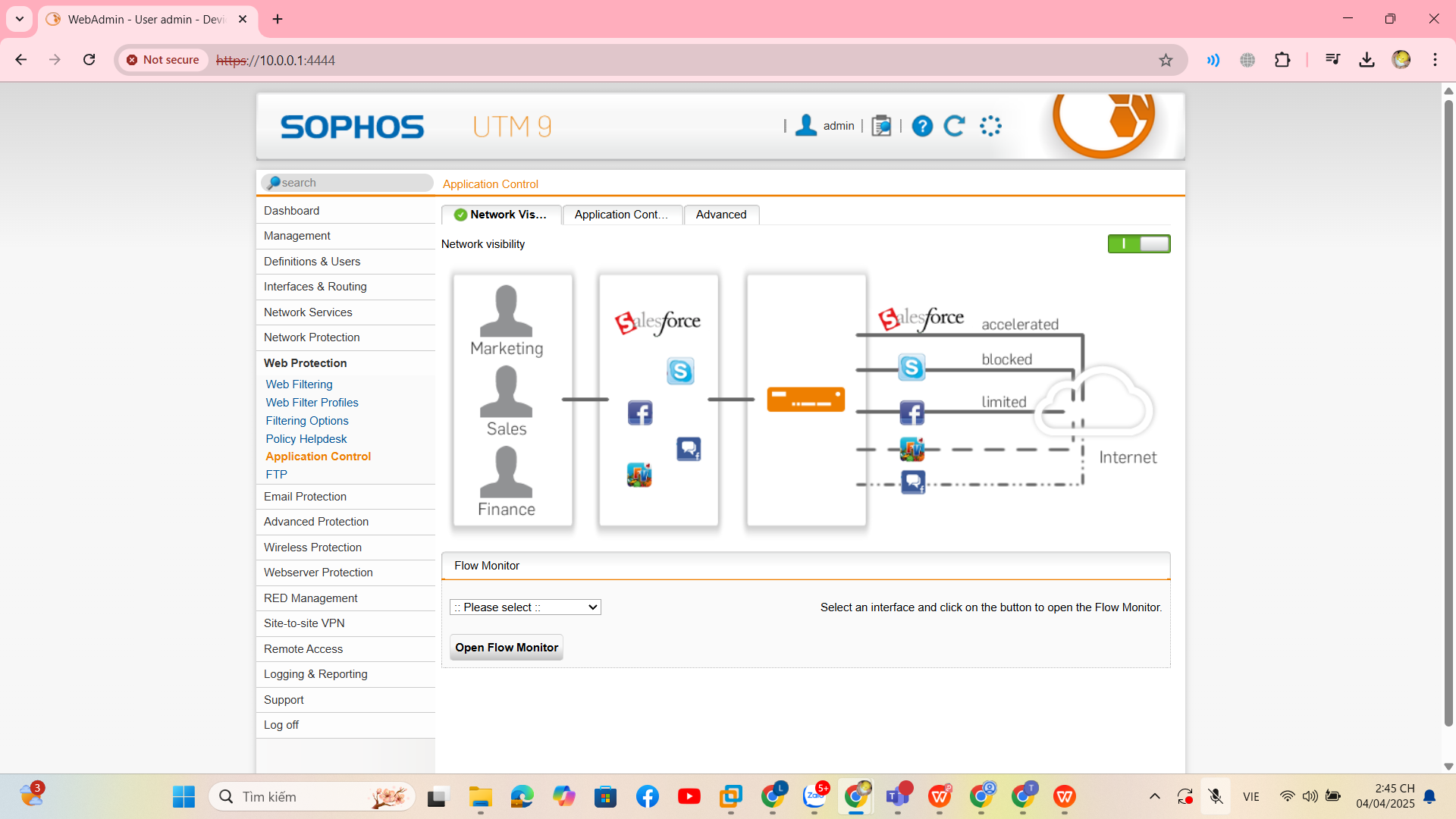
Lap 6

Tên: Lê Tiến Lên

**1. Tổng quan về xây dựng chính sách kiểm soát ứng dụng**

Trong Sophos UTM, việc xây