6
Lab

Tường lửa Sophos UTM:
Chính sách ứng dụng

SOPHOS UTM Firewall – Application Control

Thực hành An toàn Mạng máy tính

GVTH: Nguyễn Thanh Hòa

Học kỳ I – Năm học 2016-2017

Lưu hành nội bộ

A. TỔNG QUAN

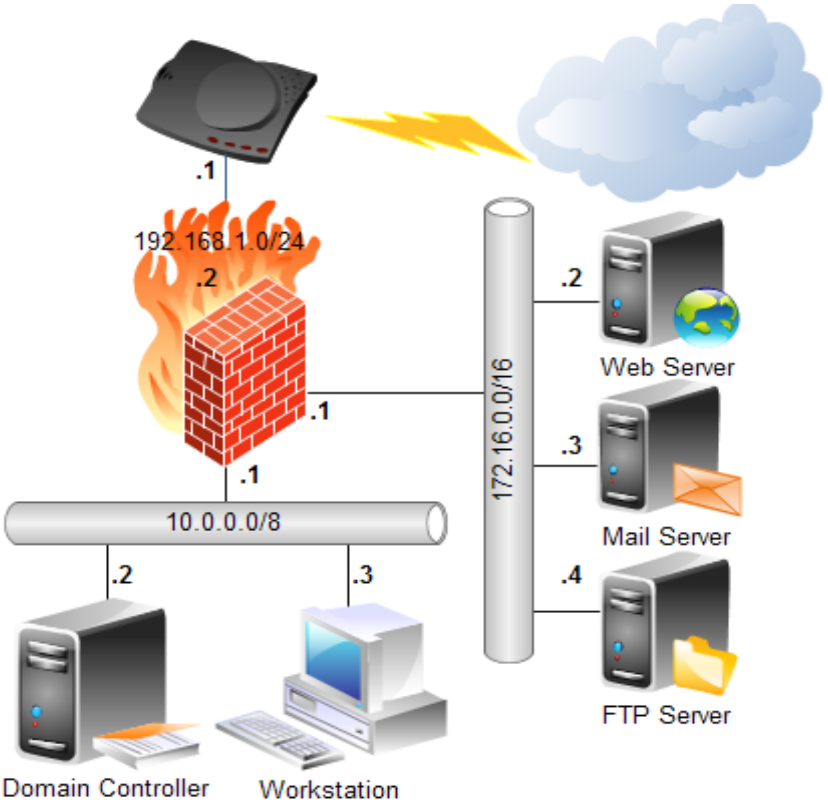
1. Mục tiêu

- Sử dụng mô hình mạng với Firewall đã thiết lập.
- Xây dựng bộ chính sách bảo vệ khi truy cập website cho người dùng.
- Tùy biến và hoàn thiện nội dung cảnh báo & thiết lập các chính sách mở rộng.

2. Môi trường & mô hình mạng

Sử dụng mô hình mạng đã xây dựng từ Lab 03.

- Mạng nội bộ: 10.0.0.0/8 với 1 Domain Controller để quản lý tập trung các máy tính theo domain.
- Vùng DMZ: 172.16.0.0/16 bao gồm các Server Web, Mail, FTP.



Hình 1. Mô hình mạng thiết lập Firewall

Thực chất trong mô hình trên, sinh viên chỉ cần chuẩn bị 2 máy tính. Trong đó:

- **Máy 1**: Windows Server 2008 làm Domain Server (1 card mạng Host-only)
- **Máy 2**: Firewall Sophos UTM 9.4

Đồng thời, dùng máy thật để kết nối vào WebAdmin của Firewall.

