## Bộ môn An toàn Thông tin – Khoa MMT&TT - UIT

3

Lab

Thiết lập mô hình

Tường lửa Sophos UTM

SOPHOS UTM Firewall Configuration

**Thực hành An toàn Hệ thống thông tin**

**Họ và Tên : Giang Thị Sông Hằng**

**2**

**Lớp CNPM2**

**Link Youtube:** [**https://youtu.be/BHIGY4KrzSo**](https://youtu.be/BHIGY4KrzSo)

**Máy** **1**: Windows Server 2008 làm Domain Server (1 card mạng Host-only)

* **Máy 2**: Firewall Sophos UTM

Đồng thời, dùng máy thật để kết nối vào WebAdmin của Firewall.

*Vùng DMZ trong mô hình chỉ để tham khảo về mô hình mạng thực tế.*

Thông tin card mạng của các máy như sau

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Server Name** |  | **Interface 1** | **Interface 2** | **Interface 3** |
| 1 | Domain Controller | IP | 10.0.0.2 |  |  |
| SM | 255.0.0.0 |  |  |
| DG | 10.0.0.1 |  |  |
| DNS | 10.0.0.2 - 8.8.8.8 |  |  |
| 2 | DMZ  (Web Server Mail Server FTP Server) | IP | 172.16.0.2 |  |  |
| SM | 255.255.0.0 |  |  |
| DG | 172.16.0.1 |  |  |
| DNS | 8.8.8.8 |  |  |
| 3 | Firewall | IP | 10.0.0.1 | 172.16.0.1 | DHCP |
| SM | 255.0.0.0 | 255.255.0.0 |  |
| DG |  |  |  |
| DNS |  |  |  |

**4**

# THỰC HÀNH

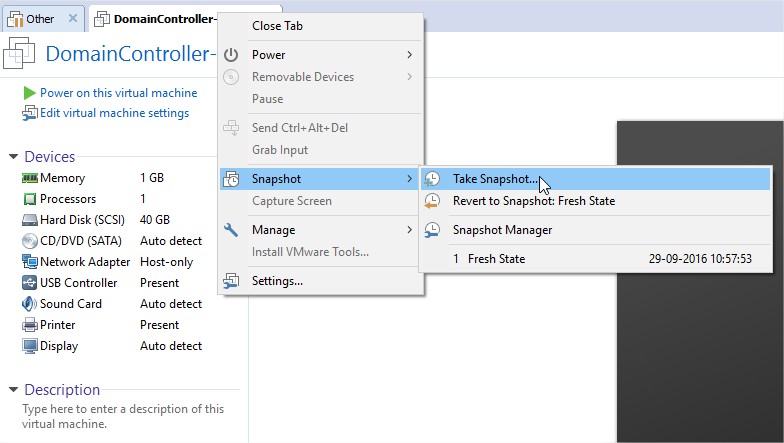
## Thiết lập máy chć Domain Controller

* **Bước 1:** Chuẩn bị máy ảo làm Domain Controller:

+ RAM: 512MB – 1GB

+ 1 Network Adapter Host-Only

+ OS: Windows Server 2008. Trong hướng dẫn này sử dụng Windows Server 2008. Sau khi cài đặt xong máy ảo Windows Server 2008, nên Snapshot (sao lưu) lại máy ảo để có thể khôi phục lại trạng thái ban đầu nếu quá trình nâng cấp bị lỗi.



*Hình 2. Thực hiện Snapshot để sao lưu trạng thái máy ảo ban đầu*

* **Bước 2:** Đặt IP cho máy Domain Controller là 10.0.0.2/8

A screenshot of a computer

Description automatically generated*Hình 3. Thay đổi IP của máy chủ*

## Lab 3: Thiết lập mô hình tường lửa Sophos UTM

**5**

A computer screen shot of a computer

Description automatically generated

* **Bước 3:** Đặt DNS Suffix bằng cách click phải lên My Computer > Propertites > Change Setting > Change > chọn More.
* A computer screen shot of a computer

  Description automatically generated

*Hình 4. Chọn More để thay đổi DNS Suffix*

Sau đó nhập DNS Suffix cần đặt.

