BAN CƠ YẾU CHÍNH PHỦ

HỌC VIỆN KỸ THUẬT MẬT MÃ

NGUYỄN VĂN AN, TRẦN THỊ BÌNH

NGÂN HÀNG CÂU HỎI THI TRẮC NGHIỆM

GIAO THỨC BẢO MẬT MẠNG MÁY TÍNH

Hà Nội, 2022

MỤC LỤC

PHẦN I. TỔNG HỢP CÁC PHẦN NỘI DUNG MÔN HỌC

Môn học: Giao thức bảo mật mạng máy tính

Khoa: Bảo mật thông tin

Các chương trình đào tạo có sử dụng môn học:

P1: ĐH Chính quy Bảo mật thông tin

P2: Các chương trình đào tạo ngành Công nghệ thông tin

Các phần nội dung môn học trong các chương trình đào tạo:

TT	Phần nội dung	P1	P2
1	Tổng quan về giao thức bảo mật mạng máy tính	☑	☑
2	Giao thức bảo mật tầng ứng dụng	☑	☑
3	Giao thức bảo mật tầng giao vận	☑	☑
4	Giao thức bảo mật tầng mạng	☑	☑
5	Giao thức bảo mật tầng truy nhập mạng	☑	☑

PHẦN II. TRÍCH LƯỢC ĐỀ CƯƠNG CHI TIẾT MÔN HỌC

1. Thông tin chung

Tên học phần	Giao thức bảo mật mạng máy tính
Tên tiếng Anh	Network Security Protocols
Số tín chỉ	2
Học phần học trước	Mạng máy tính

2. Mục tiêu học phần

2.1. Mục tiêu chung

Học phần này cung cấp kiến thức tổng quan về an toàn mạng máy tính, kiến thức về các giao thức xác thực, kiến thức về các giao thức an toàn mạng riêng ảo, kiến thức về các giao thức an toàn dịch vụ, kiến thức về các giao thức an toàn mạng không dây và một số giao thức khác.

2.2. Mục tiêu cụ thể

Mục tiêu	Mô tả
M1	Trình bày được đặc điểm của các giao thức bảo mật mạng máy tính tiêu biểu
M2	Trình bày được hoạt động của các giao thức bảo mật mạng máy tính tiêu biểu
M3	Giải thích được cơ chế bảo mật trong các giao thức bảo mật mạng máy tính
M4	Lựa chọn được giao thức, mô hình triển khai giao thức để giải quyết yêu cầu bảo mật mạng máy tính cụ thể.
M5	Trình bày được các yêu cầu đối với việc thiết kế giao thức bảo mật mạng máy tính

3. Mô tả học phần

Học phần này trước hết giới thiệu tổng quan về an toàn mạng, bao gồm: Tầm quan trọng của an toàn máy tính và an toàn mạng,các kiểu tấn công mạng cơ bản, các kỹ thuật và dịch vụ an toàn, mô hình an toàn mạng, các giao thức an toàn mạng. Tiếp đó, học phần trình bày về các giao thức xác thực gồm: PAP/CHAP, Kerberos, EAP, Radius, 802.1x. Phần tiếp theo trình bày về các giao thức an toàn mạng riêng ảo: PPTP, L2TP, SSL-VPN, IPSEC-VPN. Sau đó, học phần trình bày về về các giao thức an toàn dịch vụ: S/MIME, PGP, HTTPS, SFTP, FTPS, SSH, v.v. Cuối cùng học phần trình bày về các giao thức an toàn mạng không dây: Tổng quan về mạng không dây, các cơ chế an toàn trong WLAN, các giao thức an toàn WEP, WPA, WPA2 (802.11i) và WTLS.

