Họ và tên: Nguyễn Thanh Ý

Lớp: 08\_CNPM

MSSV: 0850080056

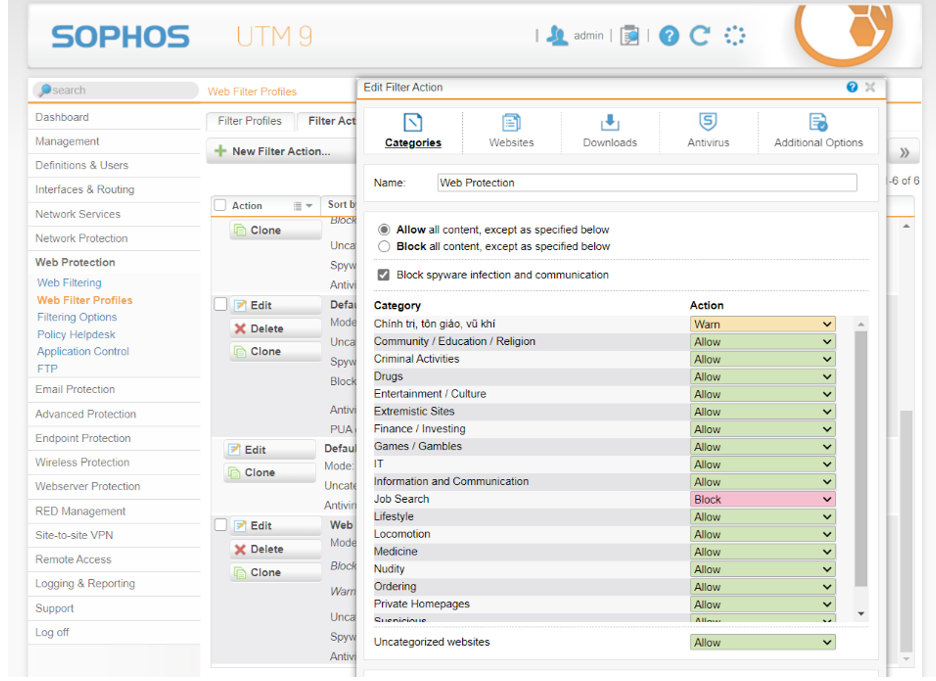
Lab 5

**Tường lửa Sophos UTM:**

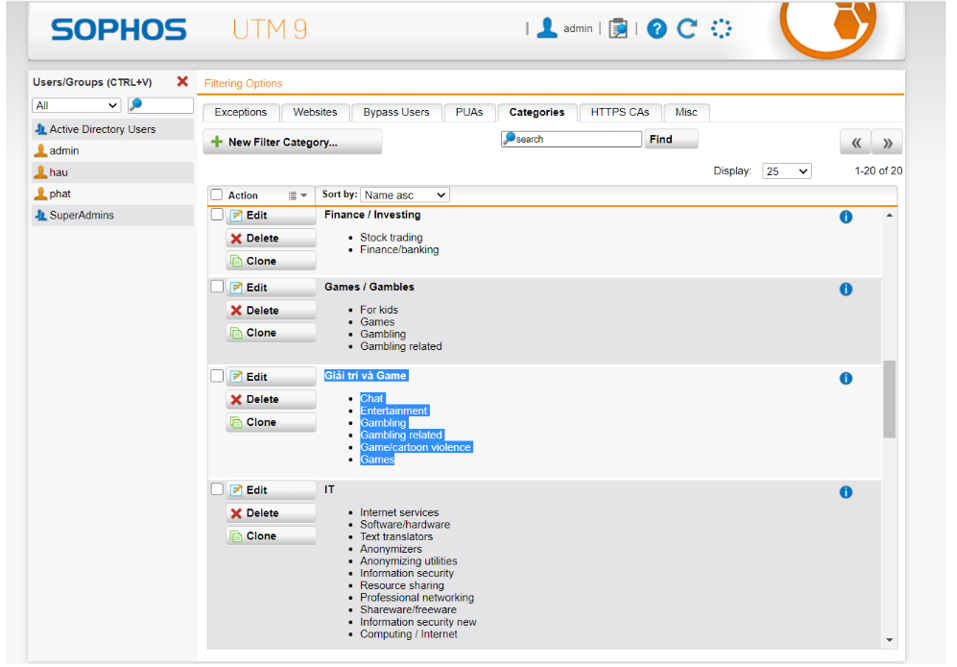
**Xây dựng chính sách Web**

**SOPHOS UTM Firewall – Web Protection**

1. **Tổng quan về xây dựng chính sách bảo vệ truy cập web**
2. Xây dựng bộ lọc tại Web Filter Profile > Tab Filter Actions > New Filter Action...

