

## NGHIÊN CỨU GIẢI PHÁP XÁC THỰC NGƯỜI DÙNG CHO HỆ THỐNG MẠNG KHÔNG DÂY SỬ DỤNG TƯỜNG LỬA TÍCH HỢP WEB PORTAL VÀ RADIUS SERVER

Trần Quang Huy\*, Vũ Việt Dũng

*Trường Đại học Công nghệ thông tin và Truyền thông – ĐH Thái Nguyên*

### TÓM TẮT

Ngày nay, mạng không dây đã rất phổ biến tại tất cả các văn phòng, khu công nghiệp, gia đình, các trường học. Tuy nhiên, cần phải có giải pháp xác thực để ngăn chặn việc truy cập trái phép. Mặt khác, tại các trường đại học, do đặc thù về số lượng người dùng rất lớn, giải pháp bảo mật mạng bằng mật khẩu Wi-Fi Protected Access (WPA) trở nên không khả thi. Vì vậy, nhóm tác giả đề xuất giải pháp xác thực bảo mật mạng không dây bằng công nghệ Captive Portal kết hợp với phương thức xác thực RADIUS. Captive Portal là một công nghệ cho phép điều khiển và giới hạn tất cả các truy cập sử dụng giao thức HTTP từ trình duyệt. Người dùng trong mạng sẽ được chuyển đến một portal để xác thực trước khi được phép truy cập internet. RADIUS là một dịch vụ mạng cho phép xác thực và cấp quyền cho người dùng trong mạng. Bài báo này sẽ mô phỏng việc kết hợp tính năng Captive portal trên tường lửa pfsense với một máy chủ Active Directory để cung cấp dịch vụ xác thực người dùng từ xa RADIUS cho hệ thống mạng không dây của Trường Đại học Công nghệ thông tin và Truyền thông – Đại học Thái Nguyên.

**Từ khóa:** *Mạng không dây cục bộ; Captive Portal; Tường lửa pfSense; dịch vụ xác thực RADIUS; dịch vụ Active Directory.*

*Ngày nhận bài: 13/3/2020; Ngày hoàn thiện: 28/4/2020; Ngày đăng: 04/5/2020*

## RESEARCH ON USER AUTHENTICATION TECHNIQUE USING WEB PORTAL INTERGRATED FIREWALL AND RADIUS SERVER FOR WIRELESS NETWORKING SYSTEM OF THAI NGUYEN UNIVERSITY OF INFORMATION AND COMMUNICATION TECHNOLOGY

Tran Quang Huy\*, Vu Viet Dung

*TNU - University of Information and Communication Technology*

### ABSTRACT

Today, wireless networks are extremely popular in all offices, industrial parks, homes, and schools. However, due to the nature of network technology, an authentication solution is needed to prevent unauthorized access. On the other hand, at universities, due to the large number of users, the network security solution using WPA password becomes not feasible. Therefore, we propose a solution to authenticate wireless network security with Captive Portal technology combined with RADIUS authentication method. Captive Portal is a technology that allows controlling and restricting all access using HTTP protocol from the browser. Users on the network will be redirected to a portal for authentication before being allowed to access the internet. RADIUS is a network service that enables authentication and authorization for users on the network. This article will present and simulate the combination of Captive portal feature on pfsense firewall with an active directory server to provide RADIUS user authentication service for ICT - Thai Nguyen university's wireless network.

**Keywords:** *WLAN; Captive Portal; pfSense; RADIUS authentication; Active Directory.*

*Received: 13/3/2020; Revised: 28/4/2020; Published: 04/5/2020*

\* Corresponding author. Email: tqhuy@ictu.edu.vn

## 1. Giới thiệu

Với sự phát triển của công nghệ thông tin ngày nay, Internet đã trở thành một công cụ mạnh mẽ và không thể thiếu đối với tất cả mọi người. Đặc biệt đối với các trường đại học, việc cung cấp kết nối mạng Internet cho người dùng là học sinh, sinh viên và giảng viên là đặc biệt cần thiết cho hoạt động giảng dạy và học tập.

Tuy nhiên, việc quản lý một hệ thống mạng không dây cũng đem lại nhiều thách thức cho các nhà quản trị.

### 1.1. Vấn đề trong bảo mật mạng không dây

Wireless Local Area Network (WLAN) hay Wi-Fi là tên một công nghệ mạng không dây sử dụng sóng vô tuyến. Công nghệ này sử dụng chuẩn 802.11 được quy định bởi tổ chức IEEE.