4. Nội dung học phần

Chương 1. Tổng quan giao thức bảo mật mạng máy tính (3 LT)

1.1. Tầm quan trọng của an toàn máy tính và an toàn mạng

1.2. Các kiểu tấn công mạng

Chương 2. Giao thức bảo mật tầng ứng dụng (3 LT)

2.1. Tổng quan về giao thức xác thực

2.2. Các giao thức PAP/CHAP

2.3. Giao thức Kerberos

Chương 3. Giao thức bảo mật tầng giao vận (9 LT)

3.1. Tổng quan về các giao thức mạng riêng ảo

3.2. Các giao thức mạng riêng ảo tầng 2

3.3. Giao thức mạng riêng ảo tầng 3

Chương 4. Giao thức bảo mật tầng mạng (3 LT)

4.1. Các giao thức an toàn thư điện tử

4.2. Giao thức an toàn dịch vụ Web (HTTPS)

4.3. Giao thức an toàn cho đăng nhập từ xa (SSH)

4.4. Các giao thức truyền file an toàn

Chương 5. Giao thức bảo mật tầng truy nhập mạng (6 LT)

5.1. Tổng quan về mạng không dây

5.2. Các cơ chế an toàn trong mạng WLAN

5.3. Các giao thức an toàn cho mạng WLAN

Chương 6. Thiết kế giao thức bảo mật mạng (6 LT)

6.1. Quy trình thiết kế giao thức bảo mật mạng máy tính.

6.2. Yêu cầu đối với việc thiết kế giao thức bảo mật mạng máy tính.

6.3. Phân tích, đánh giá giao thức bảo mật mạng máy tính.

PHẦN III. PHÂN RÃ CHUẨN ĐẦU RA HỌC PHẦN

1. Các chuẩn đầu ra được đánh giá

TT	Ký hiệu	Chuẩn đầu ra	P1	P2
1	CLO1	Trình bày được đặc điểm, hoạt động của các giao thức bảo mật mạng máy tính	☑	☑
2	CLO2	Giải thích được cơ chế bảo mật trong các giao thức bảo mật mạng máy tính	☑	☑
3	CLO3	Lựa chọn được giao thức, mô hình triển khai giao thức để giải quyết yêu cầu bảo mật mạng máy tính cụ thể.	☑	☑

2. Các nhóm câu hỏi

TT	Ký hiệu	Nhóm câu hỏi	Cấp độ	Gốc	Dẫn xuất
1	1	CLO1. TRÌNH BÀY ĐƯỢC ĐẶC ĐIỂM, HOẠT ĐỘNG CỦA CÁC GIAO THỨC BẢO MẬT MẠNG MÁY TÍNH			
2	1.1	Phân loại giao thức bảo mật mạng	NB	25	0
3	1.2	Đặc điểm của giao thức tầng ứng dụng	NB	12	8
4	1.3	Đặc điểm của giao thức tầng giao vận	NB	12	8
5	1.4	Đặc điểm của giao thức tầng mạng	NB	12	8
6	1.5	Đặc điểm của giao thức tầng truy nhập mạng	NB	12	8
7	1.6	Hoạt động của giao thức tầng ứng dụng	TH	15	5
8	1.7	Hoạt động của giao thức tầng giao vận	TH	15	5
9	1.8	Hoạt động của giao thức tầng mạng	TH	15	5
10	1.9	Hoạt động của giao thức tầng truy nhập mạng	TH	15	5
11	2	CLO2. GIẢI THÍCH ĐƯỢC CƠ CHẾ BẢO MẬT TRONG CÁC GIAO THỨC BẢO MẬT MẠNG MÁY TÍNH			
12	2.1	Ứng dụng mật mã trong các giao thức bảo mật mạng	TH	10	0
13	2.2	Cơ chế bảo mật trong giao thức tầng ứng dụng	VD	15	5
14	2.3	Cơ chế bảo mật trong giao thức tầng giao vận	VD	15	5
15	2.4	Cơ chế bảo mật trong giao thức tầng mạng	VD	15	5
16	2.5	Cơ chế bảo mật trong giao thức tầng truy nhập mạng	VD	15	5
17	3	CLO3. LỰA CHỌN GIAO THỨC, MÔ HÌNH TRIỂN KHAI GIAO THỨC ĐỂ GIẢI QUYẾT YÊU CẦU BẢO MẬT MẠNG MÁY TÍNH CỤ THỂ			
18	3.1	Tình huống 1: Kết nối mạng văn phòng nhỏ với Internet	VD	15	0

TT	Ký hiệu	Nhóm câu hỏi	Cấp độ	Gốc	Dẫn xuất
19	3.2	Tình huống 2: Kết nối mạng doanh nghiệp (LAN, DMZ) với Internet	VD	15	0
20	3.3	Tình huống 3: Kết nối nhiều chi nhánh của doanh nghiệp qua Internet	VD	15	0
Tổng				**72**	**73**

PHẦN IV. MA TRẬN ĐỀ THI

1. Chương trình ĐH Chính quy Bảo mật thông tin (P1)

Tổng số câu hỏi: 50 câu. Thời gian làm bài: 60 phút.