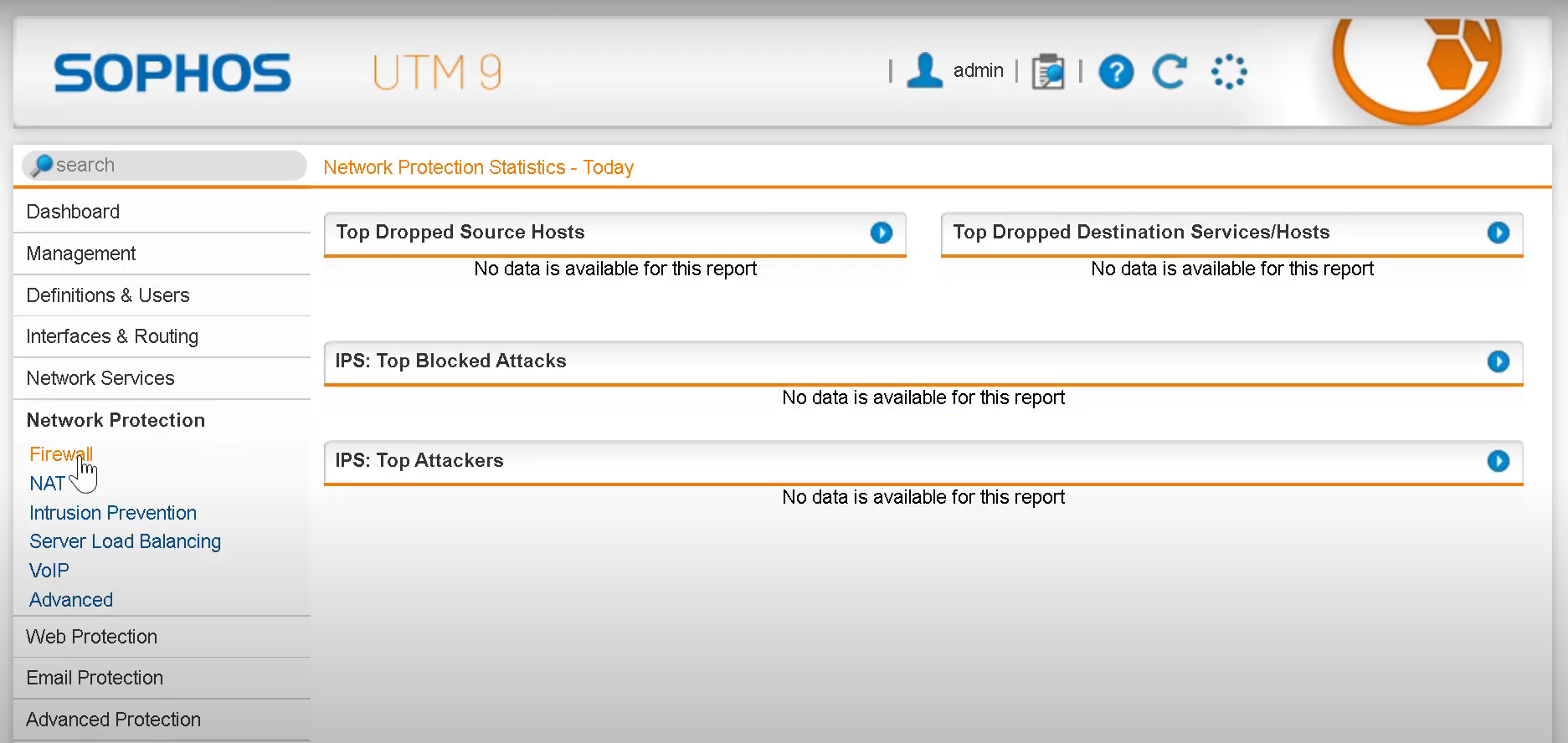


1. Tạo và áp dụng chính sách tại Web Filter Profiles > Filter Profiles

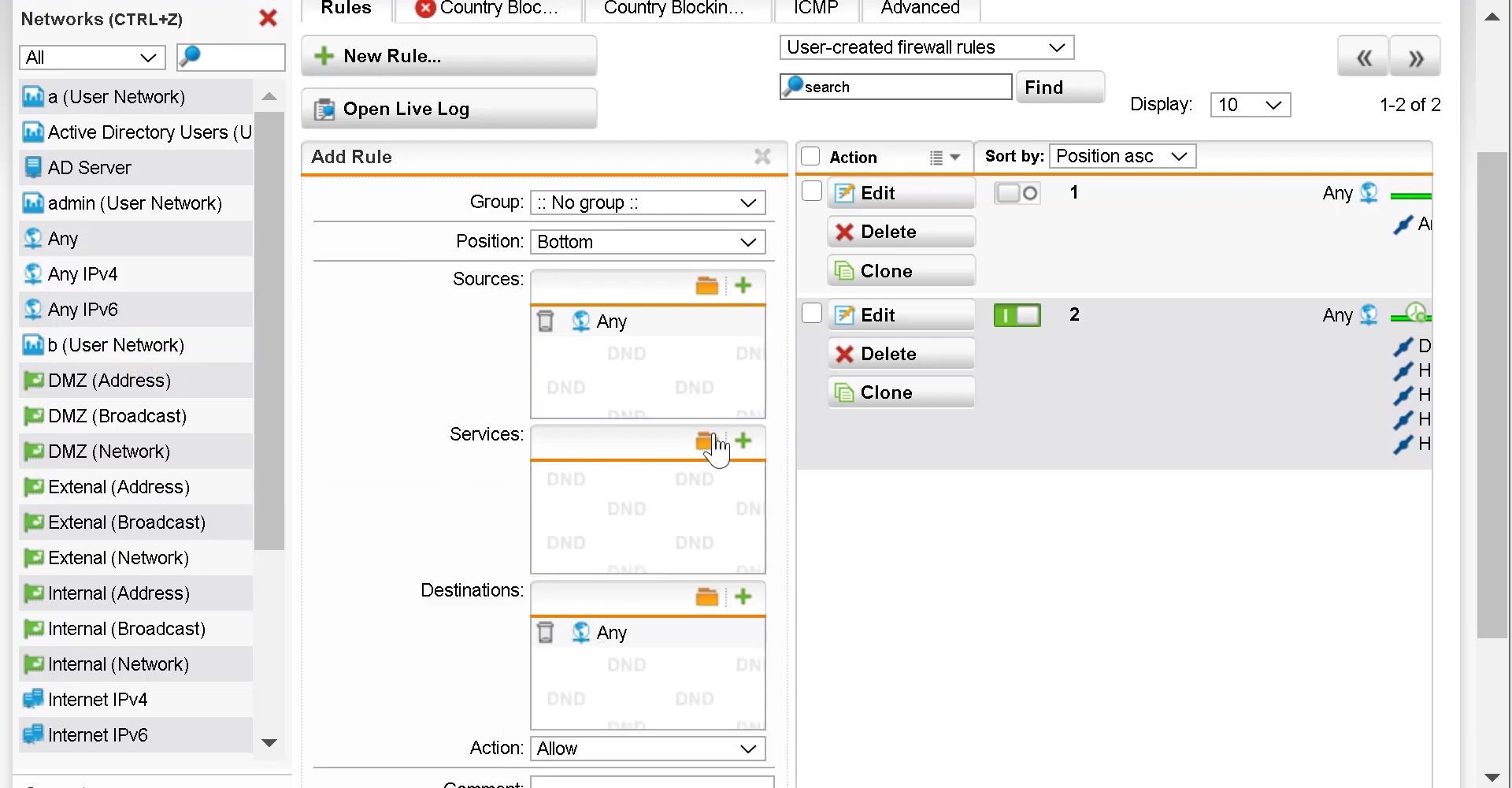


1. **Xây dựng bộ chính sách bảo vệ truy cập Web**
2. Chỉ cho phép toàn bộ người dùng sử dụng Internet để truy cập web, sử dụng email qua các giao thức SMTP, IMAP, POP3, chặn tất cả các dịch vụ khác.

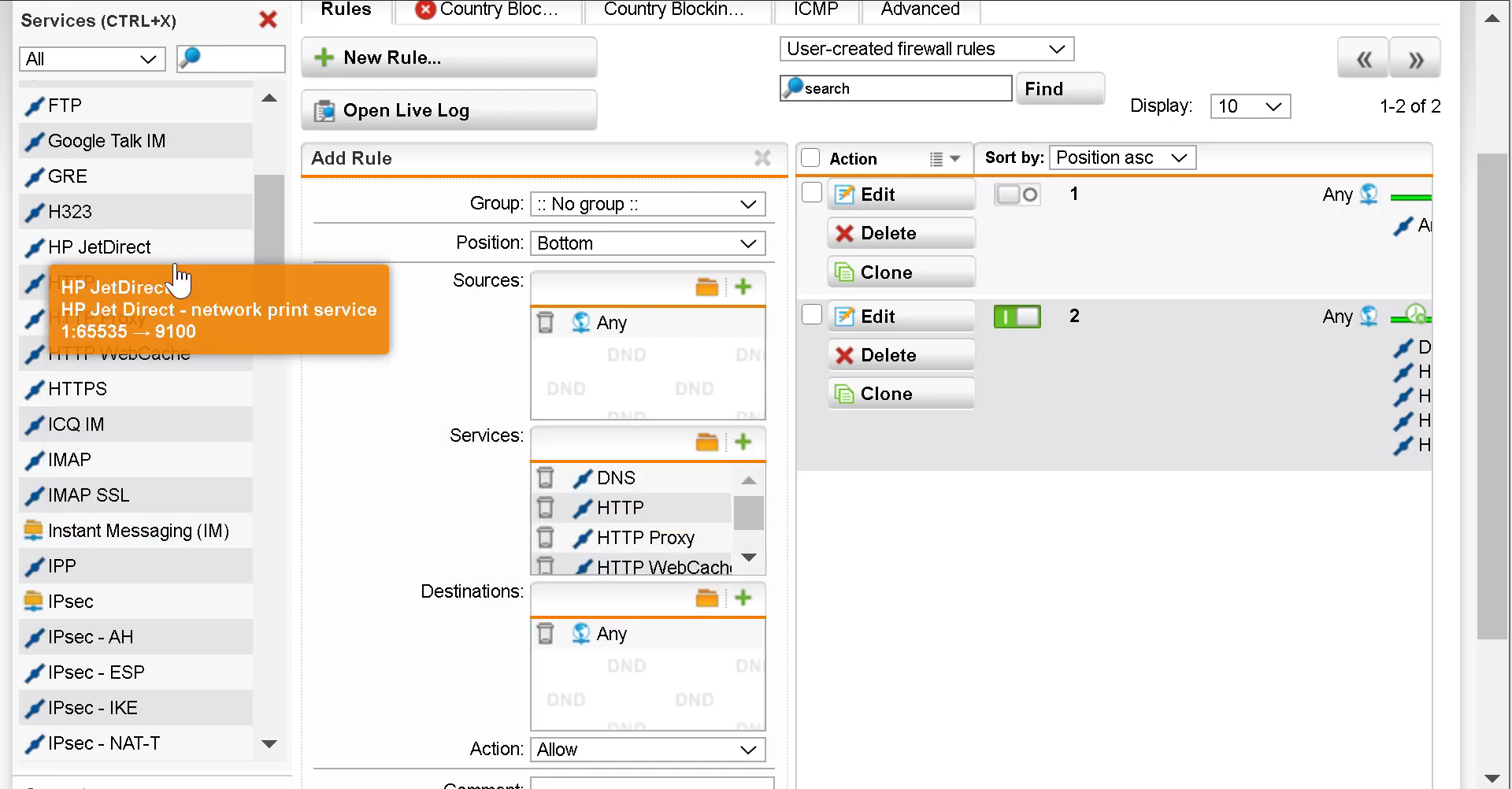
* Chọn Networld protection 🡪 Fire Wall



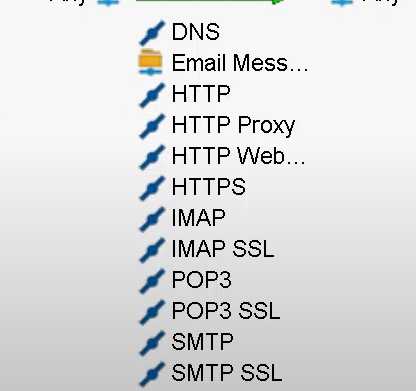
* Tạo rule mới và kéo thả `any` cho sources và destinations

