PHÂN NHÓM ĐỀ TÀI CHUYÊN ĐỀ II

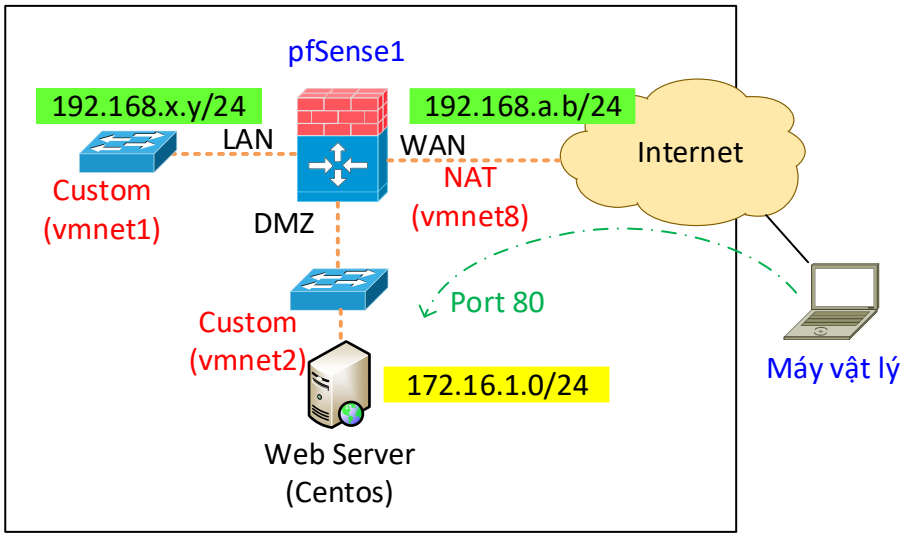
Nhóm 1

Hãy trình bày đặc điểm, cách khai báo Rule và Alias trong pfSense.

Xây dựng mô hình LAB như hình dưới, cài đặt Web Server (dùng Centos) và khai báo Rule cho phép máy tính vật lý truy cập được vào Web Server.

Địa chỉ cổng WAN & DMZ đặt IP tĩnh. Địa chỉ WAN và LAN tùy thuộc vào VMWare.

Chụp hình để minh họa khai báo và kết quả thực hiện.

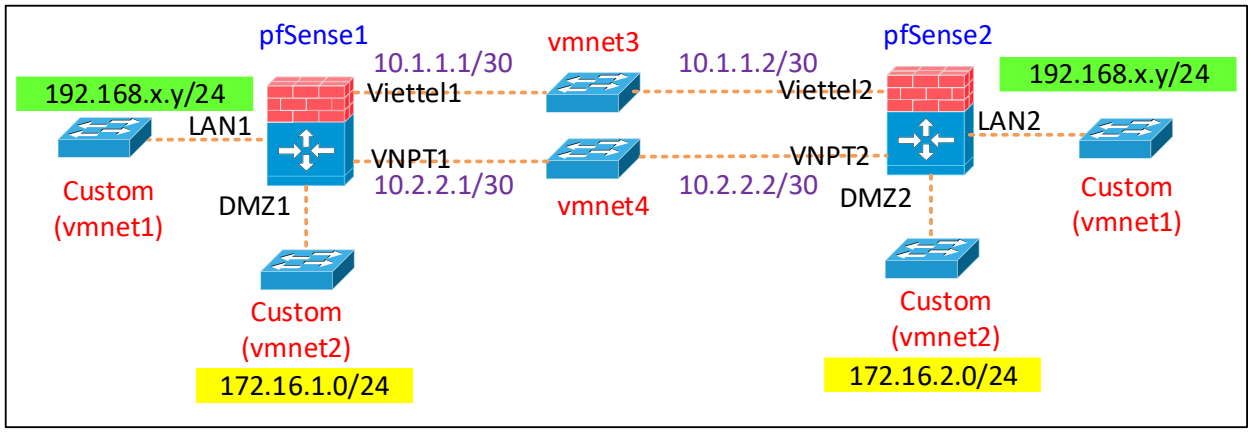


Nhóm 2

Giới thiệu tính năng cân bằng tải (Load Balancing and Failover) qua nhiều đường truyền trong pfSense và cách thức khai báo.

Xây dựng mô hình LAB như hình dưới, khai báo cân bằng tải qua 2 đường truyền.

Chụp hình để minh họa khai báo và kết quả thực hiện.

