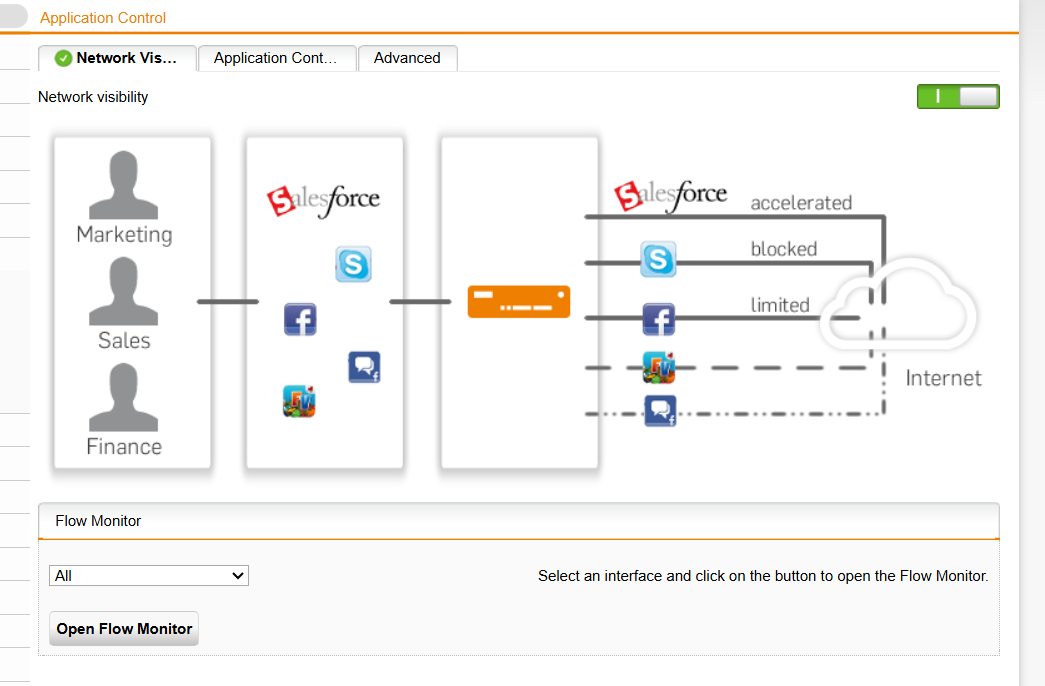
**LAB 6 SOPHOS UTM Firewall – Application Control**

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

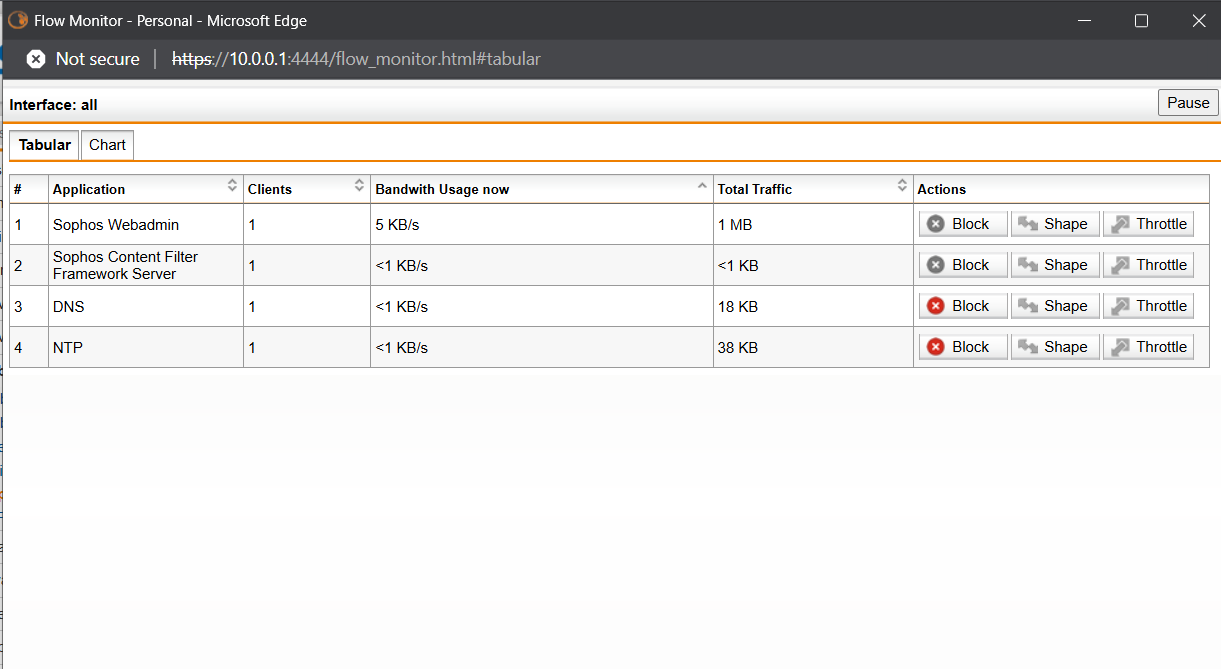
Trong Sophos UTM, việc xây dựng các quy tắc kiểm soát các ứng dụng mạng được