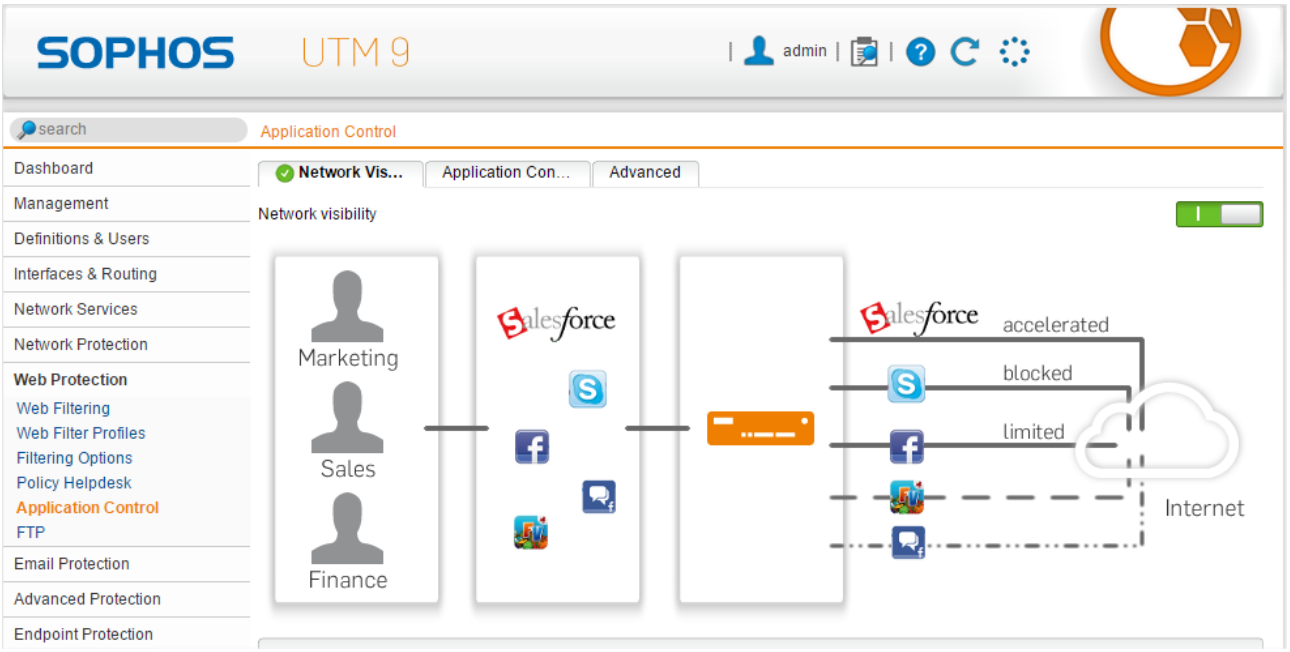
Vùng DMZ trong mô hình chỉ để tham khảo về mô hình mạng thực tế.

Kiểm tra lại mô hình mạng hoạt động bình thường trước khi tiếp tục thực hành.

