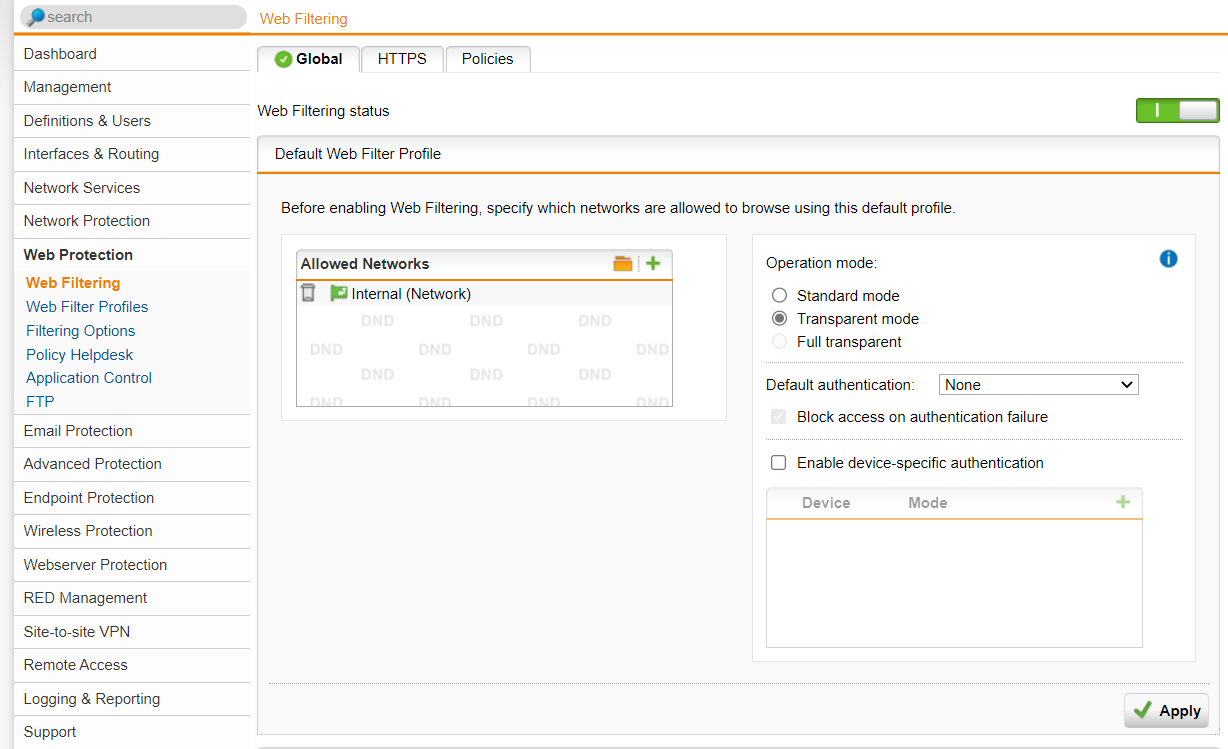
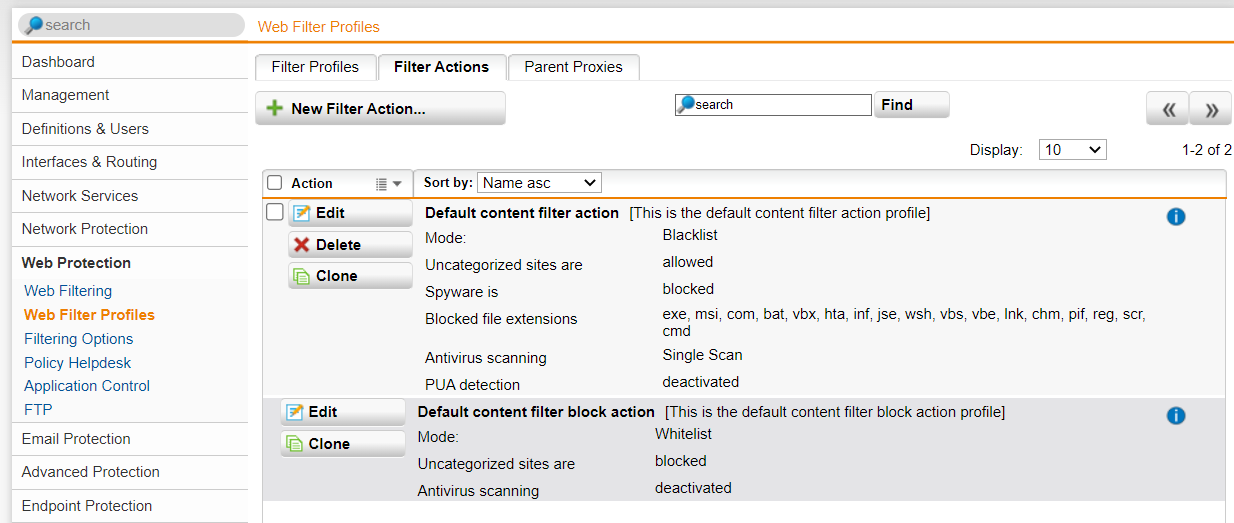
Tên: Phạm Hoàng Anh

