**Phạm Hồ Bình An\_1050080127\_10DH\_CNPM2**

**BÀI TẬP 3:**

Bước 1: Kiểm tra hệ thống

Mô tả: Bật máy Domain Controller (DC) và máy tường lửa Sophos UTM.

Ghi chú hình ảnh: (Hình ảnh hiển thị trạng thái khởi động của DC và UTM)

Yêu cầu: Kiểm tra rằng các dịch vụ (Active Directory, DNS, …) đều đang chạy ổn định.

Bước 2: Kết nối vào WebAdmin Sophos UTM

Mô tả: Mở trình duyệt web, truy cập vào địa chỉ của WebAdmin (ví dụ: https://<IP\_UTM>:4444).

Ghi chú hình ảnh: (Ảnh giao diện đăng nhập của WebAdmin)

Bước 3: Cấu hình Authentication Server

Mô tả: Trong WebAdmin, vào Definitions & Users > Authentication Services. Chọn tab Servers và nhấn New Authentication Server.

Cấu hình:

Chọn Type: Active Directory

Nhập Domain Name (ví dụ: uit.local), Server Address (địa chỉ IP của DC), Base DN (ví dụ: DC=uit,DC=local), Bind DN và Password.

Ghi chú hình ảnh: (Ảnh hiển thị form cấu hình Authentication Server)

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Nội dung do AI tạo ra có thể không chính xác.

**Bước 4: Tại phần Server, chọn dấu “+” để nhập thông tin Domain Controller**

Trong giao diện **Authentication Services** (thuộc **Definitions & Users**), bạn sẽ thấy mục **Servers**.

Nhấn nút **“+”** để thêm một **Network Definition** mới cho Domain Controller.

Tại cửa sổ **Add Network Definition**, điền các thông tin như sau:

**Name**: Đặt tên (ví dụ: **AD Server**)

**Type**: **Host**

**IPv4 address**: Địa chỉ IP của Domain Controller (ví dụ: **10.0.0.2**)

**DHCP Settings**: (để mặc định hoặc cấu hình thêm nếu cần)

**DNS Settings**: (để mặc định hoặc cấu hình thêm nếu cần)

**Comment**: Thêm ghi chú (nếu cần)

**Advanced**: Chỉnh sửa bổ sung (nếu cần)

Cuối cùng, nhấn **Save** để lưu lại.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Nội dung do AI tạo ra có thể không chính xác.

**Bước 5: Cấu hình Bind DN cho Domain Controller**

Ở mục **Authentication Services**, sau khi đã thêm Network Definition (ở Bước 4), bạn sẽ thấy trường **Bind DN** trong phần cấu hình Active Directory.

**Nhập giá trị Bind DN** theo định dạng LDAP, ví dụ:

ini

Sao chép Chỉnh sửa

CN=administrator,CN=Users,DC=uit,DC=local

Trong đó:

**administrator** là tên tài khoản quản trị trong AD.

**Users** là container (hoặc Organizational Unit) chứa tài khoản administrator.

**uit** và **local** tương ứng với tên miền mà bạn đã thiết lập (có thể thay đổi nếu domain khác).

Sau khi nhập **Bind DN**, tiếp tục nhập mật khẩu của tài khoản administrator (hoặc tài khoản có quyền đọc thông tin user trong AD).

Kiểm tra lại cấu hình:

**Domain**: uit.local

**Bind DN**: CN=administrator,CN=Users,DC=uit,DC=local

**Password**: Mật khẩu của tài khoản administrator

Cuối cùng, nhấn **Test** (nếu có) để xác minh rằng Sophos UTM có thể kết nối và xác thực với Domain Controller bằng thông tin Bind DN này.

**Bước 6: Kiểm tra kết nối đến Domain Controller**

Tại giao diện **Add Authentication Server** (hoặc **Edit Authentication Server** nếu bạn đang chỉnh sửa), sau khi đã điền **Bind DN** (Bước 5):

Nhập mật khẩu của tài khoản Administrator (hoặc tài khoản có quyền tương đương) trên máy Domain Controller.

Cổng mặc định của dịch vụ AD là **389** (LDAP) hoặc **636** (LDAPS) nếu sử dụng SSL.

Nhấn nút **Test** để kiểm tra kết nối.

