Tên : Nguyễn Việt Trường Thông

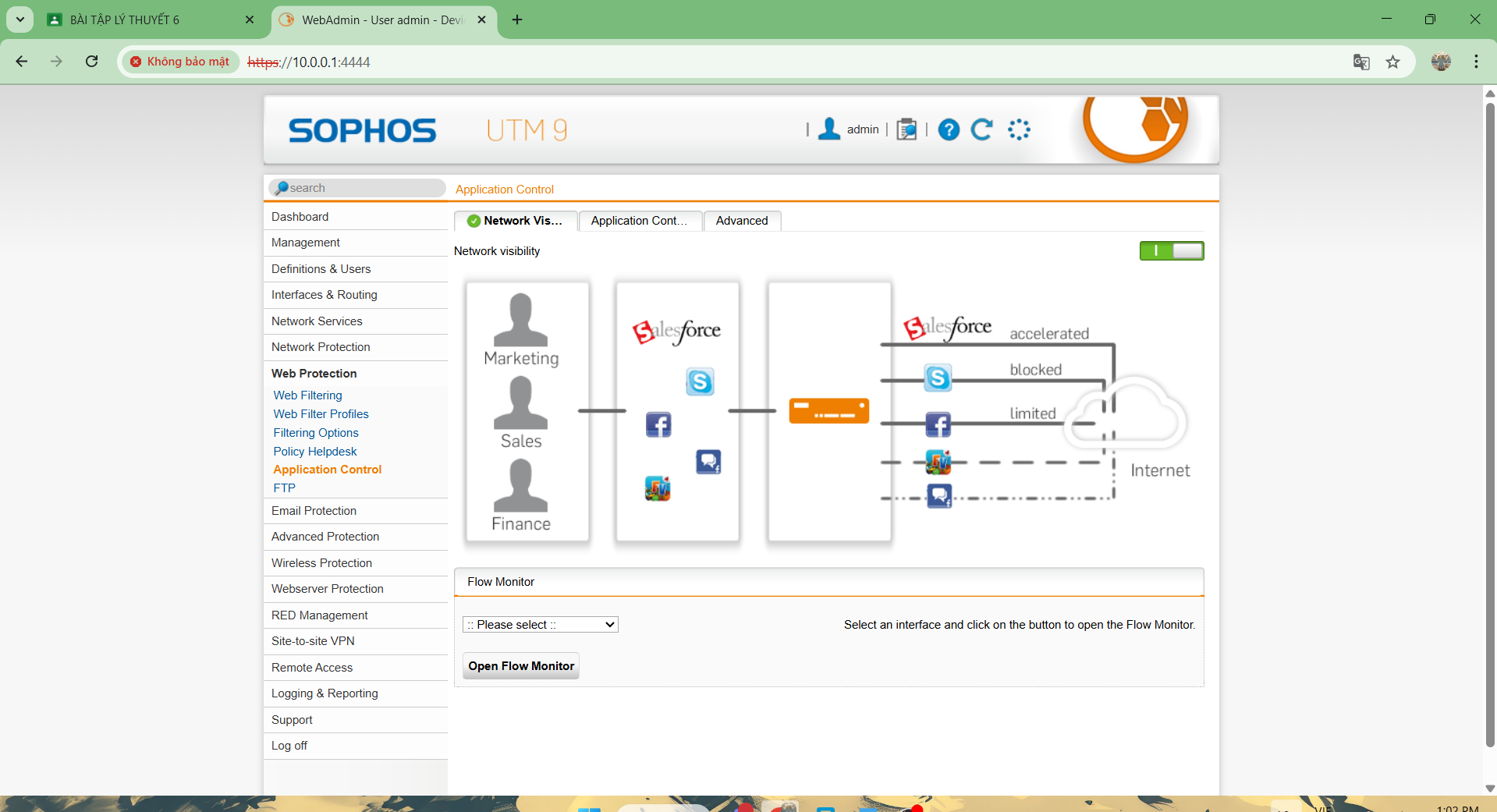
Lớp : 10 ĐH\_CNPM3

MSSV : 1050080204

LAB 6

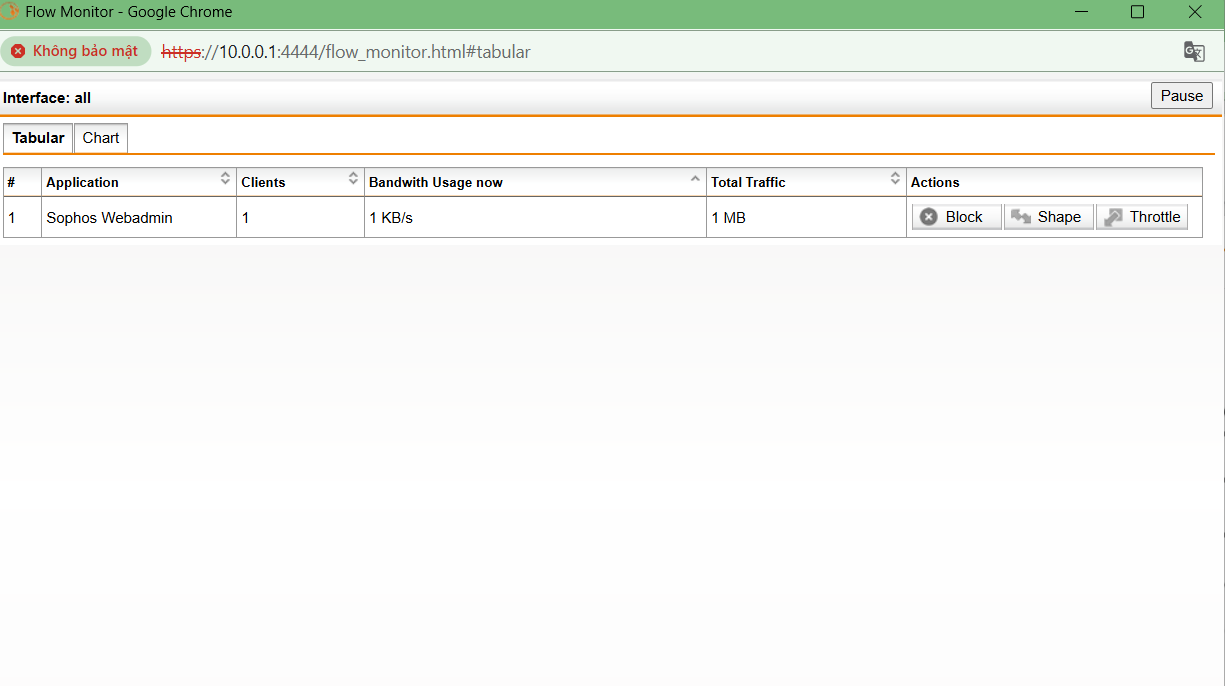
Bước 1 : Tổng quan về xây dựng chính sách kiểm soát ứng dụng