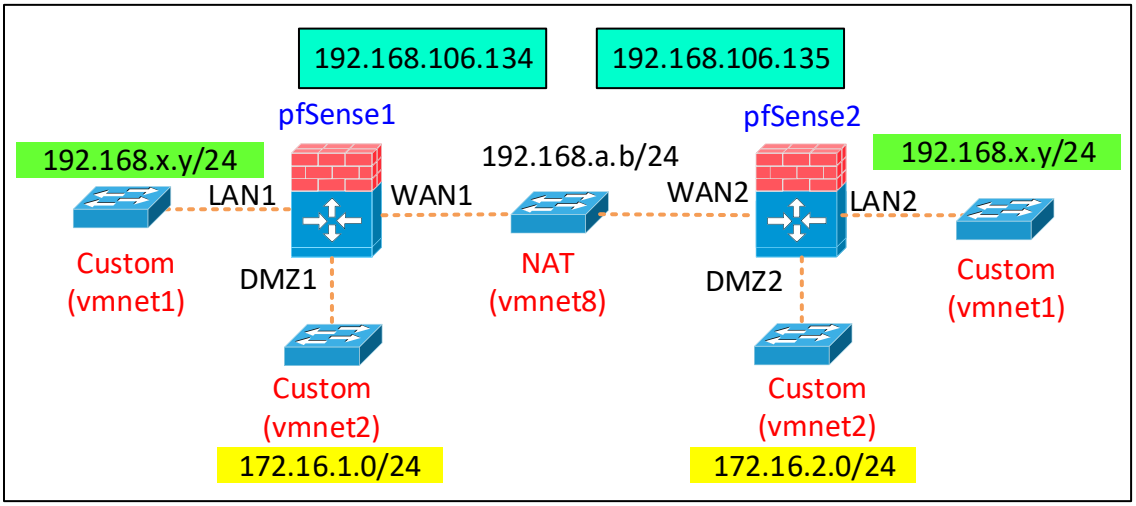


Nhóm 3

Giới thiệu hoạt động của IPSec VPN trong pfSense.

Xây dựng mô hình LAB như hình dưới, khai báo IPSec VPN Site-to-Site giữa 2 Firewall.

Chụp hình để minh họa khai báo và kết quả thực hiện.

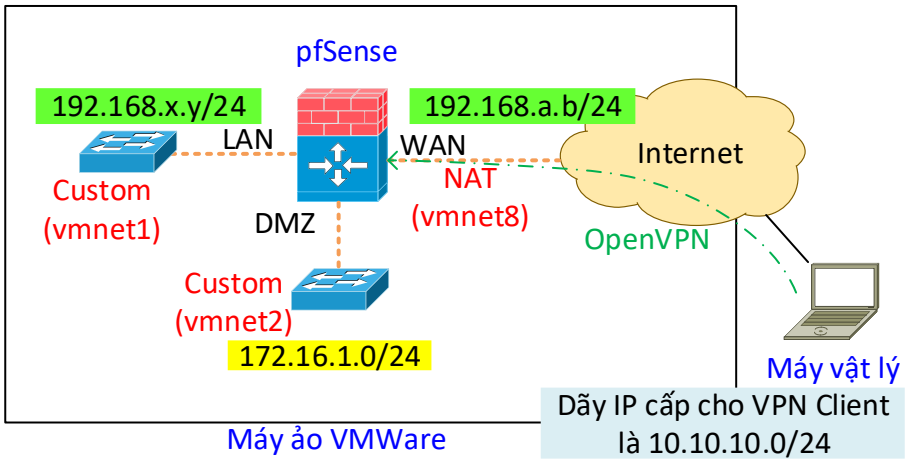


Nhóm 4

Giới thiệu OpenVPN và cách khai báo trong pfSense.

Xây dựng mô hình LAB như hình dưới, khai báo OpenVPN cho pfSense, cài đặt VPN Client và Ping thông đến cổng DMZ của Firewall.

Chụp hình để minh họa khai báo và kết quả thực hiện.

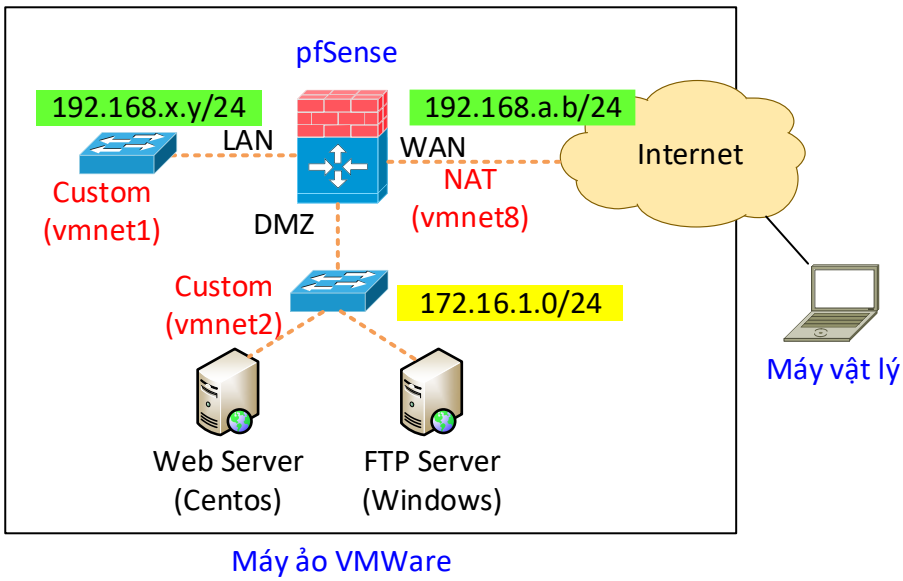


Nhóm 5

Giới thiệu tính năng Port Forward trong pfSense.

Xây dựng mô hình LAB như hình dưới, khai báo Port Forward để dùng địa chỉ cổng WAN cho phép kết nối đến Web Server (Port 80) và FTP Server (Port 21).

Chụp hình để minh họa khai báo và kết quả thực hiện.