Tài liệu được phép sử dụng: Không

Cấu trúc đề thi:

Ký hiệu	Nhóm câu hỏi	Cấp độ	Tổng số	Số lượng	Hệ số điểm
1	CLO1. TRÌNH BÀY ĐƯỢC ĐẶC ĐIỂM, HOẠT ĐỘNG CỦA CÁC GIAO THỨC BẢO MẬT MẠNG MÁY TÍNH				
1.1	Phân loại giao thức bảo mật mạng	NB	20	2	1
1.2	Đặc điểm của giao thức tầng ứng dụng	NB	20	2	1
1.3	Đặc điểm của giao thức tầng giao vận	NB	20	2	1
1.4	Đặc điểm của giao thức tầng mạng	NB	25	2	1
1.5	Đặc điểm của giao thức tầng truy nhập mạng	NB	25	2	1
1.6	Hoạt động của giao thức tầng ứng dụng	TH	30	3	1
1.7	Hoạt động của giao thức tầng giao vận	TH	25	3	1
1.8	Hoạt động của giao thức tầng mạng	TH	25	4	1
1.9	Hoạt động của giao thức tầng truy nhập mạng	TH	30	4	1
2	CLO2. GIẢI THÍCH ĐƯỢC CƠ CHẾ BẢO MẬT TRONG CÁC GIAO THỨC BẢO MẬT MẠNG MÁY TÍNH				
2.1	Ứng dụng mật mã trong các giao thức bảo mật mạng	TH	20	5	1
2.2	Cơ chế bảo mật trong giao thức tầng ứng dụng	VD	20	3	1
2.3	Cơ chế bảo mật trong giao thức tầng giao vận	VD	20	3	1
2.4	Cơ chế bảo mật trong giao thức tầng mạng	VD	20	3	1
2.5	Cơ chế bảo mật trong giao thức tầng truy nhập mạng	VD	20	3	1
3	CLO3. LỰA CHỌN GIAO THỨC, MÔ HÌNH TRIỂN KHAI ĐỂ GIẢI QUYẾT YÊU CẦU BẢO MẬT MẠNG MÁY TÍNH CỤ THỂ				
3.1	Tình huống 1: Kết nối mạng văn phòng nhỏ với Internet	VD	15	3	1
3.2	Tình huống 2: Kết nối mạng doanh nghiệp (LAN, DMZ) với Internet	VD	15	3	1
3.3	Tình huống 3: Kết nối nhiều chi nhánh của doanh nghiệp qua Internet	VD	15	3	1

Ký hiệu	Nhóm câu hỏi	Cấp độ	Tổng số	Số lượng	Hệ số điểm
Tổng số câu hỏi trong đề thi				**50**	

Thống kê tỉ lệ các nhóm câu hỏi trong ma trận[1]

CLO / Cấp độ	CLO1	CLO2	CLO3	**Tổng theo cấp độ**	**Tỉ lệ theo cấp độ**
NB	10			**10**	**20%**
TH	14	5		**19**	**34%**
VD		12	9	**21**	**42%**
Tổng theo CLO	**24**	**17**	**9**		
Tỉ lệ theo CLO	**48%**	**34%**	**18%**		

2. Các chương trình đào tạo ngành Công nghệ thông tin (P2)

Tổng số câu hỏi: 50 câu. Thời gian làm bài: 60 phút.

