## 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**

**2**

# **TỔNG QUAN**

## Mục tiêu

* + Xây dựng mô hình mạng với Firewall.
  + Tìm hiểu, thiết đặt và sử dụng Firewall doanh nghiệp SOPHOS.

## Giới thiệu về Firewall SOPHOS

**Sophos UTM** (Unify Threat Management) là một giải pháp tường lửa bảo mật hoàn chỉnh cho doanh nghiệp được sử dụng rất phổ biến bao gồm nhiều tính năng như Network Protection, Web Protection, Endpoint Protection, Load Balancing WAN, QoS, ...

* **Network Protection:** Thiết lập tường lửa ngăn chặn sự tấn công mạng từ bên ngoài và bên trong, tạo các bộ quy tắc truy cập mạng giúp chỉ cho phép các ứng dụng được phép truy cập mạng, chặn theo quốc gia, chặn tấn công Dos, tính năng IPS...
* **Web Protection:** Thiết lập các quy tắc truy cập web như cho phép hoặc chặn website, chặn download, block quảng cáo, chặn các trang web độc hại, khóa website theo từ khóa, tính năng proxy, caching...
* **Endpoint Protection:** Quản lý antivirus cho máy trạm, Sophos UTM Home cấp bản quyền miễn phí cho 10 máy trạm sử dụng Sophos Antivirus.

Thông tin chi tiết về phiên bản thương mại tại [https://www.sophos.com/en-](https://www.sophos.com/en-us/products/unified-threat-management.aspx) [us/products/unified-threat-management.aspx](https://www.sophos.com/en-us/products/unified-threat-management.aspx)

*Sophos cho phép đăng ký dùng thử bản thương mại UTM trong 30 ngày, trong điều kiện thực hành, sinh viên có thể dùng bản này để thử nghiệm.*

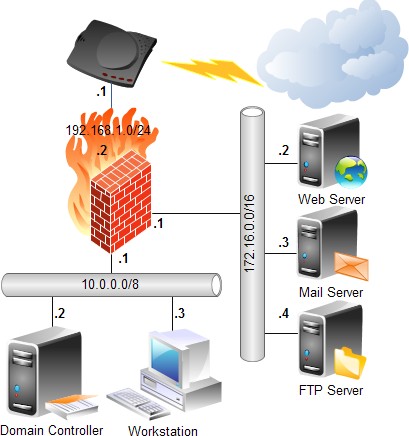
## Môi trường & mô hình mạng

Xây dựng mô hình mạng với tường lửa Sophos UTM bảo vệ 2 lớp mạng

* Mạng nội bộ: 10.0.0.0/8 với 1 Domain Controller để quản lý tập trung các máy tính theo domain.
* Vùng DMZ: 172.16.0.0/16 bao gồm các Server Web, Mail, FTP.

*Trong bài thực hành này sẽ thực hiện cài đặt và thiết lập Domain Controller và Firewall Sophos UTM. Sinh viên cần xem kỹ và thiết lập như hướng dẫn cụ thể của bài lab.*

**3**



*Hình 1. Mô hình mạng thiết lập Firewall*

Thực chất trong mô hình trên, sinh viên chỉ cần chuẩn bị 2 máy tính (VMWare). Trong đó:

* **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

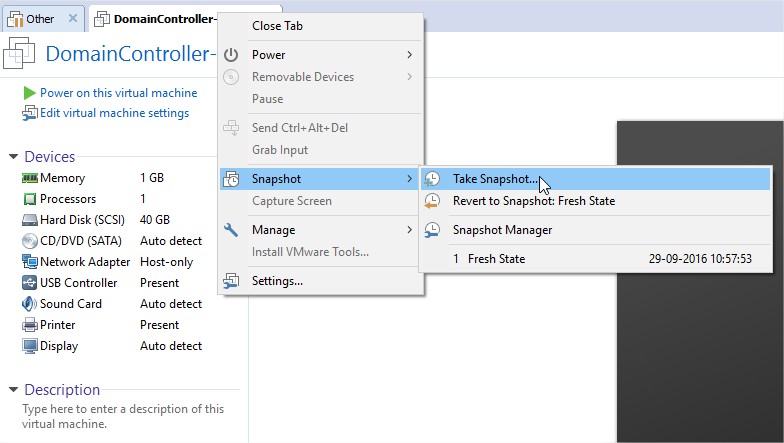
## Thiết lập máy chć Domain Controller

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

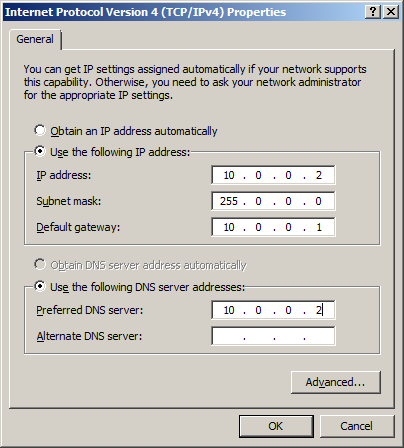
+ RAM: 512MB – 1GB

+ 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*

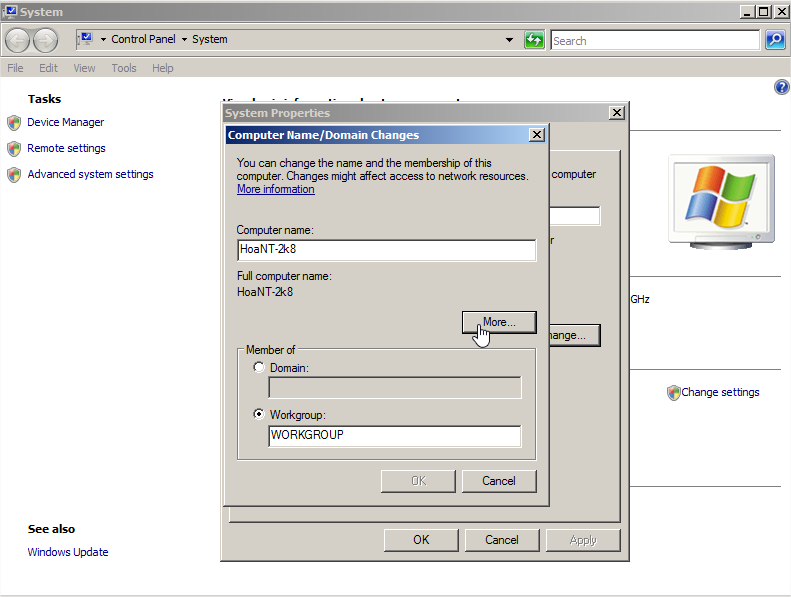
* **Bước 2:** Đặt IP cho máy Domain Controller là 10.0.0.2/8

*Hình 3. Thay đổi IP của máy chủ*

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

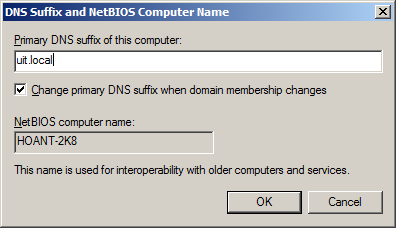
**5**

* **Bước 3:** Đặt DNS Suffix bằng cách click phải lên My Computer > Propertites > Change Setting > Change > chọn More.