Trong WLAN, các thiết bị kết nối và truyền dữ liệu thông qua sóng vô tuyến. Vì vậy nên hệ thống mạng WLAN là mở với tất cả các thiết bị trong vùng phủ sóng. Điều này cho phép người dùng có thể sử dụng hệ thống mạng mà không cần xác thực hay đăng nhập. Để giải quyết vấn đề đó người ta đã nghiên cứu ra các chuẩn cho phép ngăn chặn các truy cập trái phép và mã hóa dữ liệu như WEP, WPA, WPA2. Tuy nhiên, các lỗ hổng trong cơ chế hoạt động của các chuẩn này hiện đã được công bố [1]. Vì vậy nếu tiếp tục được sử dụng, người dùng có thể bẻ khóa và truy cập vào hệ thống mà không cần xác thực. Từ đó, chúng có thể tiến hành nghe lén và đánh cắp thông tin của những người dùng khác.

### 1.2. Vấn đề quản lý người dùng

Thêm vào đó, với một hệ thống mạng không dây ở quy mô lớn, có số lượng người dùng nhiều, như ở các trường đại học, hạ tầng mạng không thể đáp ứng nhu cầu của tất cả người dùng tại cùng một thời điểm. Điều này sẽ dẫn đến việc hệ thống mạng thường xuyên bị tắc nghẽn, người dùng mới không thể kết nối vào mạng, hoặc không thể truy cập được các tài nguyên trên Internet. Hơn nữa, ngoài nhóm người dùng thông thường, còn có nhóm

người dùng là khách đến làm việc tại trường trong khoảng thời gian ngắn. Lúc này, việc sử dụng cơ chế bảo mật thông qua mật khẩu dùng chung trở nên không hiệu quả. Vì vậy cần có cơ chế, quản lý người dùng linh động, và giới hạn băng thông mạng để tránh lãng phí tài nguyên.

## 2. Đề xuất giải pháp

Qua các vấn đề đã trình bày ở phần trên và đánh giá các giải pháp sẵn có, cùng với việc phân tích các đặc thù của hệ thống mạng không dây cho các trường đại học. Nhóm tác giả cho rằng, để đáp ứng được yêu cầu về bảo mật và xác thực cho hệ thống mạng, giải pháp sử dụng tường lửa pfSense có tích hợp công nghệ Captive Portal là rất phù hợp. Tuy nhiên, cần kết hợp thêm với các cơ chế quản lý tài khoản người dùng linh động, phù hợp cho nhiều đối tượng sử dụng khác nhau. Chính vì vậy, nhóm đề xuất thực hiện giải pháp kết hợp giữa công nghệ Captive Portal và dịch vụ Active Directory trên máy chủ Microsoft. Để thực hiện được việc xác thực dựa trên cơ sở dữ liệu người dùng của dịch vụ AD, cần có một giải pháp trung gian đó là dịch vụ xác thực người dùng từ xa - Remote Authentication Dial-In User Service (RADIUS).

### 2.1. Công nghệ Captive Portal

Captive Portal là công nghệ cho phép sử dụng một web portal để xác thực người dùng, mỗi khi người dùng cần truy cập Internet, trình duyệt sẽ chuyển họ đến một trang web được cấu hình bởi người quản trị [2]. Công nghệ này sử dụng giao thức truyền thông bảo mật như TLS để truyền dữ liệu, vì vậy sẽ ngăn chặn các nguy cơ bị đánh cắp dữ liệu. Mặc dù tổ chức IEEE đã phát triển một giao thức xác thực và bảo mật cải tiến có tên là 802.1X để giải quyết các lỗ hổng của chuẩn WPA2 [3]. Tuy nhiên, chuẩn 802.1X có yêu cầu thiết bị chạy một giao thức phức tạp hơn so với Captive Portal. Vì vậy 802.1X không được áp dụng rộng rãi trong mạng WLAN. Một ưu điểm nữa của Captive Portal đó là việc xác

thực thông qua trình duyệt web nên người sử dụng sẽ không cần phải cài đặt thêm các phần mềm điều khiển truy cập ở trên thiết bị của họ, kể cả là các thiết bị di động. Mặt khác, Captive Portal cho phép quản trị viên linh hoạt trong quản trị cơ sở dữ liệu người dùng bằng khả năng kết hợp với nhiều loại dịch vụ mạng khác, ví dụ như Active Directory hay LDAP.