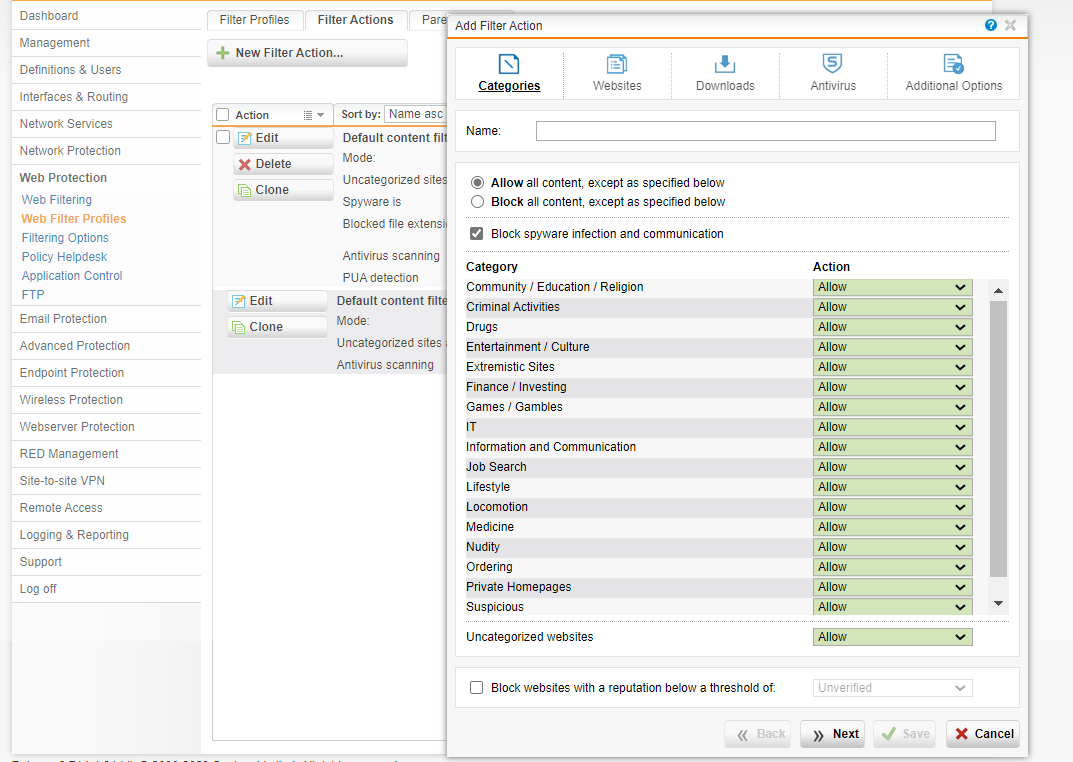
MSSV: 0850080003

Lớp: 08\_ĐH\_CNPM

**Lab5: Sophos UTM Web Protection**

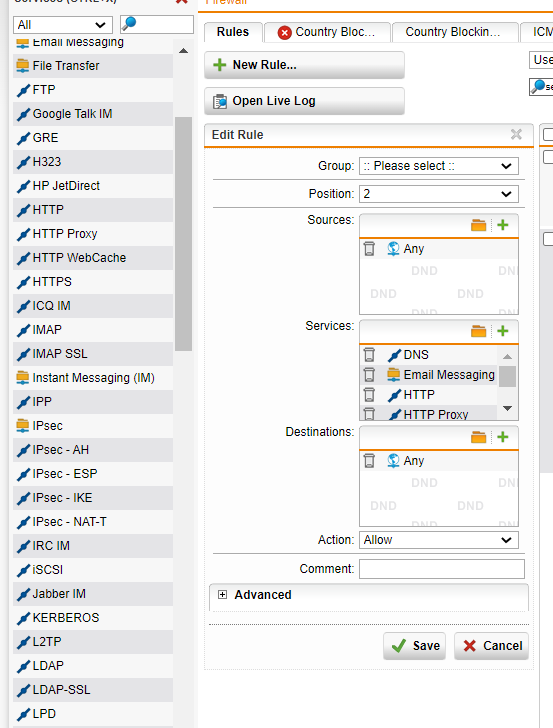




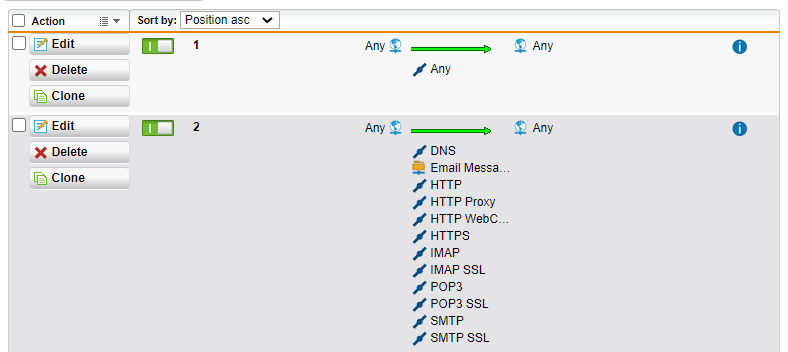
Xây dựng bộ lọc tại **Web Filter Profile** > Tab **Filter Actions** > New **Filter Action**...

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 khác.

Network Protection -> Firewall -> tab Rules -> chọn New Rule… Sau đó kéo lần lượt các rule.



Sau khi hoàn thành xong, bắt đầu bật Rule vừa được tạo.



1. Chặn truy cập tất cả website từ Trung Quốc và toàn bộ khu vực Trung Đông

(Iran, Iraq, Syria, …).

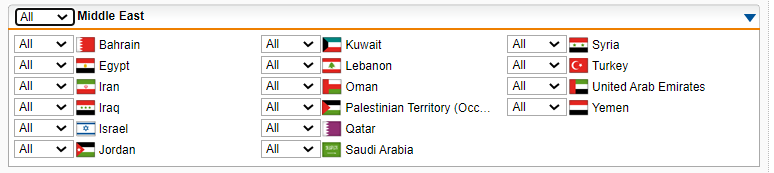
vào Network Protection -> Firewall -> tab Country Blocking -> bật chức năng này lên



Chuyển China từ Off thành All



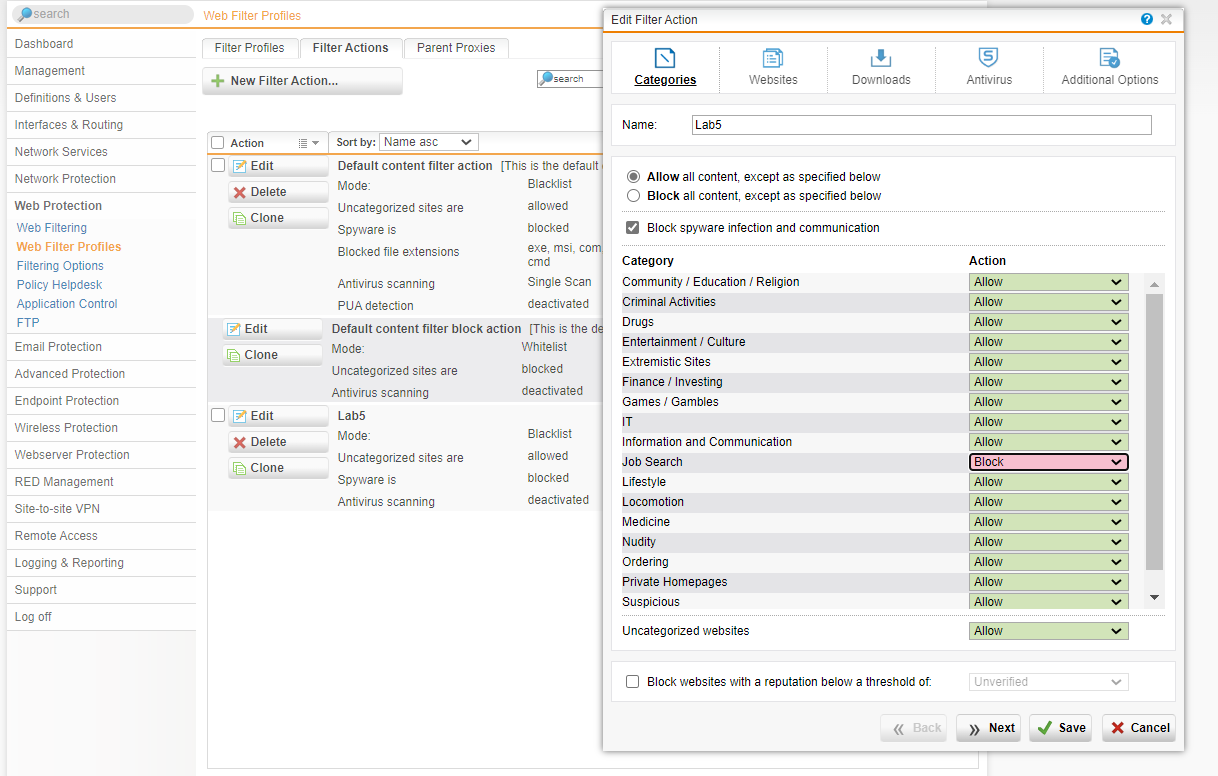
Chuyển cả Middle East tương tự như trung Quốc