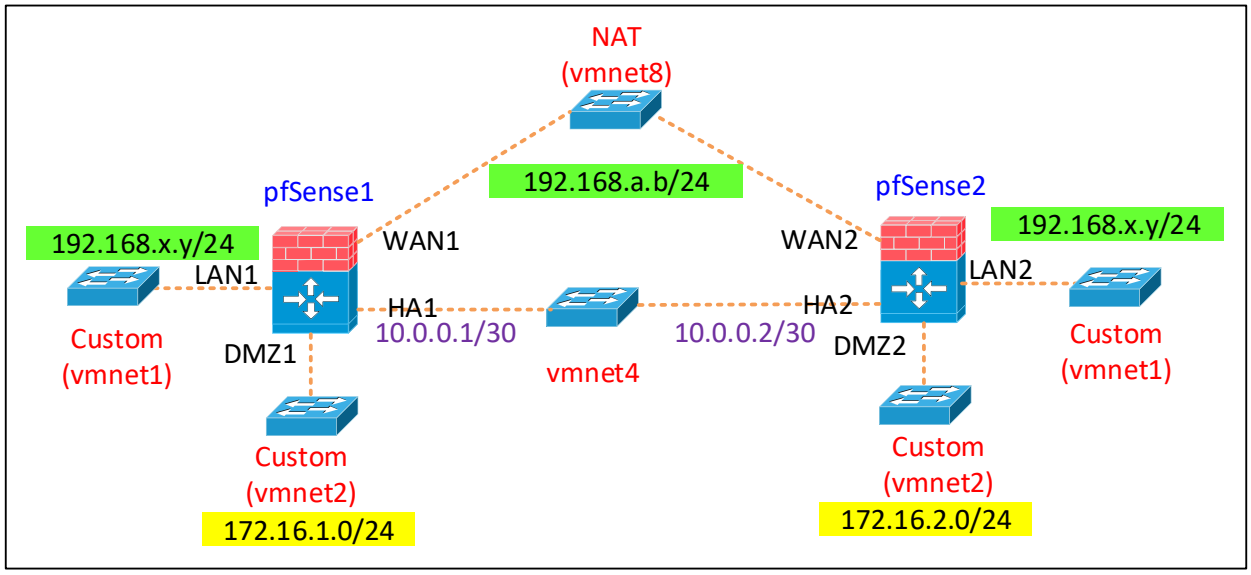


Nhóm 6

Giới thiệu tính năng High Availability (**HA**) và Common Address Redundancy Protocol (**CARP**) trong pfSense.

Xây dựng mô hình LAB như hình dưới, khai báo dự phòng thiết bị pfSense sử dụng tính năng HA & CARP.

Chụp hình để minh họa khai báo và kết quả thực hiện.

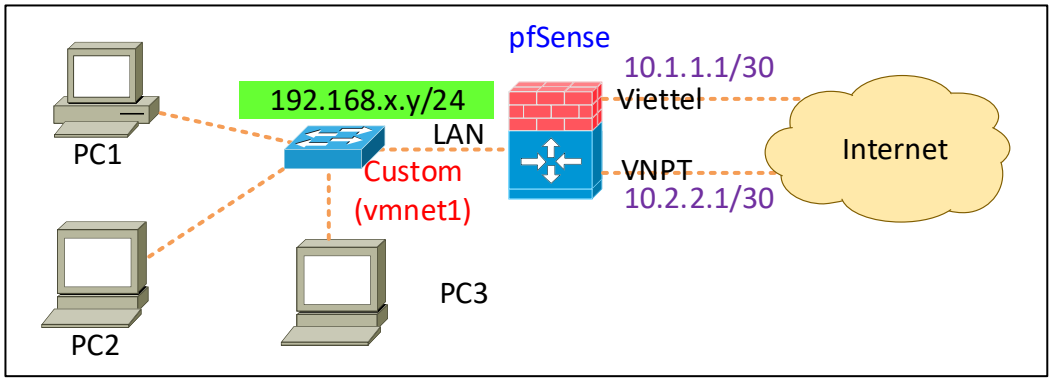


Nhóm 7

Giới thiệu các khai báo Firewall Rule và Gateway Group trong pfSense.

Xây dựng mô hình LAB như hình dưới, khai báo để PC1 kết nối ra ngoài ưu tiên hướng Viettel, nếu đường truyền Viettel bị sự cố thì chuyển sang hướng dự phòng là VNPT. PC2 sẽ ngược lại, ưu tiên VNPT và dự phòng Viettel. PC3 sẽ chạy cân bằng (Load-balance) cả 2 hướng Viettel và VNPT.

Chụp hình để minh họa khai báo và kết quả thực hiện.

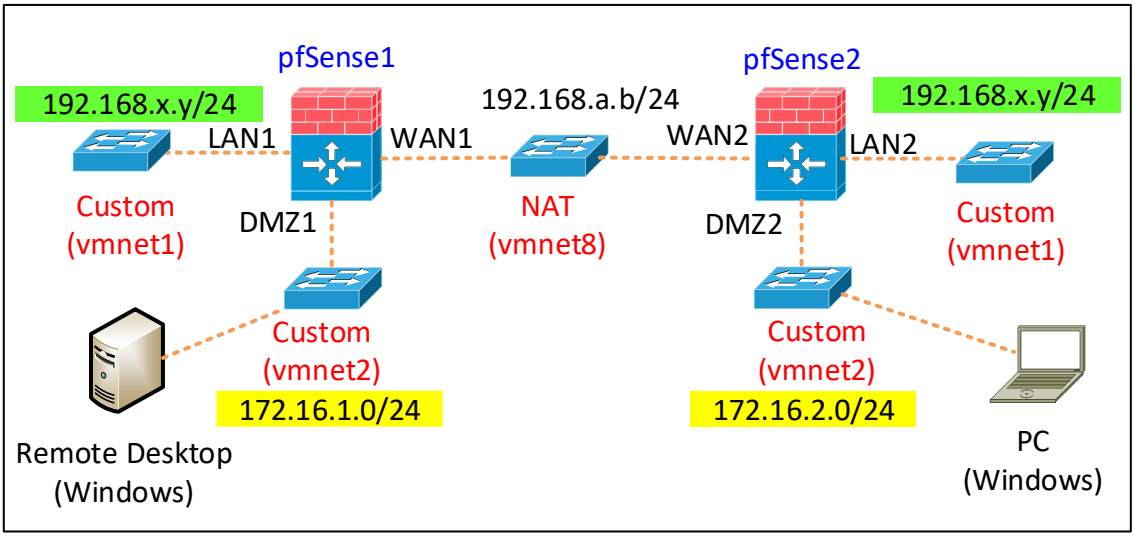


Nhóm 8

Giới thiệu các nội dung cần khai báo chính cho Firewall Rule trong pfSense.

