Tấn công phát lại thông báo (Replay Attack)

Là việc kẻ tấn công thu một thông báo trong một phiên liên lạc hợp lệ, sau đó lợi dụng thông báo đó để giả mạo một trong các bên liên lạc.

Là việc kẻ tấn công giả mạo một trong hai bên liên lạc; khi bên kia gửi tới thông báo nào thì kẻ tấn công gửi lại đúng thông báo đó.

Là việc kẻ tấn công đứng giữa hai bên liên lạc; khi một bên gửi đi một thông báo, kẻ tấn công sẽ thu được, chỉnh sửa theo ý mình và gửi lại cho bên kia.

Là việc kẻ tấn công đứng giữa hai bên liên lạc; khi một bên gửi đi một thông báo, kẻ tấn công sẽ thu lại để tìm hiểu nội dung, đồng thời gửi lại cho bên kia mà không có sự thay đổi nào.

* + - * 1. Bạn được yêu cầu chọn các thuật toán mật mã khóa bí mật để sử dụng trong một giao thức mạng, bạn sẽ chọn các thuật toán nào sau đây?

RC4, AES

RSA, SHA1

3DES, CRT

Elgamal, DES

* + - * 1. Chọn phát biểu ĐÚNG NHẤT về giao thức an toàn mạng.

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

Trong chồng giao thức TCP/IP, khi áp dụng triển khai các cơ chế an toàn bằng cách thay đổi các 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.

Trong chồng giao thức TCP/IP, khi áp triển khai các cơ chế an toàn bằng cách thay đổi các 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.

Trong chồng giao thức TCP/IP, khi áp triển khai các cơ chế an toàn bằng cách thay đổi các 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.

* + - * 1. Tại sao mã xác thực thông báo (MAC) có thể xác thực được nguồn gốc của dữ liệu?

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

Vì trong MAC có sử dụng hàm băm.

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

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

* + - * 1. Trong các giao thức an toàn mạng, mật mã khóa công khai KHÔNG giúp đảm bảo tính chất an toàn nào của thông tin?

Tính khả dụng.

Tính bí mật.

Tính toàn vẹn.

Tính xác thực.

* + - * 1. Xác thực là

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

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).

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).

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

* + - * 1. Chọn phát biểu đúng về giao thức EAP

Kiến trúc phân tầng của EAP gồm: tầng phương thức xác thực EAP, tầng EAP, tầng datalink

Kiến trúc phân tầng của EAP gồm: tầng phương thức xác thực EAP, tầng network, tầng datalink

Kiến trúc phân tầng của EAP gồm: tầng phương thức ủy quyền EAP, tầng EAP, tầng datalink

Kiến trúc phân tầng của EAP gồm: tầng phương thức ủy quyền EAP, tầng Internet, tầng datalink

* + - * 1. Hãy chọn phát biểu ĐÚNG NHẤT về đại lượng “nonce” được sử dụng trong các giao thức xác thực.

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

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

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.

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.

**Câu 9.** Trong sơ đồ xác thực sau:

1. Alice → Bob: "Alice", TA, sigA(TA)
2. Bob:

− Kiểm tra tính hợp lệ của TA

− Kiểm tra chữ ký;

− Chấp nhận nếu chữ ký hợp lệ;

Trong bước 2, Bob sử dụng khóa nào để kiểm tra chữ ký?

Khóa công khai của Alice

Khóa bí mật của Alice

Khóa công khai của Bob

Khóa bí mật của Bob

**Câu 10.** Chọn phát biểu đúng về giao thức PAP (Password Authentication Protocol).

PAP là giao thức xác thực 1 chiều

PAP sử dụng tham số nonce

Không thể thực hiện xác thực hai chiều bằng giao thức PAP

PAP là giao thức xác thực dạng thách đố-giải đố

**Câu 11**. 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.

Khóa K có thời hạn sử dụng nhất định; trong thời hạn đó, Alice có thể thiết lập số phiên liên lạc tùy ý với Bob.

Khóa K chỉ được sử dụng cho một phiên liên lạc; phiên liên lạc đó phải được diễn ra trong một thời hạn nhất định.

Alice có thể sử dụng khóa K trong khoảng thời gian tùy ý để thiết lập số phiên liên lạc tùy ý với Bob.

Mỗi khi muốn liên lạc với Bob, Alice gửi yêu cầu tới Sandy để được cung cấp khóa K cho phiên liên lạc; nhờ vậy Alice không cần phải ghi nhớ thông tin nào về khóa để liên lạc với Bob.