3. Cấm truy cập tất cả các website tìm kiếm việc làm, trong đó có một số website

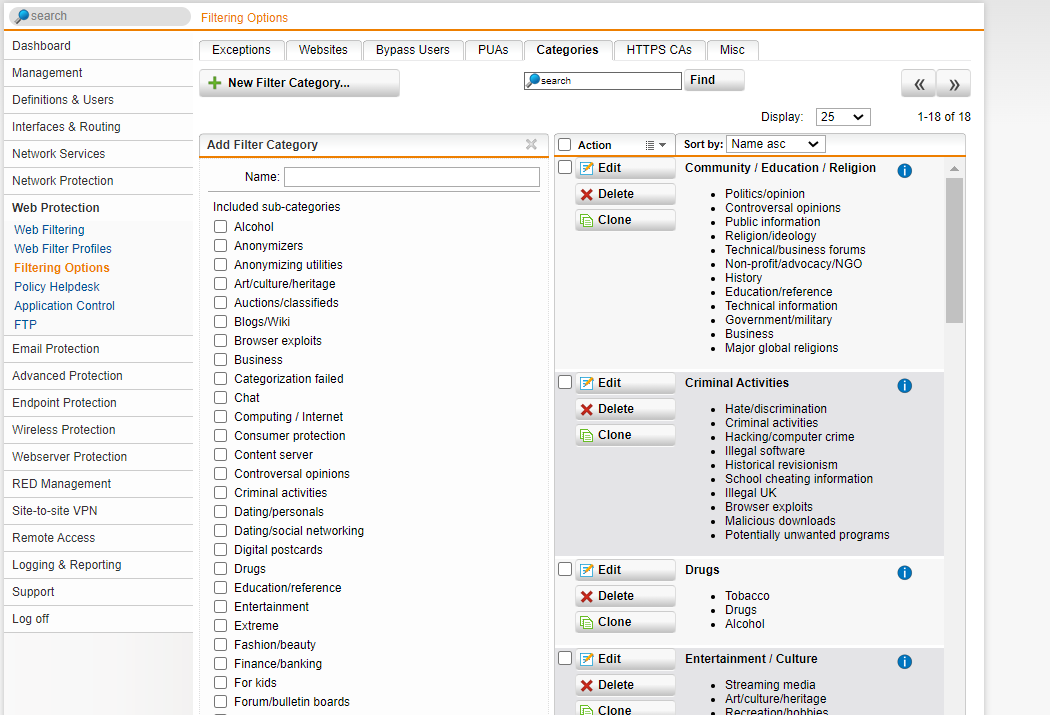
tìm kiếm việc làm tại TP.HCM.

Web Filter Profiles -> ở tab Filter Actions -> chọn Edit của filter ‘Lab5’ đã tạo trước đó -> chuyển Job Search thành Block.



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

Web Protection -> Filtering Options -> Categories -> New Filter Category…

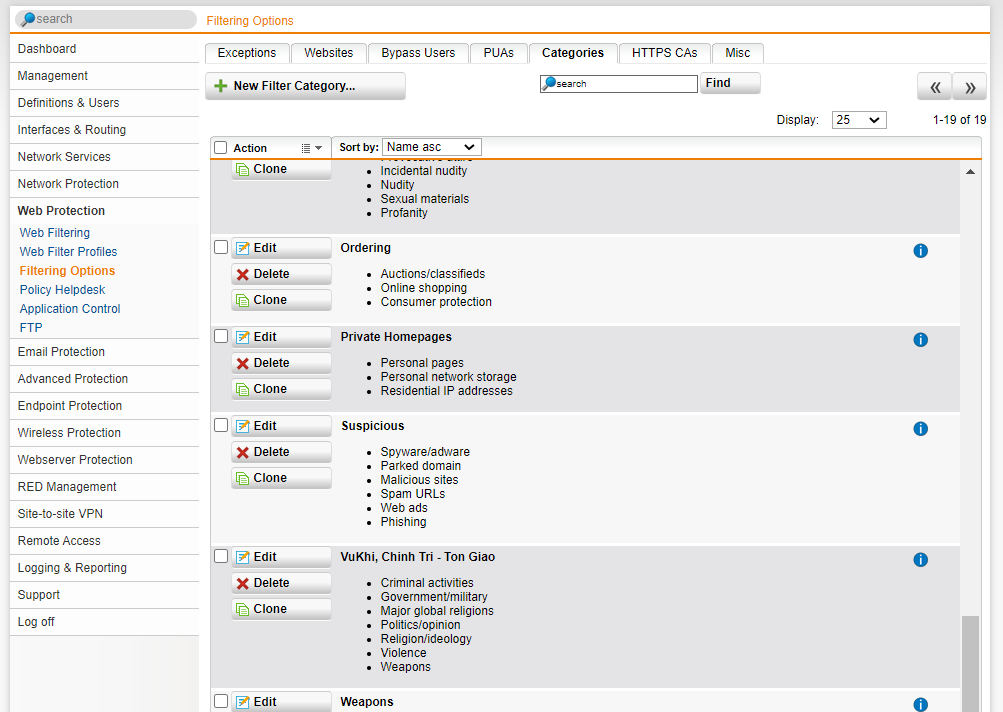


Chọn các lựa chọn sau:

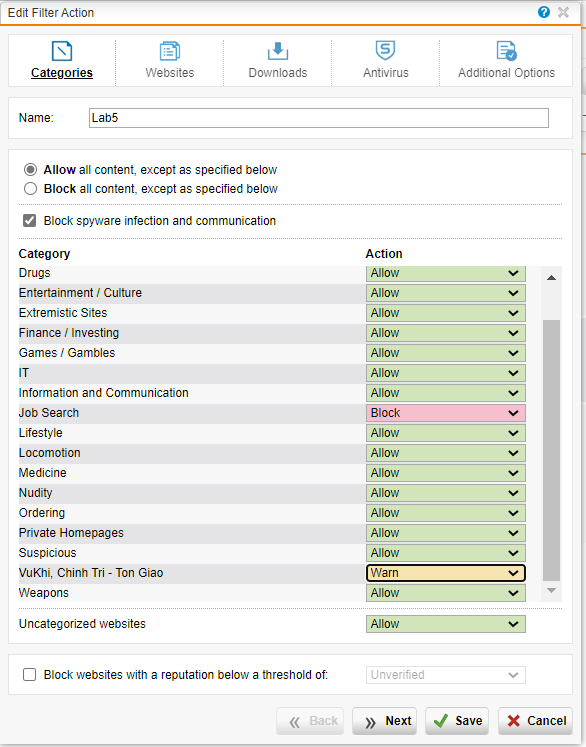
* Criminal activities (Hoạt động tội phạm)
* Government/military (Chính phủ/quân đội)
* Politics/opinion (Chính trị/quan điểm)
* Major global religions (Các tôn giáo lớn trên thế giới)
* Religion/ideology (tôn giáo/ý tưởng chính trị)
* Violence (Bạo lực)
* Weapons (Vũ khí)

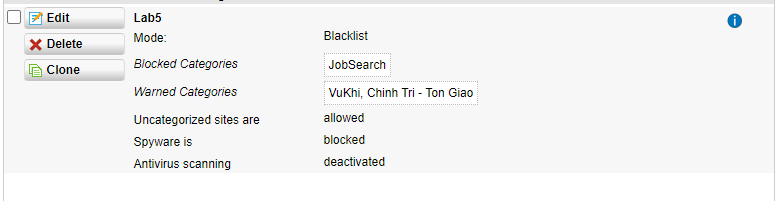
Click save để lưu.

Ta sẽ tạo được một danh mục ‘Vukhi, Chinh Tri – Ton Giao’.



Web Filter Profiles -> ở tab Filter Actions -> chọn Edit của filter ‘Lab5’ đã tạo trước đó -> chuyển ‘Vukhi, Chinh Tri – Ton Giao’ thành Warn.





Thêm hoàn tất.

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.

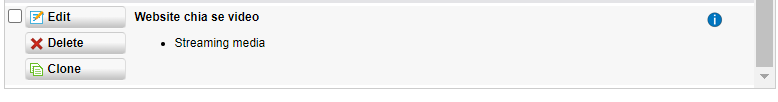
Web Protection -> Filtering Options -> Categories -> New Filter Category…



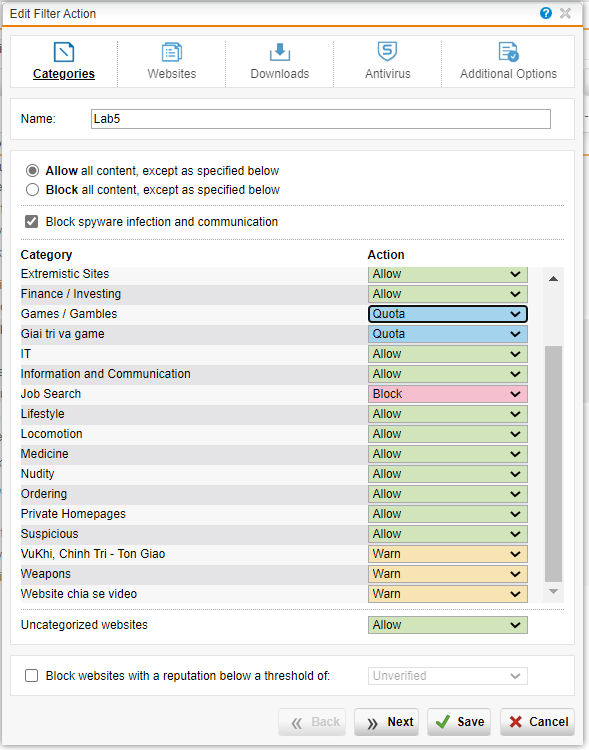
Với các lựa chọn:

* Chat
* Entertainment
* Gambling
* Gambling related
* Game/cartoon violence
* Games

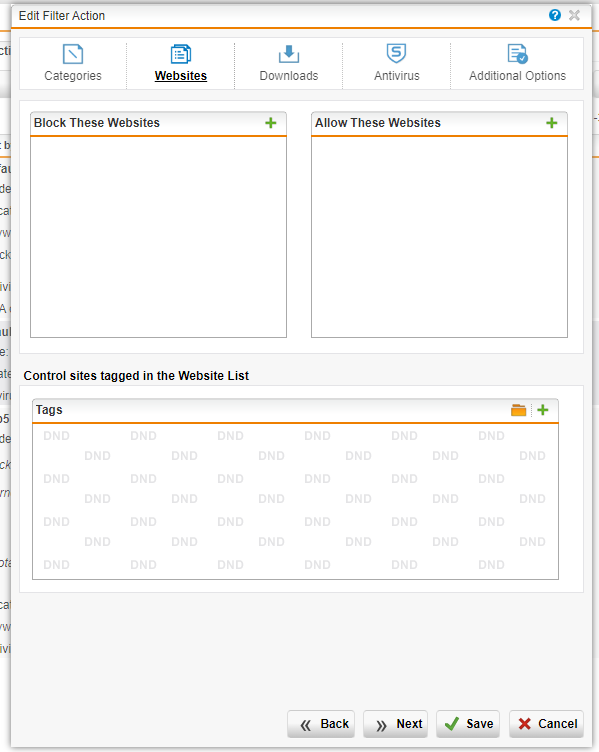
Tương tự thêm 1 filter



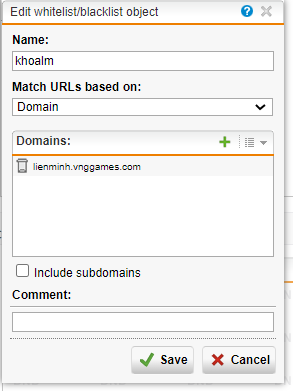
Web Filter Profiles -> ở tab Filter Actions -> chọn Edit của filter ‘Lab5’ đã tạo trước đó -> ta chuyển đổi như hình.