Nếu nhận được thông báo **“Server test passed”**, nghĩa là Sophos UTM đã kết nối thành công đến Domain Controller với thông tin xác thực vừa nhập.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, số

Nội dung do AI tạo ra có thể không chính xác.

**Bước 7: Lưu lại cấu hình và kiểm tra kết quả**

Sau khi đã điền đầy đủ thông tin (Domain Name, Bind DN, Password, v.v.) và kiểm tra kết nối thành công, hãy nhấn **Save** để lưu lại cấu hình.

Trở lại danh sách **Authentication Servers**, bạn sẽ thấy server AD vừa tạo xuất hiện với trạng thái đã được cấu hình (ví dụ: adirectory hoặc tên bạn đặt).

Xác nhận rằng **Base DN** và các thông số hiển thị đúng như bạn mong muốn.

Ảnh có chứa văn bản, phần mềm, Phông chữ, Trang web

Nội dung do AI tạo ra có thể không chính xác.

**Bước 8: Cấu hình chính sách xác thực cho Web Protection**

Mô tả: Vào Web Protection > Filtering Options > Authentication và thiết lập Mode: Active Directory SSO.

Ghi chú hình ảnh: (Ảnh hiển thị cấu hình chế độ xác thực)

**Bước 8: Tạo 2 user mới trên Domain Controller**

**Mở công cụ quản trị Active Directory Users and Computers**

Vào **Start > Administrative Tools > Active Directory Users and Computers**.

**Tạo tài khoản người dùng (user)**

Trong **Active Directory Users and Computers**, chọn **OU** hoặc **container** nơi bạn muốn tạo user (ví dụ: Users hoặc một OU riêng).

Nhấn chuột phải, chọn **New > User**.

Điền **First name**, **Last name**, **User logon name** (ví dụ: a và b, hoặc nguyenvana, nguyenvanb).

Thiết lập mật khẩu, xác nhận mật khẩu.

Hoàn tất việc tạo user.

**Ví dụ**

Tạo 2 tài khoản: **a** và **b**, tương ứng với Nguyễn Văn A và Nguyễn Văn B.

Ảnh có chứa ảnh chụp màn hình, văn bản, phần mềm, số

Nội dung do AI tạo ra có thể không chính xác.

**Kiểm tra tài khoản**

Sau khi tạo, đảm bảo rằng tài khoản hiển thị trong **Active Directory Users and Computers**.

Đăng nhập thử (nếu cần) để xác minh mật khẩu và quyền truy cập.

**Thay đổi chính sách mặc định (tùy chọn)**

Nếu muốn mở rộng bài lab, bạn có thể vào **Group Policy Management** > **Edit Default Domain Policy** để thay đổi một số thiết lập bảo mật hoặc chính sách người dùng.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Nội dung do AI tạo ra có thể không chính xác.

**Bước 9: Thiết lập Proxy Server cho Domain**

**Mở Group Policy Management** trên Domain Controller

Vào **Start > Administrative Tools > Group Policy Management**.

Xác định **GPO** (Group Policy Object) áp dụng cho người dùng trong domain (ví dụ: **Default Domain Policy** hoặc một GPO riêng).

**Chỉnh sửa GPO (User Configuration)**

Trong **Group Policy Management**, chuột phải vào GPO tương ứng và chọn **Edit**.

Điều hướng đến **User Configuration > Windows Settings > Internet Explorer Maintenance > Connection**.

**Cấu hình Proxy Settings**

Chọn **Connection** để hiển thị các tùy chọn cấu hình Proxy.

Tại mục **Proxy Settings**, thiết lập **HTTP Proxy** là **10.0.0.1** và **Port** là **8080** (hoặc theo yêu cầu cấu hình Sophos UTM).

Xác nhận các thông số khác (nếu cần), như **Secure Proxy**, **FTP Proxy**, **Socks**.

**Áp dụng Group Policy**

Sau khi thiết lập xong, đóng cửa sổ cấu hình GPO.

Các máy client trong domain sẽ nhận thiết lập proxy thông qua GPO.

**Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Nội dung do AI tạo ra có thể không chính xác.**

**Kiểm tra**

Trên máy client đã join domain, đăng nhập bằng tài khoản domain.

Mở **Internet Explorer** hoặc trình duyệt tích hợp Group Policy để xem Proxy được thiết lập tự động là 10.0.0.1:8080.

Thử truy cập internet để đảm bảo máy client sử dụng proxy do Sophos UTM cung cấp.

*Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình, phần mềm

Nội dung do AI tạo ra có thể không chính xác.*

**Bước 10: Cập nhật lại Group Policy**

**Mở Command Prompt** (CMD) với quyền Administrator trên máy Domain Controller hoặc trên máy client (đã join domain).

Gõ lệnh:

bash

gpupdate /force

Lệnh này giúp cập nhật (hoặc áp dụng) các thay đổi mới nhất từ Group Policy.

Quan sát thông báo trả về, nếu hiển thị **“User Policy update has completed successfully”** hoặc tương tự, nghĩa là việc cập nhật chính sách đã hoàn tất.

*Ảnh có chứa văn bản, phần mềm, ảnh chụp màn hình, Trang web

Nội dung do AI tạo ra có thể không chính xác.*

**Bước 11: Cấu hình tự động tạo tài khoản người dùng (Auto User Creation)**

**Truy cập vào mục Authentication Services**

Trong **WebAdmin** của Sophos UTM, điều hướng đến **Definitions & Users** > **Authentication Services**.

**Chọn tab Global Settings**

Tại đây, bạn sẽ thấy các tùy chọn liên quan đến việc xác thực và tạo tài khoản người dùng.

**Bật tính năng “Create users automatically via End-User Portal”**

Đánh dấu hoặc bật tùy chọn **Create users automatically**.

Khi tùy chọn này được kích hoạt, bất kỳ user nào xác thực thành công (thông qua AD, LDAP, hoặc giao thức tương ứng) lần đầu tiên sẽ tự động được tạo tài khoản trong Sophos UTM.

**Nhấn Apply**

Sau khi bật tùy chọn, nhấn **Apply** để lưu và áp dụng thay đổi.

Ảnh có chứa văn bản, Trang web, phần mềm, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Bước 12: Prefetch Directory Users (Kéo user từ Domain vào Sophos UTM)**

**Chọn Tab Advanced** trong **Authentication Services**

Từ giao diện **WebAdmin** của Sophos UTM, đi đến **Definitions & Users** > **Authentication Services** > chọn **Advanced** (thường nằm ở phía trên hoặc tab riêng).

**Tại phần “Prefetch Directory Users”**, nhấn biểu tượng **“+”** để bắt đầu quá trình tiền tải (prefetch) người dùng từ Active Directory.

**Chọn các User cần đồng bộ**

Trong danh sách **Active Directory Browser**, tìm 2 user đã tạo ở Bước 9 (ví dụ: Nguyễn Văn A, Nguyễn Văn B).

Kéo (drag) các user này xuống khu vực **DND** (Drag and drop to the right order) bên dưới, hoặc sử dụng nút mũi tên để thêm user vào danh sách sẽ được đồng bộ.

**Nhấn “Save”** để lưu cấu hình

Sau khi chọn xong user, nhấn **Save** để xác nhận quá trình **Prefetch**.

Lúc này, 2 user sẽ được đưa vào danh sách người dùng đã được đồng bộ trong Sophos UTM.

***Lưu ý:*** *Việc* ***Prefetch Directory Users*** *cho phép bạn chủ động chọn và thêm người dùng từ AD vào Sophos UTM, thay vì chờ người dùng tự đăng nhập lần đầu. Điều này hữu ích khi bạn muốn gán chính sách cụ thể cho từng user trước khi họ bắt đầu sử dụng hệ thống.*

*Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Trang web

Nội dung do AI tạo ra có thể không chính xác.*

Chắc chắn rồi, đây là chi tiết bước 13 trong hướng dẫn thiết lập Rules tường lửa Sophos UTM:

**Bước 13: Bật đồng bộ hóa backend khi đăng nhập và áp dụng**

**Chọn "Enable backend sync on login"**:

Tìm hộp kiểm (checkbox) có nhãn "Enable backend sync on login".

Tích vào hộp kiểm này.

**Giải thích:**

Khi tùy chọn này được bật, Sophos UTM sẽ tự động đồng bộ hóa thông tin người dùng từ máy chủ backend (ví dụ: Active Directory) mỗi khi người dùng đăng nhập vào hệ thống.

Điều này đảm bảo rằng thông tin người dùng luôn được cập nhật, chẳng hạn như khi người dùng thay đổi mật khẩu hoặc được thêm/xóa khỏi nhóm.