Hiện nay đã có rất nhiều giải pháp quản lý truy cập được tích hợp công nghệ Captive Portal bao gồm cả giải pháp thương mại và phần mềm nguồn mở. Ví dụ như:

- Air Marshall, một tường lửa mềm được phát triển dựa trên nền tảng hệ điều hành Linux.
- PacketFence, phần mềm quản lý truy cập mạng với tính năng Captive Portal (open source)
- pfSense, là một tường lửa mềm trên nền tảng FreeBSD (open source). pfSense có khả năng cài đặt thêm các gói phần mềm của bên thứ ba nhằm hỗ trợ, mở rộng chức năng.

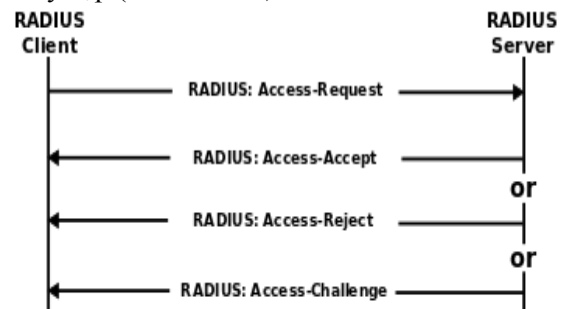
## 2.2. RADIUS Server

RADIUS là viết tắt của Remote Authentication Dial-In User Service là một giao thức mạng, hoạt động trên cổng UDP 1812 cung cấp quản lý xác thực tập trung (Authentication), ủy quyền (Authorization) và kiểm toán (Accounting) cho phép quản lý người dùng kết nối và sử dụng dịch vụ mạng [4]. RADIUS hoạt động trên mô hình Client – Server và chạy trên lớp ứng dụng của bộ giao thức TCP/IP, RADIUS thường chạy như một dịch vụ trên máy chủ UNIX hoặc Microsoft Windows Server.

Mô hình hoạt động của RADIUS bao gồm 02 thành phần chính: NAS (Network Access Server) và RADIUS Server. Trong đó: NAS là máy chủ sẽ nhận thông tin đăng nhập của người dùng bao gồm tên đăng nhập và mật khẩu thông qua một giao thức. Đó có thể là giao thức PPP đối với các dịch vụ Dial-up và DSL, hoặc cũng có thể là giao thức HTTPS đối với các dịch vụ web. Sau đó, NAS sẽ gửi thông báo yêu cầu truy cập đến máy chủ RADIUS. Kết nối giữa NAS và máy chủ

RADIUS được mã hóa bằng một chuỗi bảo mật (shared secret) được định sẵn giữa 2 đầu. Các thông tin được gửi đến máy chủ RADIUS bao gồm: thông tin đăng nhập, thường ở dạng tên người dùng và mật khẩu, hoặc chứng chỉ bảo mật. Ngoài ra có thể bao gồm các thông tin khác mà NAS biết về người dùng, ví dụ như địa chỉ IP, địa chỉ MAC v.v.

Máy chủ RADIUS sẽ kiểm tra thông tin bằng cách sử dụng các phương thức xác thực như PAP, CHAP hoặc EAP. Sau đó máy chủ RADIUS sẽ phản hồi cho NAS thông tin về trạng thái truy cập như sau: 1. Từ chối truy cập, 2. Yêu cầu thêm thông tin, 3. Chấp nhận truy cập (Xem hình 1).



Hình 1. Cơ chế hoạt động của RADIUS

### Từ chối truy cập - Access Reject

Người dùng bị từ chối truy cập vào tất cả các tài nguyên mạng. Lý do có thể bao gồm việc không cung cấp chứng nhận hoặc tài khoản người dùng không xác định hoặc không hoạt động, bị khóa, v.v.

### Yêu cầu gửi thêm thông tin truy cập - Access Challenge

Yêu cầu thông tin bổ sung từ người dùng như mật khẩu phụ, mã PIN, mã thông báo hoặc thẻ. Access Challenge cũng được sử dụng trong các hộp thoại xác thực phức tạp hơn, khi đường hầm (tunnel) bảo mật được thiết lập giữa máy người dùng và máy chủ RADIUS để giấu thông tin đăng nhập khỏi NAS.