****

* Để web truy cập được Internet thì cần phải có DNS và HTTP, nên ta thêm các DNS, HTTP, HTTP Proxy, HTTP Webcaching, HTTPS vào services

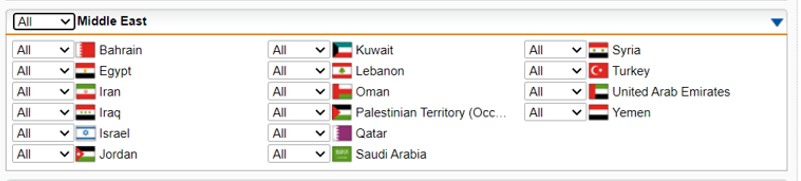
****

* Để sử dụng email qua các giao thức SMTP, IMAP, POP3, chặn tất cả các dịch vụ khác thì thêm các dịch vụ email Messaging, SMTP, SMTP SSL, IMAP, IMAP SSL, POP3, POP3 SSL. Sau đó nhấn save để tạo mới rule thì được các dịch vụ dưới đây



1. Chặn truy cập tất cả website từ Trung Quốc và toàn bộ khu vực Trung Đông (Iran, Iraq, Syria, ...).

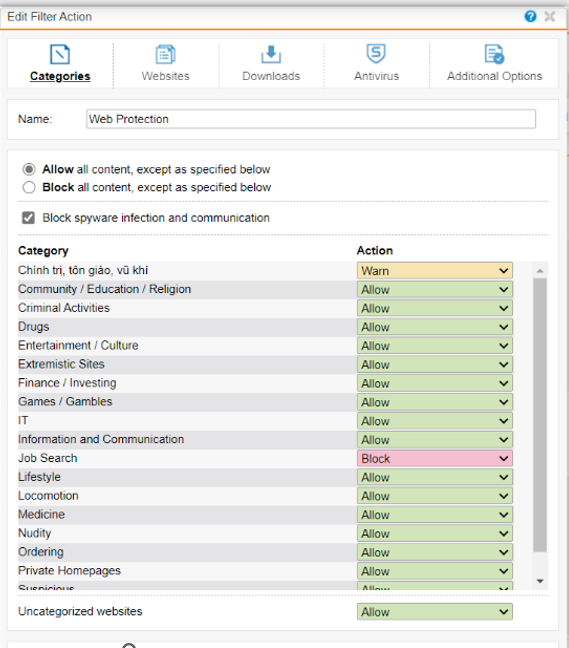
* Chặn hết tất cả các website từ các nước ở khu vực Trung Đông



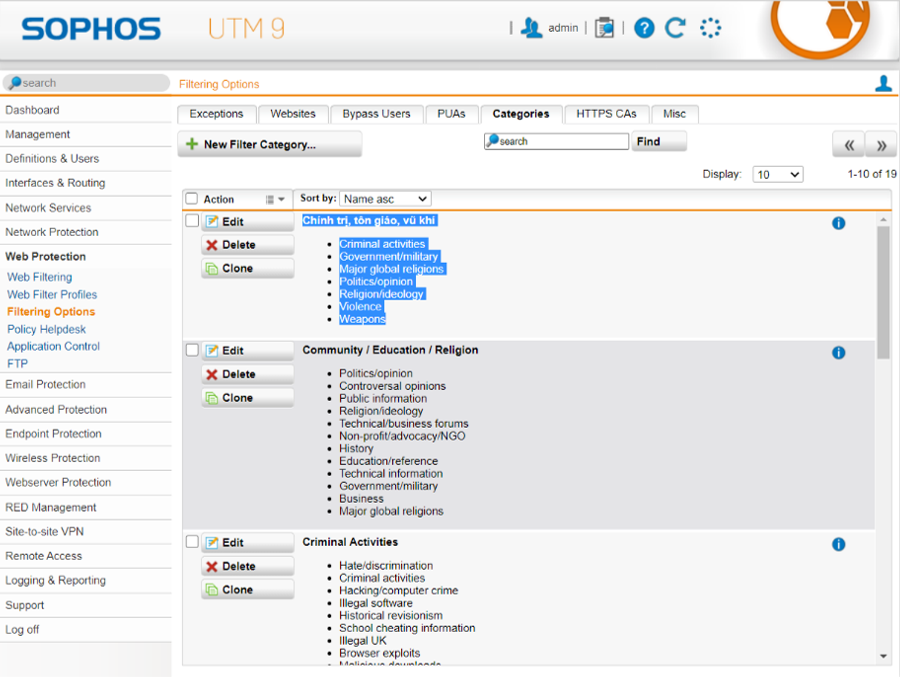
* Và Trung Quốc:



1. Cấm truy cập tất cả các website tìm kiếm việc làm, trong đó có một số website tìm kiếm việc làm tại TP.HCM.

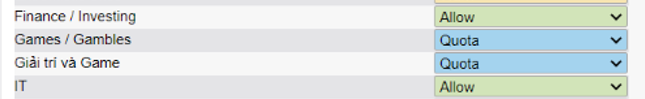


1. Cảnh báo khi truy cập các website về vũ khí, chính trị - tôn giáo. Không cảnh báo với các website giáo dục.



1. 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

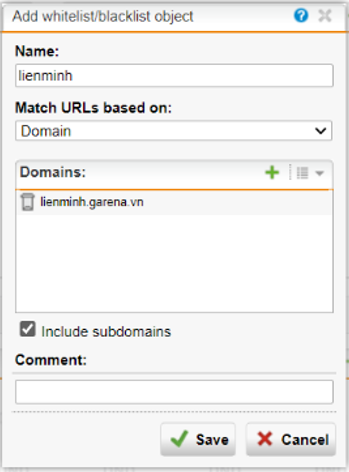
* Giới hạn truy cập với website Giải trí và Game:



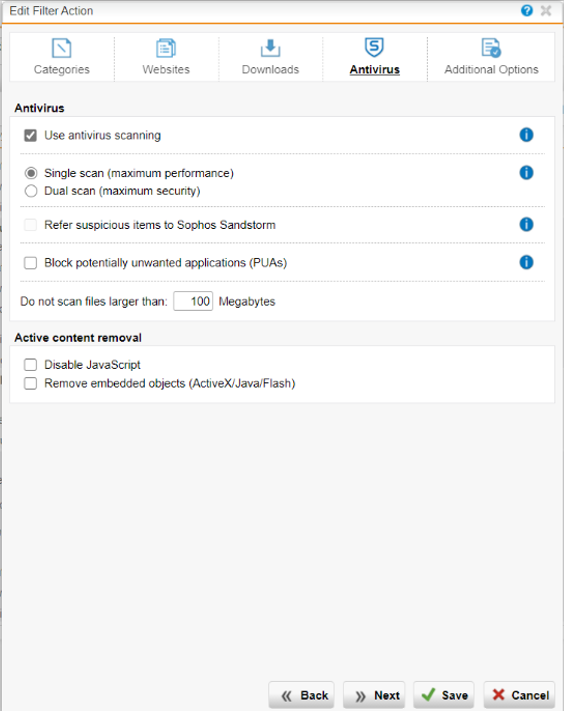
* Cảnh báo khi truy cập đối với các website giải trí dạng chia sẻ video như Youtube.com, vimeo.com (Streaming Media)