**Câu 12.** Chọn phát biểu đúng về giao thức EAP

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

EAP là giao thức xác thực sử dụng nonce và timestamp

EAP không thể triển khai xác thực 2 chiều.

EAP là giao thức bắt tay 3 bước.

**Câu 13**. 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 chỉ trong một chi nhánh

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

**Câu 14**. Hãy cho biết số hiệu của giao thức AH

Đáp án: {51}

**Câu 15.** Mỗi đầu mối IPsec phải duy trì một cơ sở dữ liệu thông tin để khi có một gói tin cần được xử lý bằng IPsec thì biết được cần xử lý như thế nào. Hãy cho biết tên viết tắt của cơ sở dữ liệu đó.

Đáp án: {SAD}

**Câu 16.** Chế độ Transport trong IPsec hoạt động ở trường hợp nào sau đây?

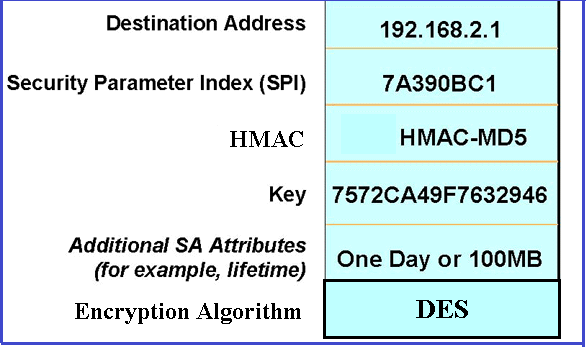
A.Host-to-host

B.Gateway-to-Gateway

C.Host-to-Gateway

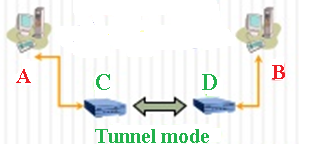
D.Router-to-Router

**Câu 17.** Hình dưới đây là ví dụ về loại SA nào được sử dụng trong IPsec?



Đáp án: {IKE SA}

**Câu 18.** Cho sơ đồ sau.



Và một cơ sở dữ liệu được IPsec sử dụng như sau:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **From** | **To** | **Protocol** | **Port** | **Policy** |
| **A** | **B** | **Any** | **Any** | **AH[HMAC-MD5]** |

Hãy chọn một đáp án đúng.

A.Đây là CSDL SPD của A

B.Đây là CSDL SAD của A

C.Đây là CSDL SPD của B

D.Đây là CSDL SAD của C

**Câu 19**. Cho biết cấu trúc của gói tin AH IPsec như sau:



Giả sử kết nối IPsec được thiết lập ở chế độ Tunnel 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.

Đáp án: {4}

**Câu 20.** Cho biết cấu trúc của gói tin ESP IPsec 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 Next Header trong ESP Trl.

Đáp án: {6}

**Câu 21**. 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?

Trả lời: {4}

**Câu 22**. 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. Trong IP Header của gói tin IP tại G1, các giá trị Source IP và Destination IP là gì?

A. 172.16.0.1, 172.16.0.2

B. 10.0.1.2, 172.16.0.2

C. 10.0.1.2, 10.0.2.2

D. 172.16.0.1, 10.0.2.2

**Câu 23**. Giao thức SSL cung cấp những dịch vụ nào sau đây?

Bí mật, Toàn vẹn, Nén dữ liệu

Bí mật, Toàn vẹn, Chống chối bỏ

Bí mật, Xác thực, Chống chối bỏ

Bí mật, Chống chối bỏ, Nén dữ liệu

**Câu 24**. Chọn phát biểu đúng về hoạt động của giao thức SSL Handshake?

A. Trong SSL Handshake, Server bắt buộc phải gửi Certificate của mình sang Client, Client không bắt buộc gửi Certificate sang cho Server

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

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

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

**Câu 25.** Chọn phát biểu đúng về khóa phiên trong SSL/TLS trong trường hợp sử dụng trao đổi khóa RSA.

A. 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.

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

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

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

**Câu 26**. Một giao thức liên lạc giữa mail client và mail server, hoạt động trên cổng TCP mặc định là 993. Hãy cho biết tên viết tắt của giao thức.