### Chấp nhận truy cập - Access Accept

Người dùng được cấp quyền truy cập. Khi người dùng được xác thực, máy chủ RADIUS sẽ thường kiểm tra xem người dùng có được phép sử dụng dịch vụ mạng được yêu cầu hay

không. Chẳng hạn một người dùng nào đó có thể được phép sử dụng mạng không dây, nhưng không được sử dụng VPN của công ty. Thông tin này có thể được lưu trữ cục bộ trên máy chủ RADIUS hoặc có thể được truy vấn tại một nguồn bên ngoài như LDAP hoặc Active Directory.

### 3. Thực nghiệm giải pháp

#### 3.1. Cơ chế hoạt động

Trong bài báo này, nhóm tác giả đề xuất phương pháp xác thực với cơ chế hoạt động như sau: Tường lửa pfSense sẽ đóng vai trò làm gateway cho các máy tính trong mạng, đồng thời đóng vai trò làm RADIUS Client trong mô hình xác thực với RADIUS Server. Người dùng trong mạng khi sử dụng máy tính hoặc thiết bị di động kết nối vào mạng sẽ được chuyển đến một cổng đăng nhập sử dụng giao thức HTTP hoặc HTTPS. Người dùng phải tiến hành xác thực bằng username và password đã được cấp. Thông tin xác thực sẽ được tường lửa pfSense gửi cho RADIUS Server thông qua một bản tin request-access. RADIUS Server lúc này sẽ tiến hành truy vấn cơ sở dữ liệu người dùng nằm trong dịch vụ Active Directory đã được cài đặt để xác thực thông tin người dùng. Sau đó RADIUS Server sẽ trả lời lại cho RADIUS Client một trong các bản tin thể hiện kết quả của việc xác thực. RADIUS Client sẽ dựa vào đó để đưa ra thông báo hiển thị trên Web Portal cho người dùng biết việc mình đã được truy cập hay chưa. Mô hình hệ thống được thể hiện thông qua hình 2.



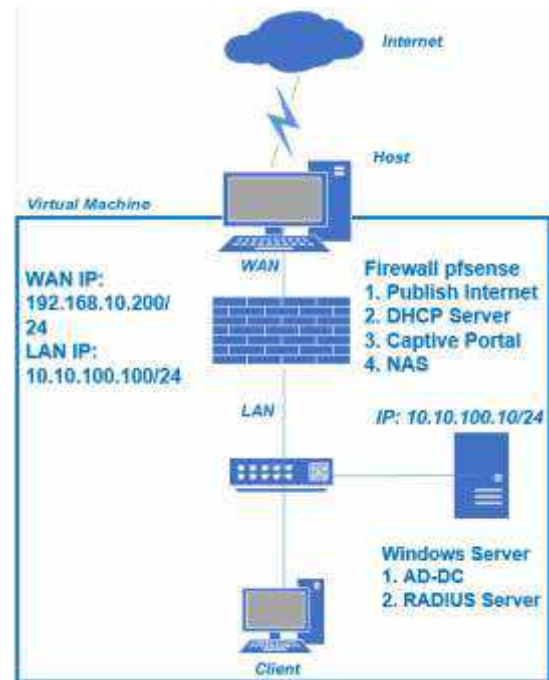
Hình 2. Mô tả cơ chế hoạt động của hệ thống

#### 3.2. Mô phỏng hệ thống

Trong phần này, nhóm tác giả sẽ tiến hành thử nghiệm các cấu hình hệ thống, với công cụ là phần mềm ảo hóa Vmware Workstation giúp mô phỏng lại hoạt động của hệ thống mạng và các máy chủ. Cụ thể bao gồm:

- Một máy ảo chạy hệ điều hành Windows Server 2012 R2 đóng vai trò làm máy chủ dịch vụ Active Directory và máy chủ RADIUS thông qua Network Policy Services. Dịch vụ Active Directory sẽ lưu trữ thông tin của người dùng cho việc xác thực, trong khi đó NPS sẽ tạo các chính sách mạng cho phép RADIUS Client (lúc này là firewall pfsense) thực hiện việc chuyển các thông tin xác thực.

- Máy ảo chạy hệ điều hành Windows 7 sẽ thực hiện các bước xác thực người dùng thông qua trình duyệt web và tài khoản người dùng đã được cấp. Đảm bảo sau khi được xác thực sẽ có khả năng truy cập Internet.