B. THỰC HÀNH

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

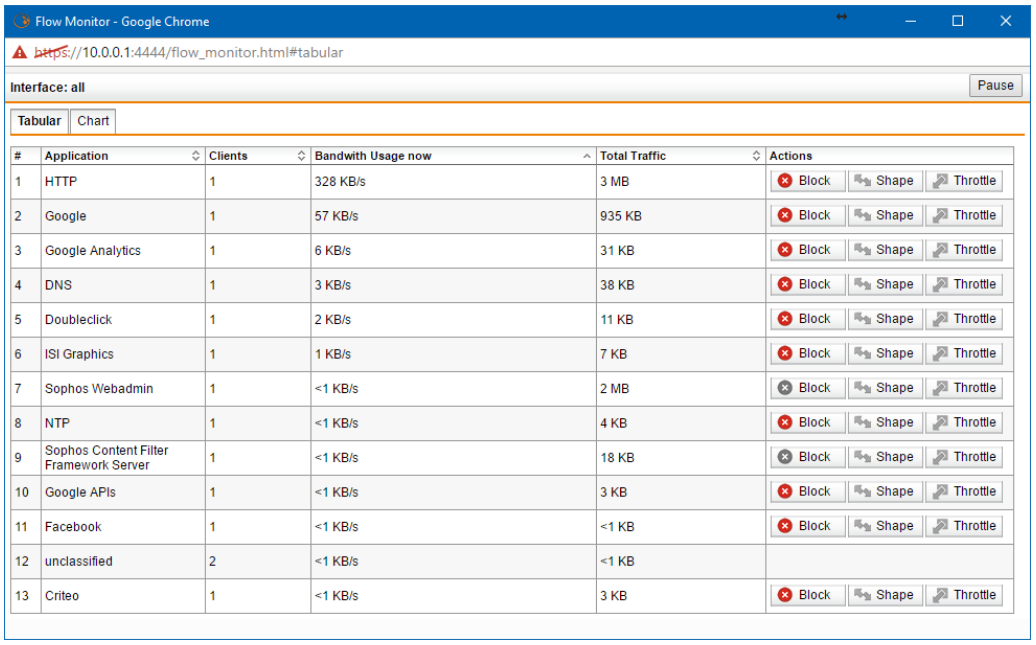
Trong Sophos UTM, việc xây dựng các quy tắc kiểm soát các ứng dụng mạng được thực hiện trong **Web Protection > Application Control**



Hình 2. Kiểm soát ứng dụng mạng

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

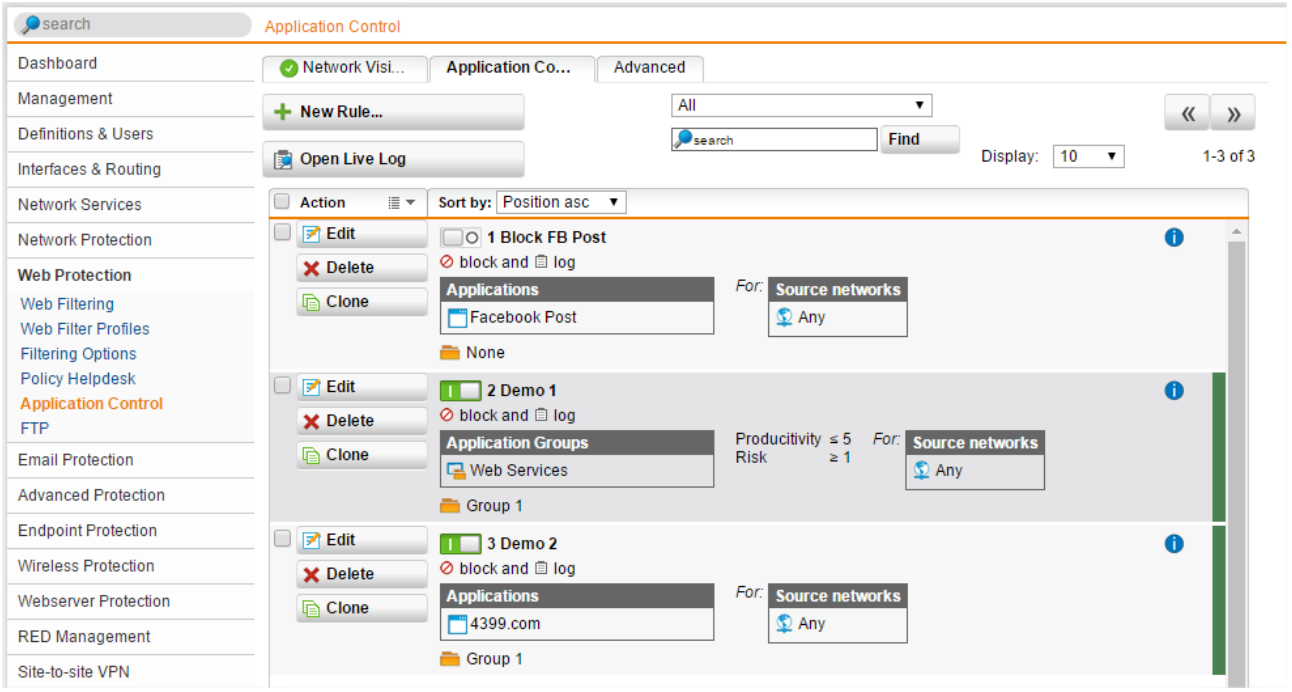
Tại đây còn cung cấp chức năng Flow Monitor cho phép theo dõi lưu lượng mạng *(network traffic)* của các ứng dụng thông qua các card mạng theo thời gian thực.