Sau đó Restart lại máy tính để áp dụng các thay đổi.

* **Bước 4:** Nâng cấp máy chủ thành Domain Controller

A computer screen shot of a blue screen

Description automatically generatedHướng dẫn này thực hiện trên Windows Server 2008, nếu sử dụng phiên bản khác có thể có một số thay đổi trong quá trình nâng cấp.

*Hình 5. Vào Start > run > nhập* ***dcpromo***

## Lab 3: Thiết lập mô hình tường lửa Sophos UTM

**6**

A computer screen shot of a computer

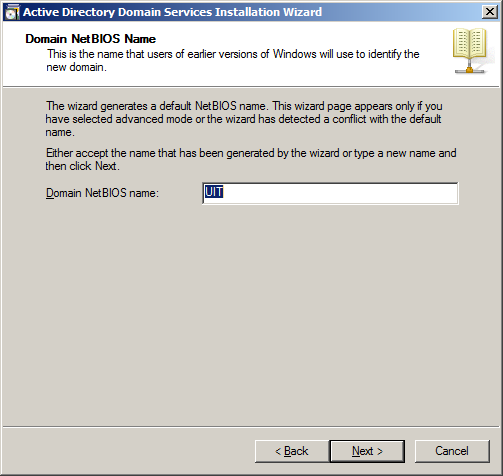
Description automatically generated

A screenshot of a computer

Description automatically generated*Hình 6. Chọn Create a new domain in a new forest*

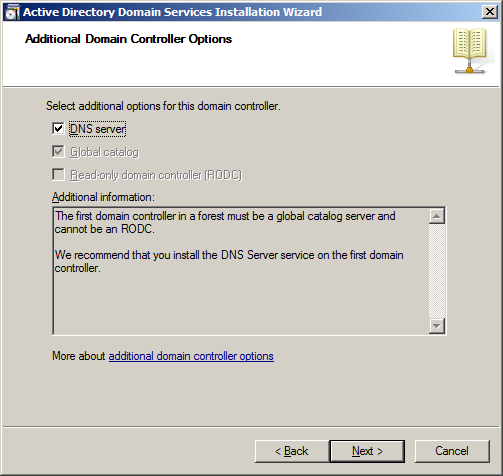
*Hình 7. Nhập domain (uit.local) cho Forest Root Domain*

**7**

Giữ các thiết lập mặc định trong các bước tiếp theo:

A computer screen shot of a computer

Description automatically generated*Hình 8. Domain NetBIOS*



*Hình 9. Chọn DNS Server*

*A screenshot of a computer

Description automatically generatedHình 10. Chọn Windows 2000*

A screenshot of a computer

Description automatically generated

**8**

*Hình 11. Thiết lập mật khẩu quản trị*

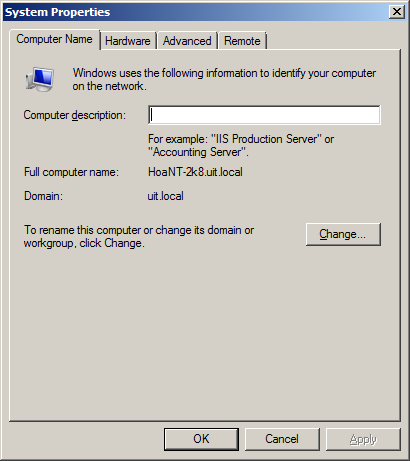
*A screenshot of a computer

Description automatically generated*

*Hình 12. Quá trình nâng cấp hoàn tất*

Sau khi nâng cấp thành công, khởi động lại server và vào Properties của Computer để kiểm tra.