Hình 3. Sơ đồ mạng

- Máy ảo chạy FreeBSD sẽ được cài tường lửa mềm pfSense sẽ đóng các vai trò như sau:

- Gateway cung cấp Internet cho các máy ảo còn lại trong mạng.
- Tường lửa triển khai các chính sách bảo mật

- Máy chủ DHCP cấp phát địa chỉ IP, các thông tin về default gateway và DNS
- Captive Portal cung cấp giao diện xác thực cho người dùng.
- RADIUS Client gửi thông tin xác thực của người dùng lên máy chủ AD

Để đảm bảo được các vai trò trên, máy ảo chạy pfSense phải có 2 NIC. Trong đó 1 NIC sẽ đóng vai trò cổng WAN kết nối ra internet và 1 NIC đóng vai trò gateway cho mạng LAN bên trong. Mô hình mạng được thực hiện như hình 3.

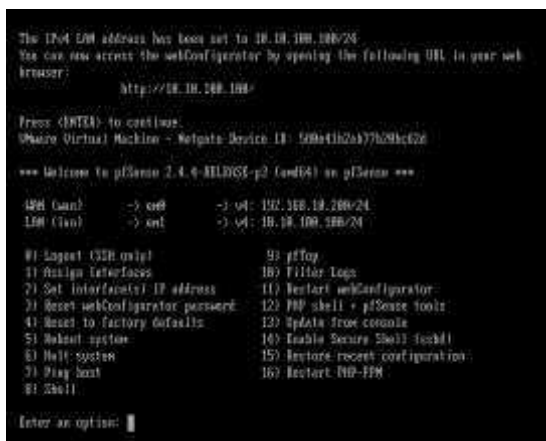
Sau khi triển khai cấu hình hệ thống cơ bản như trên, phần tiếp theo nhóm tác giả sẽ trình bày các bước cấu hình kết hợp tường lửa pfSense và máy chủ AD phục vụ cho việc quản trị và xác thực người dùng. Cụ thể bao gồm các bước như sau:

- Cấu hình tường lửa pfSense làm Captive Portal;
- Cấu hình máy chủ AD làm RADIUS Server;
- Cấu hình các chính sách mạng và cơ chế bảo mật trên tường lửa pfSense;
- Khởi tạo và quản lý người dùng.

### 3.2.1. Cấu hình firewall pfSense làm Captive Portal

Các bước thực hiện cấu hình cụ thể như sau:

Bước 1: Cài đặt pfSense và cấu hình các network interface như hình 4.



Hình 4. pfSense sau khi cài đặt

Bước 2: Cấu hình DHCP Server, cấu hình DNS Resolver.

Bước 3: Bật tính năng Captive Portal trên trang quản trị, lựa chọn cổng mạng, cấu hình

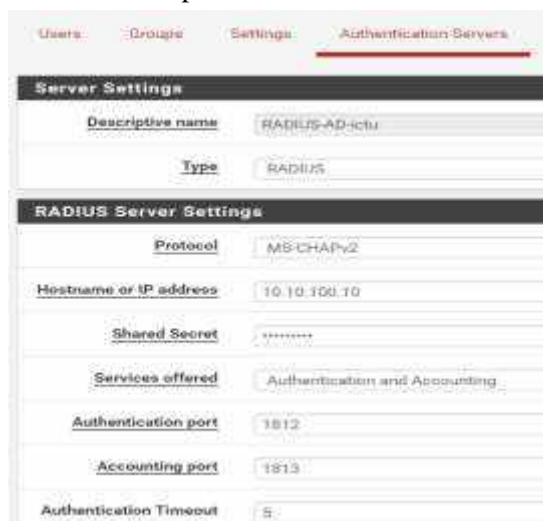
xác thực, và cấu hình tùy chọn. Một số cấu hình chi tiết và giải thích được mô tả ở phía dưới [5]:

1. Lựa chọn cổng mạng: Công nghệ Captive Portal sử dụng một cổng LAN của tường lửa pfSense. Cổng này được đặt địa chỉ IP tĩnh và sẽ có vai trò là địa chỉ Default Gateway cho tất cả các máy khác trong mạng.

2. Cấu hình Maximum Concurrent Connection: Cấu hình giới hạn kết nối đồng thời. Tùy chọn này sẽ giới hạn số lượng kết nối đối với mỗi một địa chỉ IP đến trang Portal, điều này sẽ giúp hạn chế việc Portal bị tấn công từ chối dịch vụ.