Đáp án: {IMAPS; imaps}

**Câu 27.** Đâu KHÔNG phải giao thức an toàn cho thư điện tử?

SMTP

IMAPS

POP3S

ESMTP

**Câu 28**. Hãy cho biết số hiệu cổng TCP mặc định của giao thức SSH (chỉ ghi phần số).

Đáp án: {22}

**Câu 29.** Thứ tự thực hiện các giao thức con trong SSH là:

SSH-TRANS, SSH-AUTH, SSH-CONN

SSH-AUTH, SSH-TRANS, SSH-CONN

SSH-CONN, SSH-TRANS, SSH-AUTH

SSH-TRANS, SSH-CONN, SSH-AUTH

**Câu 30.** Sau khi kết thúc giao thức SSH-TRANS, giữa SSH Server và SSH Client

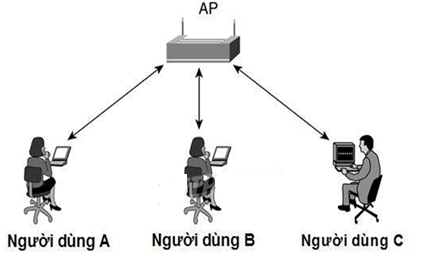
thỏa thuận được 4 khóa phiên đối xứng. Trong đó 2 khóa được sử dụng để mã hóa và xác thực thông điệp từ Server tới Client, 2 khóa được sử dụng để mã hóa và xác thực thông điệp từ Client đến Server.

thỏa thuận được 1 khóa phiên đối xứng để mã hóa và xác thực thông điệp trao đổi sau đó giữa Server và Client.

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.

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.

**Câu 31**. Sơ đồ sau đây mô tả mạng WLAN nào?



A. BSS

ESS

CSS

Ad-hoc

**Câu 32.** Trong giao thức WEP, tên viết tắt của thuật toán mật mã được sử dụng để mã hóa dữ liệu giữa Access Point và các máy trạm là:

Đáp án: {RC4}.

**Câu 33.** Giao thức WEP được định nghĩa trong chuẩn nào sau đây?

802.11

802.11i

802.1x

802.15

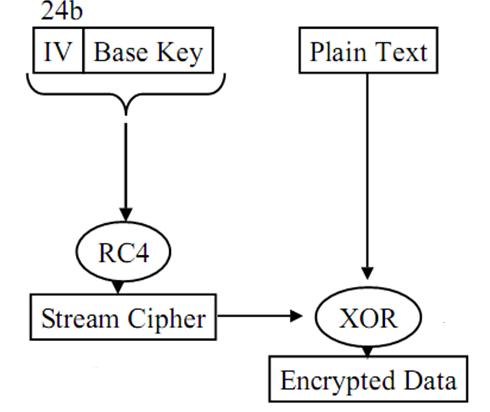
**Câu 34.** Sơ đồ mã hóa sau đây mô tả về giao thức WLAN nào?

WEP

WPA

WPA2

TKIP



**Câu 35.** Vào năm 2004, sau khi chuẩn IEEE 802.11i được chính thức ban hành, Wi-Fi Alliance đã đưa ra 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 36**. Chế độ mã hóa dựa trên AES được thực thi trong WPA2 là?