dựng các quy tắc kiểm soát các ứng dụng mạng được

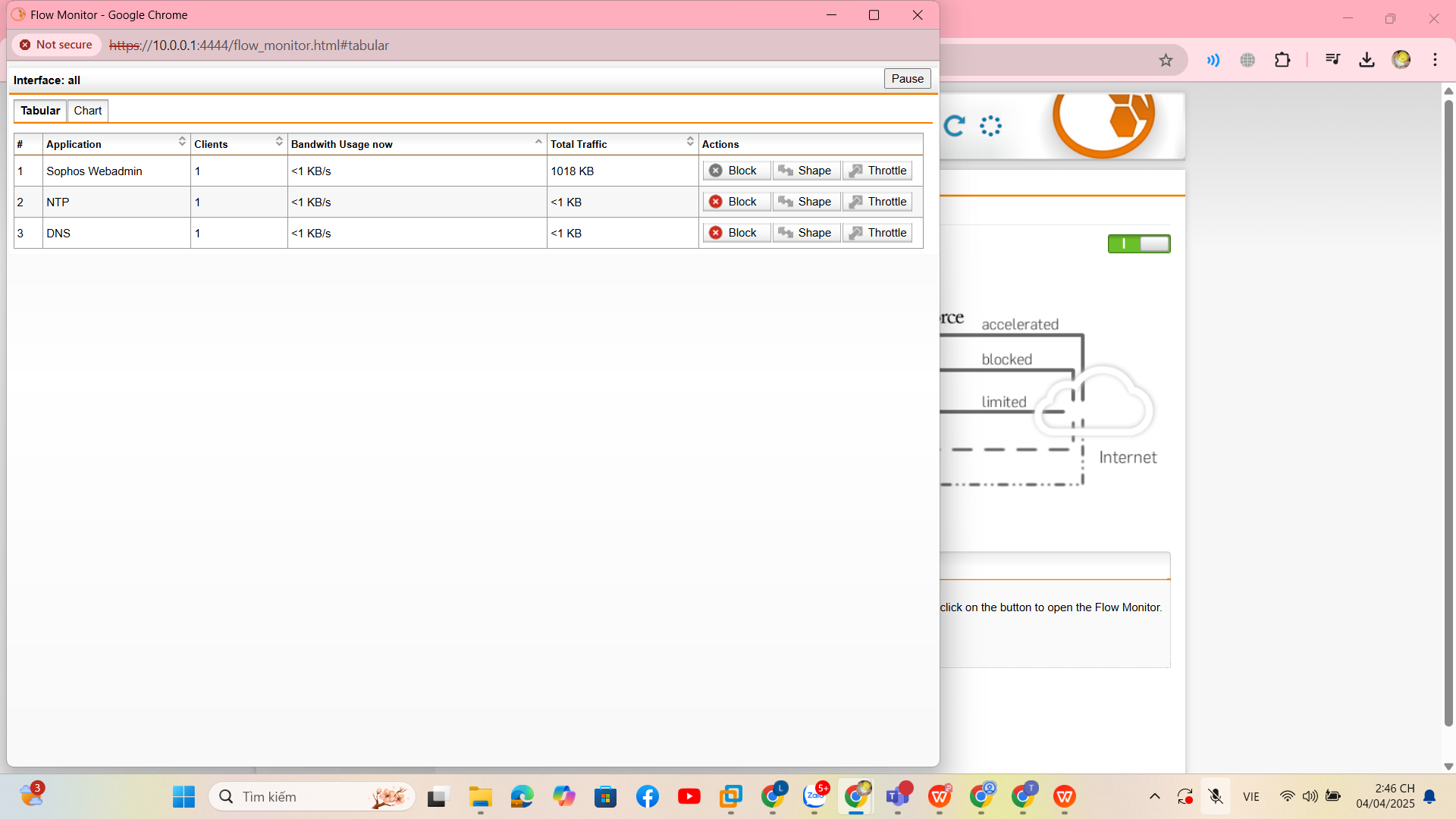
thực hiện trong **Web Protection > Application Control**