Việc đồng bộ hóa này cũng giúp ngăn chặn tình trạng quá tải xác thực khi có nhiều người dùng đăng nhập cùng lúc.

**Nhấn "Apply"**:

Tìm nút "Apply" (thường nằm ở cuối trang hoặc gần khu vực cài đặt).

Nhấn vào nút "Apply" để lưu các thay đổi.

**Lưu ý:**

Sau khi nhấn "Apply", các thay đổi sẽ được áp dụng ngay lập tức.

Hãy chắc chắn rằng bạn đã kiểm tra kỹ các cài đặt trước khi nhấn "Apply" để tránh các lỗi không mong muốn.

**Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Trang web

Nội dung do AI tạo ra có thể không chính xác.**

Phần 2: Thiết lập một số kịch bản quy định về chính sách với tài khoản tại Domain

a) Kịch bản 1: Quản trị muốn cấm tài khoản nhân viên Nguyễn Văn A truy cập các trang web tìm kiếm việc làm (Job Search) khi sử dụng tài khoản được cấp trong domain.

Bước 1: Tại WebAdmin Firewall Sophos UTM, vào Web Protection > chọn Web Filtering và bật bộ lọc này. Chọn Standard mode và nhấn Apply.

Phân tích chi tiết:

Truy cập WebAdmin Firewall Sophos UTM:

Bước đầu tiên là đăng nhập vào giao diện quản trị WebAdmin của tường lửa Sophos UTM.

Sử dụng trình duyệt web và nhập địa chỉ IP hoặc tên miền của Sophos UTM để truy cập.

Đăng nhập bằng tài khoản quản trị có quyền truy cập vào cấu hình tường lửa.

Điều hướng đến Web Protection > Web Filtering:

Sau khi đăng nhập, tìm và chọn mục "Web Protection" trong menu bên trái.

Trong phần "Web Protection", chọn "Web Filtering".

Mục này cho phép bạn cấu hình các chính sách lọc web để kiểm soát truy cập internet của người dùng.

Bật bộ lọc Web Filtering:

Tìm tùy chọn để bật hoặc kích hoạt bộ lọc "Web Filtering".

Thông thường, sẽ có một công tắc hoặc nút để bật/tắt tính năng này.

Bật bộ lọc này để bắt đầu áp dụng các chính sách lọc web.

Chọn Standard mode:

Trong phần cấu hình chế độ lọc, chọn "Standard mode".

Giải thích:

Standard mode: Cho phép bạn tạo các chính sách lọc web dựa trên danh mục website (website categories) và các quy tắc tùy chỉnh.

Transparent mode: Thường được sử dụng khi Sophos UTM hoạt động ở chế độ cầu nối (bridge mode) và không yêu cầu cấu hình proxy trên máy khách.

Full transparent: Tương tự như Transparent mode nhưng áp dụng cho tất cả lưu lượng truy cập web.

Nhấn Apply:

Sau khi chọn "Standard mode", nhấn nút "Apply" để lưu các thay đổi.

Việc này sẽ kích hoạt bộ lọc web với chế độ Standard mode và áp dụng các cấu hình mặc định.

**Ảnh có chứa văn bản, phần mềm, Trang web, Website

Nội dung do AI tạo ra có thể không chính xác.**

Bước 2: Để tạo quy tắc lọc web mới, vào Web Protection > Web Filter Profiles > Chọn New Filter Action...

Phân tích chi tiết:

Điều hướng đến Web Protection > Web Filter Profiles:

Sau khi bạn đã bật bộ lọc web ở bước 1, bước tiếp theo là tạo một quy tắc lọc web mới.

Trong menu bên trái, tìm và chọn "Web Protection".

Trong phần "Web Protection", chọn "Web Filter Profiles".

Mục này cho phép bạn quản lý các cấu hình lọc web (Web Filter Profiles) và các hành động lọc (Filter Actions).

Chọn New Filter Action...:

Trong giao diện "Web Filter Profiles", bạn sẽ thấy các tab như "Filter Profiles", "Filter Actions", và "Parent Proxies".

Chọn tab "Filter Actions".

Tìm và nhấn vào nút "New Filter Action..." (thường có biểu tượng dấu cộng "+").

Thao tác này sẽ mở ra một cửa sổ hoặc trang mới để bạn tạo một hành động lọc web mới.