**9**



* **Bước 5:** Tiến hành Snapshot lại để lưu lại trạng thái máy ảo lúc này.

## Cài đặt và cấu hình máy Firewall Sophos UTM

Sinh viên có thể tải miễn phí file cài đặt Sophos UTM 9.4 (*UTM v9 software appliance*) tại đây <https://www.sophos.com/en-us/support/utm-downloads.aspx>

(bản asg-9.406-3.1.iso ~ 832MB). *Trong Lab sử dụng Sophos UTM 9.4*

* + **Bước 1:** Tải Sophos UTM 9.4, ta được file ISO cài đặt **asg-9.406-3.1.iso**
  + **Bước 2:** Tạo máy ảo mới bằng VMware và load file iso của Sophos UTM 9 để cài đặt tường lửa Sophos UTM.

A screenshot of a computer

Description automatically generated

*Hình 13. Chọn file cài đặt asg-9.406-3.1.iso*

**10**

Máy ảo để Firewall Sophos hoạt động có thông số như sau:

* RAM 1GB *(hoặc 2GB)*
* Có 3 card mạng:

+ Card 1: Host-only

+ Card 2: Host-only

+Card 3: Bridge *(kết nối Internet qua máy thật)*

*A screenshot of a computer

Description automatically generated*

*Hình 14. Cấu hình máy ảo có thể sử dụng Sophos UTM ổn định*

* A screenshot of a computer error

  Description automatically generated**Bước 3:** Khởi động máy ảo và nhấn Enter để bắt đầu cài đặt

*Hình 15. Cài đặt Sophos UTM 9*

## Lab 3: Thiết lập mô hình tường lửa Sophos UTM

**11**

Sau đó, chọn **Start** để bắt đầu

**A screenshot of a computer error

Description automatically generatedBước 4:** Thiết lập ngôn ngữ và múi giờ

A computer screen shot of a keyboard

Description automatically generated

A screenshot of a computer

Description automatically generated

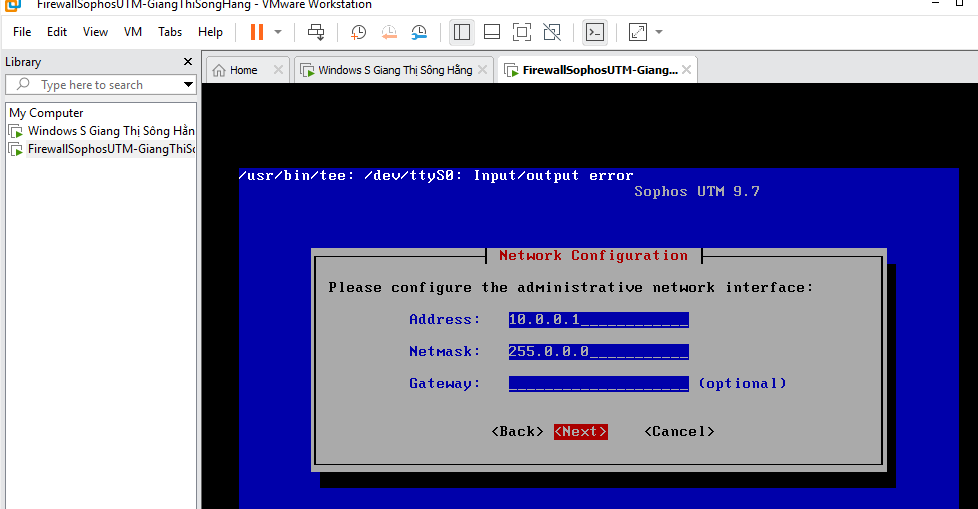
*Hình 16. Chọn ngôn ngữ English và múi giờ Ho\_Chi\_Minh*

## Lab 3: Thiết lập mô hình tường lửa Sophos UTM

**12**

* **Bước 5:** Chọn card mạng eth0 và thiết lập IP mặc định cho trang quản trị
* *A screenshot of a computer