Xây dựng mô hình LAB như hình dưới, khai báo để PC từ Site 2 kết nối Remote Desktop sang Site 1.

Chụp hình để minh họa khai báo và kết quả thực hiện.

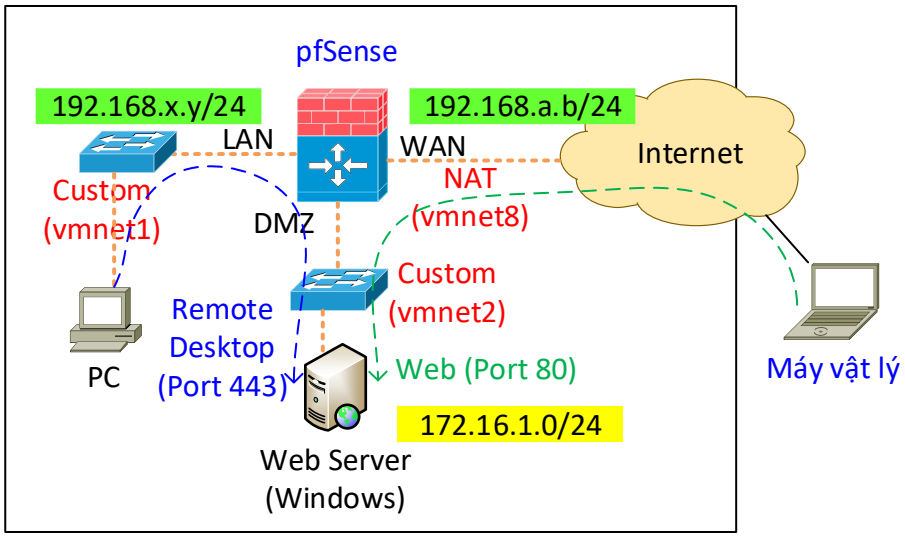


Nhóm 9

Giới thiệu những tính năng của pfSense Firewall.

Xây dựng mô hình LAB như hình dưới, khai báo để PC kết nối Remote Desktop đến Web Server (Dùng Windows) và cho phép bên ngoài truy cập dịch vụ Web của Web Server.

Chụp hình để minh họa khai báo và kết quả thực hiện.

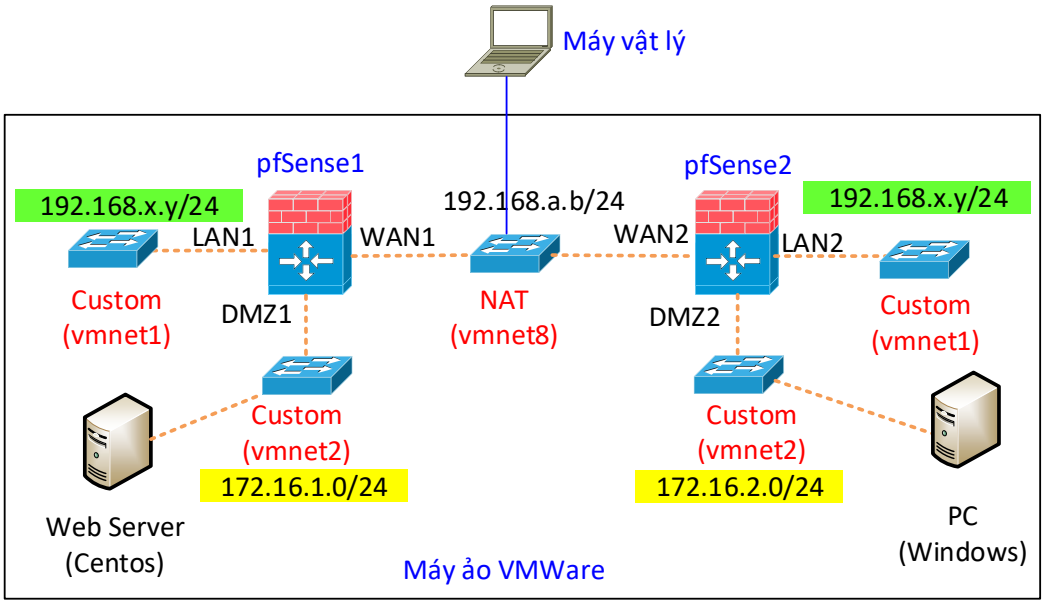


Nhóm 10

Giới thiệu về pfsense và tính năng Statefull Firewall của pfSense.

Xây dựng mô hình LAB như hình dưới, khai báo để cho phép máy tính vật lý kết nối Remote Desktop đến PC (Dùng Windows) và truy cập dịch vụ Web của Web Server.

Chụp hình để minh họa khai báo và kết quả thực hiện.