#	Application	Clients	Bandwith Usage now	Total Traffic	Actions
1	HTTP	1	328 KB/s	3 MB	Block Shape Throttle
2	Google	1	57 KB/s	935 KB	Block Shape Throttle
3	Google Analytics	1	6 KB/s	31 KB	Block Shape Throttle
4	DNS	1	3 KB/s	38 KB	Block Shape Throttle
5	Doubleclick	1	2 KB/s	11 KB	Block Shape Throttle
6	ISI Graphics	1	1 KB/s	7 KB	Block Shape Throttle
7	Sophos Webadmin	1	<1 KB/s	2 MB	Block Shape Throttle
8	NTP	1	<1 KB/s	4 KB	Block Shape Throttle
9	Sophos Content Filter Framework Server	1	<1 KB/s	18 KB	Block Shape Throttle
10	Google APIs	1	<1 KB/s	3 KB	Block Shape Throttle
11	Facebook	1	<1 KB/s	<1 KB	Block Shape Throttle
12	unclassified	2	<1 KB/s	<1 KB	
13	Criteo	1	<1 KB/s	3 KB	Block Shape Throttle

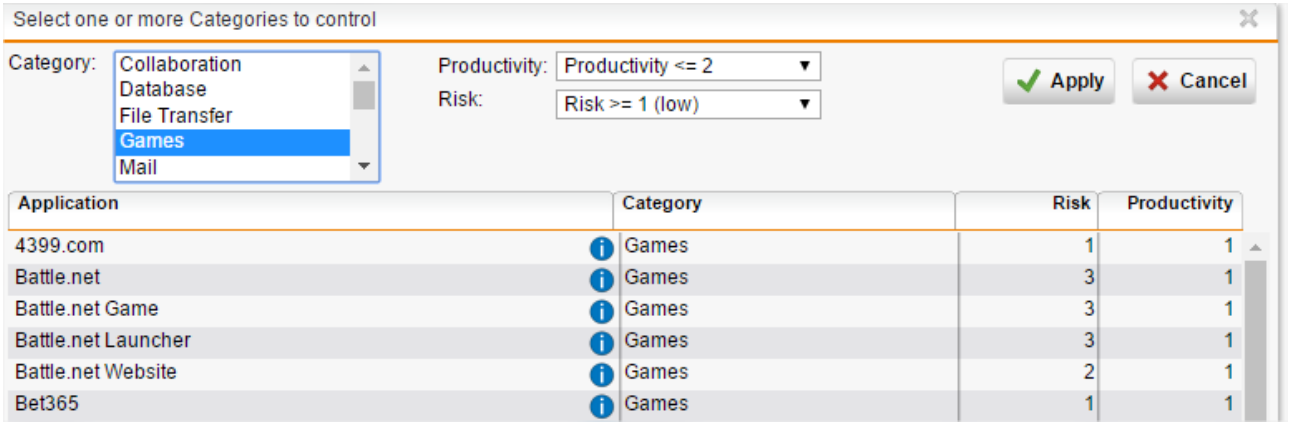
Hình 3. Theo dõi network traffic và chặn theo thời gian thực

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



Hình 4. Xây dựng các chính sách cho các ứng dụng mạng

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.