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

Sau đó nhập DNS Suffix cần đặt. Trong hướng dẫn này sử dụng tên uit.local, để phân biệt khi thực hiện sinh viên đặt theo dạng **tên 2 sinh viên.local.** Ví dụ **vietnam.local**



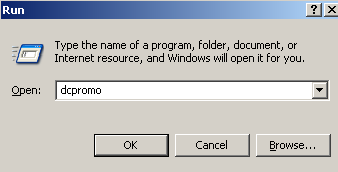
Sau đó Restart lại máy tính để áp dụng các thay đổi.

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

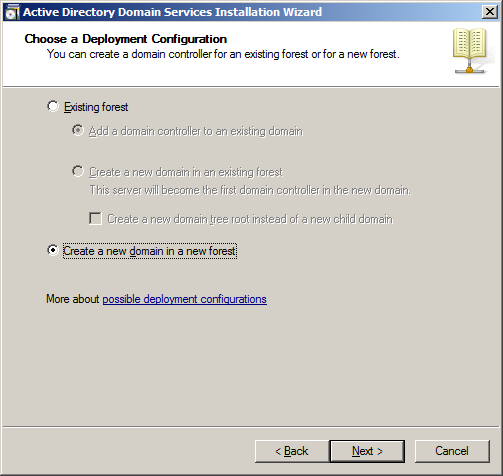
Hướng dẫn này thực hiện trên Windows Server 2008, nếu sử dụng phiên bản khác có thể có một số thay đổi trong quá trình nâng cấp.

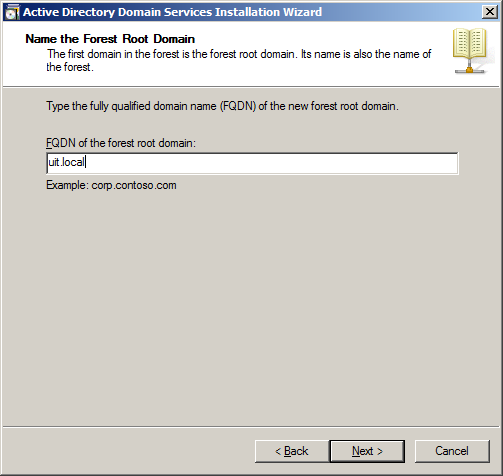
## Lab 3: Thiết lập mô hình tường lửa Sophos UTM

**6**



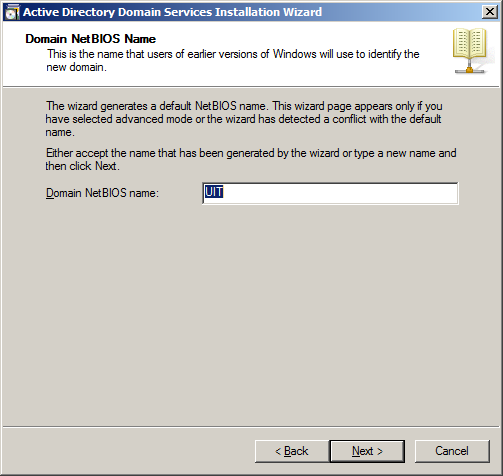
*Hình 5. Vào Start > run > nhập* ***dcpromo***



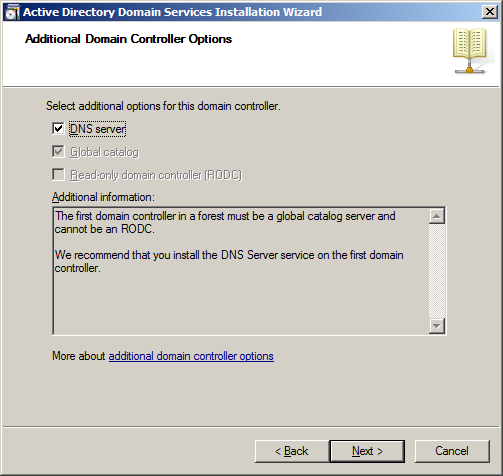
*Hình 6. Chọn Create a new domain in a new forest*

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

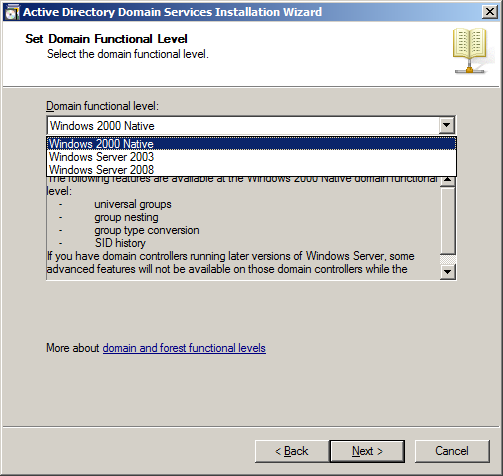
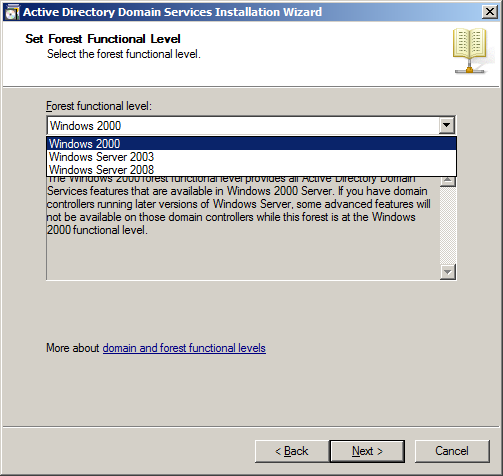
**7**