Tài liệu được phép sử dụng: Không

Cấu trúc đề thi:

Ký hiệu	Nhóm câu hỏi	Cấp độ	Tổng số	Số lượng	Hệ số điểm
1	CLO1. TRÌNH BÀY ĐƯỢC ĐẶC ĐIỂM, HOẠT ĐỘNG CỦA CÁC GIAO THỨC BẢO MẬT MẠNG MÁY TÍNH				
1.1	Phân loại giao thức bảo mật mạng	NB	20	2	1
1.2	Đặc điểm của giao thức tầng ứng dụng	NB	20	2	1
1.3	Đặc điểm của giao thức tầng giao vận	NB	20	2	1
1.4	Đặc điểm của giao thức tầng mạng	NB	25	2	1
1.5	Đặc điểm của giao thức tầng truy nhập mạng	NB	25	2	1
1.6	Hoạt động của giao thức tầng ứng dụng	TH	30	3	1
1.7	Hoạt động của giao thức tầng giao vận	TH	25	3	1
1.8	Hoạt động của giao thức tầng mạng	TH	25	3	1
1.9	Hoạt động của giao thức tầng truy nhập mạng	TH	30	3	1
2	CLO2. GIẢI THÍCH ĐƯỢC CƠ CHẾ BẢO MẬT TRONG CÁC GIAO THỨC BẢO MẬT MẠNG MÁY TÍNH				
2.1	Ứng dụng mật mã trong các giao thức bảo mật mạng	TH	20	6	1
2.2	Cơ chế bảo mật trong giao thức tầng ứng dụng	VD	20	2	1

[1] Ví dụ này cho thấy có sự chênh lệch đáng kể về số lượng các câu hỏi để đánh giá các CLO. Cụ thể là có quá ít số câu hỏi để đánh giá CLO3.

Ký hiệu	Nhóm câu hỏi	Cấp độ	Tổng số	Số lượng	Hệ số điểm
2.3	Cơ chế bảo mật trong giao thức tầng giao vận	VD	20	2	1
2.4	Cơ chế bảo mật trong giao thức tầng mạng	VD	20	2	1
2.5	Cơ chế bảo mật trong giao thức tầng truy nhập mạng	VD	20	2	1
3	CLO3. LỰA CHỌN GIAO THỨC, MÔ HÌNH TRIỂN KHAI GIAO THỨC ĐỂ GIẢI QUYẾT YÊU CẦU BẢO MẬT MẠNG MÁY TÍNH CỤ THỂ				
3.1	Tình huống 1: Kết nối mạng văn phòng nhỏ với Internet	VD	15	6	1
3.2	Tình huống 2: Kết nối mạng doanh nghiệp (LAN, DMZ) với Internet	VD	15	4	1
3.3	Tình huống 3: Kết nối nhiều chi nhánh của doanh nghiệp qua Internet	VD	15	4	1
Tổng số câu hỏi trong đề thi				**50**	

Thống kê tỉ lệ các nhóm câu hỏi trong ma trận[2]

CLO / Cấp độ	CLO1	CLO2	CLO3	**Tổng theo cấp độ**	**Tỉ lệ theo cấp độ**
NB	10			**10**	**20%**
TH	12	6		**18**	**36%**
VD		8	14	**22**	**44%**
Tổng theo CLO	**22**	**14**	**14**		
Tỉ lệ theo CLO	**44%**	**28%**	**28%**		

[2] Ví dụ này cho thấy có vẻ như đề hơi khó, khi mà số lượng câu hỏi mức độ "Nhận biết" chỉ chiếm 20%. Tuy nhiên, điều này là không đúng. Cấp độ cao không đồng nghĩa với độ khó cao. Đối với thi trắc nghiệm, các câu nhận biết có thể yêu cầu phải "ghi nhớ" nhiều, và do đó không hề dễ hơn so với câu thông hiểu.

Tuy nhiên, cũng cần lưu ý rằng trong ví dụ này, số lượng câu hỏi được bốc cho CLO3 là hơi nhiều so với tổng số câu được xây dựng. Tỉ lệ mong muốn là 1/5 (Có một số trường yêu cầu tổng số câu hỏi trong mỗi nhóm phải nhiều hơn tối thiểu 5 lần so với số câu cần bốc trong nhóm).