Giải thích:

Filter Actions (Hành động lọc): Là các quy tắc xác định cách Sophos UTM xử lý lưu lượng truy cập web. Ví dụ: cho phép truy cập, chặn truy cập, quét virus, v.v.

Bằng cách tạo một "Filter Action" mới, bạn có thể định nghĩa cụ thể hành động nào sẽ được thực hiện khi người dùng truy cập vào các trang web mà bạn muốn kiểm soát (ví dụ: các trang web tìm kiếm việc làm trong kịch bản này).

**Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Trang web

Nội dung do AI tạo ra có thể không chính xác.**

**Chắc chắn rồi, hãy cùng phân tích chi tiết bước 3 trong phần 2 của hướng dẫn này:**

Bước 3: Thiết lập chính sách cấm truy cập các website tìm việc (Job Search)

Phân tích chi tiết:

Thiết lập chính sách với thể loại website:

Trong cửa sổ "New Filter Action" mà bạn đã mở ở bước 2, bạn sẽ thấy các tùy chọn để cấu hình hành động lọc web.

Tìm đến phần cho phép bạn chọn hoặc chỉ định thể loại website (website categories) mà bạn muốn áp dụng chính sách.

Trong trường hợp này, bạn cần chọn hoặc chỉ định thể loại liên quan đến "Job Search" hoặc "Career".

Chọn hành động "Block" (Chặn):

Sau khi chọn thể loại website, bạn cần chỉ định hành động mà Sophos UTM sẽ thực hiện khi người dùng truy cập vào các trang web thuộc thể loại này.

Chọn hành động "Block" hoặc "Deny" để cấm truy cập vào các trang web tìm việc.

Đặt tên cho Filter Action:

Đặt tên cho Filter Action để dễ dàng nhận biết và quản lý sau này.

Ví dụ: "Block Job Search" hoặc "Cam Truy Cap Tim Viec".

Lưu lại:

Sau khi hoàn tất các cấu hình, nhấn nút "Save" hoặc "Apply" để lưu lại Filter Action mới.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Trang web

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, phần mềm, Phông chữ, số

Nội dung do AI tạo ra có thể không chính xác.

**Bước 4: Vào Web Protection > chọn Web Filtering > Tại Tab Policies: Tạo 1 Policy mới và áp dụng cho user a**

**Phân tích chi tiết:**

**Điều hướng đến Web Protection > Web Filtering > Tab Policies:**

Trong giao diện WebAdmin của Sophos UTM, tìm và chọn "Web Protection" từ menu bên trái.

Chọn "Web Filtering".

Trong giao diện "Web Filtering", chọn tab "Policies".

Tab "Policies" cho phép bạn tạo và quản lý các chính sách lọc web (Web Filtering Policies) để áp dụng cho người dùng, nhóm người dùng, hoặc thời gian cụ thể.

**Tạo 1 Policy mới:**

Trong tab "Policies", tìm và nhấn nút "Add Policy" hoặc "New Policy" (thường có biểu tượng dấu cộng "+").

Thao tác này sẽ mở ra một cửa sổ hoặc trang mới để bạn tạo một chính sách lọc web mới.

**Áp dụng cho user a:**

Trong cửa sổ tạo Policy, bạn cần chỉ định người dùng hoặc nhóm người dùng mà chính sách này sẽ được áp dụng.

Trong trường hợp này, bạn cần thêm người dùng "a" (hoặc tên người dùng cụ thể) vào danh sách người dùng được áp dụng chính sách.

Thường có các tùy chọn để chọn người dùng từ Active Directory hoặc từ danh sách người dùng cục bộ.

**Chọn Filter Action (Hành động lọc):**

Chọn Filter Action mà bạn đã tạo ở bước 3 (ví dụ: "Block Job search for").

Hành động này sẽ xác định cách Sophos UTM xử lý lưu lượng truy cập web của người dùng "a".

**Thiết lập thời gian (Time event):**

Bạn có thể thiết lập thời gian mà chính sách này có hiệu lực.

Ví dụ: "Always" (luôn luôn) hoặc chỉ định thời gian cụ thể (ví dụ: giờ làm việc).

**Lưu lại:**

Sau khi hoàn tất các cấu hình, nhấn nút "Save" hoặc "Apply" để lưu lại Policy mới.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, Phông chữ, Trang web, phần mềm

Nội dung do AI tạo ra có thể không chính xác.