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

*Hình 8. Domain NetBIOS*

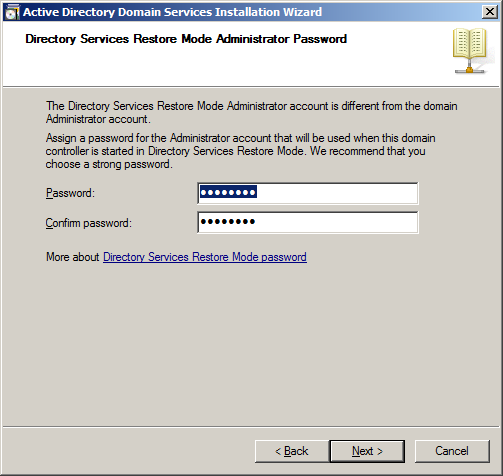


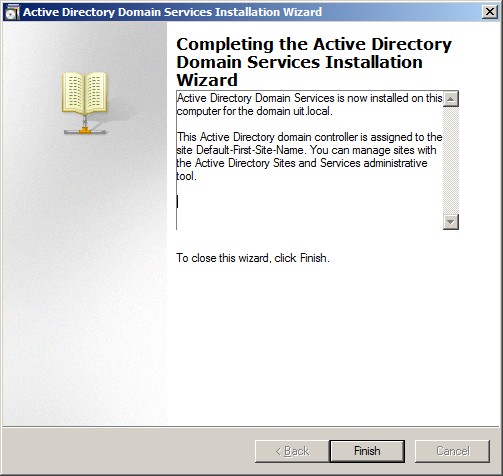
*Hình 9. Chọn DNS Server*



*Hình 10. Chọn Windows 2000*

**8**

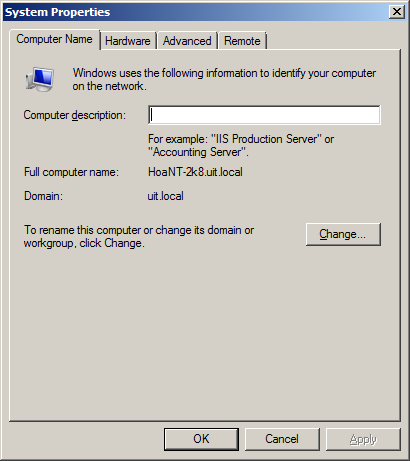


*Hình 11. Thiết lập mật khẩu quản trị*

*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**



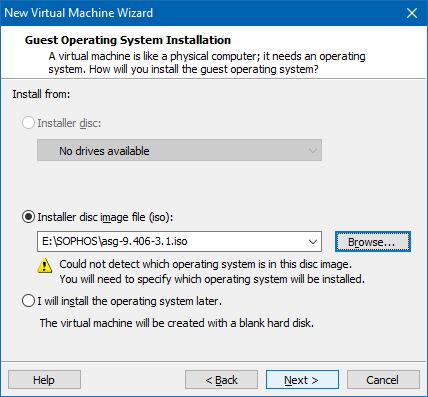
* **Bước 5:** Tiến hành Snapshot lại để lưu lại trạng thái máy ảo lúc này.

## 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.



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

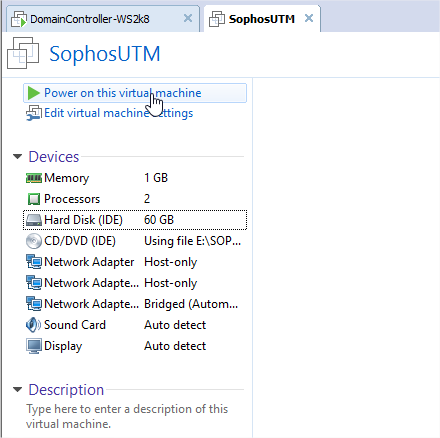
**10**

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)*

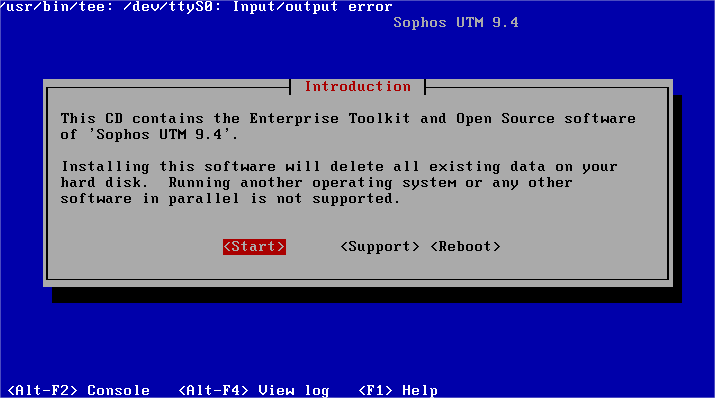
*Hình 14. Cấu hình máy ảo có thể sử dụng Sophos UTM ổn định*

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

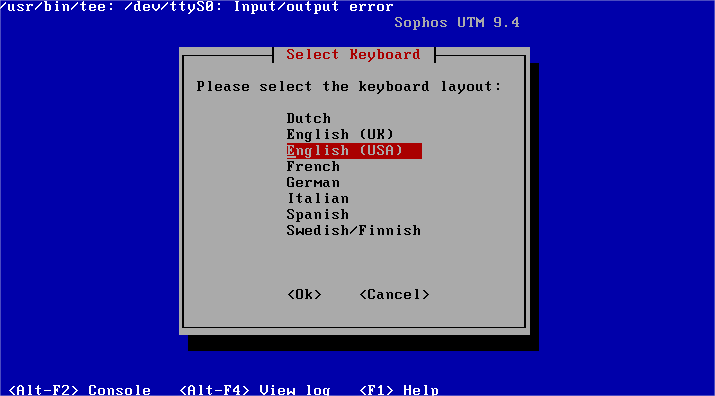
*Hình 15. Cài đặt Sophos UTM 9*

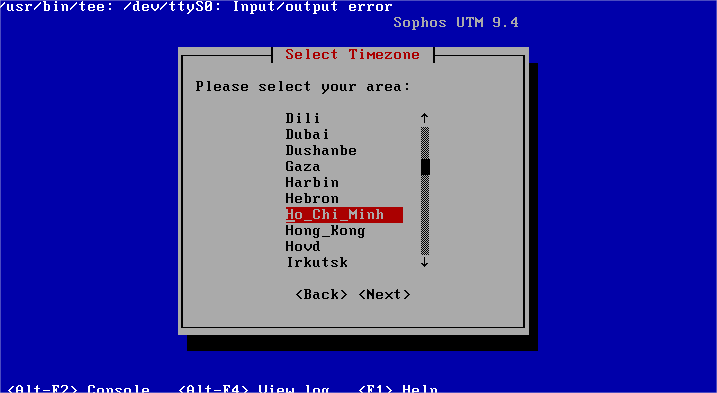
## Lab 3: Thiết lập mô hình tường lửa Sophos UTM

**11**

Sau đó, chọn **Start** để bắt đầu

* **Bước 4:** Thiết lập ngôn ngữ và múi giờ

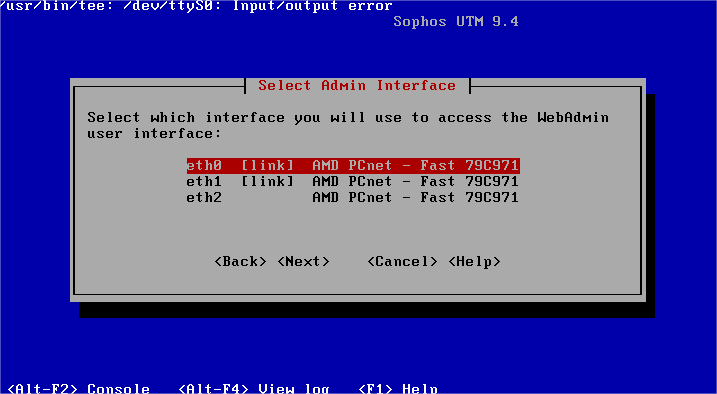




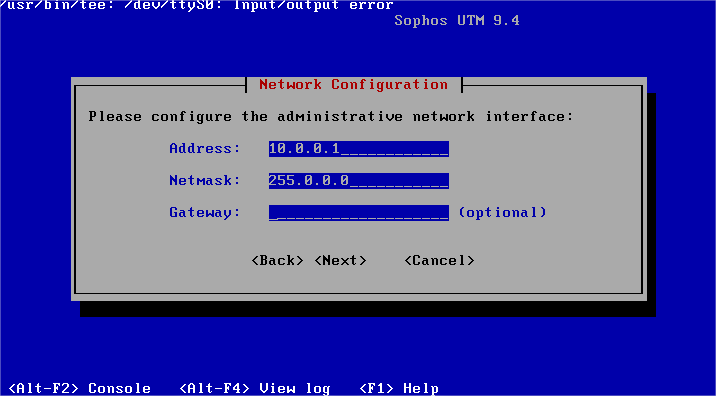
*Hình 16. Chọn ngôn ngữ English và múi giờ Ho\_Chi\_Minh*