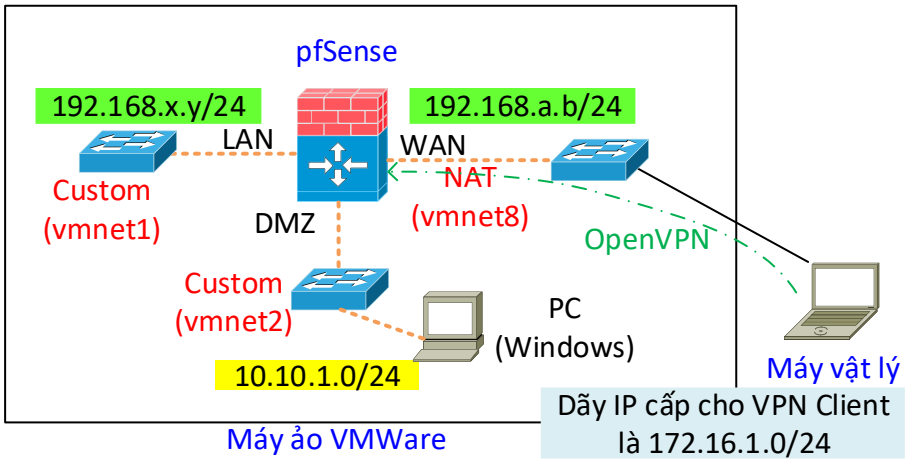


Nhóm 11

So sánh Remote Access VPN và Site-to-Site VPN, nêu đặc điểm của OpenVPN.

Xây dựng mô hình LAB như hình dưới, khai báo OpenVPN cho pfSense, cài đặt VPN Client và Ping thông đến địa chỉ của PC.

Chụp hình để minh họa khai báo và kết quả thực hiện.

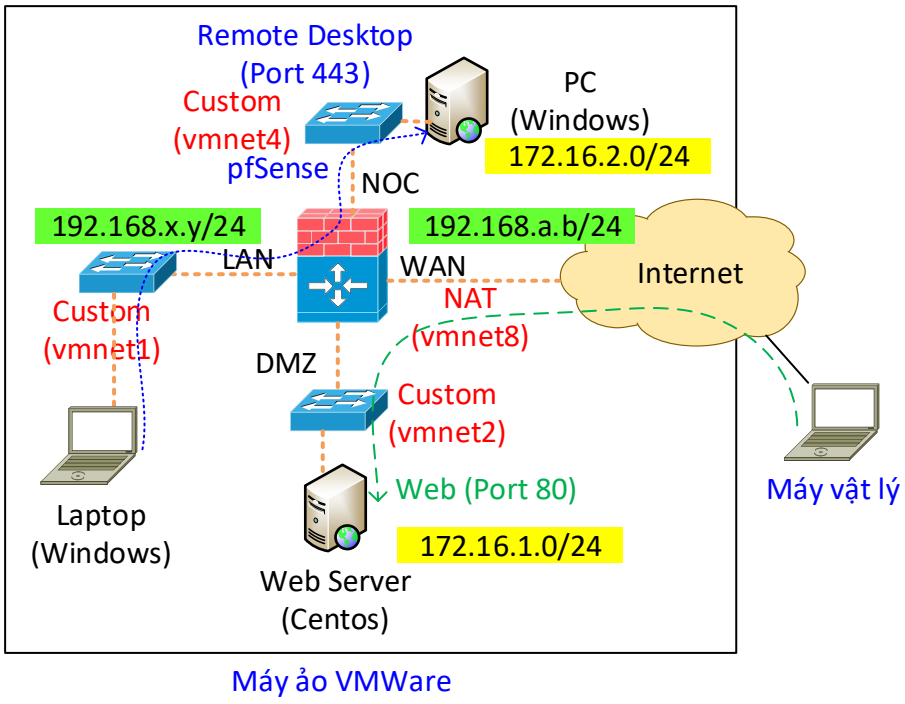


Nhóm 12

Giới thiệu về pfSense và tính năng những tính năng chính của pfSense.

Xây dựng mô hình LAB như hình dưới, khai báo để Laptop kết nối Remote Desktop đến PC và cho phép bên ngoài truy cập dịch vụ Web của Web Server.

Chụp hình để minh họa khai báo và kết quả thực hiện.

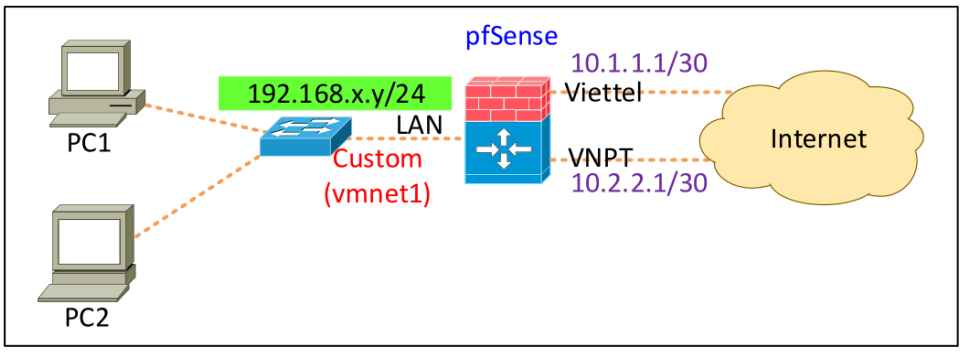


Nhóm 13

Nêu đặc điểm của pfSense và cách thức hoạt động của Gateway Group.