Hình 5. Chọn loại danh mục và đánh giá ứng dụng để xây dựng quy tắc

Việc 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:

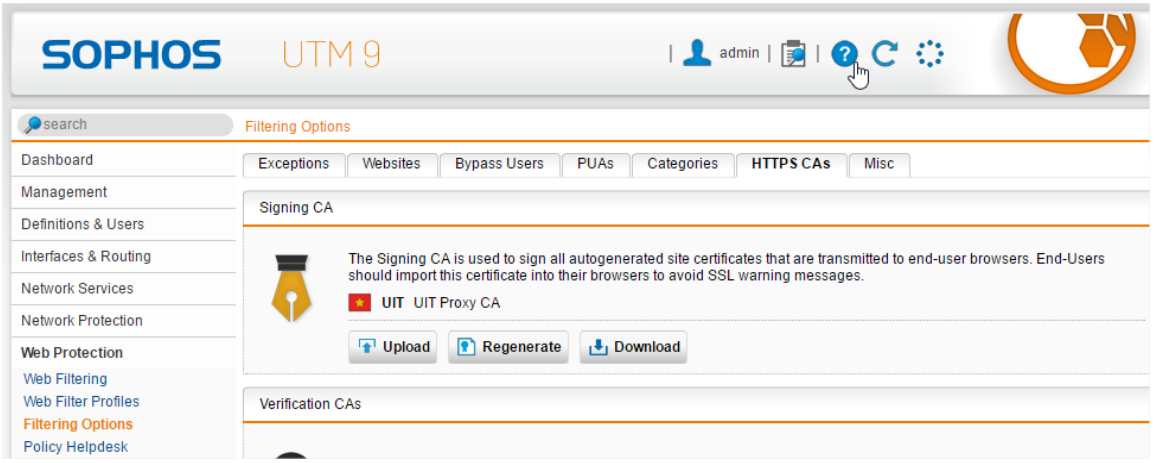
Hệ thống mạng nội bộ xây dựng theo mô hình domain như đã xây dựng gồm 3 user: Administrator (Quản trị), user a và b (tương ứng 2 user trong nhóm sinh viên đã tạo).

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*



Hình 6. Tải về Signing CA và import vào máy DC

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).