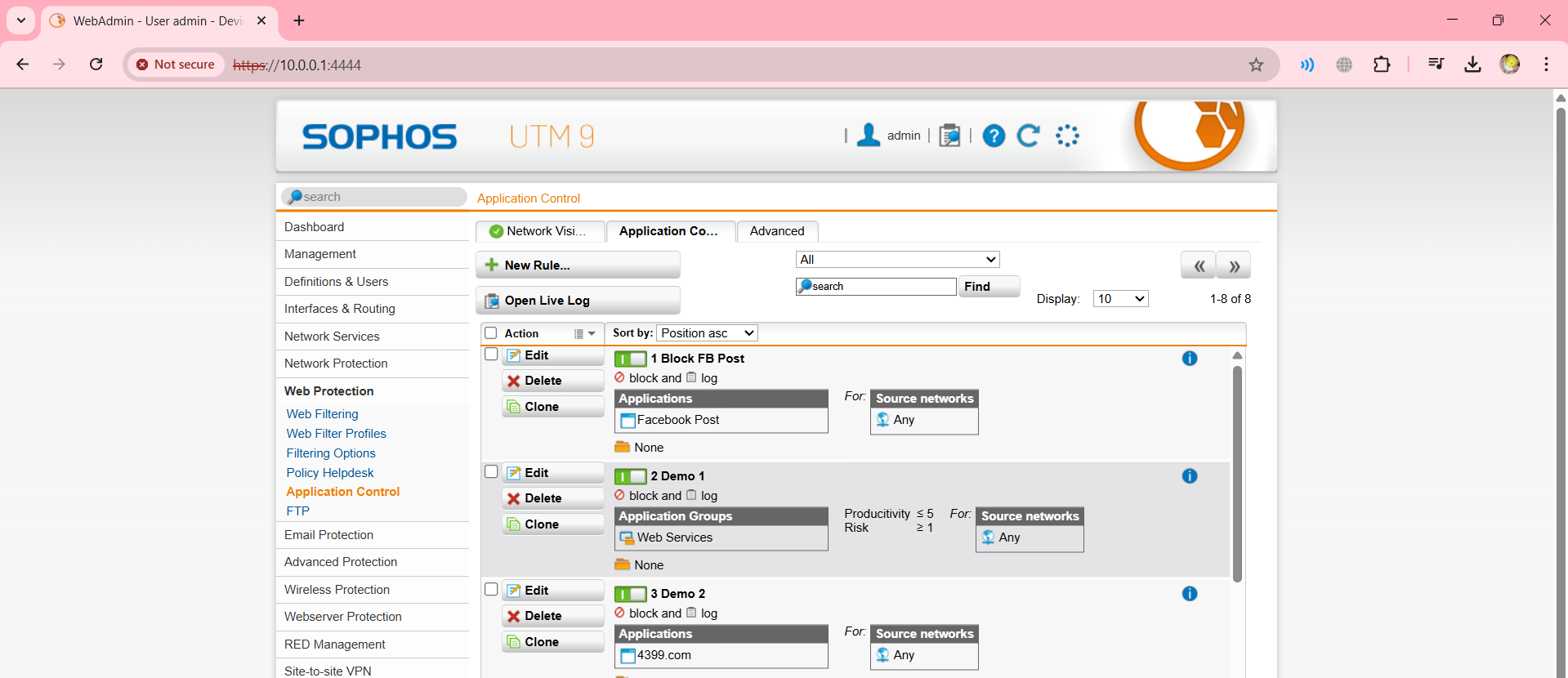
Để tiến hành thiết lập các quy tắc, cần bật Network visibility.

Tại đây còn cung cấp chức năng Flow Monitor cho phép theo dõi lưu lượng mạng

*(network traffic)* của các ứng dụng thông qua các card mạng theo thời gian thực.



Để thiết lập các quy tắc, ta thực hiện ở tab Application Control Rules.



Khi xây dựng chính sách, có thể thực hiện chính sách kiểm soát (Control by) theo

loại ứng dụng *(Applications)* hoặc theo bộ lọc động *(Dynamic filter)* dựa theo đánh

giá từ Sophos về năng suất *(Productivity)* và độ nguy hiểm *(Risk)* của loại ứng dụng

đó.

iệc xây dựng các quy tắc tương tự các Web Filter Profiles.

**2.**

**Xây dựng bộ chính sách kiểm soát ứng dụng và triển khai CA (HTTPS)**

Thiết lập các chính sách đảm bảo các yêu cầu 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

Máy người dùng sử dụng trình duyệt **Chrome version 49.0** để truy cập Internet.