PHẦN V. BỘ CÂU HỎI THI

1. CLO1. TRÌNH BÀY ĐƯỢC ĐẶC ĐIỂM, HOẠT ĐỘNG CỦA CÁC GIAO THỨC BẢO MẬT MẠNG MÁY TÍNH

1.1. Phân loại giao thức bảo mật mạng (NB)

Câu 1. Đâu là tên của một giao thức an toàn mạng?
A. Diffie-Helman (DH)
B. Cipher Block Chaining (CBC)
C. Authenticated Encryption with Associated Data (AEAD)
D. Message Authentication Code (MAC)

Câu 2. Đâu KHÔNG phải là tên của một giao thức an toàn mạng?
A. Secure Hash Algorithm (SHA)
B. Secure Socket Layer (SSL)
C. Secure Shell (SSH)
D. Transport Layer Security (TLS)

1.2. Đặc điểm giao thức bảo mật tầng ứng dụng (NB)

Câu 3. 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.
Đáp án: {SMTPS; smtps}

Câu 4. Một giao thức cho phép mail client nhận thư từ mail server, hoạt động trên cổng TCP mặc định là 995. Hãy cho biết tên viết tắt của giao thức.
Đáp án: {POP3S; pop3s}

1.3. Đặc điểm giao thức bảo mật tầng giao vận (NB)

1.4. Đặc điểm giao thức bảo mật tầng mạng (NB)

1.5. Đặc điểm giao thức bảo mật tầng truy nhập mạng (NB)

1.6. Hoạt động của giao thức bảo mật tầng ứng dụng (TH)

Câu 5. Sau khi kết thúc giao thức SSH-TRANS, giữa SSH Server và SSH Client
A. 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.
B. thỏa thuận được 1 khóa phiên đối xứng để mã hóa và xác thực thông điệp trao đổi sau đó giữa Server và Client.
C. 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.
D. 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.

1.7. Cơ chế bảo mật trong giao thức tầng ứng dụng (TH)

Câu 6. Chọn phát biểu SAI về giao thức SSH
A. SSH Server có thể được xác thực bằng mật khẩu hoặc khóa công khai.
B. Trong SSH luôn luôn yêu cầu xác thực 2 chiều.
C. SSH Client có thể được xác thực bằng mật khẩu hoặc khóa công khai.
D. Ở phía Client, SSH hỗ trợ xác thực từng người dùng hoặc xác thực máy trạm.

1.8. Hoạt động của giao thức bảo mật tầng giao vận (TH)

1.9. Hoạt động của giao thức bảo mật tầng mạng (TH)

1.10. Hoạt động của giao thức bảo mật tầng truy nhập mạng (TH)

2. CLO2. GIẢI THÍCH ĐƯỢC CƠ CHẾ BẢO MẬT TRONG CÁC GIAO THỨC BẢO MẬT MẠNG MÁY TÍNH

2.1. Ứng dụng của mật mã trong giao thức bảo mật mạng (TH)

Câu 7. Chọn phát biểu đúng về vai trò của hàm băm (bao gồm hàm băm không khóa và hàm băm có khóa) trong giao thức an toàn mạng.
A. Hàm băm có thể sử dụng để đảm bảo tính xác thực thông tin và xác thực thực thể.
B. Hàm băm có thể được sử dụng để đảm bảo tính xác thực và khả dụng của thông tin.
C. Hàm băm có thể được sử dụng để đảm bảo tính toàn vẹn và bí mật thông tin truyền đi.
D. Hàm băm có thể được sử dụng để đảm bảo tính xác thực và bí mật thông tin truyền đi.

Câu 8. 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.
/D

Câu 9. Trong một giao thức an toàn mạng, chứng thư số khóa công khai được sử dụng để
A. xác nhận một khóa công khai thuộc về chủ thể được nêu danh trong chứng thư.
B. kiểm tra chữ ký số của chủ thể được nêu danh trong chứng thư.
C. mã hóa thông tin gửi cho chủ thể được nêu danh trong chứng thư.
D. trao đổi khóa phiên với chủ thể được nêu danh trong chứng thư.