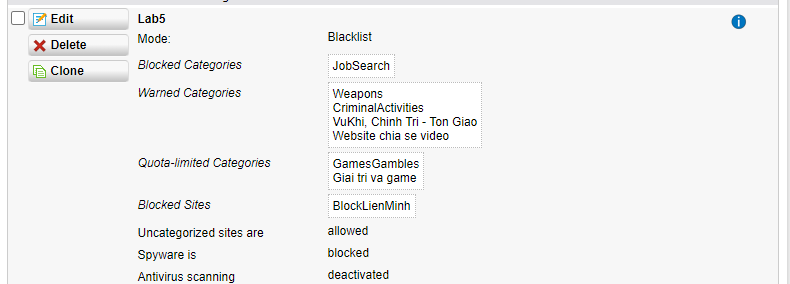
Vào tab Websites -> chọn “+” như hình



Điền thông tin rồi nhấn Save.

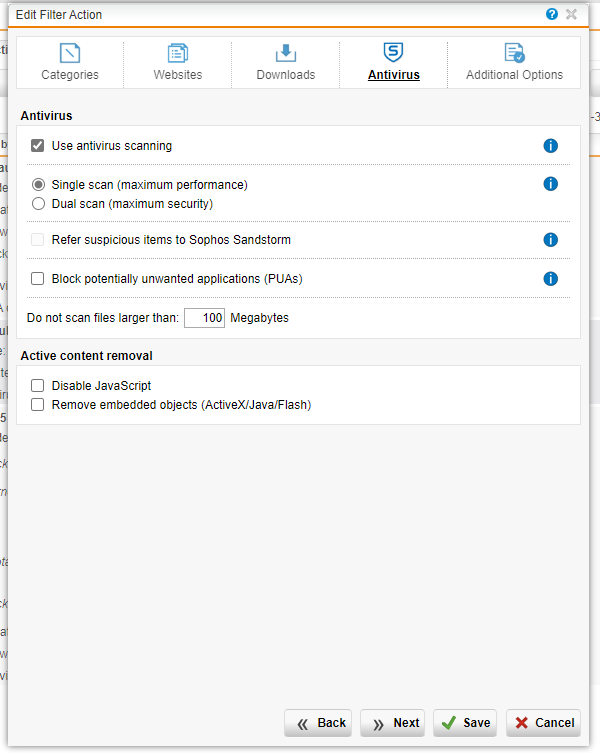


Thêm hoàn tất



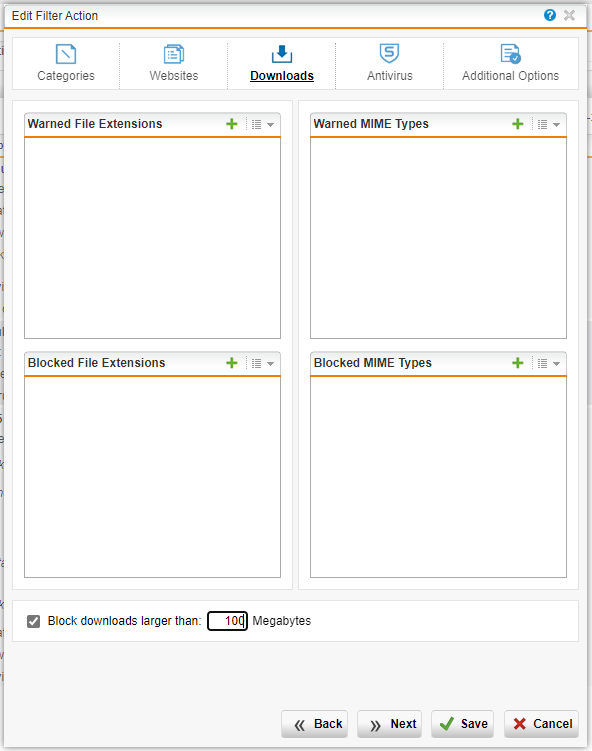
1. Quét virus khi download tập tin.

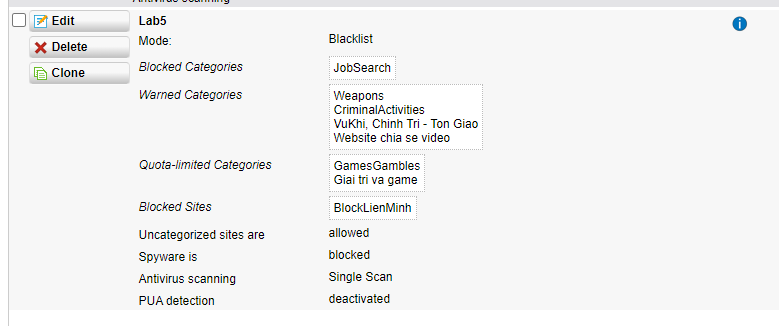
Web Filter Profiles -> ở tab Filter Actions -> chọn Edit của filter ‘Lab5’ đã tạo trước đó -> Chọn vào tab Antivirus -> tích chọn Use antivirus scanning. Chọn Save để lưu lại lựa chọn.



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

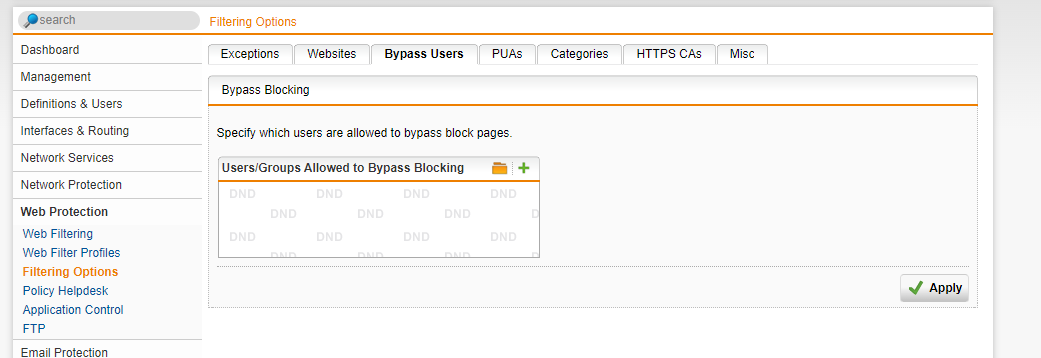
Web Filter Profiles -> ở tab Filter Actions -> chọn Edit của filter ‘Lab5’ đã tạo trước đó -> Chọn vào tab Downloads -> tích chọn Block downloads larger than và chỉnh sửa lại thành 100. Cuối cùng chọn Save để lưu