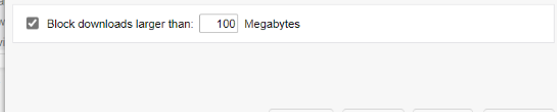
* Cấm hẵng đối với website lienminh.garena.vn



1. Quét virus khi download tập tin.

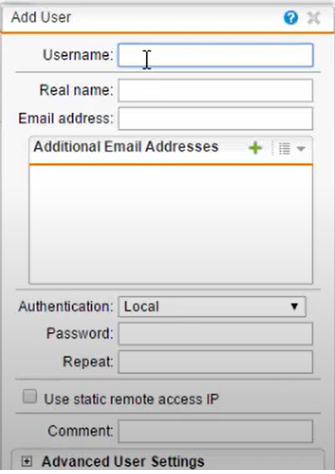


1. Không cho download các file lớn hơn 100MB.

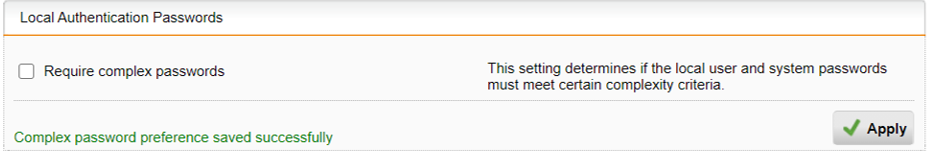


1. Khi truy cập vào website bị chặn thì có thể mở khóa trực tiếp để bỏ chặn website đó với tài khoản manager / 12345 (thiết lập tại Sophos Firewall – xem kết quả minh họa).

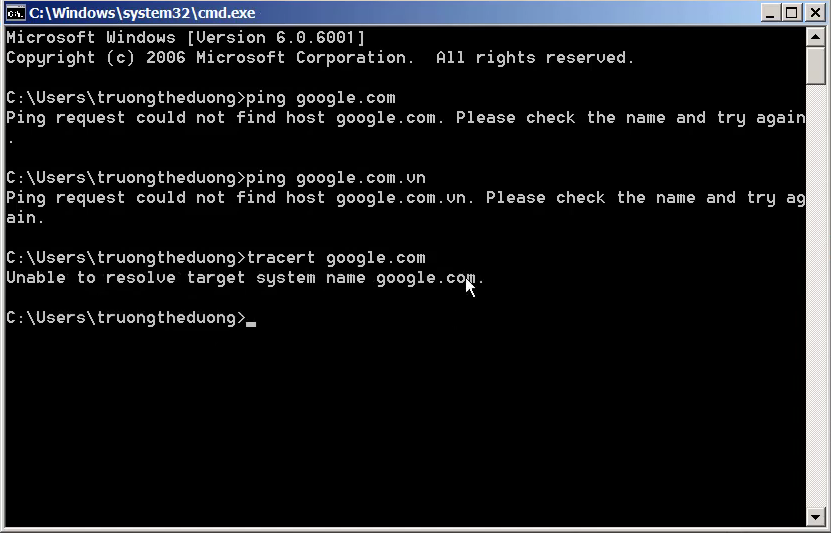
* Thêm User mới:



