Phạm Hồ Bình An\_1050080127\_10DH\_CNPM2

BÀI TẬP 3 LAB 3:

1. Thiết lập máy chć Domain Controller

* Bước 1: Chuẩn bị máy ảo làm Domain Controller:

+ RAM: 512MB – 1GB

+ 1 Network Adapter Host-Only

+ OS: Windows Server 2008. Trong hướng dẫn này sử dụng Windows Server 2008. Sau khi cài đặt xong máy ảo Windows Server 2008, nên Snapshot (sao lưu) lại máy ảo để có thể khôi phục lại trạng thái ban đầu nếu quá trình nâng cấp bị lỗi.

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.

*Thực hiện Snapshot để sao lưu trạng thái máy ảo ban đầu*

Bước 2: Đặt IP cho máy Domain Controller là 10.0.0.2/8Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, màn hình

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

* Bước 3: Đặt DNS Suffix bằng cách click phải lên My Computer > Propertites > Change Setting > Change > chọn More.

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.

Sau đó nhập DNS Suffix cần đặt. Trong hướng dẫn này sử dụng tên uit.local, để phân biệt khi thực hiện sinh viên đặt theo dạng tên 2 sinh viên.local. Ví dụ vietnam.local

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

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

Sau đó Restart lại máy tính để áp dụng các thay đổi.

* Bước 4: Nâng cấp máy chủ thành Domain Controller

Hướng dẫn này thực hiện trên Windows Server 2008, nếu sử dụng phiên bản khác có thể có một số thay đổi trong quá trình nâng cấp.  
  
  
Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình, Phông chữ

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

*Vào Start > run > nhập dcpromo*

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

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

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, màn hình

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

Giữ các thiết lập mặc định trong các bước tiếp theo:Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, màn hình

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

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, màn hình

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

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

Nội dung do AI tạo ra có thể không chính xác. Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, màn hình

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

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

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

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, máy tính

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

Sau khi nâng cấp thành công, khởi động lại server và vào Properties của Computer để kiểm tra.

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, màn hình

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

* Bước 5: Tiến hành Snapshot lại để lưu lại trạng thái máy ảo lúc này.

1. Cài đặt và cấu hình máy Firewall Sophos UTM

Sinh viên có thể tải miễn phí file cài đặt Sophos UTM 9.4 (*UTM v9 software appliance*) tại đây <https://www.sophos.com/en-us/support/utm-downloads.aspx>

(bản asg-9.406-3.1.iso ~ 832MB). *Trong Lab sử dụng Sophos UTM 9.4*

* Bước 1: Tải Sophos UTM 9.4, ta được file ISO cài đặt asg-9.406-3.1.iso
* Bước 2: Tạo máy ảo mới bằng VMware và load file iso của Sophos UTM 9 để cài đặt tường lửa Sophos UTM.

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

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

Máy ảo để Firewall Sophos hoạt động có thông số như sau:

* RAM 1GB *(hoặc 2GB)*
* Có 3 card mạng:

+ Card 1: Host-only

+ Card 2: Host-only

+Card 3: Bridge *(kết nối Internet qua máy thật)*Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

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

* Bước 3: Khởi động máy ảo và nhấn Enter để bắt đầu cài đặtẢnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

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

Sau đó, chọn Start để bắt đầuẢnh có chứa văn bản, ảnh chụp màn hình, màn hình, Phông chữ

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

* Bước 4: Thiết lập ngôn ngữ và múi giờ

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

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

Ảnh có chứa văn bản, ảnh chụp màn hình

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

*Hình 16. Chọn ngôn ngữ English và múi giờ Ho\_Chi\_Minh*

Lab 3: Thiết lập mô hình tường lửa Sophos UTM

* Bước 5: Chọn card mạng eth0 và thiết lập IP mặc định cho trang quản trịẢnh có chứa văn bản, ảnh chụp màn hình, màn hình, Phông chữ

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

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

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

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

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

Quá trình cài đặt diễn ra trong 6 bước:Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình, phần mềm

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

Sau khi cài đặt thành công, hệ thống sẽ thông báo thông tin địa chỉ IP đăng nhập vào trang quản trị WebAdmin là https://10.0.0.1:4444/