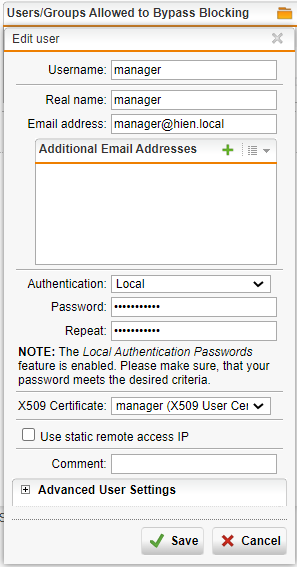


8. Khi truy cập vào website bị chặn thì có thể mở khóa trực tiếp để bỏ chặn website đó với tài khoản manager / 12345 (thiết lập tại Sophos Firewall – xem kết quả minh họa).

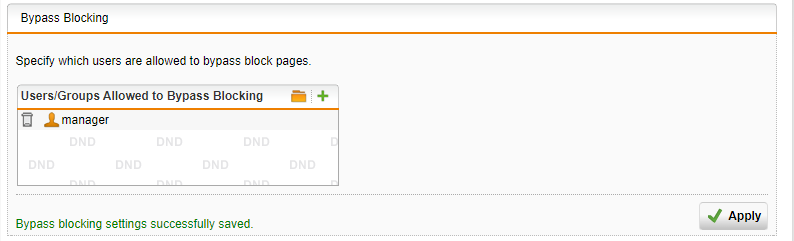
Web Protection -> ở Filter Options -> chọn tab Bypass Blocking -> chọn biểu tượng dấu “+”



Nhập thông tin:



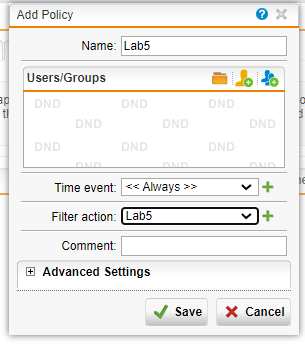
Sau khi nhấn save:



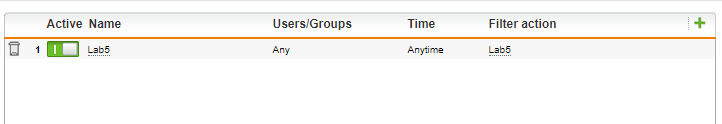
Để test ta sẽ cần cấp chính sách cho mạng. Ta sẽ vào **Web Protection** -> **Web Filtering** -> chọn ta **Policies ->** chọn **+**



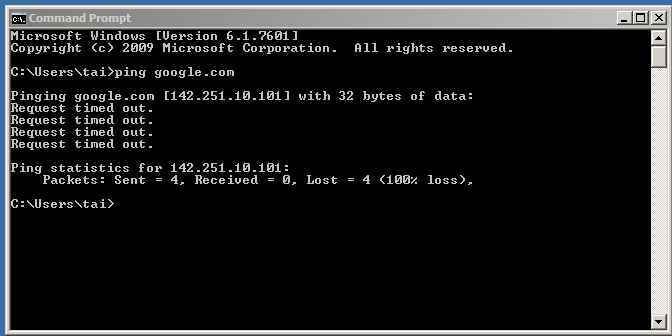
Nhập các thông tin cho chính sách:

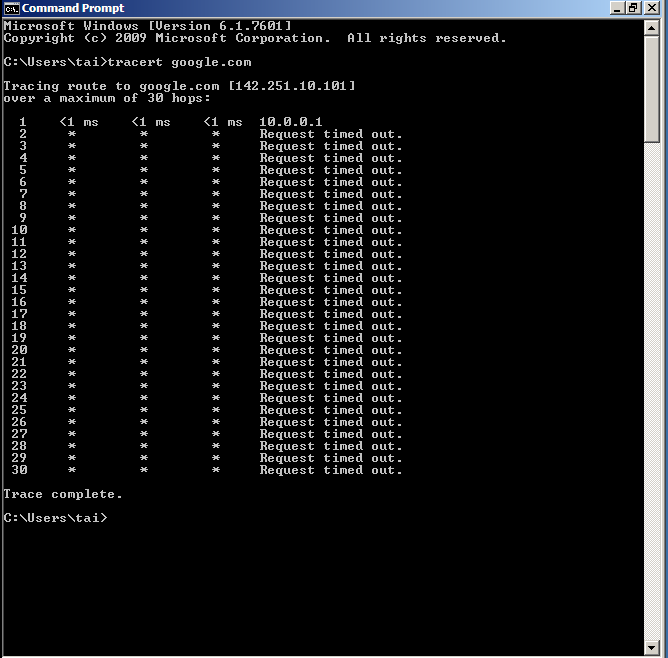


Cuối cùng bật lên và bắt đầu test thử.