  Description automatically generatedHình 17. Chọn card mạng eth0 cho WebAdmin của Firewall*



*Hình 18. Thiết lập IP quản trị 10.0.0.1 cho Firewall*

**13**

*A computer screen shot of a computer

Description automatically generated*Quá trình cài đặt diễn ra trong 6 bước:

*Hình 20. Chờ quá trình cài đặt hoàn thành*

Sau khi cài đặt thành công, hệ thống sẽ thông báo thông tin địa chỉ IP đăng nhập vào trang quản trị WebAdmin là https://10.0.0.1:4444/

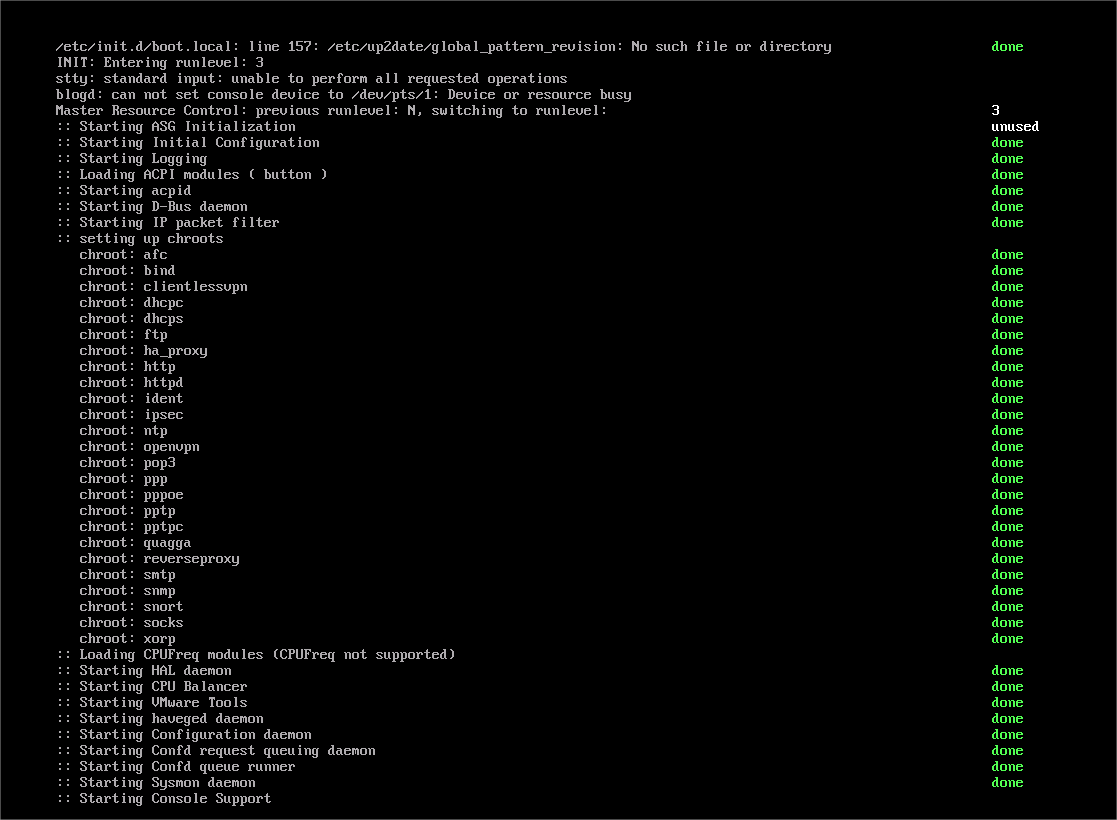
A computer screen shot of a error message