3. Idle Time Out và Hard Time Out: 2 tùy chọn này sẽ ngắt kết nối người dùng khi người dùng không hoạt động hoặc sau một khoảng thời gian nhất định.

4. Traffic Quota: tùy chọn cho phép giới hạn số băng thông mà một người dùng được sử dụng trong một phiên kết nối. Tính cả download và upload.



Hình 5. Cấu hình RADIUS Client trên pfsense

5. Concurrent user logins: vô hiệu hóa tính năng này sẽ giúp giới hạn việc nhiều người dùng chung một tài khoản để kết nối vào Internet.

6. Phương thức xác thực: sử dụng xác thực trên RADIUS Server.

7. Enable HTTPS login: Bật tính năng truy cập Portal thông qua giao thức HTTPS.

Bước 4: Cấu hình RADIUS Client tại mục Authentication Server. Cấu hình như hình 5.

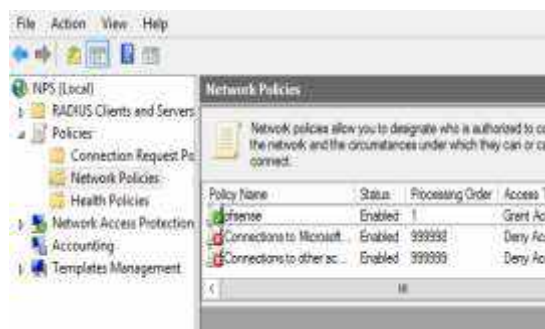
### 3.2.2. Cấu hình máy chủ AD làm RADIUS Server

Để cài đặt một máy chủ AD làm RADIUS Server cần cài đặt dịch vụ Network Policy Service. Sau đó tiến hành khai báo một RADIUS Client như hình 6.



**Hình 6.** Khai báo RADIUS Client

Sau khi cấu hình xong RADIUS Client cần cấu hình một network policies, trong đó chỉ ra đâu là nhóm người dùng được cấp quyền để xác thực. Ngoài ra, chúng ta cũng có thể chỉ rõ phương thức xác thực được sử dụng. Hình 7 chỉ ra một chính sách đang được áp dụng cho RADIUS Server



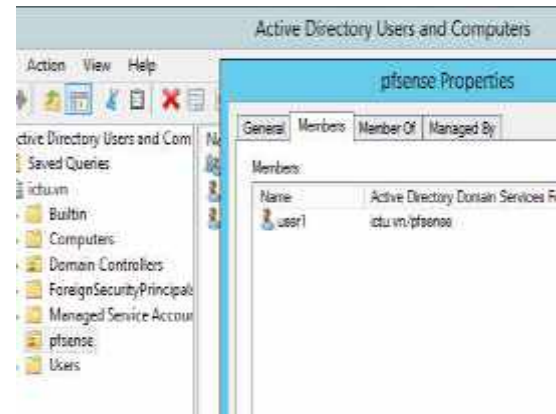
**Hình 7.** Cấu hình Network Policies

### 3.2.3. Khai báo và quản trị người dùng

Dịch vụ AD của Windows Server cung cấp khả năng quản trị người dùng rất chi tiết và

linh hoạt, cùng với đó là khả năng tích hợp với các hệ thống ứng dụng khác tạo thành một hệ thống đăng nhập đồng bộ (Single Sign-on). Người sử dụng chỉ cần sử dụng một tài khoản cho tất cả các dịch vụ trong hệ thống mạng.

Để thực hiện mô phỏng hệ thống cho bài báo này, nhóm tác giả thực hiện tạo 1 group trên AD có tên là pfSense và 1 user để thử nghiệm việc xác thực như hình 8:



**Hình 8.** Tạo người dùng trong hệ thống

Ngoài những đối tượng người dùng thông thường trong hệ thống, không thể không tính đến nhóm đối tượng là người dùng khách, nhóm này có đặc điểm là chỉ hoạt động trong thời gian ngắn. Chính vì vậy, cần có giải pháp để cung cấp Internet tạm thời đến cho nhóm người dùng này. Công nghệ Captive Portal trong tường lửa pfSense có cung cấp một tính năng cho phép người sử dụng đăng nhập thông qua các Voucher có giới hạn thời gian. Cơ chế này rất linh động và phù hợp với đối tượng người dùng trên. Hình 9 mô tả các bước cấu hình bật tính năng đăng nhập thông qua Voucher và danh sách các Voucher được tạo ra.