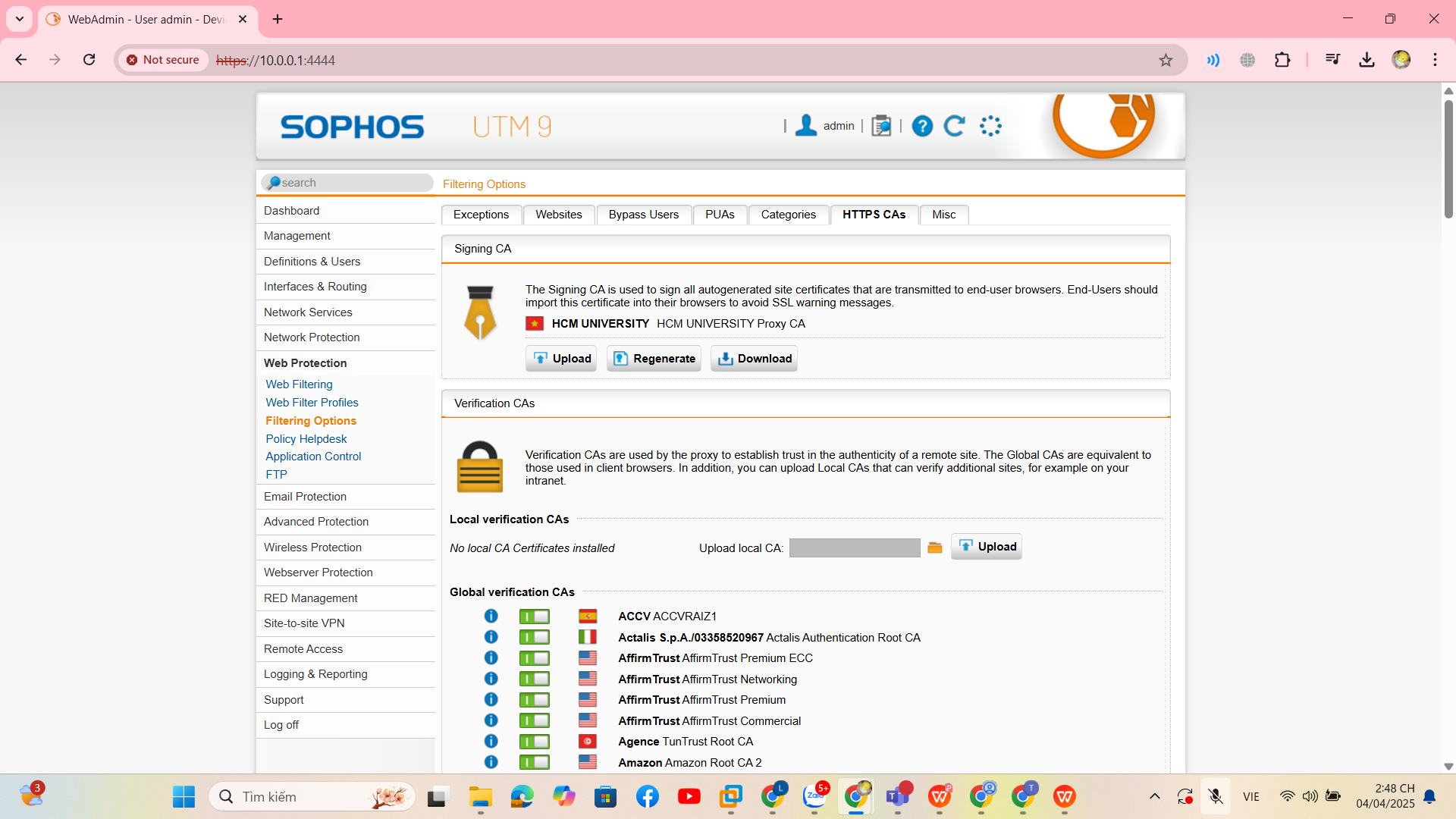
**Thiết lập bộ Chính sách kiểm soát ứng dụng & giải quyết các vấn đề:**