Xây dựng mô hình LAB như hình dưới, khai báo để các PC truy cập dịch vụ (HTTP & HTTPS) thì ưu tiên đi ra hướng Viettel, nếu đường truyền Viettel bị sự cố thì chuyển sang hướng dự phòng là VNPT. Nếu truy cập dịch vụ Email (POP3, SMTP) thì ưu tiên VNPT và dự phòng Viettel. Nếu truy cập các dịch vụ khác sẽ chạy cân bằng (Load-balance) cả 2 hướng Viettel và VNPT.

Chụp hình để minh họa khai báo và kết quả thực hiện.

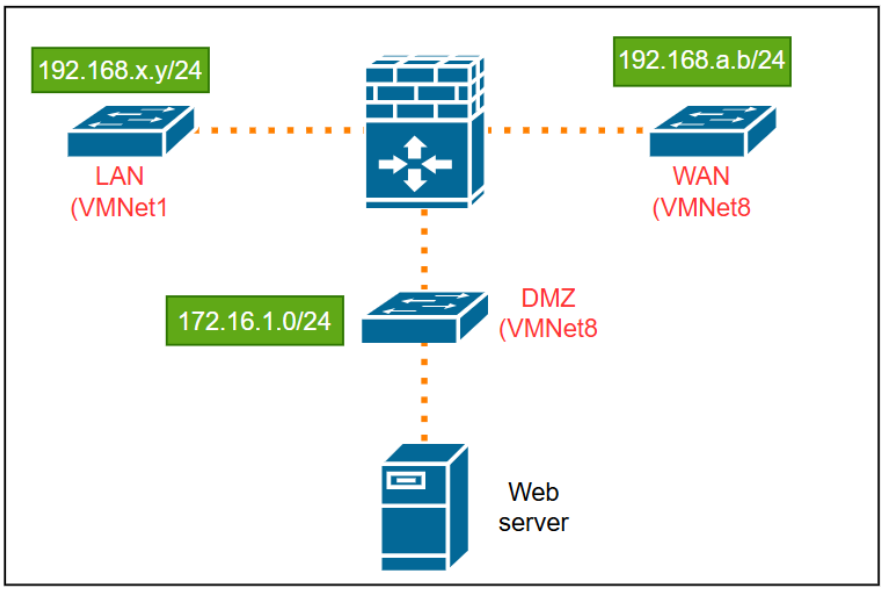


Nhóm 14

Trình bày khái niệm Traffic Shaping và vai trò trong quản lý băng thông mạng. Phân tích các cơ chế Traffic Shaping trong pfSense (Priority Queues, Limiters). Ứng dụng thực tế trong doanh nghiệp hoặc trường học.

Xây dựng mô hình LAB như hình dưới, khai báo để giới hạn tốc độ khi truy cập Web Server là 10Mpbs còn truy cập ra mạng Internet (WAN) tối đa 5Mbps trong giờ làm việc (8h-17h), ngoài giờ này không giới hạn.

Chụp hình để minh họa khai báo và kết quả thực hiện.

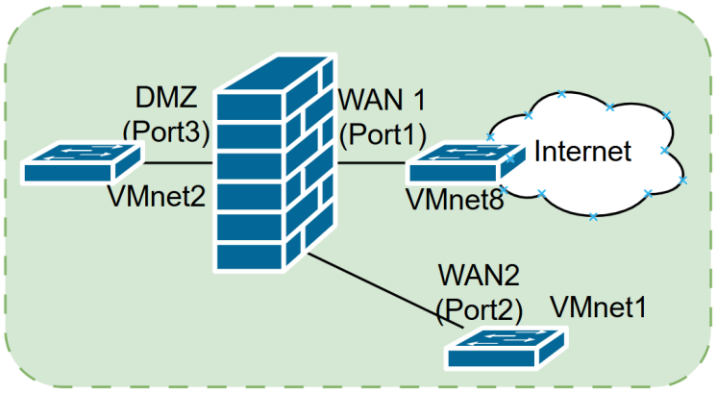


Nhóm 15

Trình bày khái niệm SD-WAN và vai trò trong tối ưu hóa kết nối mạng. Phân tích các tính năng SD-WAN trong FortiGate (Load Balancing, Path Selection, Failover). So sánh SD-WAN của FortiGate với Load Balancing của pfSense.

Xây dựng mô hình LAB như hình dưới, khai báo cho phép các truy cập Web (HTTP, HTTPS) ưu tiên cổng WAN1 và dự phòng ở WAN2, truy cập Email (POP3, SMTP) ưu tiên WAN2 và dự phòng WAN1, các truy cập khác Load-Sharing giữa 2 cổng.

Chụp hình để minh họa khai báo và kết quả thực hiện.



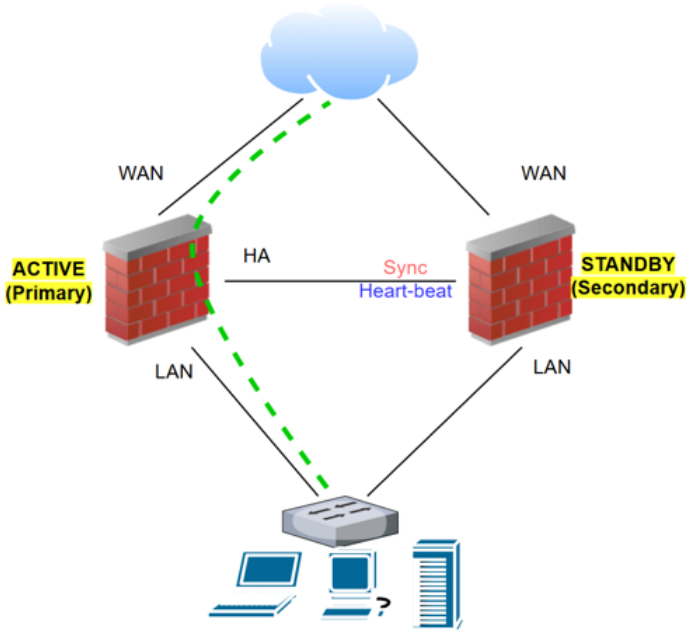
Nhóm 16

Trình bày khái niệm High Availability (HA) và vai trò trong đảm bảo tính liên tục của hệ thống mạng. Phân tích tính năng HA trong FortiGate, bao gồm các chế độ Active-Passive và Active-

Active, sử dụng FortiGate Clustering Protocol (FGCP). So sánh HA trong FortiGate với CARP trong pfSense (ưu/nhược điểm, khả năng triển khai).