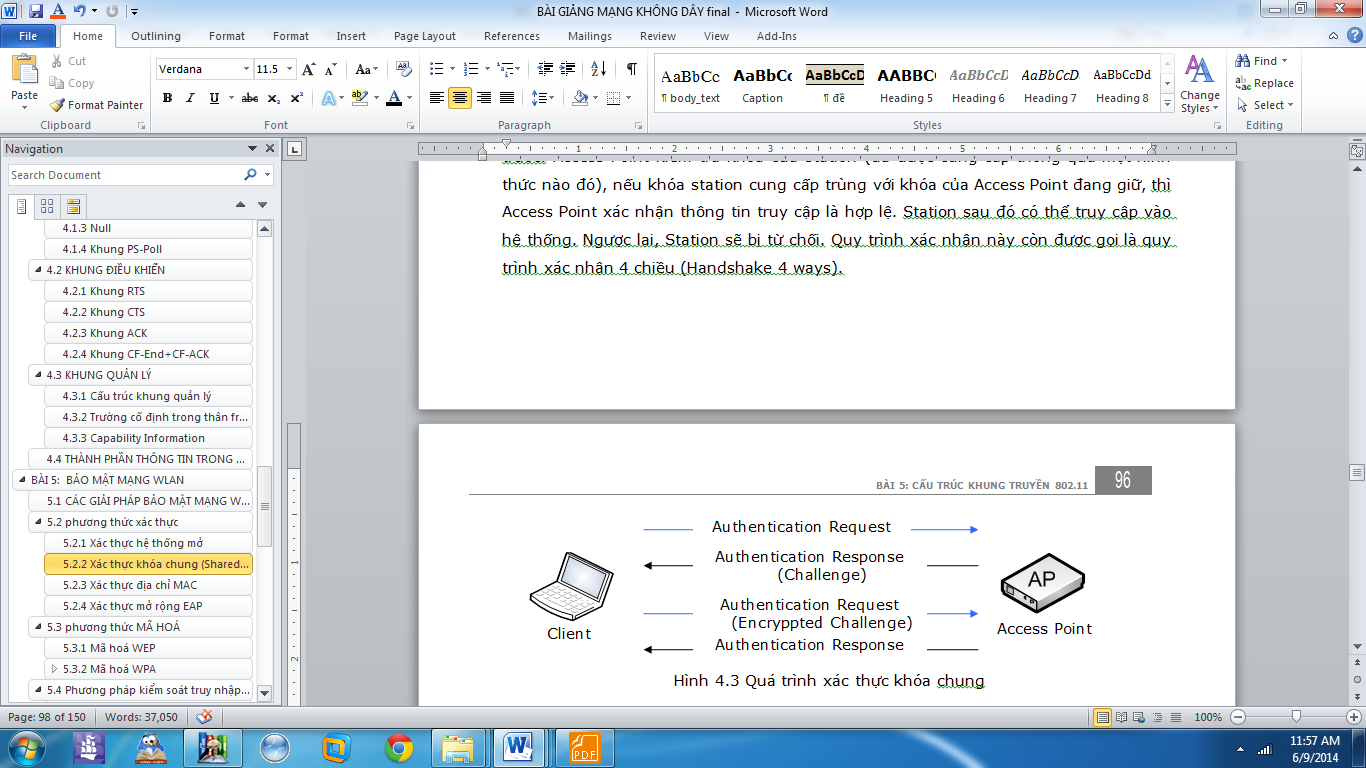
CCMP

CBC

ECB

TKIP

**Câu 37.** Sơ đồ sau mô tả phương pháp xác thực nào được sử dụng trong WLAN?



Xác thực dựa trên khóa chia sẻ trước

Xác thực dựa trên địa chỉ MAC

Xác thực mở

Xác thực mở rộng EAP

**Câu 38.** 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:

Đáp án: {WEP}.

**Câu 39**. Chọn phát biểu SAI về giao thức WPA?

WPA sử dụng thuật toán kiểm tra toàn vẹn CRC32

WPA sử dụng thuật toán mã hóa dữ liệu RC4

WPA sử dụng phương pháp xác thực dựa trên khóa chia sẻ trước

WPA sử dụng giá trị IV dài 48 bit

**Câu 40.** Chọn phát biểu SAI về WPA2.

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

WPA2 bắt buộc hỗ trợ mã hóa bằng AES.

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

WPA2 hỗ trợ xác thực bằng giao thức EAP.

**Câu 41.** Trong một giao thức an toàn mạng ở tầng Liên mạng (Internet) của chồng giao thức TCP/IP

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

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.

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

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.

**Câu 42**. 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.

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

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

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

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

**Câu 43.** 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 SAI.

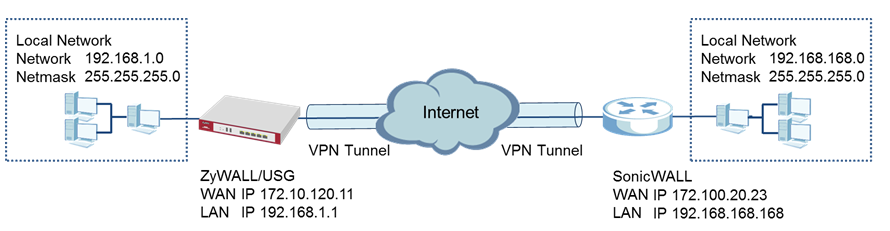
Việc triển khai SSL/TLS là hoàn toàn trong suốt với tầng ứng dụng trong mô hình TCP/IP

Trình duyệt trên Web Client phải được cài đặt để hỗ trợ SSL/TLS

Phần mềm máy chủ web trên Web Server phải được cài đặt để hỗ trợ SSL/TLS.

Cả hai hai bên trình duyệt trên Web Client và phần mềm máy chủ web trên Web Server phải được cài đặt để hỗ trợ SSL/TLS.

**Câu 44.** Xét mô hình kết nối VPN sau sử dụng IPsec.



Hãy chọn phát biểu ĐÚNG.

Có thể triển khai IPsec cho mô hình mạng trên ở chế độ Tunnel.

Có thể triển khai IPsec cho mô hình mạng trên ở chế độ Transport

Không thể triển khai IPsec ở chế độ Tunnel.

Không thể triển khai IPsec ở cả hai chế độ Transport và Tunnel.

**Câu 45.** 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.

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.

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.

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.

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.