1. Khắc phục lỗi HTTPS khi truy cập web tại máy DC.

***Gợi ý:*** Vào Web Protection > Filtering Options > tab HTTPS Cas > Tải Signing

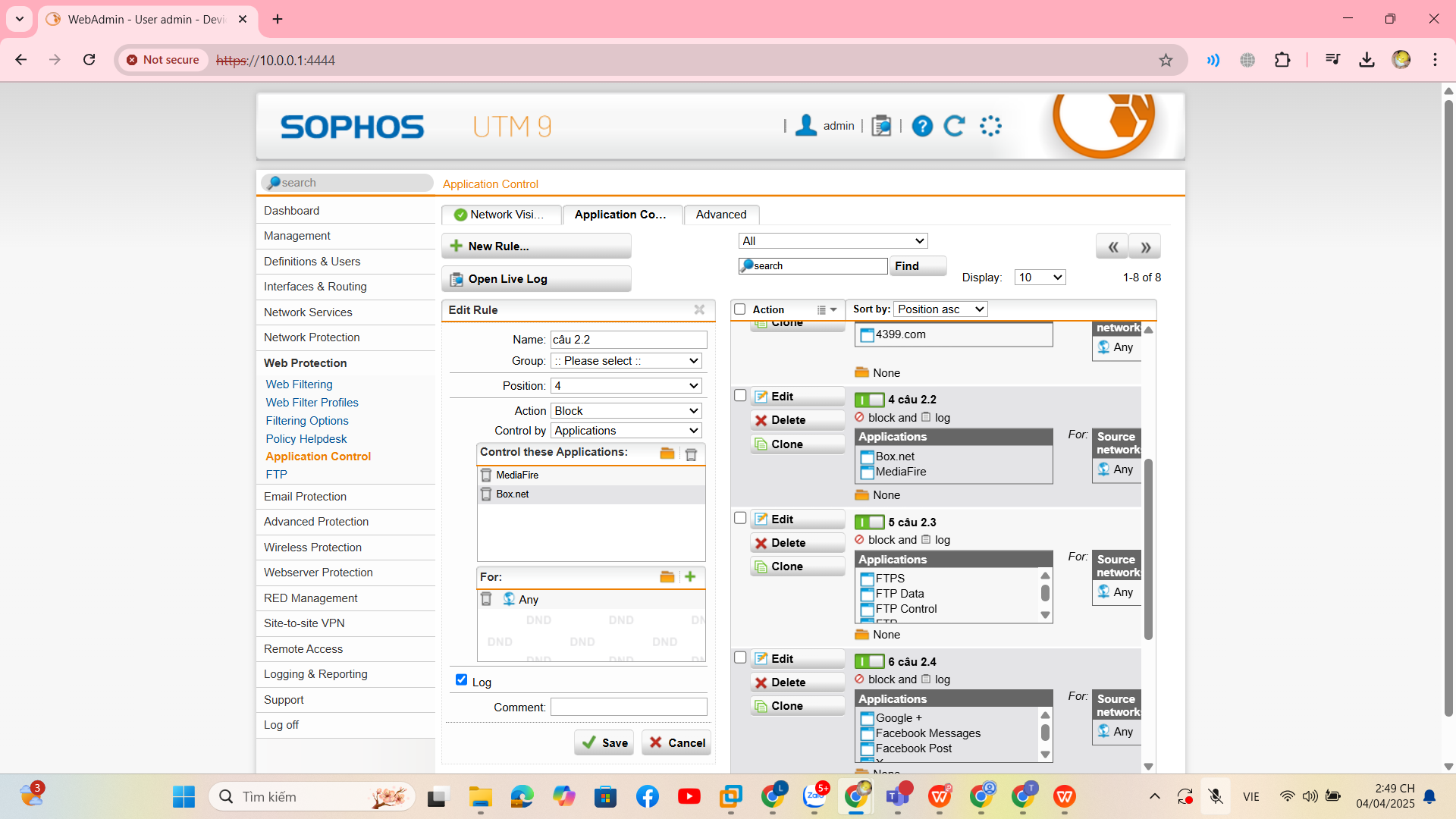
CA và cài đặt vào ***Trusted Root Certification Authorities*** của máy DC. *Sinh*