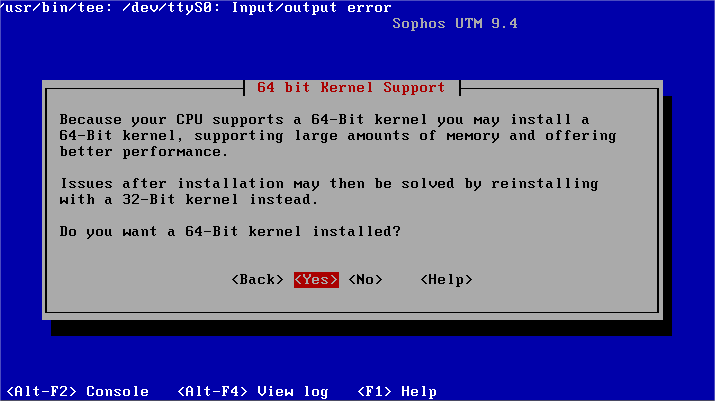
## Lab 3: Thiết lập mô hình tường lửa Sophos UTM

**12**

* **Bước 5:** Chọn card mạng eth0 và thiết lập IP mặc định cho trang quản trị

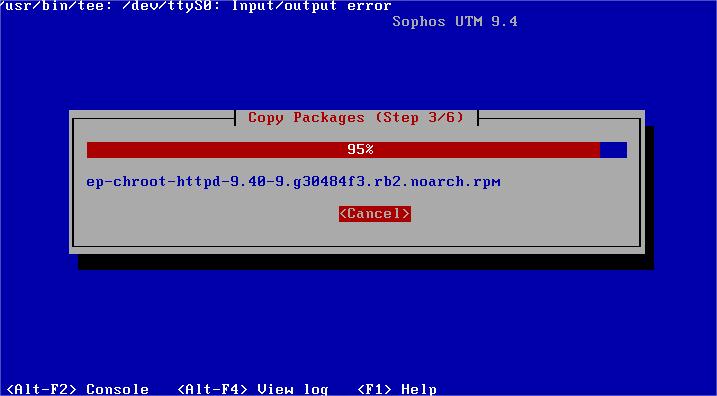
*Hình 17. Chọn card mạng eth0 cho WebAdmin của Firewall*



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

*Hình 19. Chọn Yes nếu sử dụng CPU hỗ trợ 64 bit kernel*

**13**

Quá trình cài đặt diễn ra trong 6 bước:

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

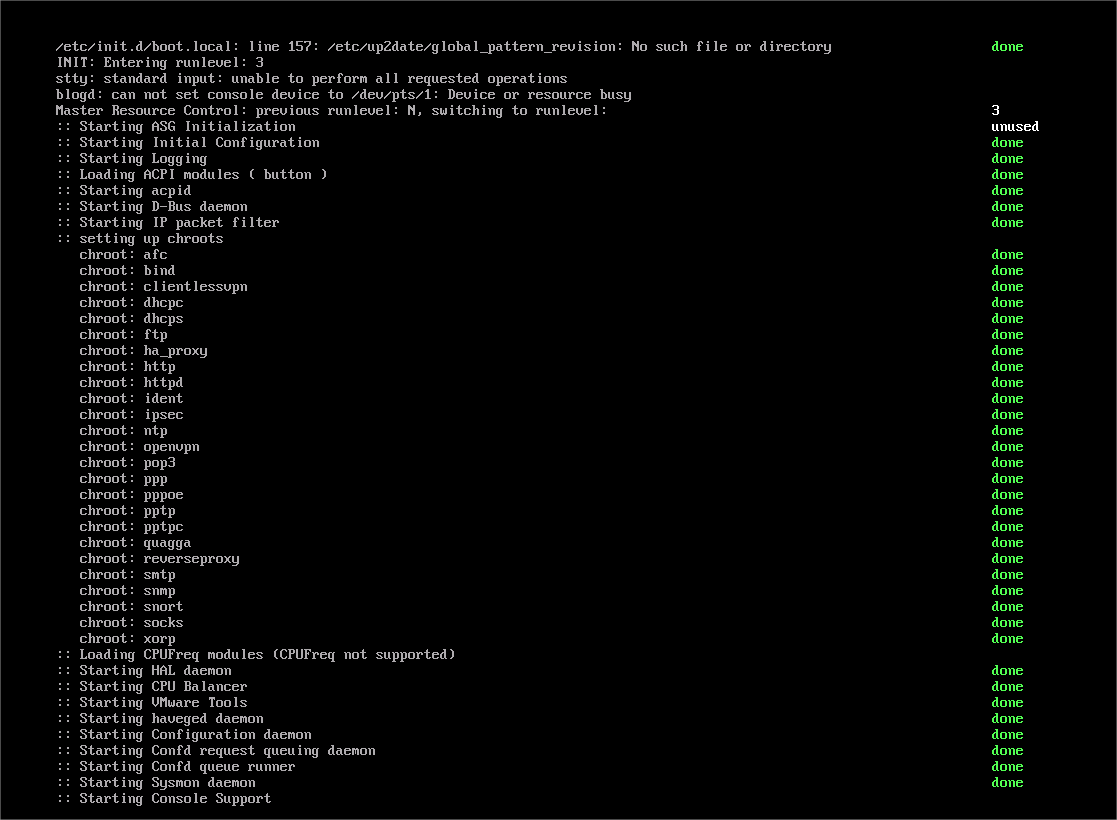
Sau khi cài đặt thành công, hệ thống sẽ thông báo thông tin địa chỉ IP đăng nhập vào trang quản trị WebAdmin là https://10.0.0.1:4444/

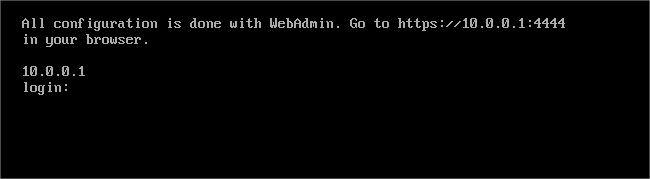


*Hình 21. Chọn Reboot để khởi động lại hệ thống*

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

**14**



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

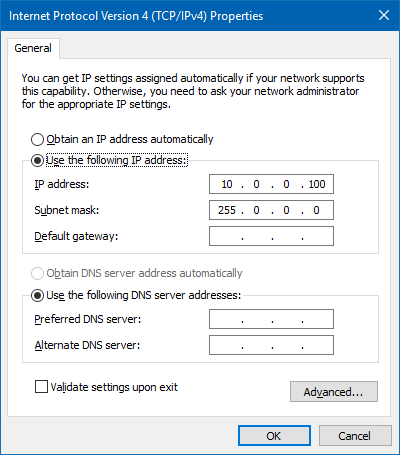
*Hình 23. Khởi động thành công Firewall*