Description automatically generated

*Hình 21. Chọn Reboot để khởi động lại hệ thống*

* **Bước 6:** Khởi động lại Firewall Sophos UTM

**14**



*Hình 22. Quá trình khởi động lại diễn ra*

*A screenshot of a computer

Description automatically generatedHình 23. Khởi động thành công Firewall*

Sau khi khởi động thành công, chúng ta sẽ thấy IP được dùng để kết nối vào trang quản trị Firewall 10.0.0.1 *(Tài khoản mặc định để đăng nhập là* ***root*** *và đặt mật khẩu ở lần đầu tiên, tuy nhiên chúng ta thực hiện các thiết lập cho Firewall qua WebAdmin)*

* **Bước 7:** Đặt IP cho card VMNet 1 để kết nối vào Firewall để quản lý

Thiết lập lớp mạng cho VMnet1 là 10.0.0.0/8 tại VMware (Chọn Edit > Vituarl Network Editor…). Sau đó đặt IP cho card VMnet1 tại máy thật thành IP khác 10.0.0.1, ví dụ 10.0.0.100/8.

**15**

A screenshot of a computer

Description automatically generated

*Hình 24. Thay đổi IP cho card VMnet1*

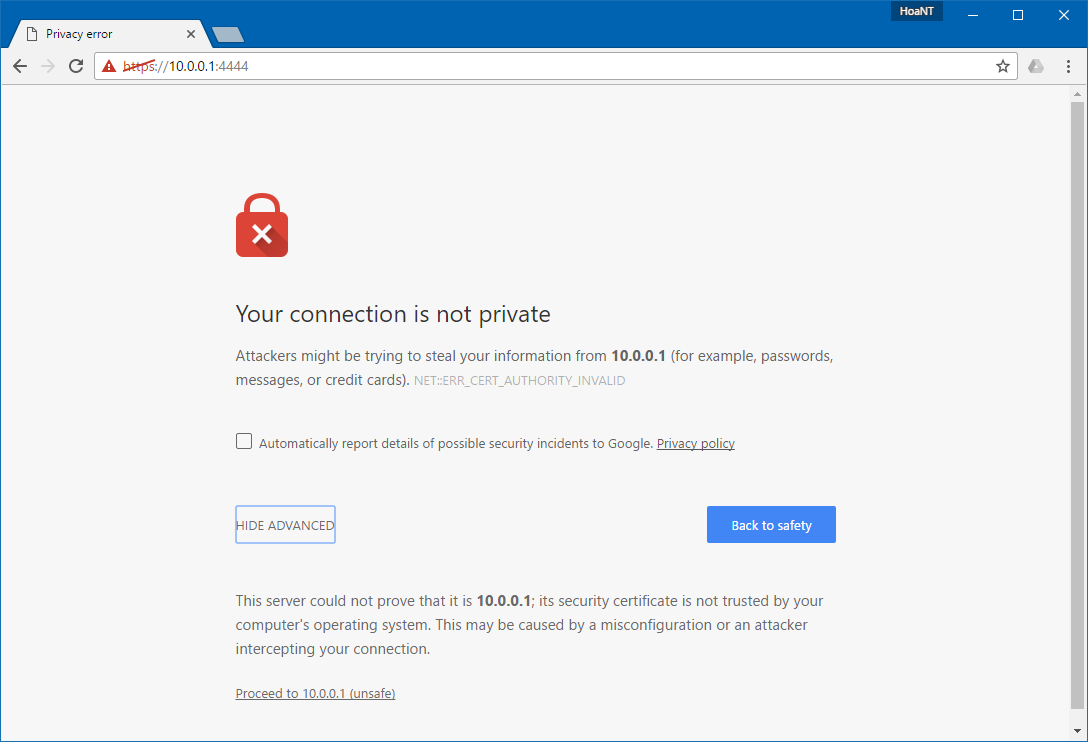
* **Bước 8:** Từ máy thật, thực hiện lệnh ping 10.0.0.1 để kiểm tra máy thật đã thấy máy firewall chưa. Nếu chưa thấy thì cần kiểm tra lại IP và card mạng.