**Hình 9.** Cấu hình Voucher

Các Voucher này sẽ được cung cấp cho người dùng để nhập vào trang đăng nhập. Chuyên viên quản trị mạng có thể tùy biến số lượng Voucher được tạo ra và thời gian sử dụng của mỗi Voucher. Khi người dùng sử dụng Voucher để đăng nhập vào hệ thống. Người quản trị có thể dễ dàng quản lý thông qua giao diện ở trên tường lửa pfSense như hình 10.

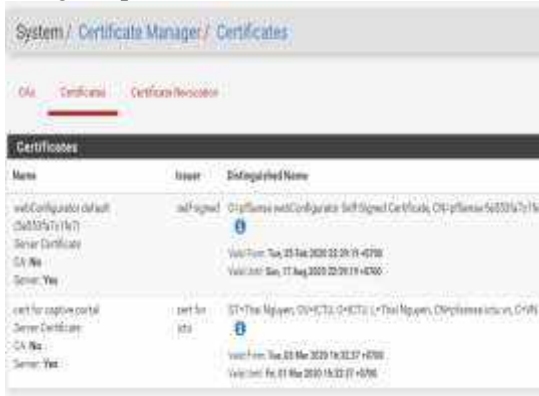


Voucher	Roll	Activated at
AvmCX8ipBH3	1	03/10/2020 08:43:05

Hình 10. Xem thông tin Voucher

### 3.2.4. Cấu hình giao thức HTTPS

Trong khuôn khổ bài báo này, nhóm tác giả sẽ thử nghiệm việc cấu hình https cho trang web portal. Tuy nhiên, do hệ thống chỉ phục vụ mục đích thử nghiệm nên các certificates được sử dụng đều là self-certificates. Việc cấu hình được thực hiện trong giao diện điều khiển của tường lửa pfSense như hình 11 và 12.



Name	Issuer	Expiry/Issued
cert for captive portal	self signed	03/10/2020 08:43:05 - 03/10/2020 08:43:05
cert for captive portal	self signed	03/10/2020 08:43:05 - 03/10/2020 08:43:05

Hình 11. Quản lý chứng chỉ số



**HTTPS Options**

**Login**  Enable HTTPS login  
When enabled, the username and password fields will be displayed in the login form. If this option is set, attempts to connect to the captive portal will be redirected to the correct interface IP.

**HTTPS server name**   
This name will be used in the form a browser will most likely display a message that resolves to the correct interface IP.

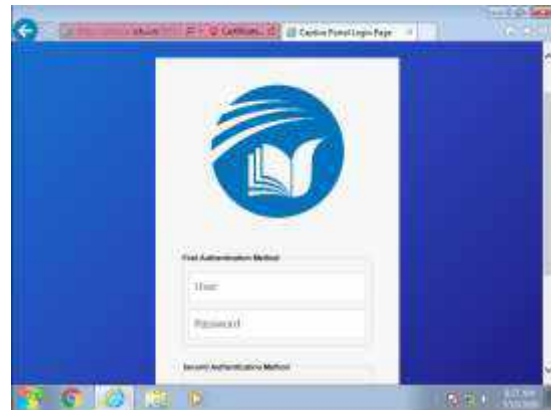
**SSL Certificate**   
If no certificates are defined, one will be generated.

**HTTPS Forwards**  Disable HTTPS Forwards  
If this option is set, attempts to connect to the captive portal will be redirected to the correct interface IP.

Hình 12. Cấu hình https

### 3.3. Thử nghiệm việc xác thực người dùng

Để thử nghiệm việc xác thực người dùng, nhóm tác giả sử dụng một máy tính chạy hệ điều hành Windows 7 làm client như mô tả ở phần trên. Thực hiện kết nối giao tiếp mạng vào hệ thống. Mở trình duyệt và truy cập một website bất kì. Ngay lập tức cửa sổ yêu cầu đăng nhập hiện ra như hình 13.



Hình 13. Giao diện Web Portal

Đây là giao diện của trang đăng nhập mặc định được cung cấp bởi tường lửa pfSense, người quản trị hoàn toàn có thể tùy biến giao diện khác cho phù hợp với tổ chức của mình. Sau khi nhập thông tin, người sử dụng được thông báo đã kết nối và được chuyển tiếp đến website mình muốn truy cập từ đầu.