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

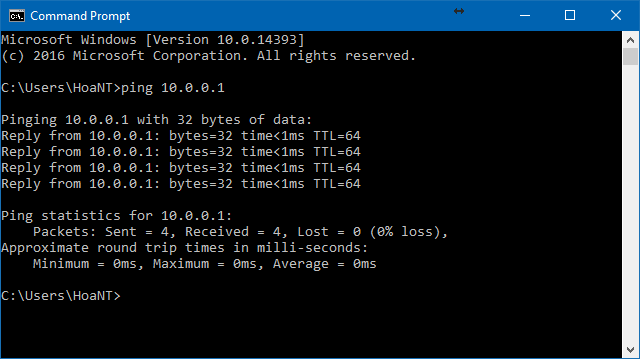
Thiết lập lớp mạng cho VMnet1 là 10.0.0.0/8 tại VMware (Chọn Edit > Vituarl Network Editor…). Sau đó đặt IP cho card VMnet1 tại máy thật thành IP khác 10.0.0.1, ví dụ 10.0.0.100/8.

**15**



*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.

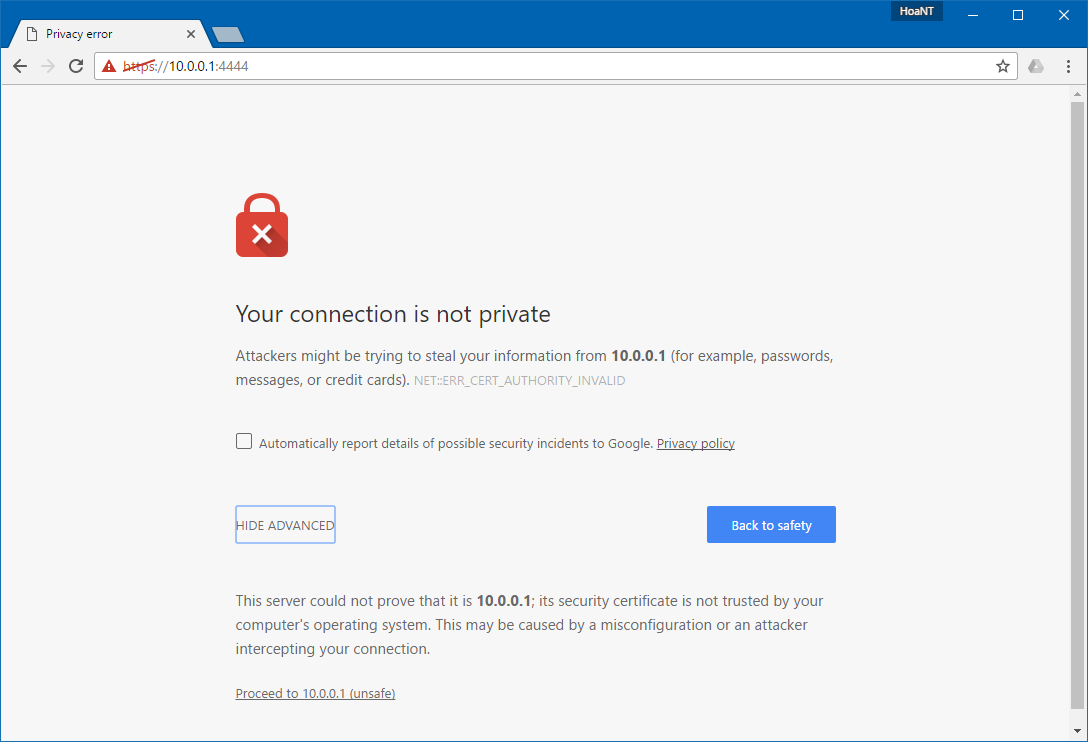


*Hình 25. Kiểm tra kết nối giữa máy thật và Firewall*

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

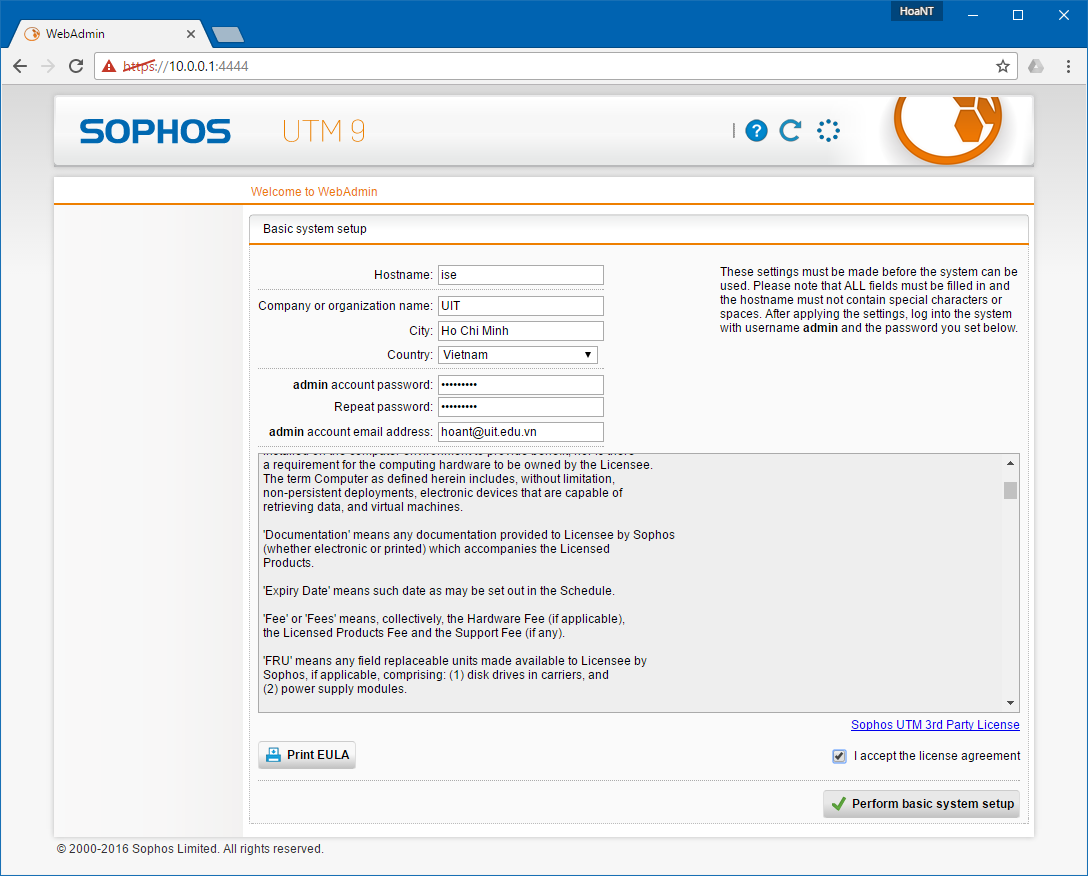
Nếu gặp cảnh báo bảo mật của trình duyệt, bỏ qua và tiếp tục truy cập WebAdmin