2.2. Cơ chế bảo mật trong giao thức tầng giao vận (VD)

2.3. Cơ chế bảo mật trong giao thức tầng mạng (VD)

2.4. Cơ chế bảo mật trong giao thức tầng truy nhập mạng (VD)

3. CLO3. LỰA CHỌN GIAO THỨC, MÔ HÌNH TRIỂN KHAI GIAO THỨC ĐỂ GIẢI QUYẾT YÊU CẦU BẢO MẬT MẠNG MÁY TÍNH CỤ THỂ

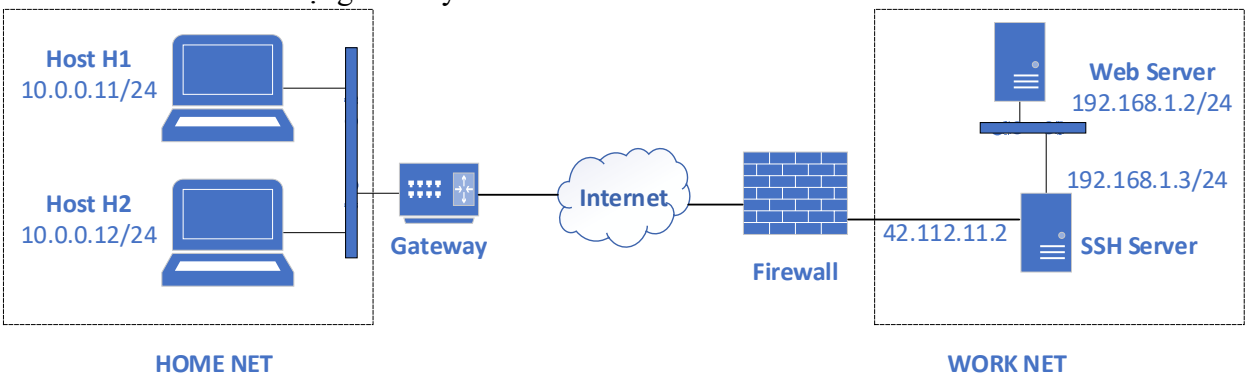
3.1. Tình huống 1: Kết nối mạng văn phòng nhỏ với Internet (VD)

3.2. Tình huống 2: Kết nối mạng doanh nghiệp (LAN, DMZ) với Internet (VD)

3.3. Tình huống 3: Kết nối nhiều chi nhánh của doanh nghiệp qua Internet (VD)

Câu 10. 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 mã hóa và ký số để đảm bảo tính bí mật và xác thực cho thông tin.
B. 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.
C. luôn phải có sự kết hợp mã hóa và ký số để đảm bảo tính bí mật và xác thực cho thông tin.
D. 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 11. Xét mô hình mạng sau đây



Giả sử SSH Server có 2 giao diện mạng, một với địa chỉ Internet và một với địa chỉ cục bộ; Firewall cho phép kết nối từ Internet đi vào SSH Server qua cổng 22. Người dùng tại HOME NET muốn kết nối tới Web Server tại WORK NET. Chọn phát biểu đúng.

A. Từ H1 có thể thiết lập kết nối tới SSH Server, sử dụng Local Port Forwarding để chuyển tiếp kết nối tới 10.0.0.11:80 sang 192.168.1.2:80. Khi đó, tất cả người dùng tại HOME NET có thể kết nối tới Web Server bằng cách nhập vào trình duyệt địa chỉ http://10.0.0.11.

B. Từ mỗi máy tại HOME NET thiết lập kết nối tới SSH Server, sử dụng Local Port Forwarding để chuyển tiếp kết nối tới 42.112.11.2:22 sang 192.168.1.2:80; sau đó có thể kết nối tới Web Server bằng cách nhập vào trình duyệt địa chỉ http://42.1112.2:22.

C. Từ H1 có thể thiết lập kết nối tới SSH Server, sử dụng Remote Port Forwarding để chuyển tiếp kết nối tới 10.0.0.11:80 sang 192.168.1.2:80. Khi đó, tất cả người dùng tại HOME NET có thể kết nối tới Web Server bằng cách nhập vào trình duyệt địa chỉ http://10.0.0.11.

D. Từ mỗi máy tại HOME NET thiết lập kết nối tới SSH Server, sử dụng Remote Port Forwarding để chuyển tiếp kết nối tới 42.112.11.2:22 sang 192.168.1.2:80; sau đó có thể kết nối tới Web Server bằng cách nhập vào trình duyệt địa chỉ http://42.1112.2:22.