A computer screen with white text

Description automatically generated

*Hình 25. Kiểm tra kết nối giữa máy thật và Firewall*

* **Bước 9:** Từ máy thật, kết nối vào WebAdmin của Firewall bằng địa chỉ https://10.0.0.1:4444

Nếu gặp cảnh báo bảo mật của trình duyệt, bỏ qua và tiếp tục truy cập WebAdmin

*Hình 26. Truy cập vào WebAdmin*

**16**

* **Bước 10:** Thiết lập các thông tin cơ bản cho Firewall Sophos và đặt mật khẩu cho tài khoản **admin**

A screenshot of a computer

Description automatically generated

Chọn **I accept the license agreement** và chọn **Perform basic system setup** và đợi khoảng 1 phút để hoàn tất quá trình thiết lập.

**17**

* **Bước 11:** Sau đó, đăng nhập bằng tài khoản **admin/ mật khẩu vừa thiết lập**
* *A screenshot of a computer

  Description automatically generatedHình 27. Đăng nhập vào WebAdmin*
* **Bước 12:** Sau khi đăng nhập thành công, chọn Cancel để bỏ qua trình Wizard.
* *A screenshot of a computer

  Description automatically generatedHình 28. Giao diện trang quản lý firewall*

## Lab 3: Thiết lập mô hình tường lửa Sophos UTM

**18**

* **Bước 13:** Cấu hình IP cho các interface của Firewall theo đúng mô hình triển khai Vào **Interface & Routing** để thiết lập các Interface
  + Tạo Interface cho vùng DMZ

*A screenshot of a computer

Description automatically generatedHình 29. Chọn New Interface và thiết lập như sau*

A screenshot of a computer

Description automatically generated

*Hình 30. Thiết lập Interface DMZ*

* + Tạo Interface External để kết nối Internet: Chọn New Interface và thiết lập như sau

A screenshot of a computer

Description automatically generated

*Hình 31. Thiết lập Interface External*

## Lab 3: Thiết lập mô hình tường lửa Sophos UTM

**19**

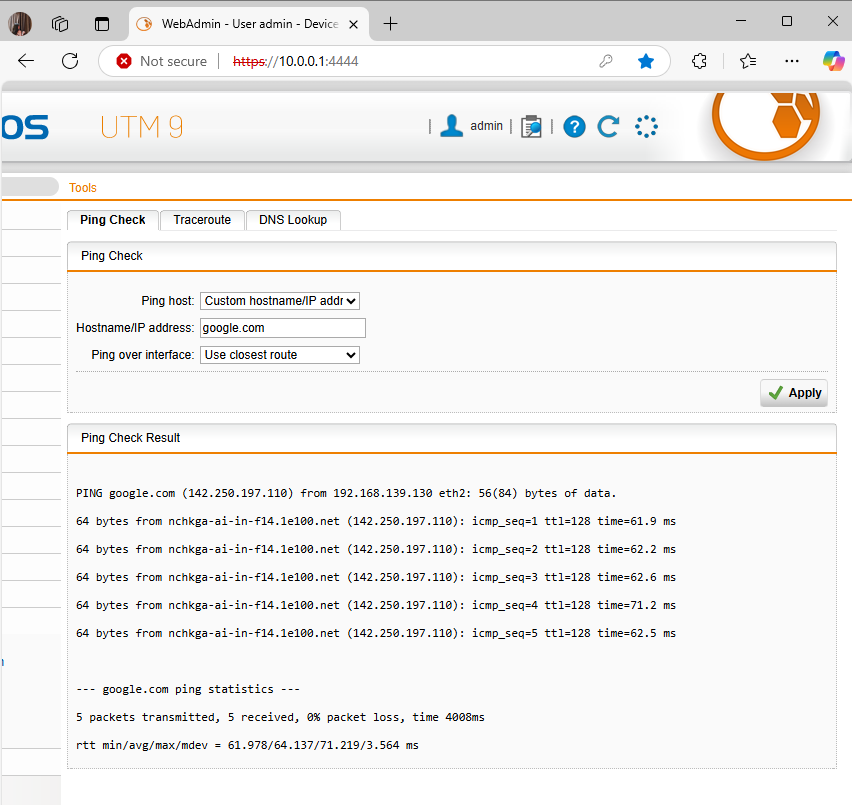
* **Bước 14:** Bật cả 3 3 interface và đặc biệt interface External đã nhận được IP từ DHCP Server hay chưa.