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, màn hình

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

* Bước 6: Khởi động lại Firewall Sophos UTM

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

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

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

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

Sau khi khởi động thành công, chúng ta sẽ thấy IP được dùng để kết nối vào trang quản trị Firewall 10.0.0.1 *(Tài khoản mặc định để đăng nhập là root và đặt mật khẩu ở lần đầu tiên, tuy nhiên chúng ta thực hiện các thiết lập cho Firewall qua WebAdmin)*

* Bước 7:    Đặt IP cho card VMNet 1 để kết nối vào Firewall để quản lý

Thiết lập lớp mạng cho VMnet1 là 10.0.0.0/8 tại VMware (Chọn Edit > Vituarl Network Editor…). Sau đó đặt IP cho card VMnet1 tại máy thật thành IP khác 10.0.0.1, ví dụ 10.0.0.100/8.

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, số

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

* Bước 8: Từ máy thật, thực hiện lệnh ping 10.0.0.1 để kiểm tra máy thật đã thấy máy firewall chưa. Nếu chưa thấy thì cần kiểm tra lại IP và card mạng.

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

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

* Bước 9: Từ máy thật, kết nối vào WebAdmin của Firewall bằng địa chỉ https://10.0.0.1:4444

Nếu gặp cảnh báo bảo mật của trình duyệt, bỏ qua và tiếp tục truy cập WebAdmin

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

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

* Bước 10: Thiết lập các thông tin cơ bản cho Firewall Sophos và đặt mật khẩu cho tài khoản admin

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

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

Chọn I accept the license agreement và chọn Perform basic system setup và đợi khoảng 1 phút để hoàn tất quá trình thiết lập.

* Bước 11: Sau đó, đăng nhập bằng tài khoản admin/ mật khẩu vừa thiết lậpẢnh 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 12: Sau khi đăng nhập thành công, chọn Cancel để bỏ qua trình Wizard.Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Trang web

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

* Bước 13: Cấu hình IP cho các interface của Firewall theo đúng mô hình triển khai Vào Interface & Routing để thiết lập các Interface
  + Tạo Interface cho vùng DMZẢnh có chứa văn bản, phần mềm, Trang web, Biểu tượng máy tính

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

*Hình 29. Chọn New Interface và thiết lập như sau*

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

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

*Hình 30. Thiết lập Interface DMZ*

* Tạo Interface External để kết nối Internet: Chọn New Interface và thiết lập như sau

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

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

* Bước 14: Bật cả 3 3 interface và đặc biệt interface External đã nhận được IP từ DHCP Server hay chưa.

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.

*Hình 32. Các Interface đã hoạt động*

Kiểm tra xem máy Firewall có kết nối được internet hay không bằng cách vào

Support > Tool > dùng tool Ping check để ping google.com dùng interface ExternalẢnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Trang web

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

Lưu ý: *Nếu không kết nối được hay interface External không nhận được IP thì chúng ta sẽ không làm gì được nữa và cần kiểm tra kỹ lại quá trình cấu hình theo các bước đã hướng dẫn hoặc khởi động lại Firewall để kiểm tra lại.*

* Bước 15: Cấu hình NAT Outbound. Cơ chế NAT sẽ xác định mạng nào sẽ NAT mạng ra ngoài Internet.

Vào Network Protection > NAT > New Masquerading Rule và cấu hình như sau:Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Trang web

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

Sau đó kích hoạt rule này. Kết quả sau khi cấu hình:Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Trang web

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

* Bước 16: Cấu hình Rule để máy chủ Domain Controller kết nối được internet bình thường. Vào Network Protection > Rule > New Rule

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, Biểu tượng máy tính, Trang web

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

* Bước 17: Kiểm tra kết nối internet của máy Domain ControllerẢnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, màn hình

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

Ảnh có chứa văn bản, phần mềm, Biểu tượng máy tính, Trang web

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

Nếu Domain Controller kết nối được Internet tức quá trình thiết lập tường lửa cơ bản đã thành công.

* Bước 18: Quay lại trang WebAdmin của Firewall thử tắt Rule Firewall và một vài Rule vừa thiết lập và quay lại máy Domain Controller để truy cập Internet và rút ra kết luận.