Lúc này trong giao diện trạng thái của Captive Portal xuất hiện thông tin của người dùng đang được kết nối như hình 14.



IP Address	Username	Authentication Method	Session Start	Session End
192.168.1.101	admin	Local	03/10/2020 08:43:05	03/10/2020 08:43:05

Hình 14. Thông tin người dùng đăng nhập

### 4. Đánh giá và kết luận

Trong khuôn khổ bài báo này, nhóm tác giả đã đề xuất một giải pháp đơn giản và hiệu quả cho việc sử dụng cơ sở dữ liệu người dùng được lưu trữ trong dịch vụ Active Directory để xác thực và truy cập Internet trong hệ thống mạng nội bộ của một trường đại học. Giải pháp này tỏ ra hiệu quả hơn so với việc

sử dụng các phương thức xác thực cục bộ như chia sẻ mật khẩu.

Qua quá trình nghiên cứu, nhóm tác giả đánh giá pfsense là một giải pháp rất tốt cho việc điều khiển truy cập mạng. Pfsense rất linh hoạt trong việc cài đặt, cấu hình và có thể hoạt động trên nhiều vai trò như tường lửa hay bộ định tuyến. Nó cũng cung cấp rất nhiều tính năng thường thấy trong các tường lửa thương mại đắt tiền. Nó có thể được cấu hình và nâng cấp thông qua giao diện web rất trực quan và dễ hiểu, quản trị viên không cần có các kiến thức liên quan đến nền tảng hệ điều hành FreeBSD mà vẫn có thể quản trị được pfsense. Ngoài ra, pfsense cũng hỗ trợ các công cụ đến từ cộng đồng người sử dụng và đến từ bên thứ ba.

Ở phần 3, nhóm tác giả đã mô tả cách thức triển khai và cấu hình xác thực cho người sử dụng thông qua một máy chủ RADIUS. Người dùng kết nối với mạng được gán địa chỉ IP bằng DHCP Server trong pfsense, khi đó bất kì truy cập nào ra ngoài internet cũng sẽ được chuyển hướng đến web portal. Chỉ khi người dùng nhập đúng thông tin tài khoản và mật khẩu thì mới được phép truy cập Internet. Các cấu hình nâng cao sẽ hạn chế việc nghe lén thông tin người dùng trong mạng cũng như việc một tài khoản bị sử dụng bởi nhiều người dùng.

Như vậy, giải pháp đã đạt được mục tiêu là cung cấp một giải pháp xác thực an toàn, linh động, dễ dàng cài đặt, triển khai với chi phí

thấp, đủ đáp ứng nhu cầu cho một hệ thống mạng không dây có quy mô lớn với nhiều đối tượng người dùng khác nhau. Tuy nhiên, cần đánh giá thêm khả năng chống chịu của hệ thống khi bị tấn công với những kĩ thuật cao hơn như thay đổi MAC address hoặc DNS Tunnel.

#### Lời cảm ơn

Bài báo này được thực hiện trong khuôn khổ của đề tài nghiên cứu khoa học cấp cơ sở số hiệu: T2019-07-12 được tài trợ bởi Trường Đại học Công nghệ thông tin và truyền thông – Đại học Thái Nguyên năm 2019. Nhóm tác giả xin trân trọng cảm ơn quý nhà trường.

#### TÀI LIỆU THAM KHẢO/ REFERENCES

- [1]. A. H. Lashkari, M. M. S. Danesh, and B. Samadi, "A Survey on Wireless Security protocols (WEP,WPA and WPA2/802.11i)," *IEEE ICCSIT 2009. 2nd IEEE International Conference*, Aug. 2009, pp. 48-52.
- [2]. G. Appenzeller, M. Roussopoulos, and M. Baker, "User-Friendly Access Control for Public Network Ports," *IEEE INFOCOM '99. Eighteenth Annual Joint Conference*, vol. 2, pp. 699-707, Mar. 1999.
- [3]. IEEE 802.1 Working Group, *802.1X – port based network access control*, 2001
- [4]. C. Rigney, A. Rubens, W. Simpson, and S. Willens, *Remote Authentication Dial in User Service (RADIUS)*, RFC2865. Jun. 2000.
- [5]. K. C. Patel, and P. Sharma, "A Review paper on pfsense – an Open source firewall introducing with different capabilities & customization," *IJARIE*, vol. 3, no. 2, pp. 635-641, 2017.