thực hiện trong Web Protection > Application Control

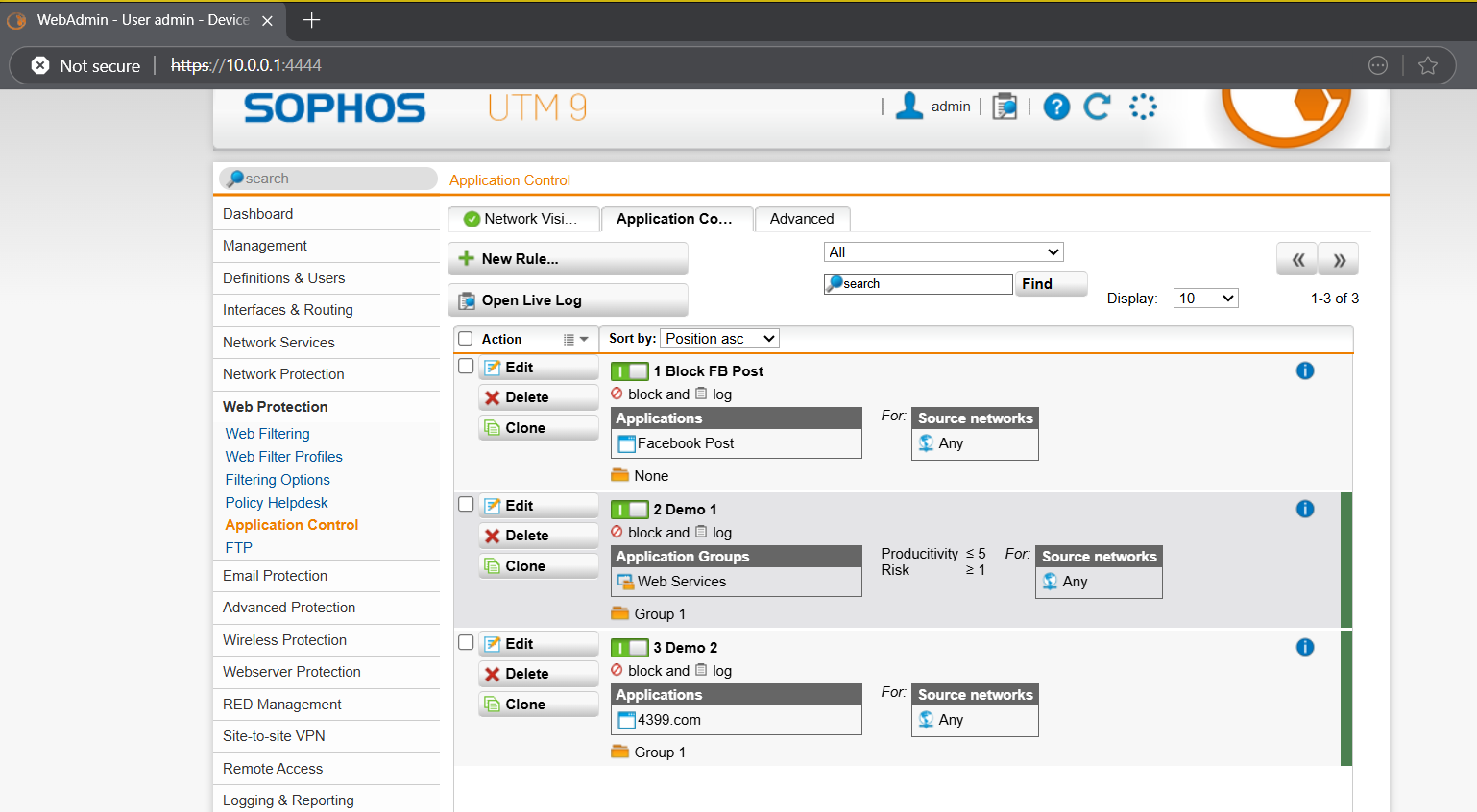
Bước 1: Để tiến hành thiết lập các quy tắc, cần bật Network visibility.