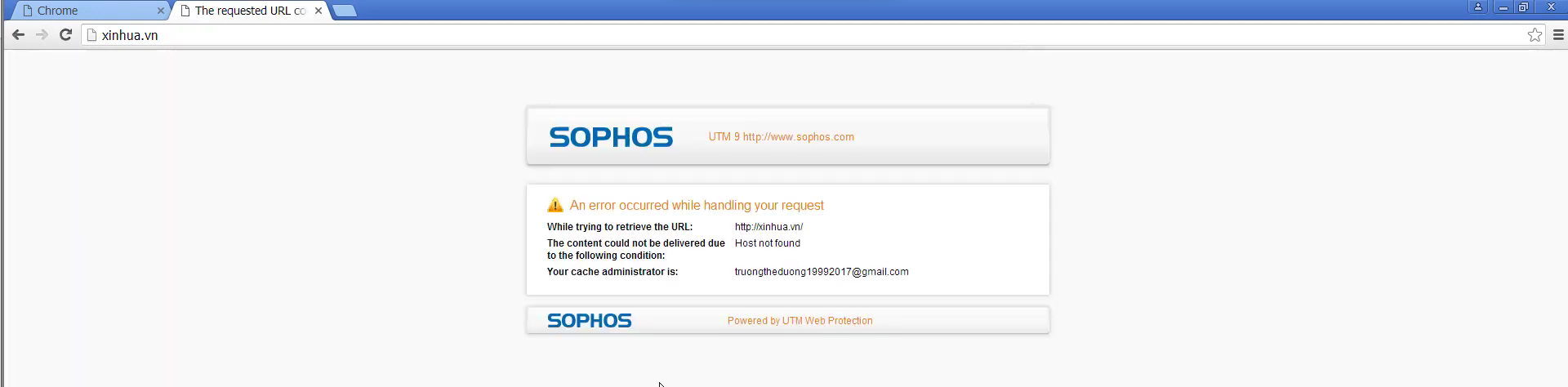
* Tắt Local Authentication Passwords

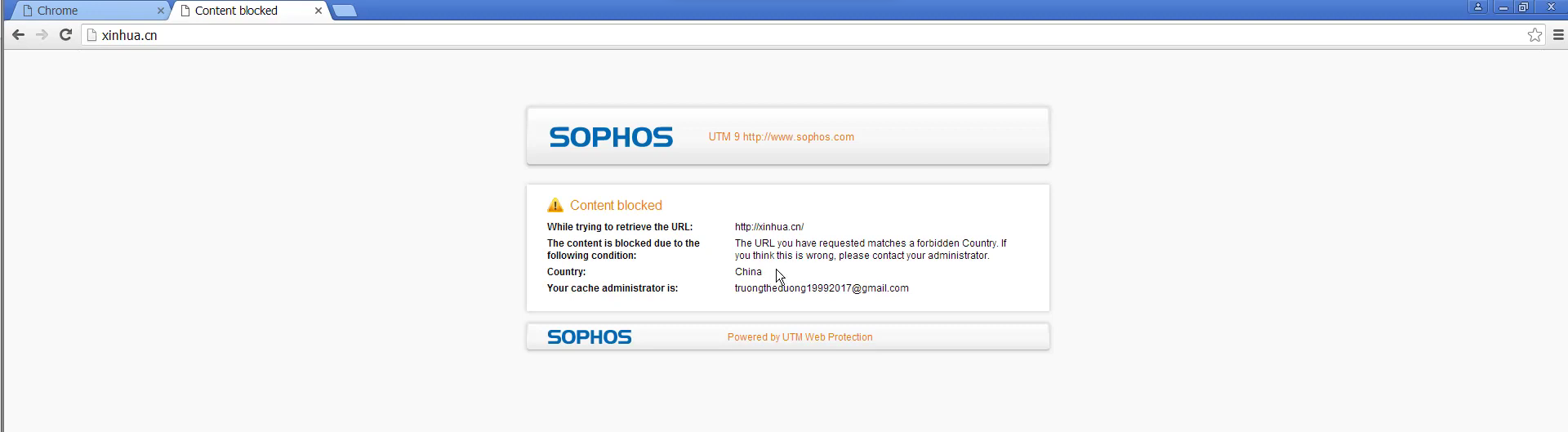


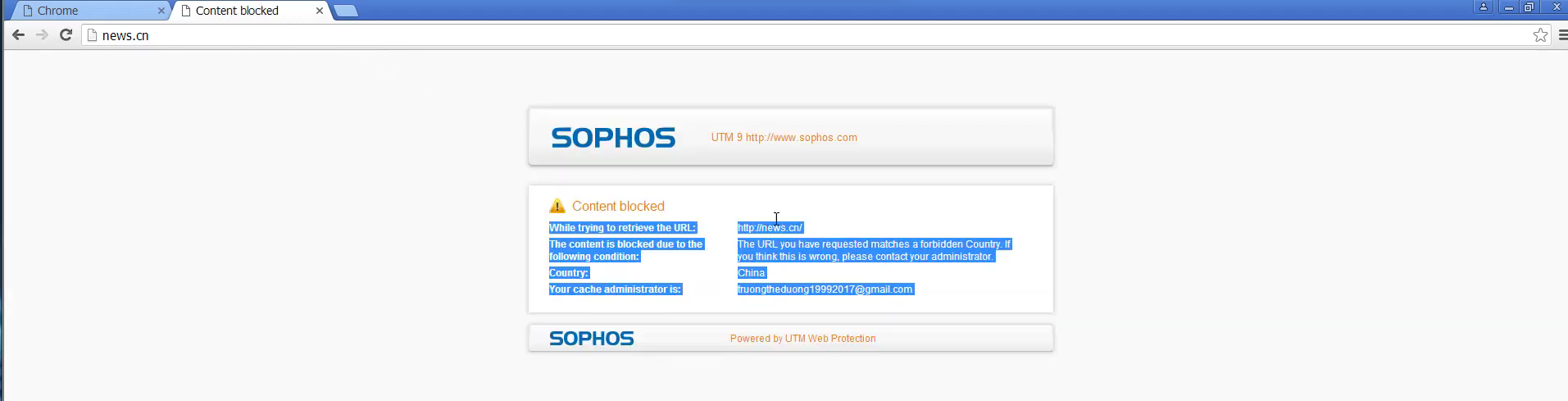
1. **Kiểm tra kết quả & ứng dụng**
2. Truy cập 1 website được phép truy cập bình thường, thao tác traceroute và ping đến website đó không thành công.



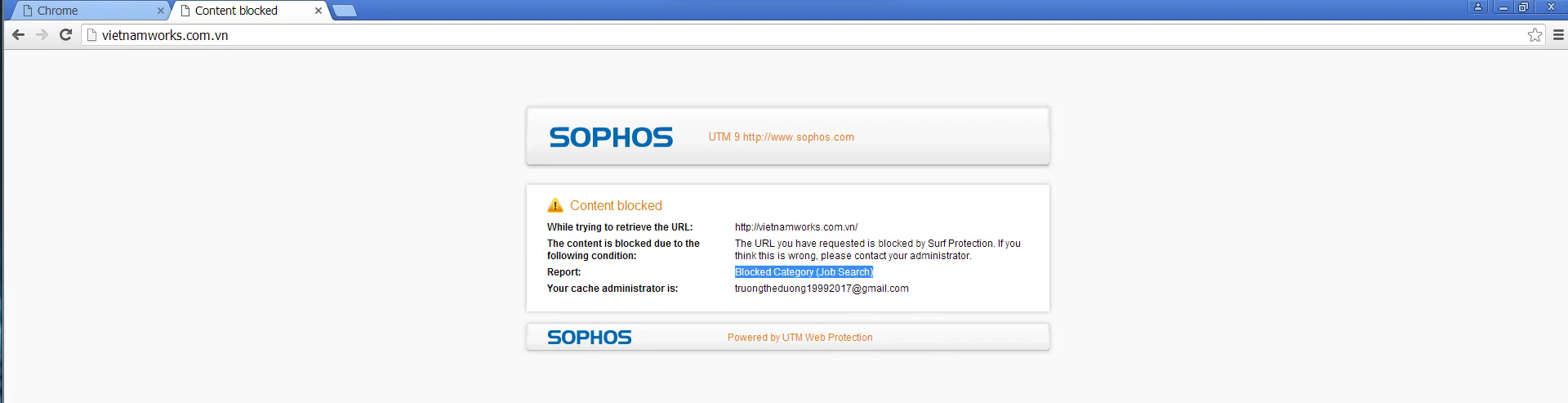
1. Không thể truy cập website báo Tân Hoa xã (xinhua.vn – news.cn) và ít nhất 2 website khác từ Trung Quốc và Trung Đông.