**16**



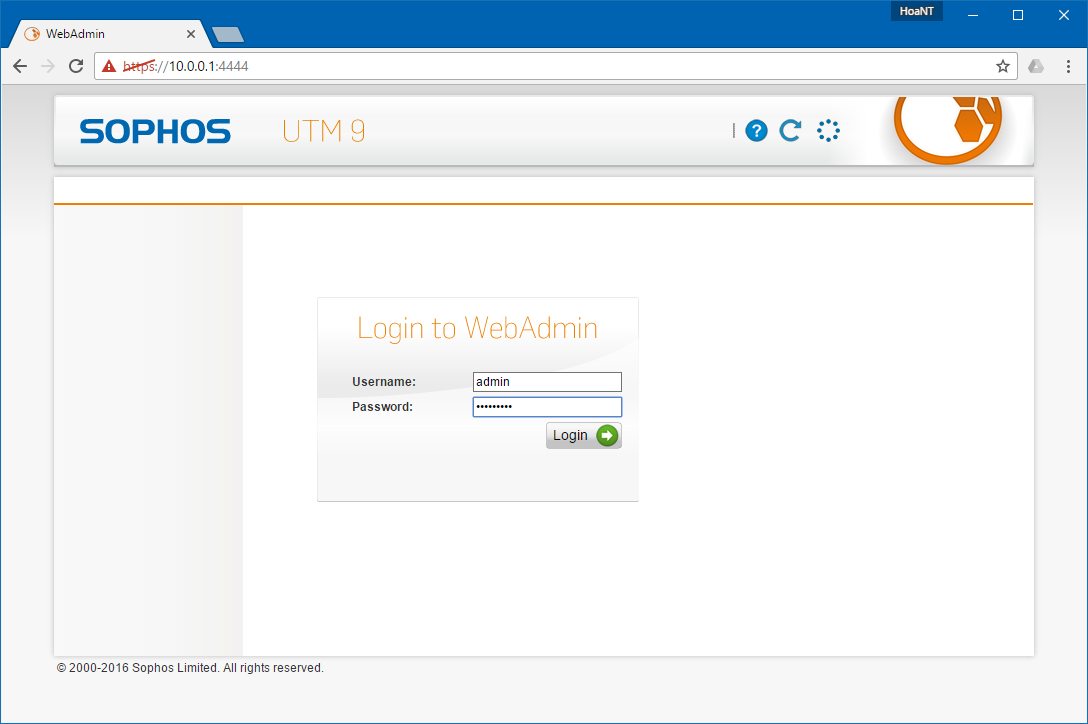
*Hình 26. Truy cập vào WebAdmin*

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

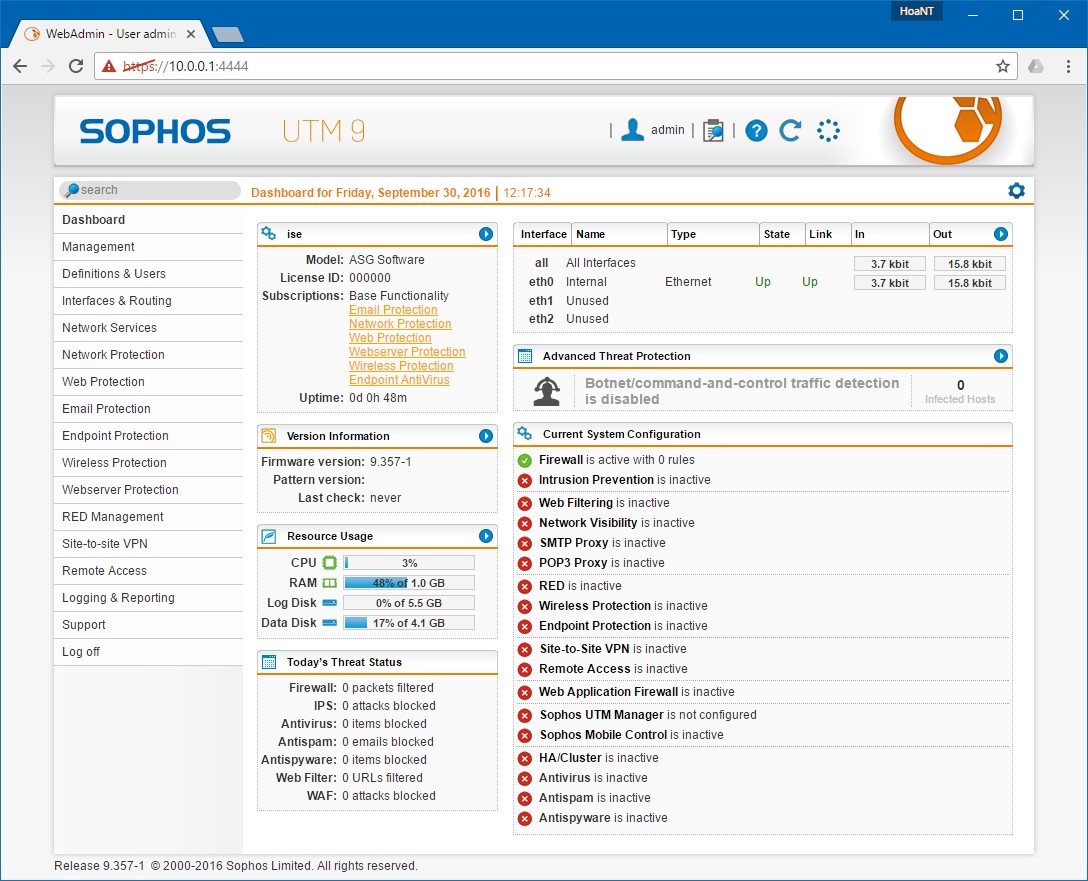


Chọn **I accept the license agreement** và chọn **Perform basic system setup** và đợi khoảng 1 phút để hoàn tất quá trình thiết lập.

**17**

* **Bước 11:** Sau đó, đăng nhập bằng tài khoản **admin/ mật khẩu vừa thiết lập**

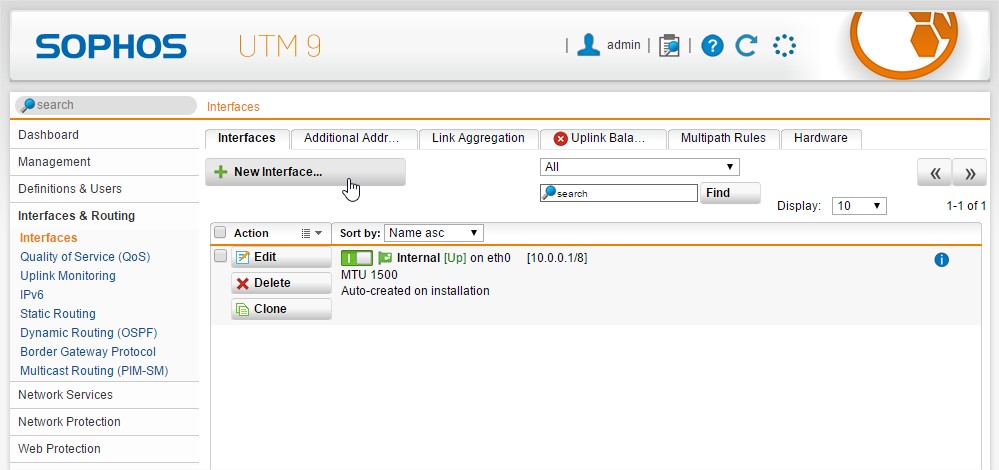
*Hình 27. Đăng nhập vào WebAdmin*

* **Bước 12:** Sau khi đăng nhập thành công, chọn Cancel để bỏ qua trình Wizard.