Bước 2: 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.



Bước 3 Để thiết lập các quy tắc, ta thực hiện ở tab Application Control Rules.



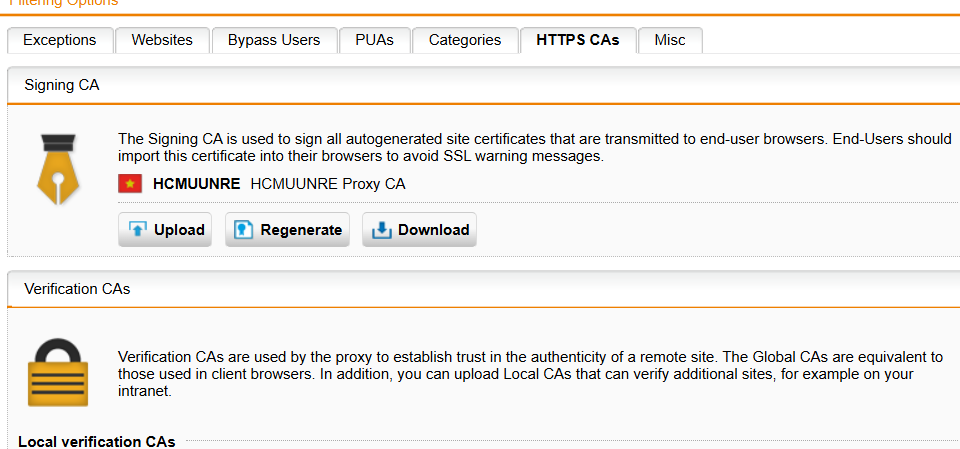
**Xây dựng bộ chính sách kiểm soát ứng dụng và triển khai CA (HTTPS)**

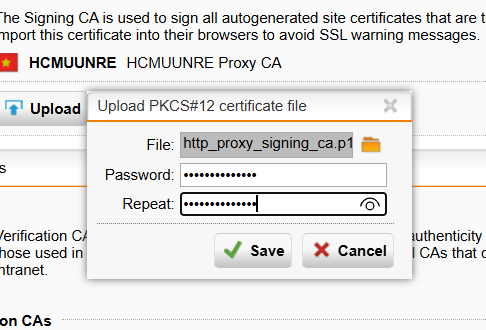
**Thiết lập bộ Chính sách kiểm soát ứng dụng & giải quyết các vấn đề:**

Bước 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.