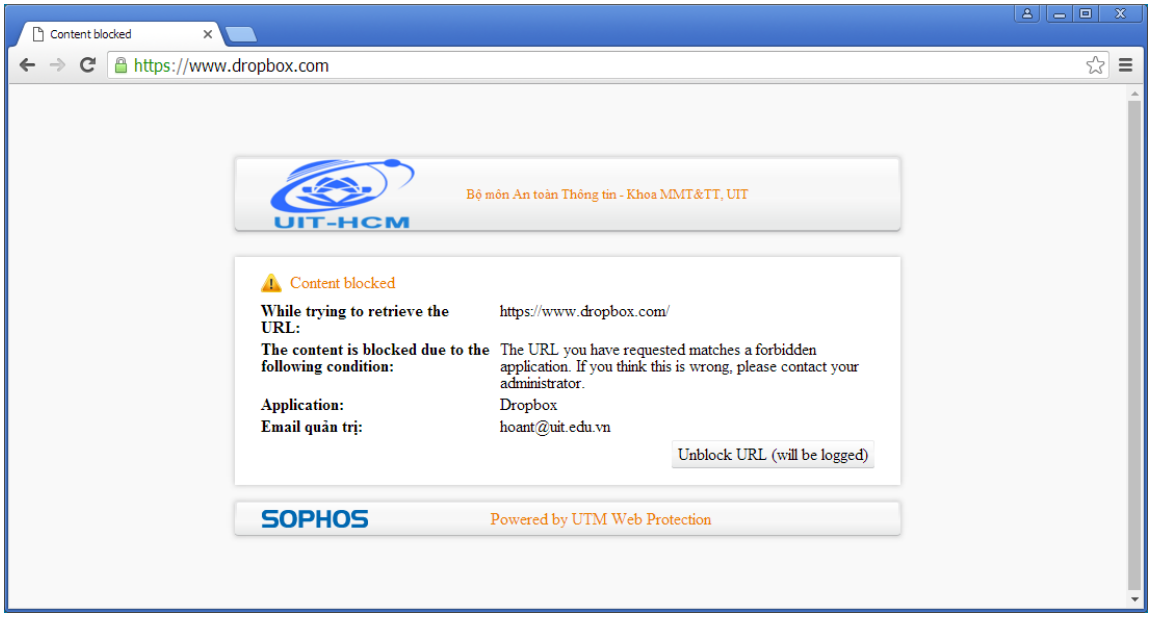
3. Kiểm tra kết quả & ứng dụng

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:

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

Hình 7. Truy cập các website HTTPS bình thường

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



Hình 8. Không thể truy cập các website Dropbox, Mediafire, ...

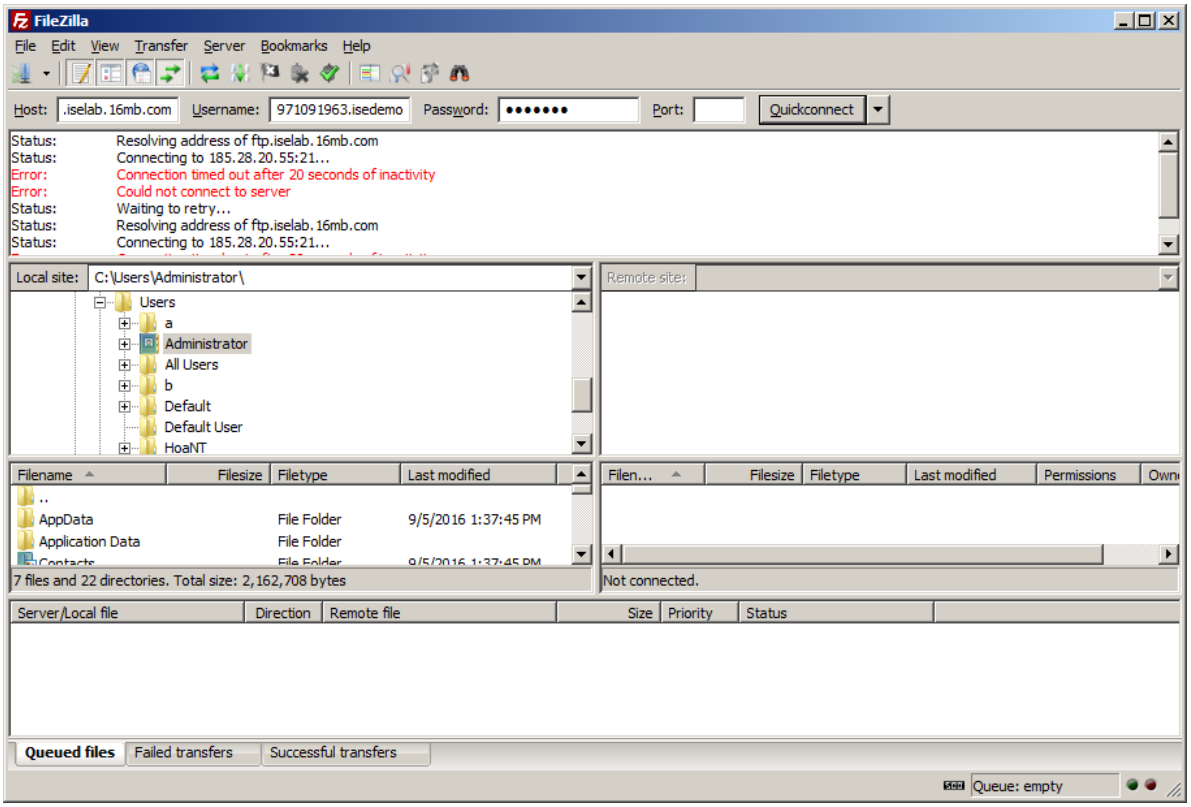
3. Kiểm tra sử dụng giao thức FTP trước và sau khi áp dụng Rule.

