**5**

Lab

Tường lửa Sophos UTM:

**Xây dựng chính sách Web**

SOPHOS UTM Firewall – Web Protection

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

GVTH: Phạm Trọng Huynh

Học kỳ II – Năm học 2022-2023

**Lưu hành nội bộ**

**Lab 5: Xây dựng chính sách Web – Sophos UTM**

**2**

**Họ và Têng : Giang Thị Sông Hằng**

**Lớp : CNPM2**

**MSSV:1050080133**

**Link youtube:** [**https://youtu.be/GlzPwnrN93s**](https://youtu.be/GlzPwnrN93s)

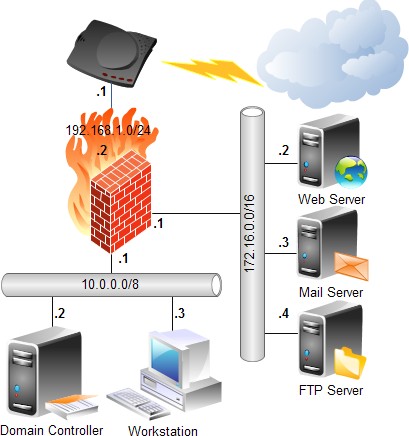
# TỔNG QUAN

## Mục tiêu

* + Sử dụng mô hình mạng với Firewall đã thiết lập.
  + Xây dựng bộ chính sách bảo vệ khi truy cập website cho người dùng.
  + Tùy biến và hoàn thiện nội dung cảnh báo & thiết lập các chính sách mở rộng.

## Môi trường & mô hình mạng

*Sử dụng mô hình mạng đã xây dựng từ Lab 03.*

* 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.

*Hình 1. Mô hình mạng thiết lập Firewall*

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

* **Máy 1**: Windows Server 2008 làm Domain Server (1 card mạng Host-only)
* **Máy 2**: Firewall Sophos UTM 9.4

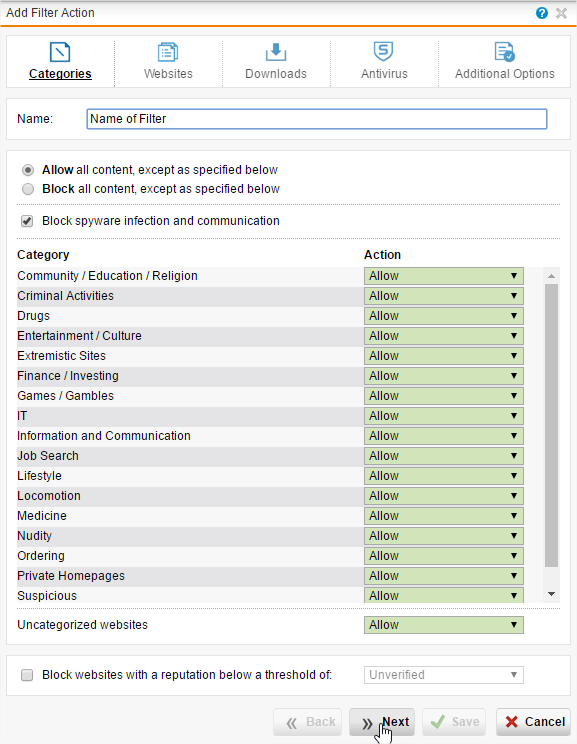
**Lab 5: Xây dựng chính sách Web – Sophos UTM**

**3**

# THỰC HÀNH

## 1. Tổng quan về xây dựng chính sách bảo vệ truy cập web

Sophos cho phép thiết lập các chính sách bảo vệ truy cập website với nhiều tùy biến mở rộng. Quy trình tạo một chính sách cơ bản:

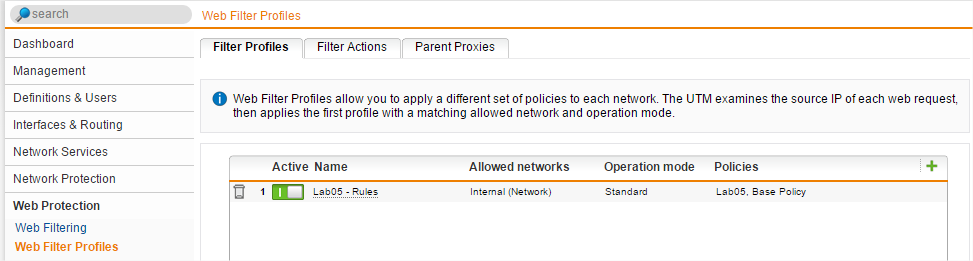
1. Xây dựng bộ lọc tại **Web Filter Profile > Tab Filter Actions > New Filter Action...**