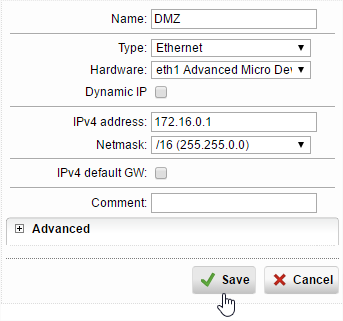
*Hình 28. Giao diện trang quản lý firewall*

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

**18**

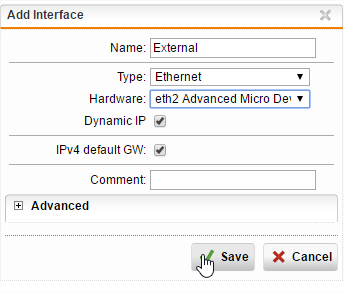
* **Bước 13:** Cấu hình IP cho các interface của Firewall theo đúng mô hình triển khai Vào **Interface & Routing** để thiết lập các Interface
  + Tạo Interface cho vùng DMZ

*Hình 29. Chọn New Interface và thiết lập như sau*



*Hình 30. Thiết lập Interface DMZ*

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

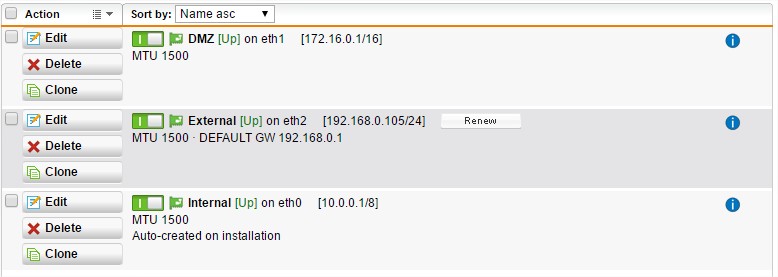


*Hình 31. Thiết lập Interface External*

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

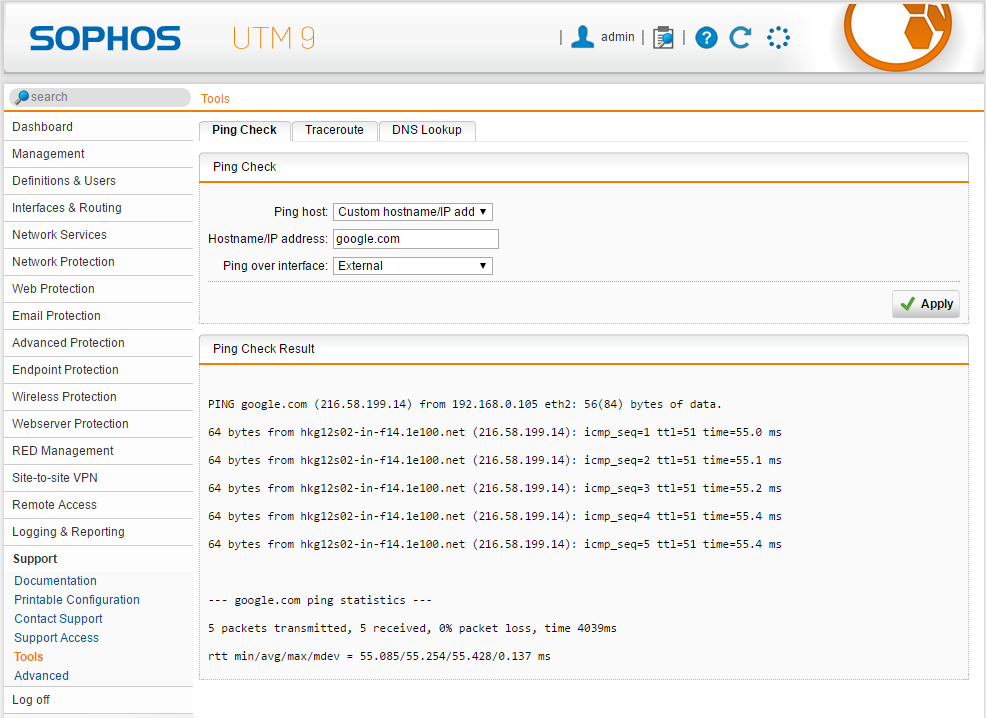
**19**

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



*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

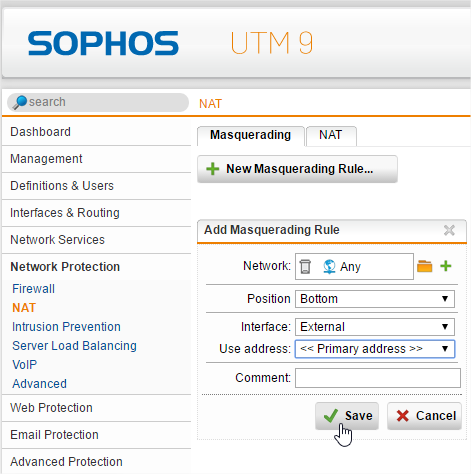
*Hình 33. Firewall đã kết nối thành công đến Internet*

**Lưu ý:** *Nếu không kết nối được hay interface External không nhận được IP thì chúng ta sẽ không làm gì được nữa và cần kiểm tra kỹ lại quá trình cấu hình theo các bước đã hướng dẫn hoặc khởi động lại Firewall để kiểm tra lại.*

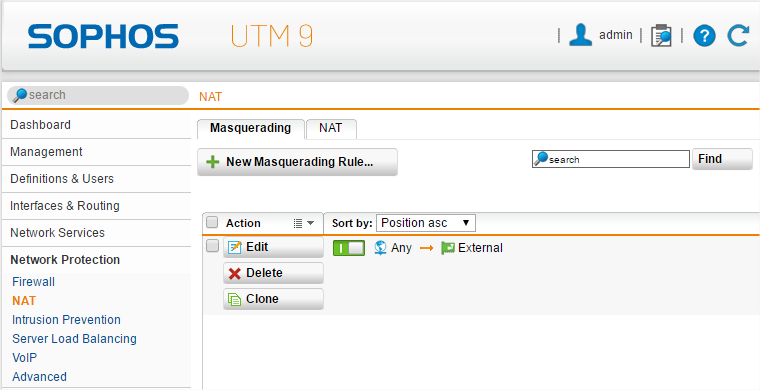
## Lab 3: Thiết lập mô hình tường lửa Sophos UTM