Trình bày các bước khai báo HA cho Fortigate theo mô hình Active – Stanby (sử dụng khai báo trước cho 1 Firewall)

Chụp hình để minh họa khai báo và kết quả thực hiện.

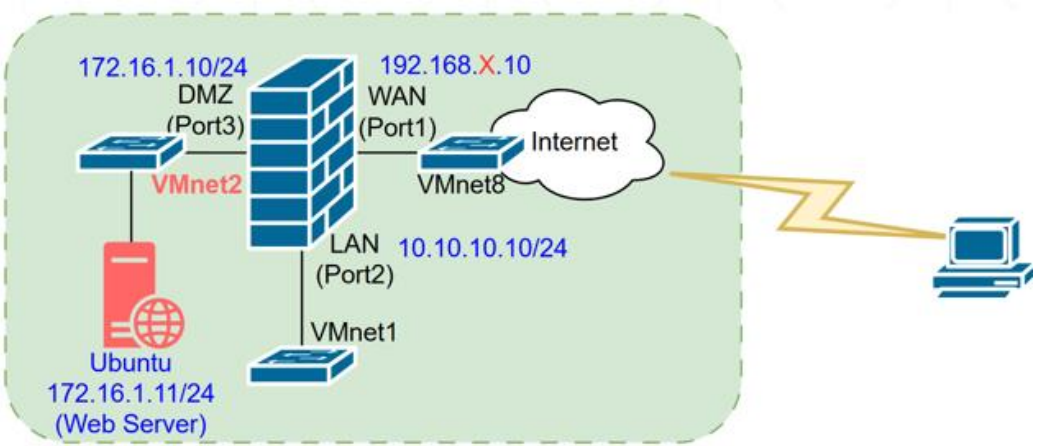


Nhóm 17

Trình bày khái niệm SD-WAN và vai trò trong quản lý lưu lượng mạng. Giới thiệu tính năng Port Forwarding và Virtual IP trong FortiGate.

Thực hiện khai báo SD-WAN cho Port 1, tạo Virtual IP cho Web Server, khai báo Port Forwarding vào Web Server (từ 8080 WAN vào 80 của Web server).

Chụp hình để minh họa khai báo và kết quả thực hiện.

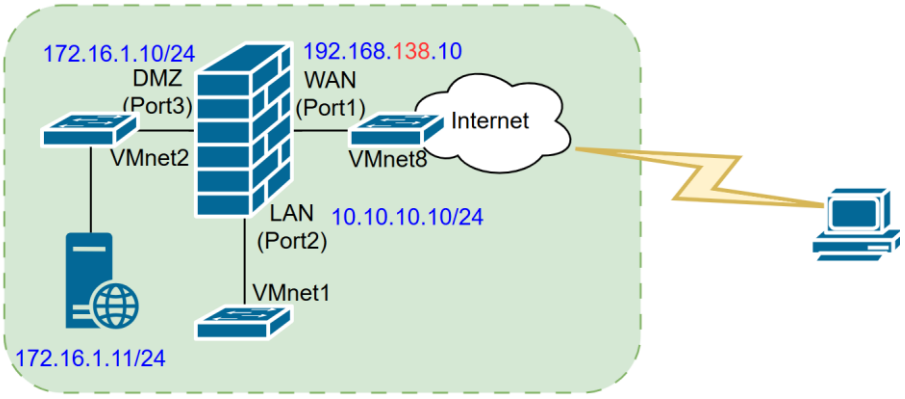


Nhóm 18

Trình bày khái niệm Port Forwarding và vai trò trong việc cho phép truy cập từ bên ngoài vào các dịch vụ nội bộ. Phân tích cách cấu hình Port Forwarding trong FortiGate thông qua Virtual IP (VIP) và Firewall Policy. Ứng dụng thực tế trong việc triển khai các dịch vụ như Web Server trong DMZ.

Trình bày các bước khai báo Port Forwarding theo sơ đồ bên dưới.

Chụp hình để minh họa khai báo và kết quả thực hiện.