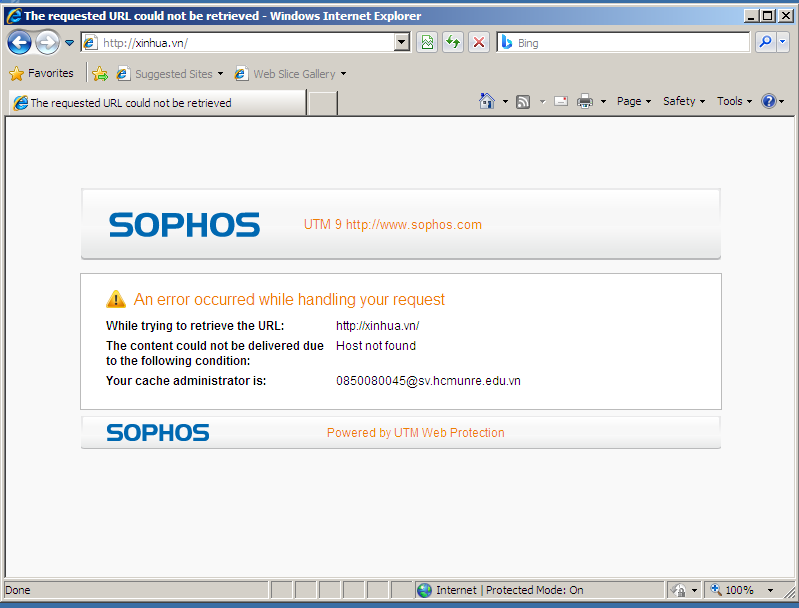


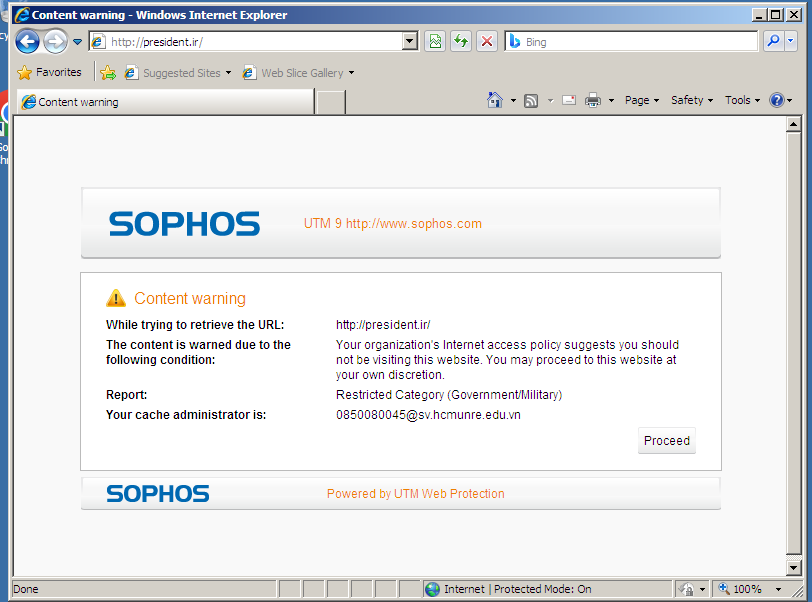
**1.** Truy cập 1 website được phép truy cập bình thường, thao tác traceroute và ping đến website đó không thành công.



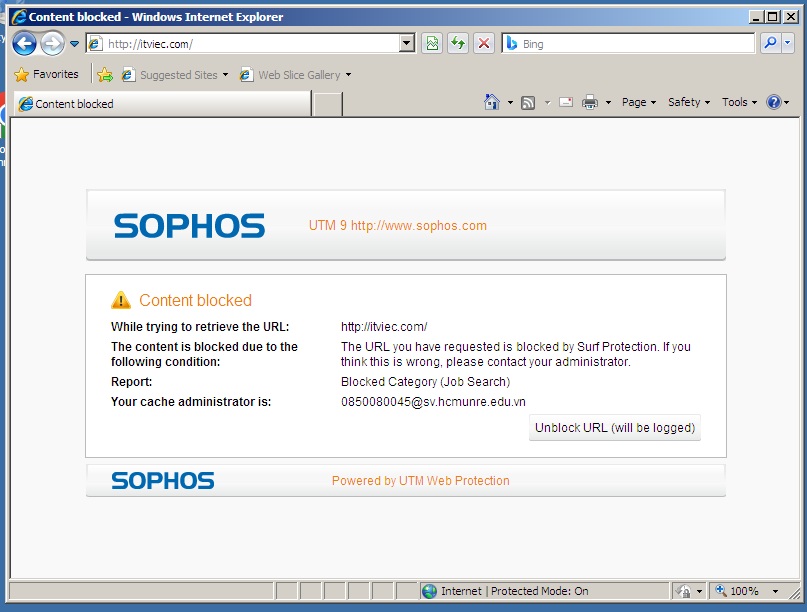


2. Không thể truy cập website báo Tân Hoa xã (xinhua.vn – news.cn) và ít nhất 2 website khác từ Trung Quốc và Trung Đông.