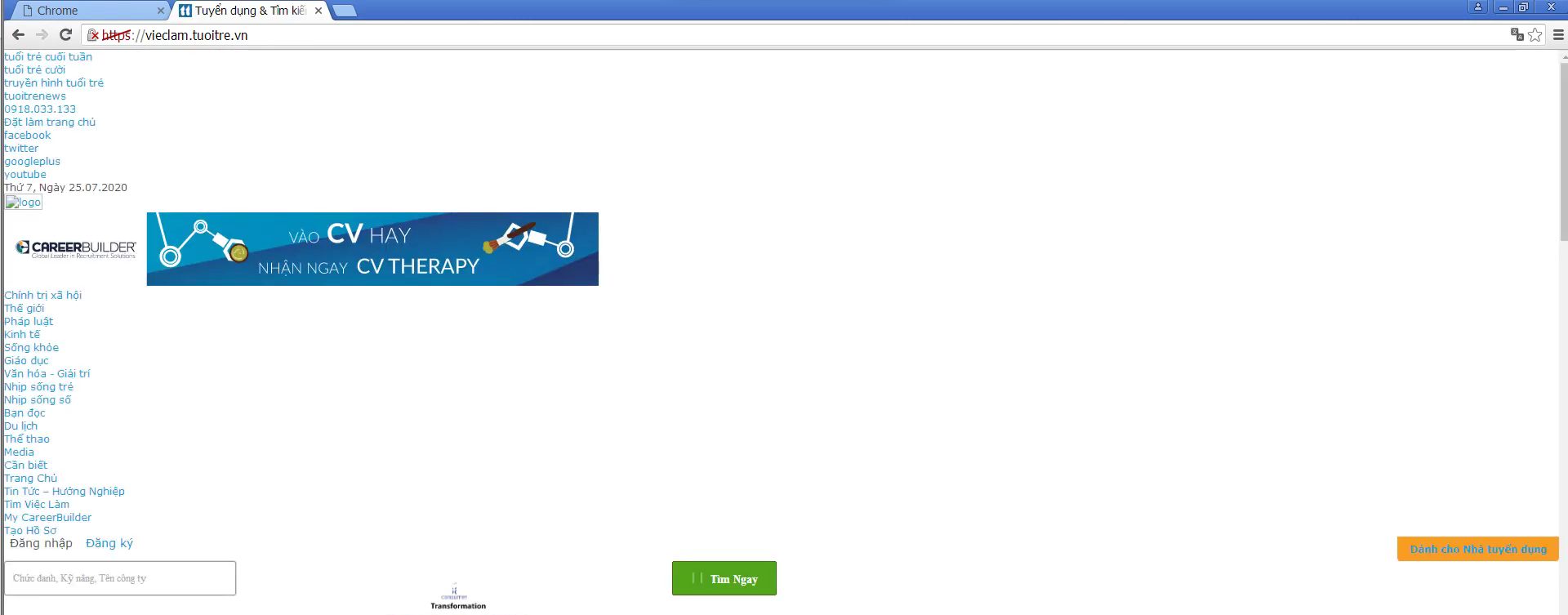


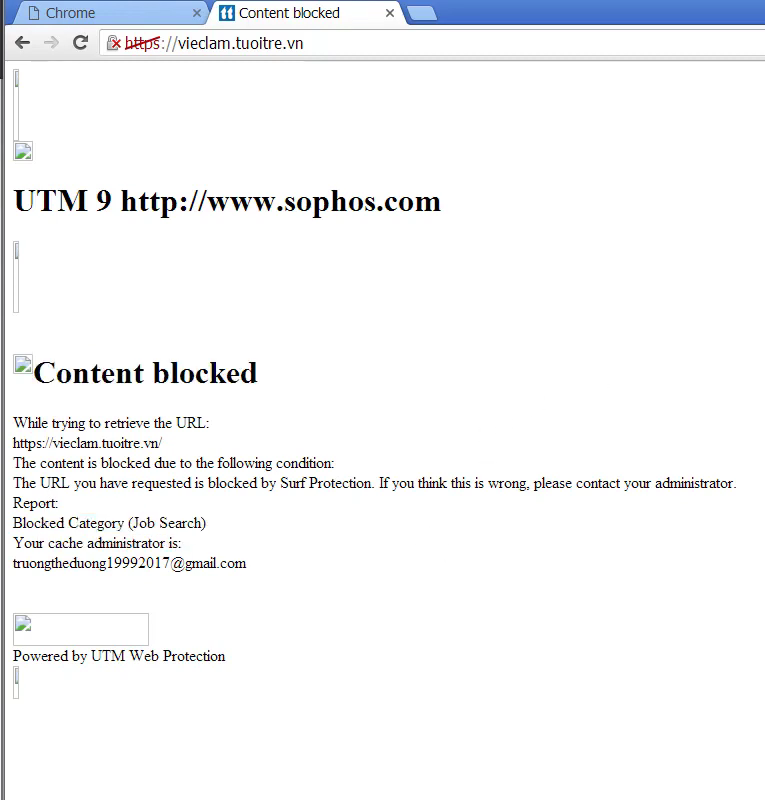


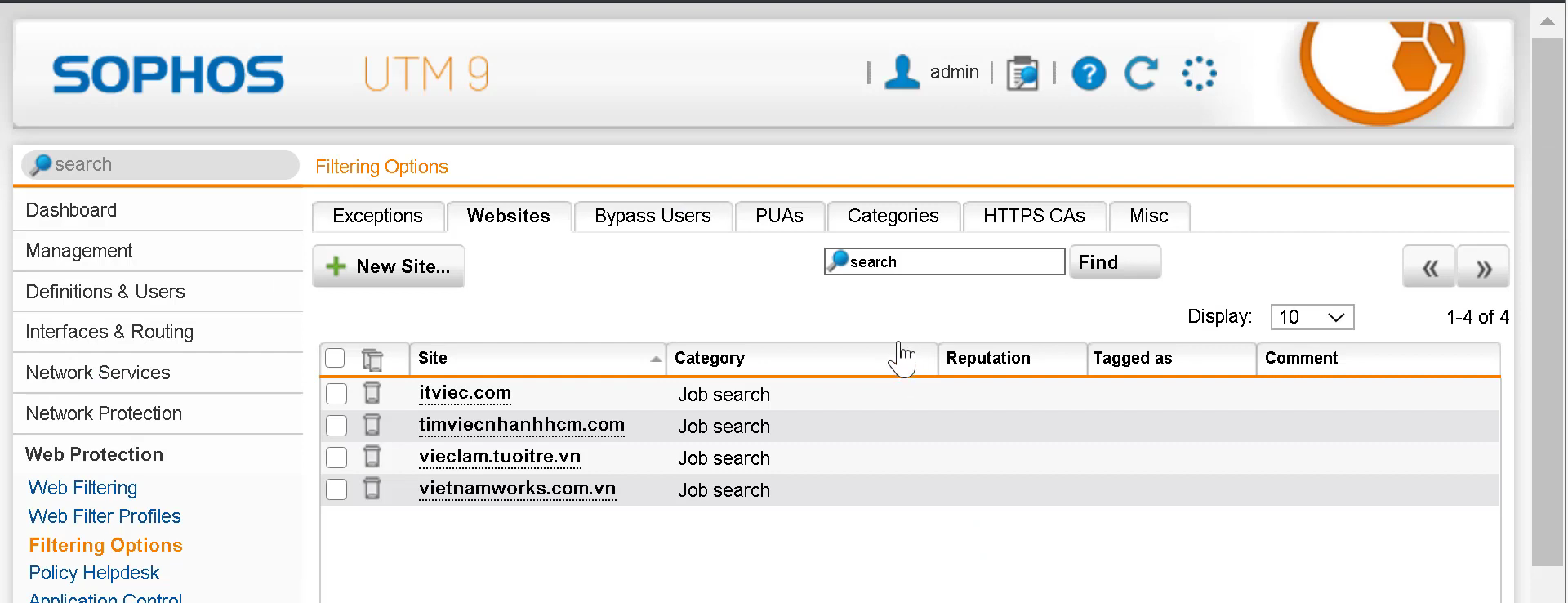


1. Không thể vào các website về tìm kiếm việc làm trên thế giới và tại Việt Nam, tại TP.HCM trong đó chặn được 4 website sau: vietnamworks.com.vn, vieclam.tuoitre.vn, timviecnhanhhcm.com, itviec.com. Nếu website nào chưa chặn được theo bộ lọc của Sophos thì chỉ định website đó ứng với thể loại Job Search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