*viên có thể xem hướng dẫn chi tiết bằng cách chọn*



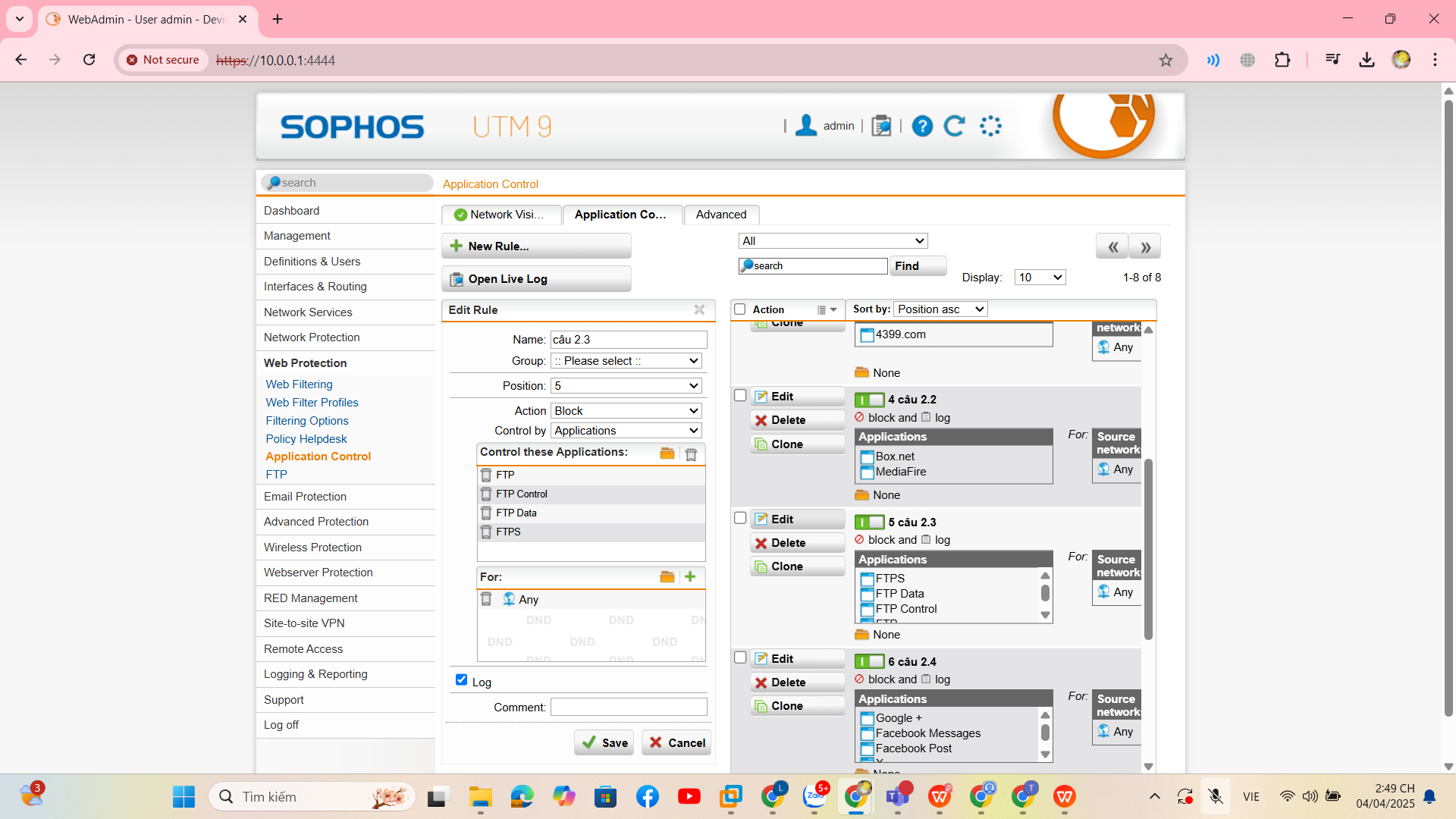
**2.** Cấm tất cả người dùng sử dụng các phương thức truyền tập tin qua Internet