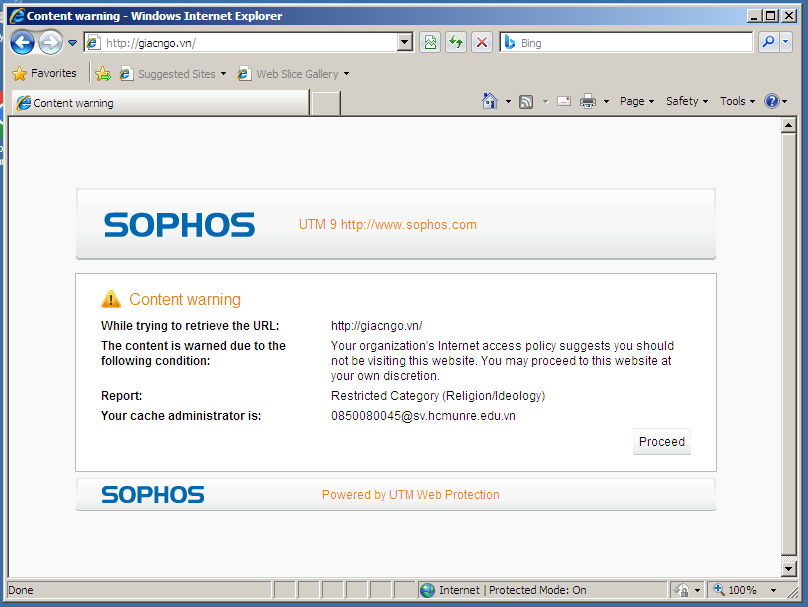




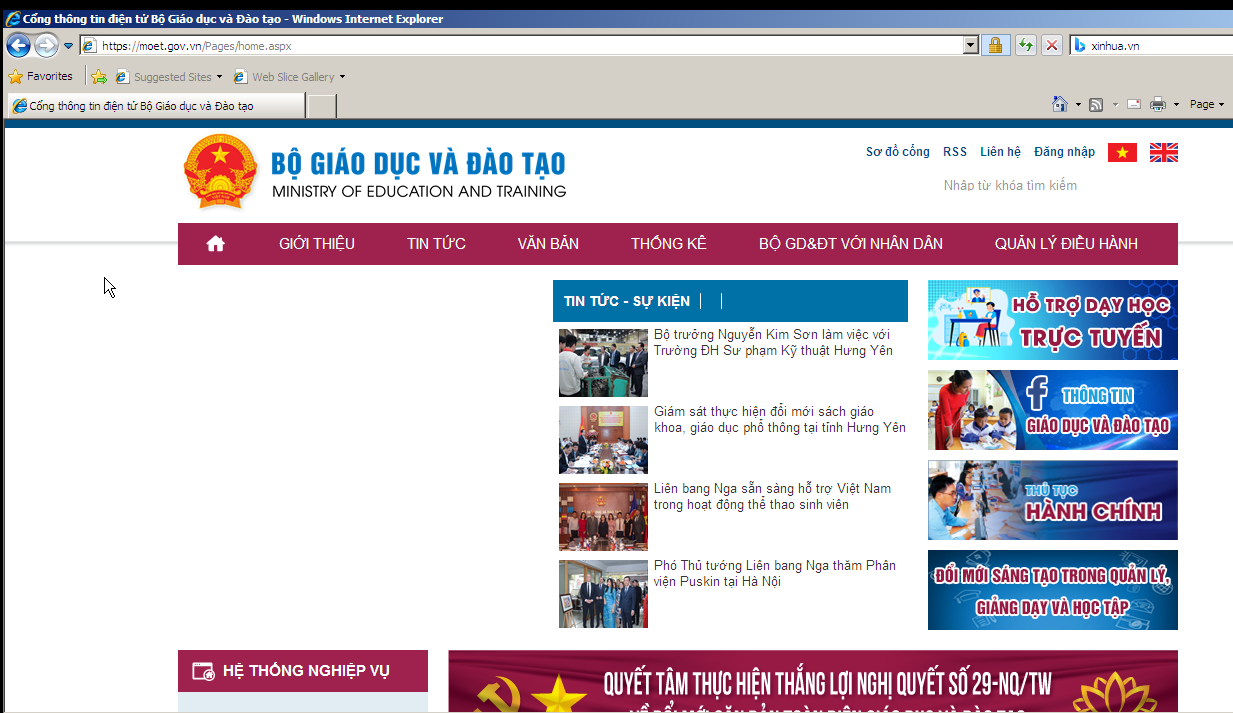
3. Không thể vào các website về tìm kiếm việc làm trên thế giới và tại Việt Nam, tại TP.HCM trong đó chặn được 4 website sau: vietnamworks.com.vn, vieclam.tuoitre.vn, timviecnhanhhcm.com, itviec.com.



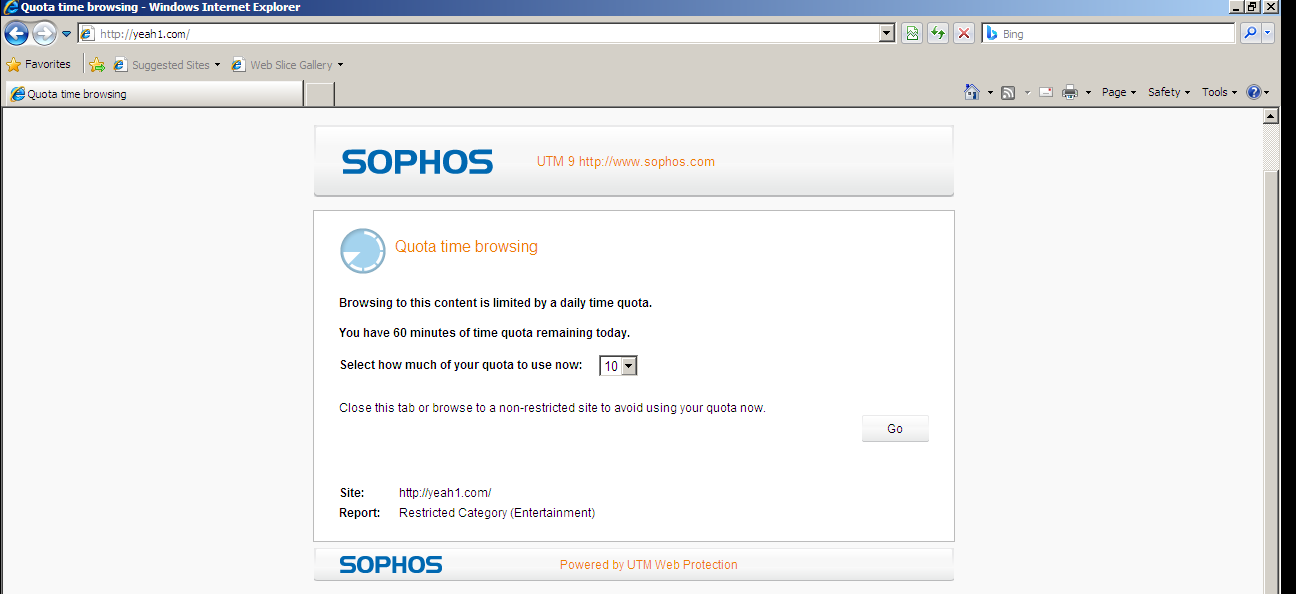
4. Hiện cảnh báo đối với một số website thuộc thể loại vũ khí, chính trị - tôn giáo như trueswords.com (vũ khí), giacngo.vn (tôn giáo), chinhphu.vn (chính trị).

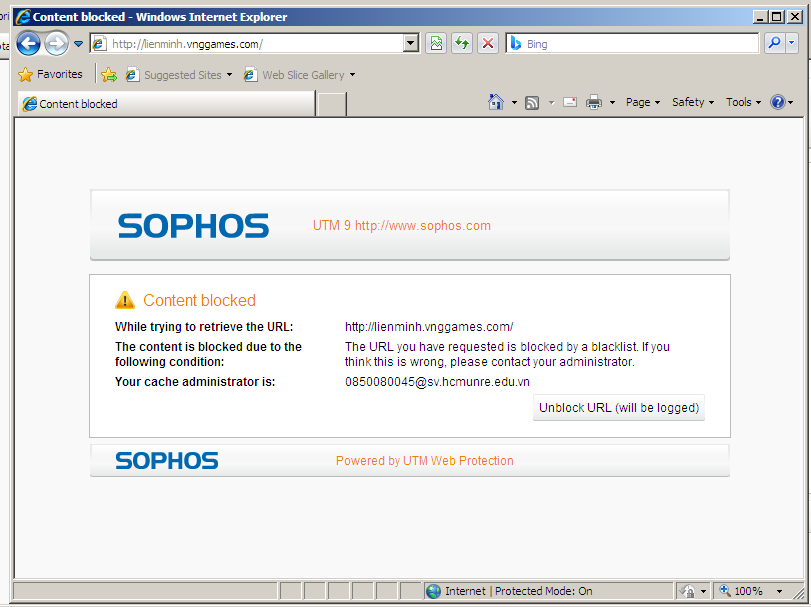


Truy cập bình thường với các website giáo dục, trường đại học như uit.edu.vn, moet.gov.vn (Bộ GD-ĐT) mà không có cảnh báo.



5. 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.





6. 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



7. 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).





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