**3. Kiểm tra kết quả & 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

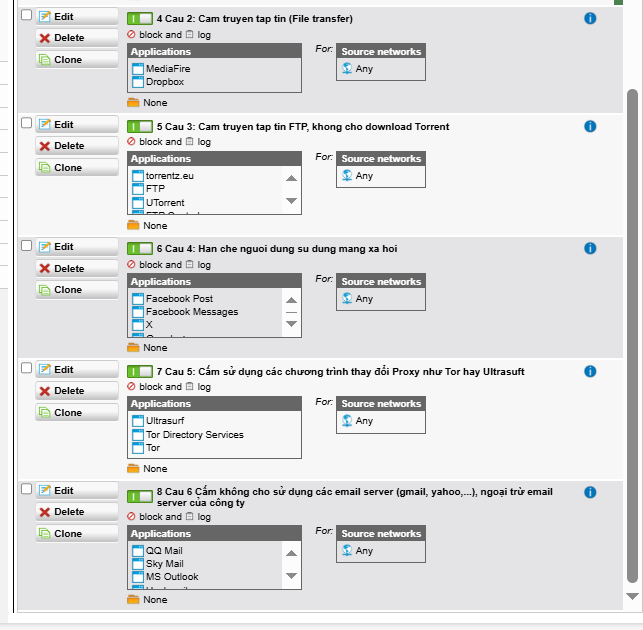
yêu cầu cần điều chỉnh lại chính sách:

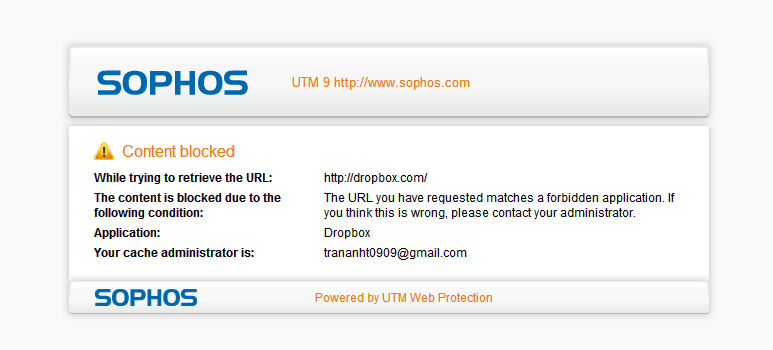
Bước 1. Khi vào các website có https trên Chrome không còn xảy ra tình trạng bị cảnh

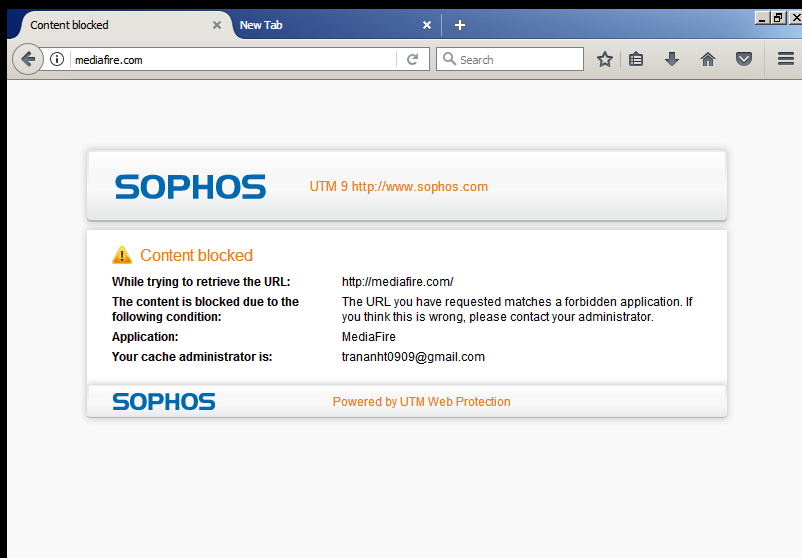
báo HTTPS



Bước 2. Không thể truy cập các website chia sẻ file như Mediafire, Dropbox,







3. Kiểm tra sử dụng giao thức FTP trước và sau khi áp dụng Rule.

Có thể sử dụng FileZilla đăng nhập qua FTP đến 1 FTP server free nào đó, sinh

viên cũng có thể sử dụng tài khoản mẫu sau đây để thử nghiệm:

FTP Server: ftp.iselab.16mb.com

User: u971091963.isedemo

Password: ise2016