Trong Sophos UTM, việc xây dựng các quy tắc kiểm soát các ứng dụng mạng được thực hiện trong Web Protection > Application Control

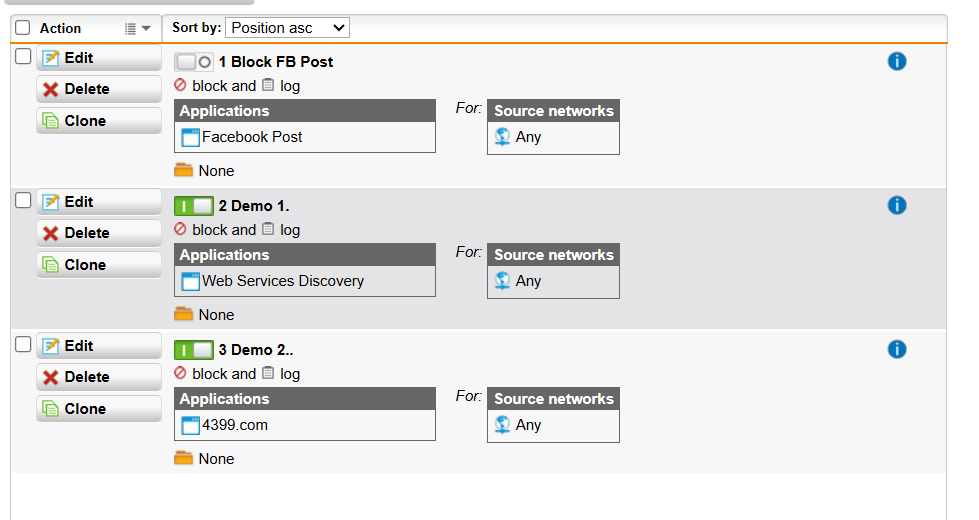


Bước 2 : Để tiến hành thiết lập các quy tắc, cần bật Network visibility.