A screenshot of a computer

Description automatically generated

*Hình 32. Các Interface đã hoạt động*

Kiểm tra xem máy Firewall có kết nối được internet hay không bằng cách vào

****Support > Tool** > dùng tool Ping check để **ping google.com** dùng interface External

*Hình 33. Firewall đã kết nối thành công đến Internet*

## Lab 3: Thiết lập mô hình tường lửa Sophos UTM

**20**

* **Bước 15:** Cấu hình NAT Outbound. Cơ chế NAT sẽ xác định mạng nào sẽ NAT mạng ra ngoài Internet.

Vào **Network Protection > NAT > New Masquerading Rule** và cấu hình như sau:

*A screenshot of a computer

Description automatically generatedHình 34. Chọn interface External*

A screenshot of a computer

Description automatically generatedSau đó kích hoạt rule này. Kết quả sau khi cấu hình:

*Hình 35. Kết quả sau khi thêm rule NAT*

## Lab 3: Thiết lập mô hình tường lửa Sophos UTM

**21**

* **Bước 16:** Cấu hình Rule để máy chủ Domain Controller kết nối được internet bình thường. Vào **Network Protection > Rule > New Rule**

A screenshot of a computer

Description automatically generated

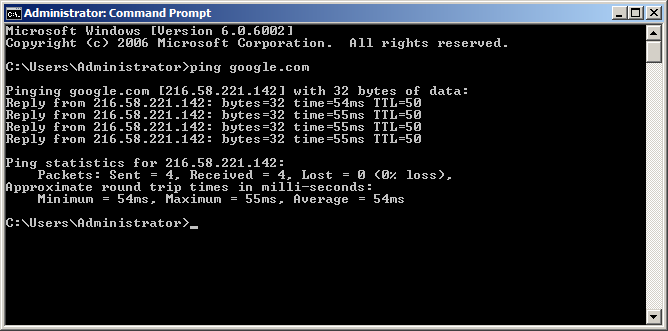
A screenshot of a computer

Description automatically generated*Hình 36. Chọn Any ở Source, Service và Destinations*

*Hình 37. Kết quả sau khi thiết lập Rule.*

## Lab 3: Thiết lập mô hình tường lửa Sophos UTM

**22**

* **Bước 17:** Kiểm tra kết nối internet của máy Domain Controller

*Hình 38. Ping thành công đến Google.com*

Nếu Domain Controller kết nối được Internet tức quá trình thiết lập tường lửa cơ bản đã thành công.

* **Bước 18:** Quay lại trang WebAdmin của Firewall thử tắt Rule Firewall và một vài Rule vừa thiết lập và quay lại máy Domain Controller để truy cập Internet và rút ra kết luận.

**Lab 3: Thiết lập mô hình tường lửa Sophos UTM**

**23**

# **CÂU HỎI**

Nêu nguyên tắc hoạt động của Firewall Sophos UTM và Domain Controller trong mô hình mạng đã thiết lập trong bài.

| **Vai trò** | **Thiết bị** | **Chức năng chính** |
| --- | --- | --- |
| Bảo mật, kiểm soát truy cập mạng | **Sophos UTM** | Firewall, NAT, Proxy, Web/DNS filtering |
| Quản lý người dùng và thiết bị | **Domain Controller** | Active Directory, DNS, DHCP, GPO |