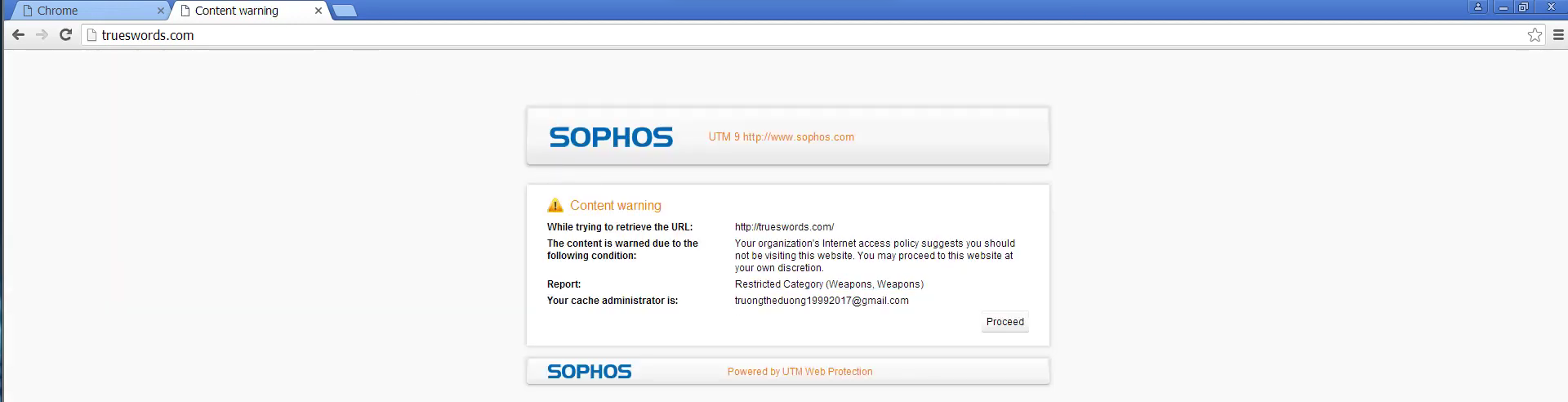


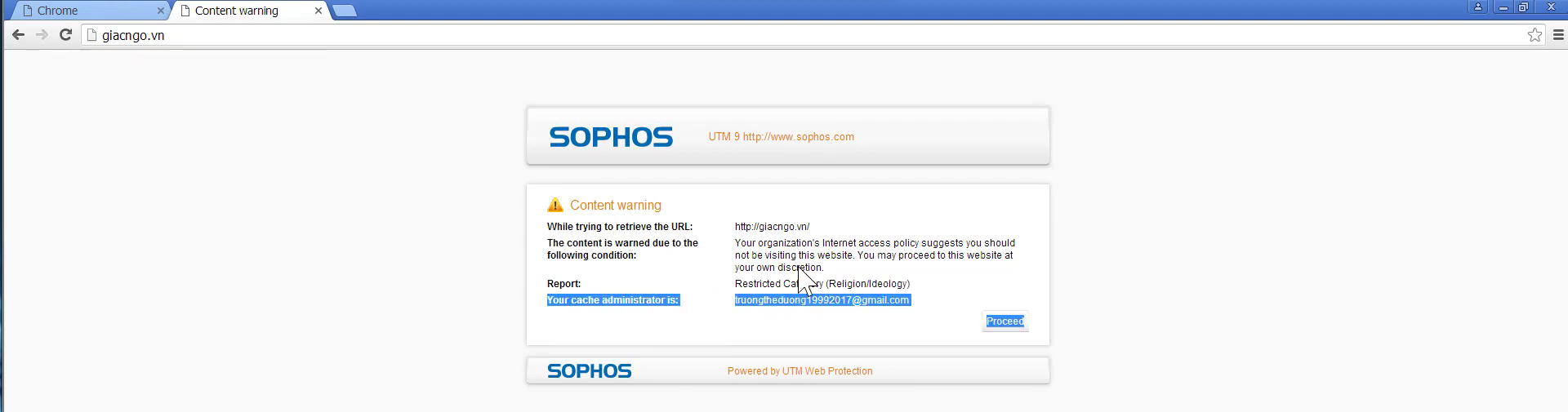


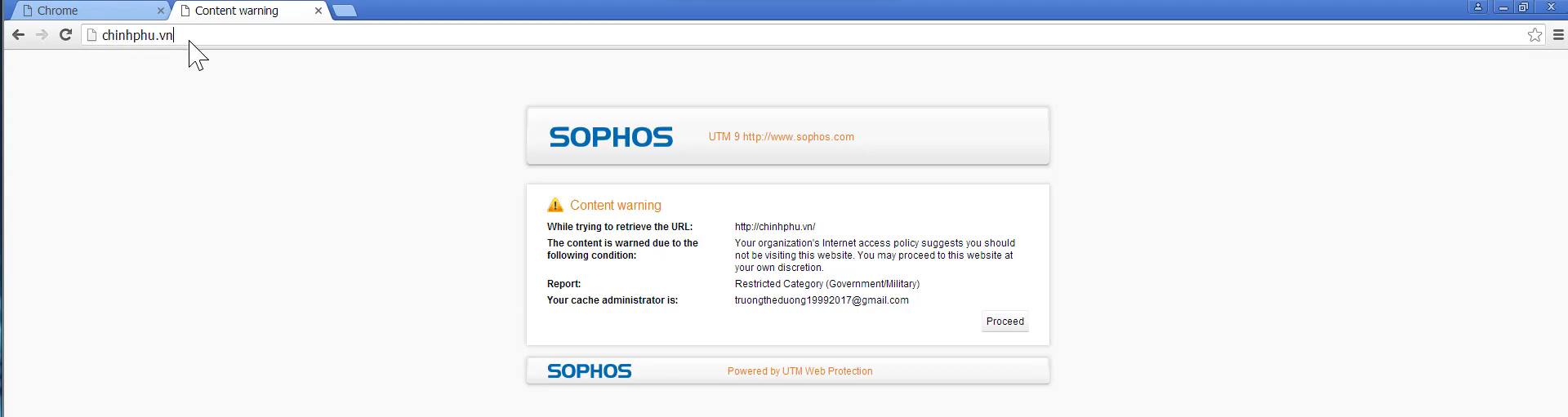




1. Hiện cảnh báo đối với một số website thuộc thể loại vũ khí, chính trị - tôn giáo như trueswords.com (vũ khí), giacngo.vn (tôn giáo), chinhphu.vn (chính trị).