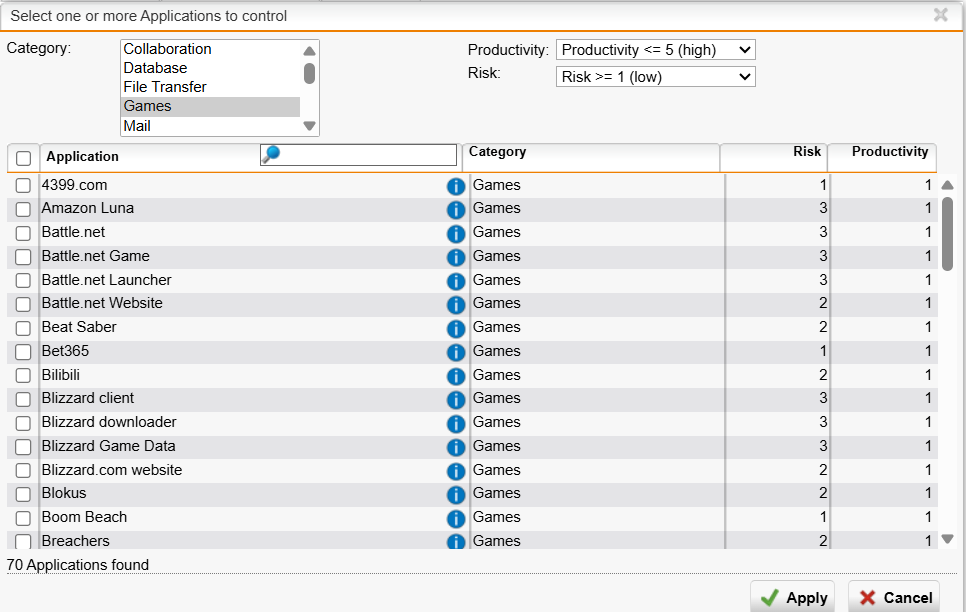
Tại đây còn cung cấp chức năng Flow Monitor cho phép theo dõi lưu lượng mạng (network traffic) của các ứng dụng thông qua các card mạng theo thời gian thực.



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.

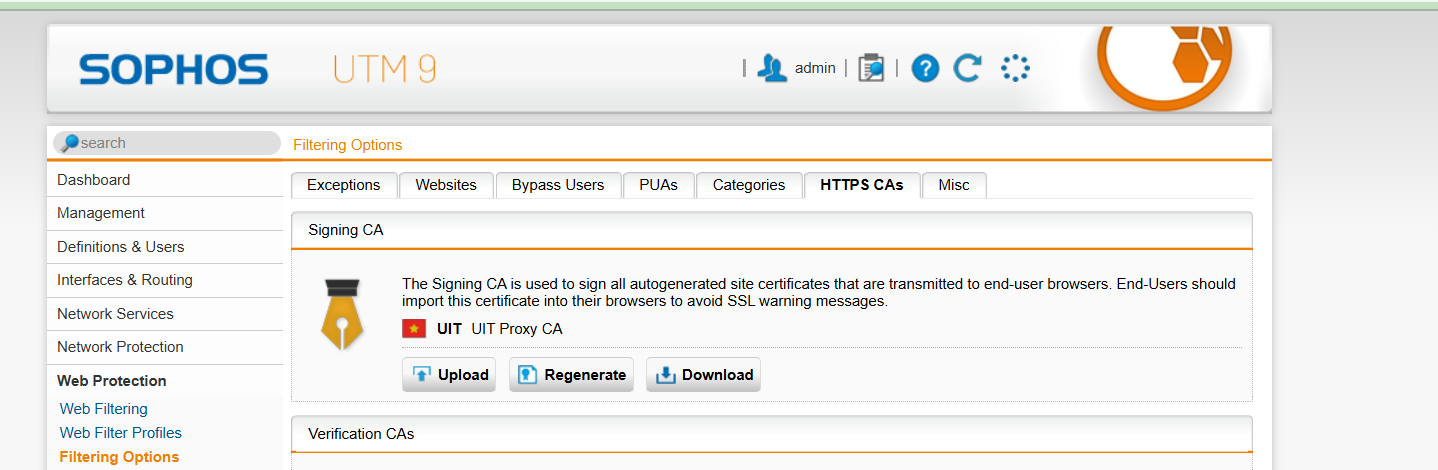


Xây dựng bộ chính sách kiểm soát ứng dụng và triển khai CA (HTTPS)

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

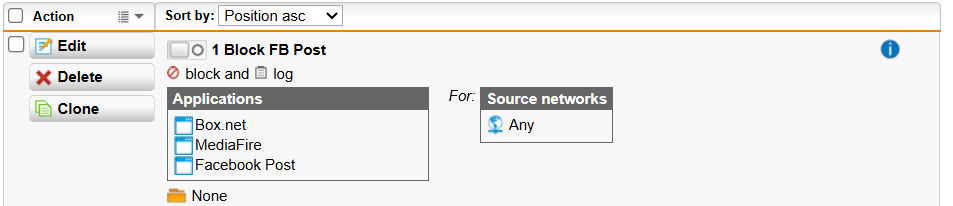
CA và cài đặt vào Trusted Root Certification Authorities của máy DC.



Bước 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



Bước 3 :

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

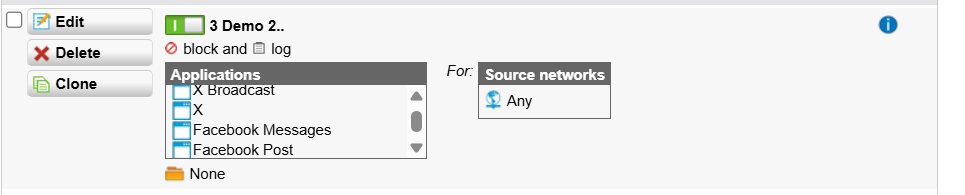
download Torrent.



Bước 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).



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