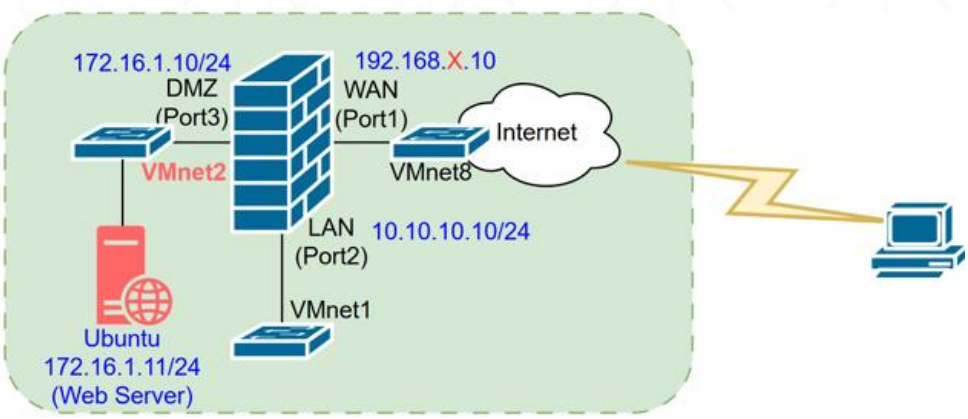


Nhóm 19

Giới thiệu tính năng Firewall Policy trong FortiGate và cách kiểm soát truy cập theo thời gian. Trình bày tính năng Port Forwarding và Virtual IP trong FortiGate.

Thực hiện khai báo tạo Virtual IP cho Web Server, khai báo Port Forwarding vào Web Server (từ 8080 WAN vào 80 của Web server), chỉ cho phép truy cập vào Server từ 8AM-5PM.

Chụp hình để minh họa khai báo và kết quả thực hiện.

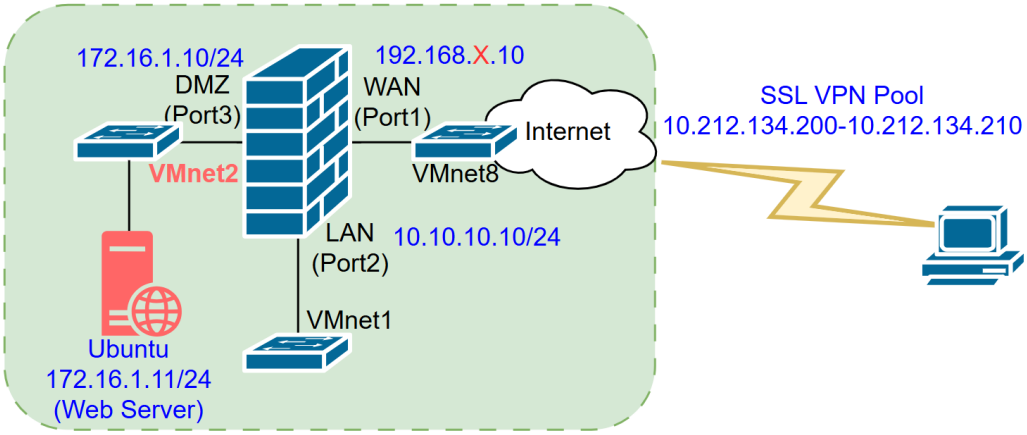


Nhóm 20

Trình bày khái niệm SSL Remote VPN và vai trò trong việc kết nối từ xa an toàn. Giới thiệu tính năng SSL VPN trong FortiGate và cách cấu hình (Portal, User Authentication).

Thực hiện khai báo tạo SSL VPN như sơ đồ bên dưới, cài đặt VPN Client (7.0) và kết nối.

Chụp hình để minh họa khai báo và kết quả thực hiện.

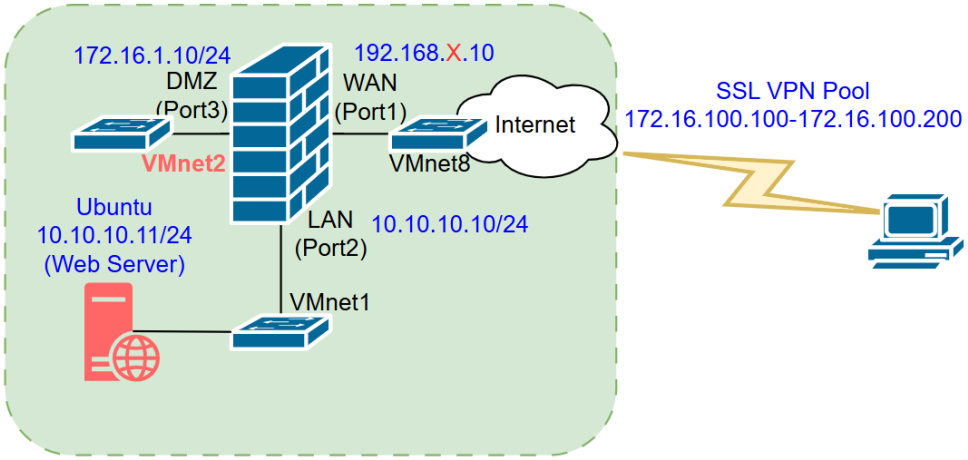


Nhóm 21

Trình bày cơ chế bảo mật của HTTPS và ứng dụng cho SSL Remote VPN. Vai trò của SSL VPN trong bảo vệ kết nối từ xa. Giới thiệu các phương thức xác thực người dùng trong SSL VPN trên FortiGate (Local, LDAP, RADIUS).

Thực hiện khai báo tạo SSL VPN như sơ đồ bên dưới, cài đặt VPN Client (7.0) và kết nối.

Chụp hình để minh họa khai báo và kết quả thực hiện.



Nhóm 22

Trình bày khái niệm IPsec VPN Remote Access và ứng dụng trong kết nối từ xa. Giới thiệu cách cấu hình IPsec VPN trên FortiGate với chế độ Dial-up.

Thực hiện khai báo tạo IPSec VPN như sơ đồ bên dưới, cho phép truy cập vào mạng LAN, cài đặt và khai báo VPN Client (7.0), KHÔNG cần thực hiện kết nối.

Chụp hình để minh họa khai báo và kết quả thực hiện.