Chắc chắn rồi, hãy cùng phân tích chi tiết bước 5 trong phần 2 của hướng dẫn này:

**Bước 5: Tại máy Domain Controller, đăng nhập vào user a để kiểm tra**

**Phân tích chi tiết:**

1. **Đăng nhập vào máy Domain Controller với tài khoản user a:**
   * Sử dụng máy tính đã được kết nối với Domain Controller.
   * Khởi động máy tính và đăng nhập bằng tài khoản người dùng "a" (hoặc tên người dùng cụ thể mà bạn đã tạo).
   * Đảm bảo rằng bạn đang đăng nhập vào domain và không phải tài khoản cục bộ.
2. **Kiểm tra khả năng đăng nhập:**
   * Sau khi đăng nhập thành công, hãy thử truy cập vào các trang web tìm việc (Job Search) mà bạn đã chặn ở các bước trước.
   * Nếu chính sách lọc web đã được áp dụng đúng cách, bạn sẽ không thể truy cập vào các trang web này.
3. **Kiểm tra chính sách Allow log on locally:**
   * Trong hướng dẫn, có đề cập đến việc thay đổi chính sách "Allow log on locally" trong Group Policy.
   * Điều này có nghĩa là bạn cần kiểm tra xem người dùng "a" có được phép đăng nhập cục bộ vào máy Domain Controller hay không.
   * Để kiểm tra, bạn có thể sử dụng Group Policy Management hoặc Local Security Policy trên máy Domain Controller.

Ảnh có chứa văn bản, ảnh chụp màn hình, thiết kế

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, phần mềm, ảnh chụp màn hình, Trang web

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, số

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Nội dung do AI tạo ra có thể không chính xác.

**Bước 6: Sau khi đã đăng nhập thành công vào user a, mở trình duyệt để kiểm tra kết quả. Khi truy cập Internet, trình duyệt sẽ yêu cầu nhập username và password ở lần đầu tiên:**

**Phân tích chi tiết:**

**Mở trình duyệt web:**

Sau khi bạn đã đăng nhập thành công vào máy tính với tài khoản người dùng "a", hãy mở trình duyệt web (ví dụ: Chrome, Firefox, Edge).

**Truy cập Internet:**

Thử truy cập vào một trang web bất kỳ.

Nếu Sophos UTM được cấu hình đúng cách, bạn sẽ nhận được một hộp thoại yêu cầu xác thực (authentication).

**Hộp thoại xác thực (Authentication Required):**

Hộp thoại này sẽ hiển thị thông báo rằng proxy (Sophos UTM) đang yêu cầu tên người dùng và mật khẩu.

Thông báo có thể khác nhau tùy thuộc vào trình duyệt và cấu hình proxy.

Trong trường hợp này, hộp thoại cho biết:

**Proxy:** moz-proxy://10.0.0.1:8080 (địa chỉ IP và cổng của proxy Sophos UTM).

**Site:** HTTP-Proxy (tên của proxy).

**Username:** a (tên người dùng đã đăng nhập).

**Password:** (yêu cầu nhập mật khẩu).

**Nhập username và password:**

Nhập tên người dùng "a" (hoặc tên người dùng cụ thể) và mật khẩu tương ứng vào hộp thoại.

Nhấn nút "OK" để xác thực.

**Hình ảnh minh họa:**

Hình ảnh chụp màn hình trong hướng dẫn cho thấy hộp thoại xác thực (Authentication Required).

Hình 26 trong tài liệu cho thấy giao diện hộp thoại xác thực.

**Giải thích thêm:**

**Yêu cầu xác thực lần đầu tiên:**

Sophos UTM yêu cầu xác thực lần đầu tiên để xác định người dùng và áp dụng các chính sách lọc web tương ứng.

Sau khi xác thực thành công, bạn có thể không cần phải nhập lại thông tin đăng nhập trong một khoảng thời gian nhất định (tùy thuộc vào cấu hình của Sophos UTM).

**Kiểm tra kết quả:**

Sau khi xác thực thành công, hãy thử truy cập lại các trang web tìm việc (Job Search) mà bạn đã chặn ở các bước trước.

Nếu chính sách lọc web đã được áp dụng đúng cách, bạn sẽ không thể truy cập vào các trang web này.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

Các bước còn lại và các kịch bản còn lại tương tự