*Hình 2. Xây dựng bộ lọc mới*

Khi xây dựng bộ lọc, Sophos cho phép nhiều tùy biến như xây dựng chính sách với các thể loại website theo bộ lọc và đánh giá từ Sophos, xây dựng chính sách với các website cụ thể, giới hạn thời gian truy cập tối đa, hạn chế các nội dung trên web, …

1. Tạo và áp dụng chính sách tại **Web Filter Profiles > Filter Profiles**

Có thể áp dụng chính sách với tất cả người dùng hoặc với người dùng cụ thể trong các khoản thời gian khác nhau



*Hình 3. Thiết lập và áp dụng chính sách*

## Lab 5: Xây dựng chính sách Web – Sophos UTM

**4**

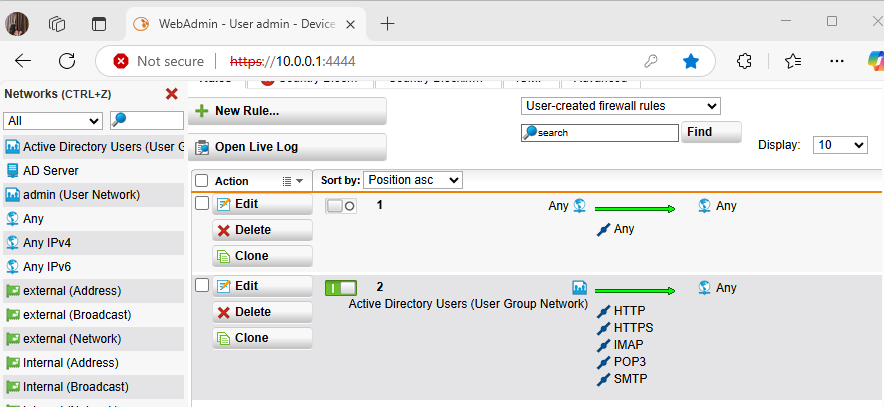
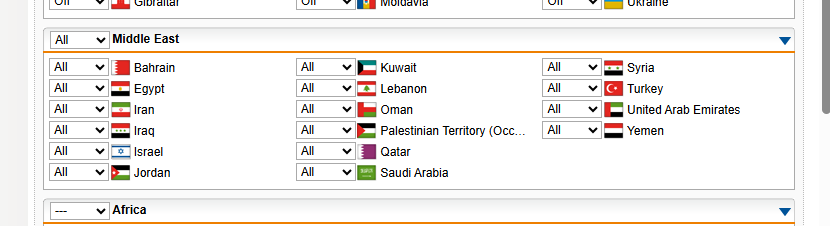
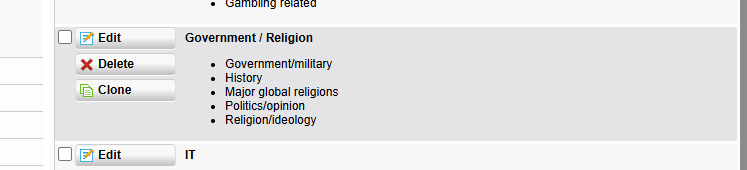
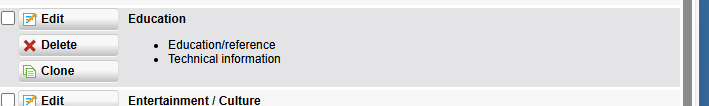
1. **Xây dựng bộ chính sách béo vệ truy cập Web**

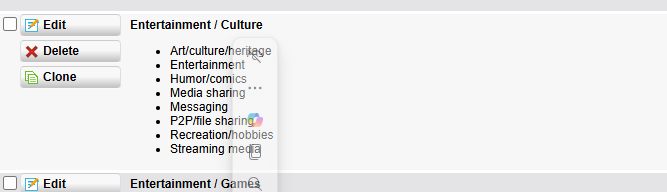
Dựa vào các nội dung đã thực hành và nghiên cứu sử dụng Sophos, sinh viên thiết lập các chính sách phù hợp để đảm bảo cho việc truy cập web an toàn cho một doanh nghiệp. Các yêu cầu và mô tả cụ thể của bộ chính sách như sau:

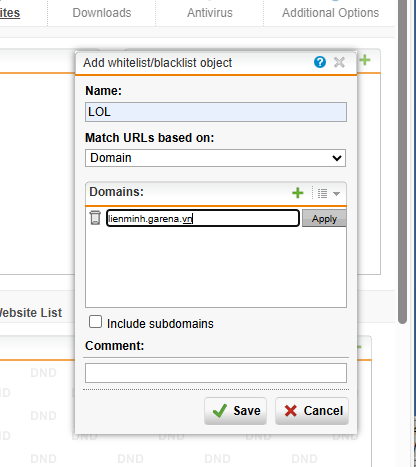
## Môi trường giả định:

Hệ thống mạng nội bộ xây dựng theo mô hình domain như đã xây dựng gồm 3 user: Administrator (Quản trị), user a và b (tương ứng 2 user trong nhóm sinh viên đã tạo). Máy người dùng sử dụng trình duyệt **Chrome version 49.0** để truy cập Internet.

