Đỗ Trần Nhật Tân

1050080198

10ĐH\_CNPM3

Lab 6

Bước 1: Truy cập giao diện và kích hoạt tính năng

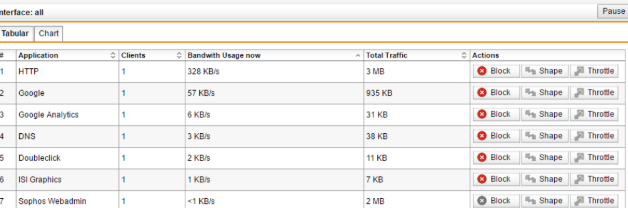
Vào mục: Web Protection > Application Control

Đây là nơi xây dựng các quy tắc kiểm soát các ứng dụng mạng

Bật Network Visibility:

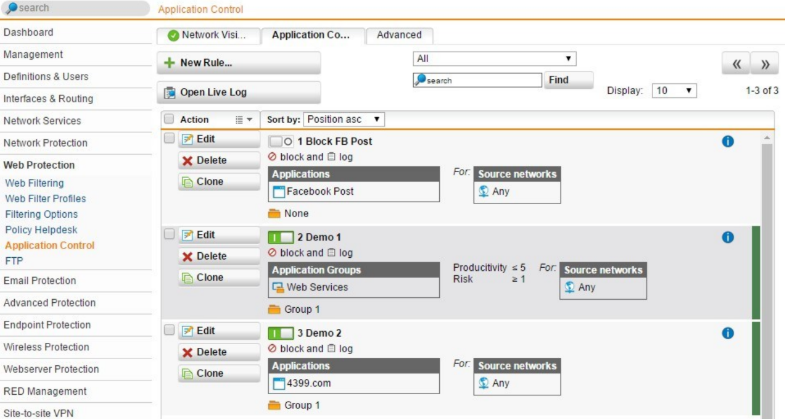
Để có thể theo dõi lưu lượng mạng (network traffic) qua các card mạng theo thời gian thực, bạn cần kích hoạt tính năng này.

Công cụ Flow Monitor sẽ hỗ trợ việc theo dõi và chặn lưu lượng mạng ngay lập tức



Bước 2: Thiết lập quy tắc kiểm soát

Chuyển đến tab Application Control Rules:



Tại đây, bạn sẽ tạo và cấu hình các chính sách kiểm soát ứng dụng

Lựa chọn phương thức kiểm soát:

Control by Applications: Kiểm soát theo từng loại ứng dụng cụ thể.

Dynamic Filter: Sử dụng bộ lọc động dựa trên đánh giá của Sophos về năng suất (Productivity) và độ nguy hiểm (Risk) của ứng dụng

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

Bước 3: Cài đặt môi trường thực hành

Mô hình mạng:

Mạng nội bộ được xây dựng theo mô hình domain với 3 người dùng:

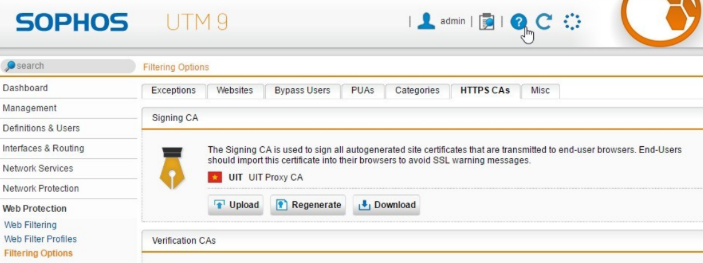
Administrator (Quản trị)

User a và User b (2 user thuộc nhóm sinh viên).

Máy trạm:

Sử dụng trình duyệt Chrome phiên bản 49.0 để truy cập Internet.

Bước 4: Thiết lập chính sách và khắc phục các vấn đề



Khắc phục lỗi HTTPS trên máy DC:

Vào Web Protection > Filtering Options > tab HTTPS CAs

Tải file Signing CA và import vào Trusted Root Certification Authorities của máy DC.

Chặn các website chia sẻ file:

Cấm người dùng truy cập các trang như Mediafire.com, box.net.

Cấm sử dụng giao thức FTP và download Torrent:

Áp dụng quy tắc để ngăn việc truyền tải file qua FTP và tải torrent.

Hạn chế truy cập mạng xã hội:

Cấm: Twitter, Google+.

Facebook: Cho phép truy cập nhưng cấm đăng status và gửi tin nhắn (nếu không khả thi, có thể cấm hoàn toàn).

Chặn các chương trình thay đổi Proxy:

Ví dụ: Tor, Ultrasurf.

Hạn chế sử dụng email server ngoài của công ty:

Cấm truy cập các email server như Gmail, Yahoo,…

Trong ví dụ này, chỉ cho phép truy cập email của công ty tại địa chỉ: http://ctmail.vnu.edu.vn.

3. Kiểm tra kết quả & ứng dụng

Bước 5: Thực hiện kiểm tra từng quy tắc

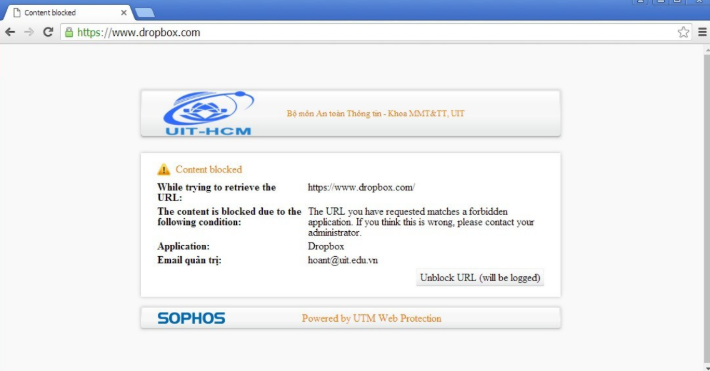
Kiểm tra HTTPS:

Mở Chrome và truy cập các website sử dụng HTTPS.

Kết quả: Không còn xuất hiện cảnh báo HTTPS

Kiểm tra truy cập các trang chia sẻ file:

Thử truy cập Mediafire, Dropbox, …



Kết quả: Các trang này bị chặn

Kiểm tra giao thức FTP:

Sử dụng FileZilla để đăng nhập qua FTP.

Thông tin mẫu:

FTP Server: ftp.iselab.16mb.com

User: u971091963.isedemo

Password: ise2016

So sánh kết quả trước và sau khi áp dụng quy tắc

Kiểm tra tải torrent:

Dùng uTorrent hoặc BitTorrent và download file .torrent để xác minh quy tắc.

Kiểm tra truy cập mạng xã hội:

Thử truy cập các nền tảng mạng xã hội phổ biến theo chính sách đã đặt ra.

Kiểm tra các công cụ thay đổi Proxy:

Thử sử dụng Ultrasurf hoặc Tor và quan sát kết quả.

Kiểm tra email server:

Truy cập các trang như gmail.com, mail.uit.edu.vn và ctmail.vnu.edu.vn để đảm bảo chỉ cho phép địa chỉ email của công ty truy cập được.