**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:

*Hình 34. Chọn interface External*

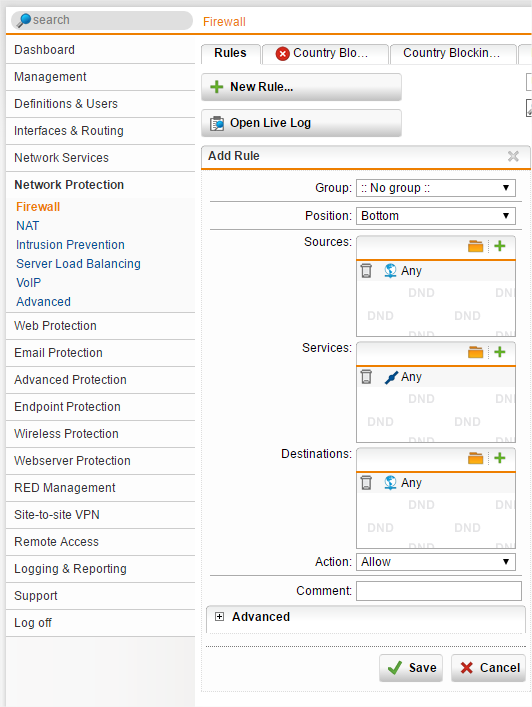
Sau đó kích hoạt rule này. Kết quả sau khi cấu hình:

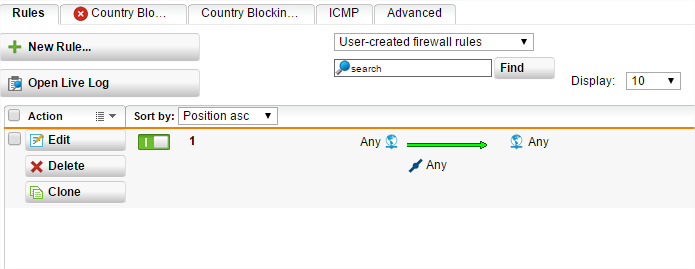
*Hình 35. Kết quả sau khi thêm rule NAT*

## 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**

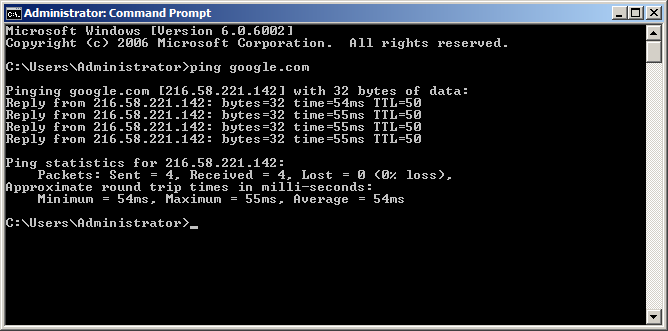


*Hình 36. Chọn Any ở Source, Service và Destinations*

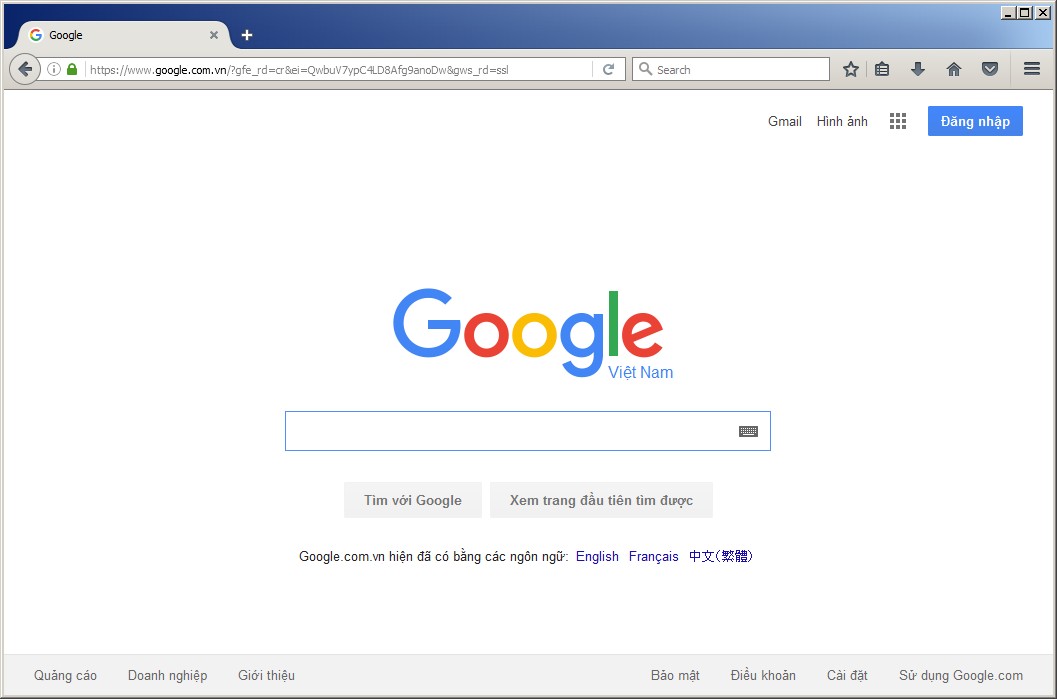
*Hình 37. Kết quả sau khi thiết lập Rule.*

## 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*



*Hình 39. Dùng trình duyệt để truy cập web và kiểm tra.*

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.

**Lưu ý:** *Sau khi hoàn thành bài Lab, giữ nguyên trạng thái của Firewall và Domain Controller server để tiếp tục thực hành về Sophos UTM trong bài lab tiếp theo.*

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

**23**

# **CÂU HỎI**

*Sau quá trình thực hành, sinh viên trả lời câu hỏi sau:*

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

# **YÊU CẦU**

* + Sinh viên tìm hiểu và thực hành theo hướng dẫn. Thực hiện cá nhân .
  + Sinh viên báo cáo kết quả thực hiện và nộp bài gồm:

## - Báo cáo:

+ Trình bày trong file Word (.doc, .docx).

+ Đặt tên theo định dạng: [Mã lớp]-LabX\_MSSV-Tên SV.

*Ví dụ: [NT101.H11.1]-Lab1\_14520000-Viet*

- **Video:**

+ Quay lại quá trình thực hiện Lab của sinh viên.

Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo. Nộp file báo cáo trên theo thời gian đã thống nhất tại classroom.

**Đánh giá**: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

* + Chuẩn bị tốt và đóng góp tích cực tại lớp.
  + Video trình bày trực quan, dễ hiểu.
  + Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

*Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.*

# **THAM KHẢO**

1. Hướng dẫn chi tiết Cấu hình Active Directory trên Windows Server 2008: [http://quantrimang.com/huong-dan-cai-dat-active-directory-tren-windows-server-](http://quantrimang.com/huong-dan-cai-dat-active-directory-tren-windows-server-2008-74472) [2008-74472](http://quantrimang.com/huong-dan-cai-dat-active-directory-tren-windows-server-2008-74472)
2. Sophos UTM 9 documentation:

<https://www.sophos.com/en-us/support/documentation/sophos-utm.aspx>

**HẾT**