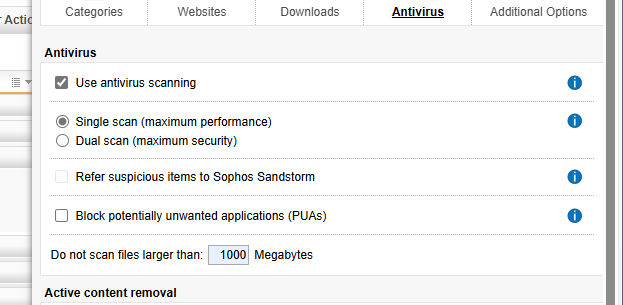
## Chính sách truy cập Internet:

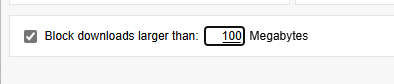
* 1. **Chỉ cho phép toàn bộ người dùng sử dụng Internet để truy cập web, sử dụng email qua các giao thức SMTP, IMAP, POP3, chặn tất cả các dịch vụ khá*.*
  2. Chặn truy cập tất cả website từ Trung Quốc và toàn bộ khu vực Trung Đông (Iran, Iraq, Syria, …).Cấm truy cập tất cả các website tìm kiếm việc làm, trong đó có một số website tìm kiếm việc làm tại TP.HCM.
  3. Cảnh báo khi truy cập các website về vũ khí, chính trị - tôn giáo. Không cảnh báo với các website giáo dục.
  4. Giới hạn truy cập các website Giải trí và Game trong tối đa 60 phút, riêng đối với các website giải trí dạng chia sẻ video như Youtube.com, vimeo.com (Streaming Media) thì chỉ cảnh báo khi truy cập.

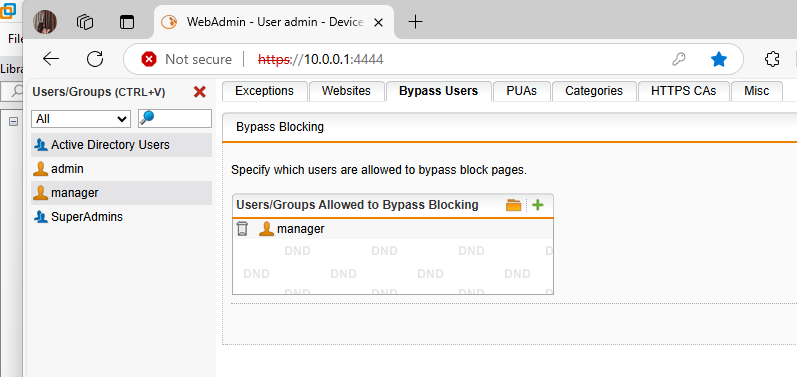


 Cấm hẳn truy cập website lienminh.garena.vn

* 1. Quét virus khi download tập tin.



* 1. Không cho download các file lớn hơn 100MB. 
  2. Khi truy cập vào website bị chặn thì có thể mở khóa trực tiếp để bỏ chặn website đó với tài khoản **manager / 12345** (thiết lập tại Sophos Firewall – *xem kết quả minh họa).*