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

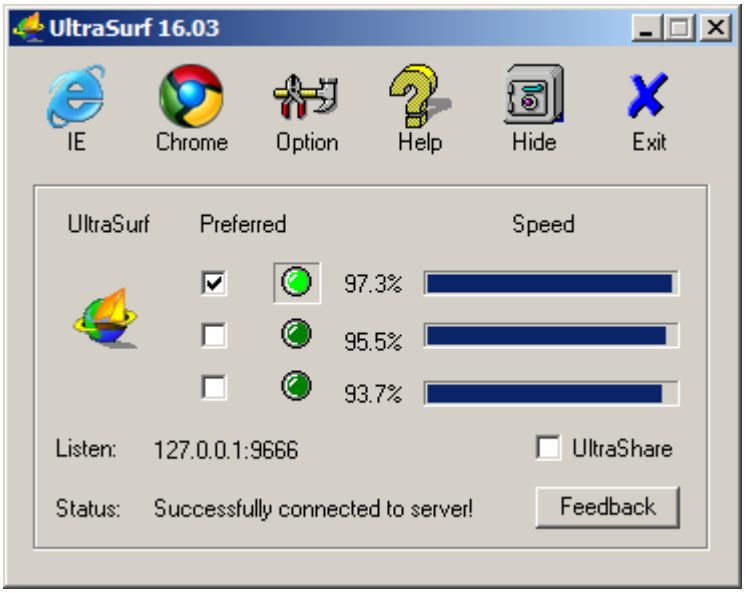
Password: ise2016



Hình 9. Kiểm tra giao thức FTP khi thực hiện Rule

Kiểm tra sử dụng uTorrent hay BitTorrent và download thông qua một tập tin .torrent nào đó để kiểm tra kết quả.

4. Thử nghiệm khi truy cập và sử dụng với các Mạng xã hội phổ biến.
5. Thử nghiệm với Ultrasuft hay Tor và kiểm tra kết quả



Hình 10. Sử dụng Ultrasurf trước và sau khi thiết lập chính sách và kiểm tra kết quả

6. Kiểm tra kết quả khi truy cập **gmail.com; mail.uit.edu.vn; ctmail.vnu.edu.vn**

4. Mở rộng

(Phần này khuyến khích thực hiện, không bắt buộc)

Tìm hiểu và nghiên cứu sử dụng một trong những tính năng còn lại của ***Sophos UTM*** *(Email Protection, Endpoint Protection, Wireless Protection, Web Server Protection, Intrusion Prevention, …)* và thực hiện minh họa cách hoạt động của chức năng đó.

C. YÊU CẦU

- Sinh viên tìm hiểu và thực hành theo hướng dẫn. Thực hiện theo nhóm hoặc cá nhân như đã đăng ký từ buổi 1.
- Sinh viên báo cáo kết quả thực hiện trực tiếp tại lớp.
- *Riêng nội dung **Mở rộng**, sinh viên có thể nghiên cứu thêm để thực hiện nộp bài theo mẫu báo cáo tại website môn học đến ngày **30/11/2016** qua email hoant@uit.edu.vn và sẽ được tính điểm bổ sung cho kết quả thực hành chung của môn học.*

Đánh giá: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

- Chuẩn bị tốt và đóng góp tích cực tại lớp.
- Thực hiện nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

Sinh viên vắng sẽ không có điểm cho bài thực hành này.

D. THAM KHẢO

Sophos UTM 9 documentation:

https://www.sophos.com/en-us/support/documentation/sophos-utm.aspx

HẾT