bằng các website chia sẻ file *(File transfer)* như **Mediafire.com, box.net**



3. Cấm tất cả người dùng sử dụng giao thức truyền tập tin FTP, không cho

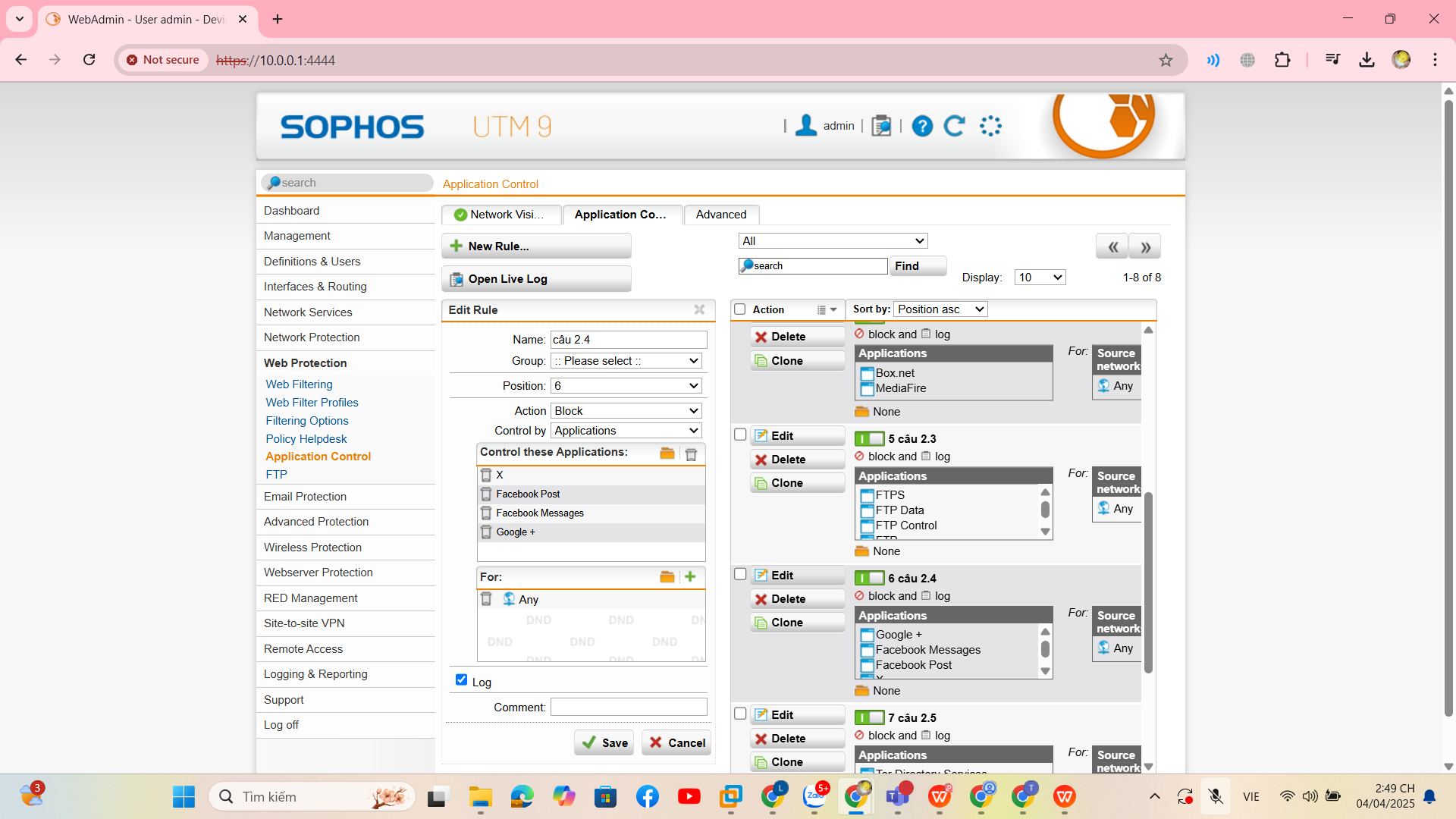
download Torrent



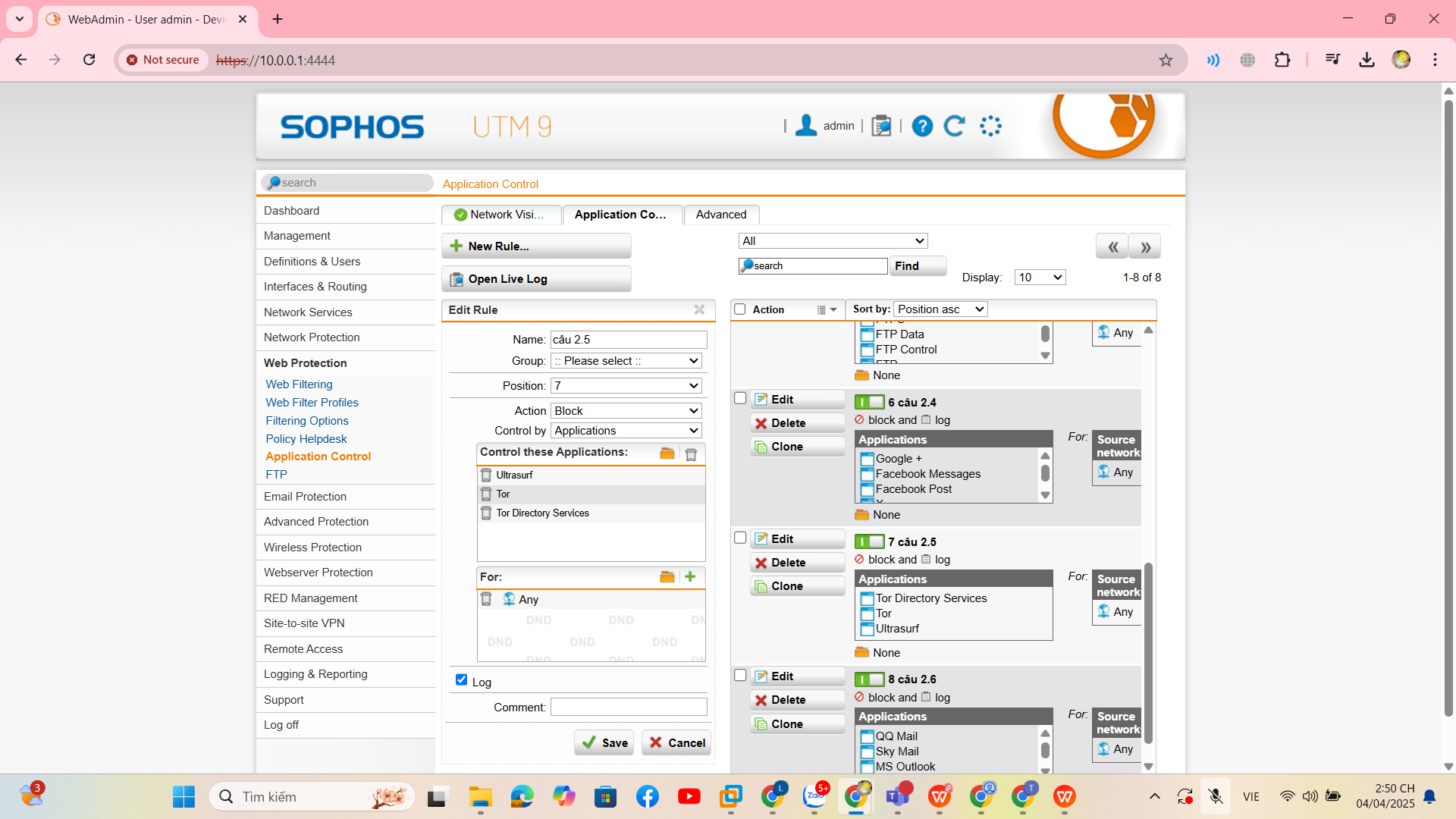
*4.* Hạn chế người dùng sử dụng mạng xã hội: Cấm sử dụng Twitter, Google+.

*Đối với Facebook cho truy cập nhưng cấm đăng status trên tường và nhắn tin trên*

*Facebook (nếu không thực hiện được thì cấm hẳn sử dụng Facebook).*



5. Cấm sử dụng các chương trình thay đổi Proxy như Tor hay Ultrasuft



6. Cấm không cho sử dụng các email server (gmail, yahoo,…), ngoại trừ email

server của công ty, trong ví dụ này giả sử cho phép http://ctmail.vnu.edu.vn

(WebMail ĐH Công nghệ - ĐHQG-HN)