**

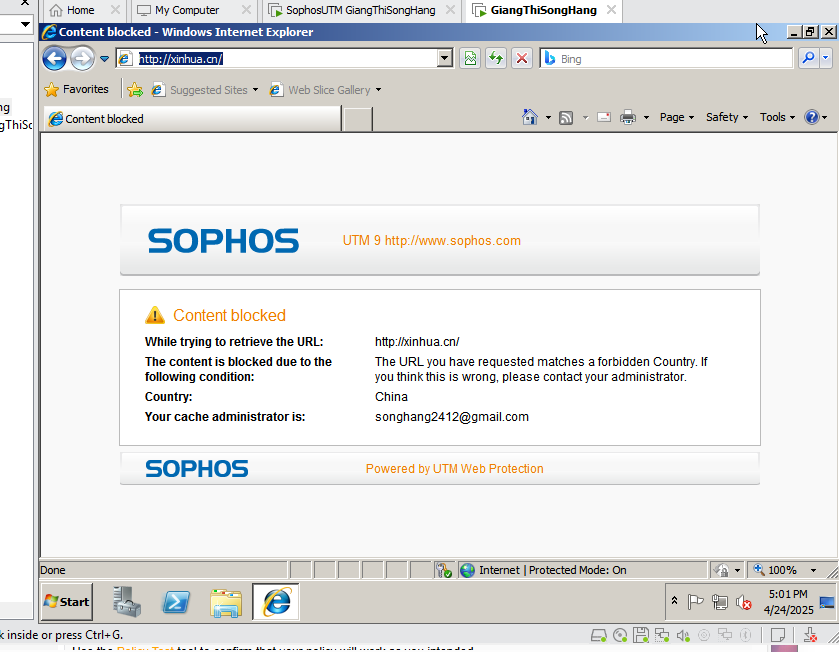
## Kiểm tra kết qué & ứng dụng

Kiểm tra kết quả sau khi đã xây dựng bộ chính sách ở bước 2 với từng trường hợp trong kịch bản kiểm tra tương ứng với các quy tắc ở phần 2 như sau, nếu chưa đúng yêu cầu cần điều chỉnh lại chính sách:

## Lab 5: Xây dựng chính sách Web – Sophos UTM

**5**

* 1. Truy cập 1 website được phép truy cập bình thường, thao tác traceroute và ping đến website đó không thành công.
  2. Không thể truy cập website báo Tân Hoa xã (xinhua.vn – news.cn) và ít nhất 2 website khác từ Trung Quốc và Trung Đông.



*Hình 4. Không thể truy cập website báo Tân Hoa xã – Trung Quốc*

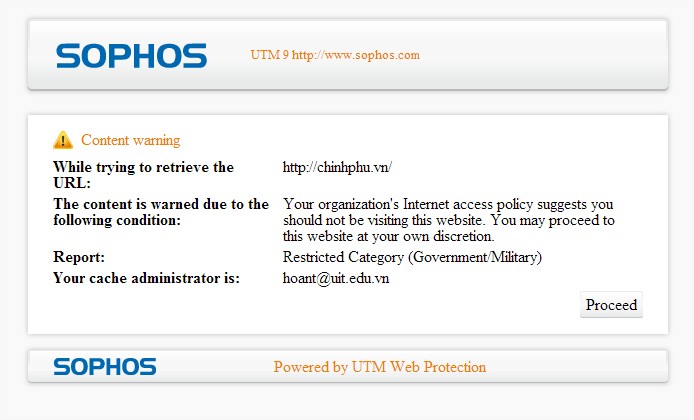
* 1. Không thể vào các website về tìm kiếm việc làm trên thế giới và tại Việt Nam, tại TP.HCM trong đó chặn được 4 website sau: vietnamworks.com.vn, vieclam.tuoitre.vn, timviecnhanhhcm.com, itviec.com. Nếu website nào chưa chặn được theo bộ lọc của Sophos thì chỉ định website đó ứng với thể loại Job Search của hệ thống để khi cần chặn chỉ cần block Job Search category *(không thêm địa chỉ web trực tiếp vào Rule).*

A screenshot of a computer error message

Description automatically generated*Hình 5. Website timviecnhanhhcm.com được đưa vào thể loại Job Search bị cấm*

**6**

* 1. Hiện cảnh báo đối với một số website thuộc thể loại vũ khí, chính trị - tôn giáo như trueswords.com (vũ khí), giacngo.vn (tôn giáo), chinhphu.vn (chính trị).



A computer screen shot of a computer

Description automatically generated*Hình 6. Cảnh báo khi truy cập chinhphu.vn, có thể truy cập khi nhấn Proceed* Truy cập bình thường với các website giáo dục, trường đại học như uit.edu.vn, moet.gov.vn (Bộ GD-ĐT) mà không có cảnh báo.

*Hình 7. Truy cập website moet.vn bình thường*

* 1. Kiểm tra khi truy cập một số website giải trí như kenh14.vn, yeah1.com,… và gamevui.vn, pokemongo.com chỉ cho phép truy cập tối đa trong 60 phút

**7**

A screenshot of a computer

Description automatically generated

*Hình 8. Giới hạn có thể truy cập web giải trí tối đa 60 phút*

Khi thiết lập Quota (quy định thời gian truy cập tối đa) thì thời gian này sẽ được tính từ khi nào và có được reset lại không? Nếu có thì reset khi nào và có cách nào thực hiện reset thủ công không? *Minh họa nếu có thể*

* Kiểm tra kết quả khi vào trang Youtube.com và Vimeo.com.

A screenshot of a computer

Description automatically generated

**11**