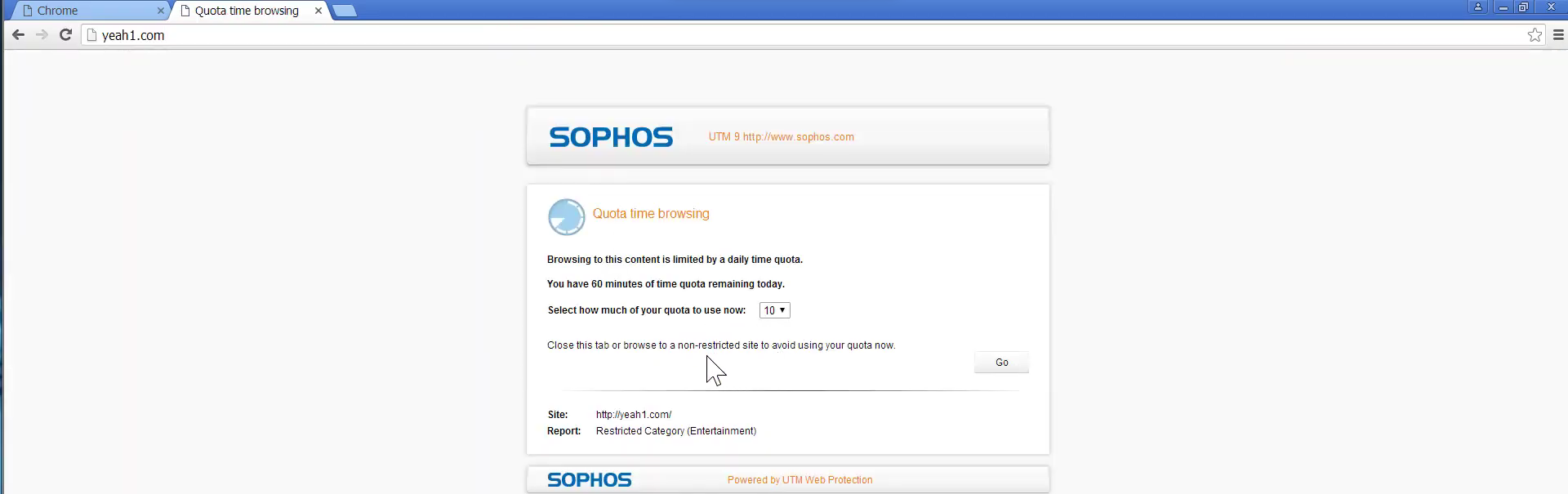


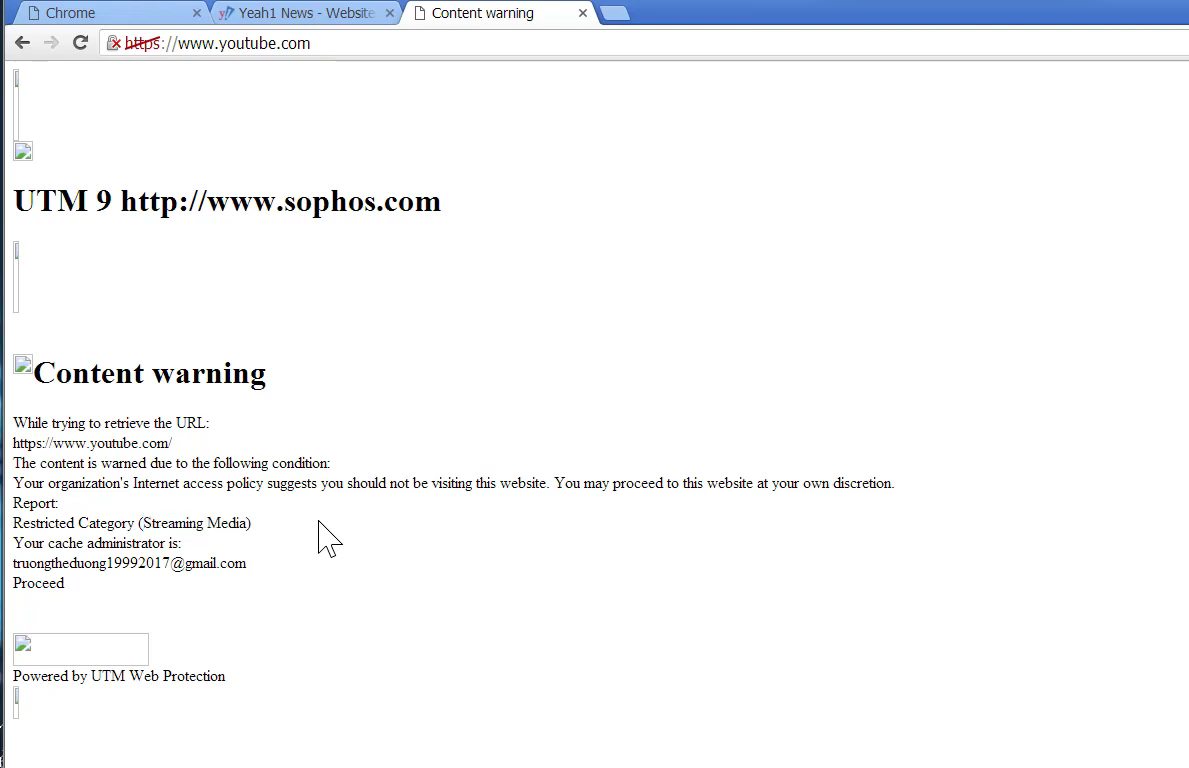


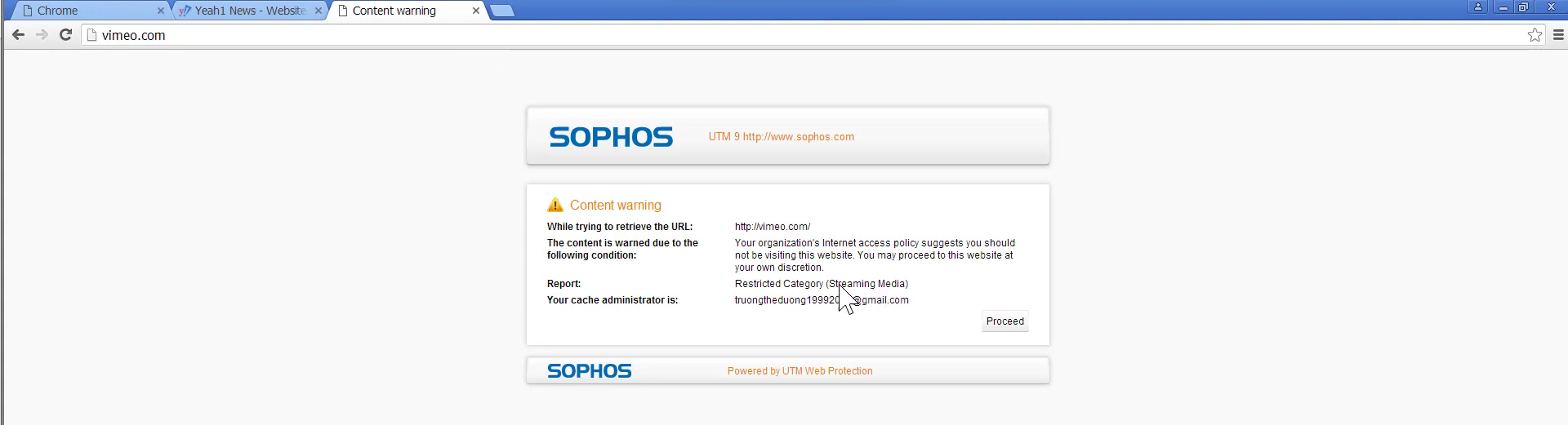
1. Kiểm tra khi truy cập một số website giải trí như kenh14.vn, yeah1.com,... và gamevui.vn, pokemongo.com chỉ cho phép truy cập tối đa trong 60 phút. Khi thiết lập Quota (quy định thời gian truy cập tối đa) thì thời gian này sẽ được tính từ khi nào và có được reset lại không? Nếu có thì reset khi nào và có cách nào thực hiện reset thủ công không? Minh họa nếu có thể

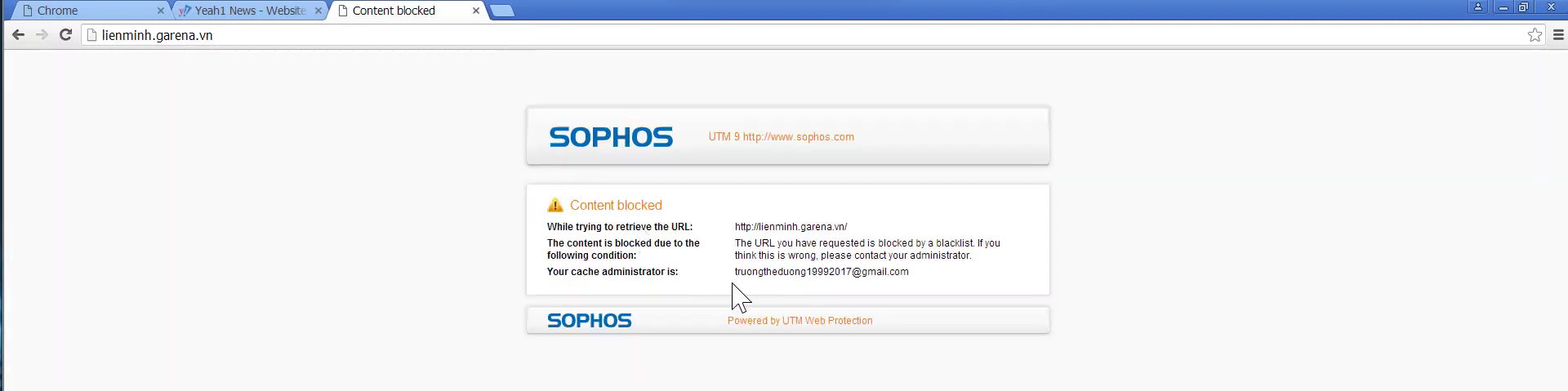
- Kiểm tra kết quả khi vào trang Youtube.com và Vimeo.com.

- Kiểm tra kết quả khi vào trang lienminh.garena.vn







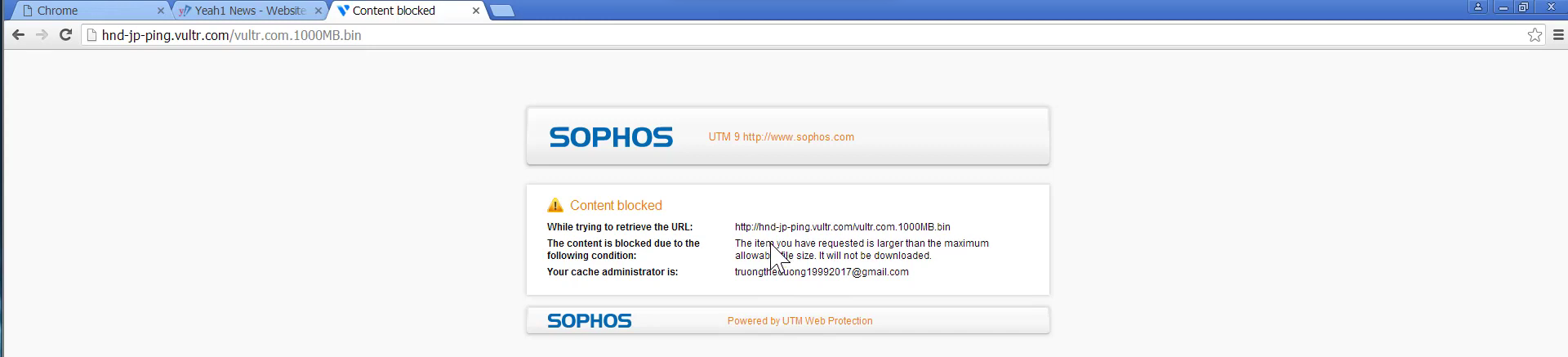


1. Thử nghiệm download 2 file có chứa virus qua http và https từ trang web EICAR tại http://www.eicar.org/download , kiểm tra kết quả.

Của em bị lỗi, em không có trang nào để test thử ạ

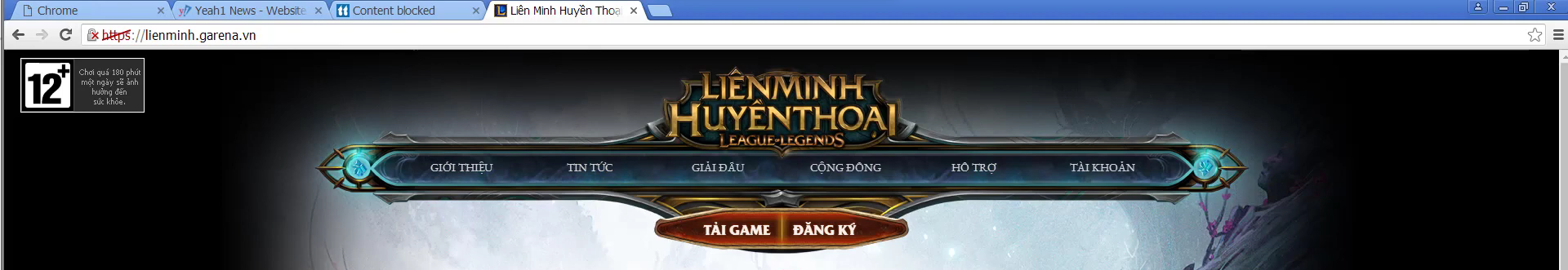
1. Thử download 1 file 100MB và 1 file 1GB từ trang http://hnd-jp-ping.vultr.com/(trang test server tại Tokyo của Vultr VPS).





1. Với các website bị chặn, khi kiểm tra sẽ xuất hiện tùy chọn Unlock





1. **Mở rộng**