Tunnel setup DFCD2024

Schema

A screenshot of a computer

Description automatically generated

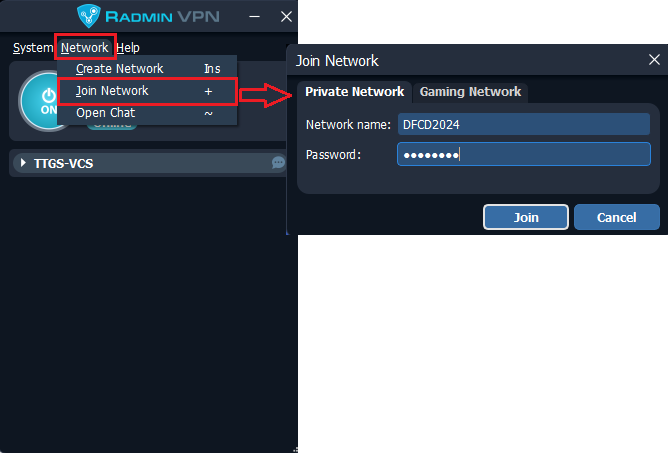
B1: Cài đặt Radmin VPN trên Windows:

Link download: <https://download.radmin-vpn.com/download/files/Radmin_VPN_1.4.4642.1.exe>

Join network đã tạo sẵn:

Network name: DFCD2024

Password: 123456a@

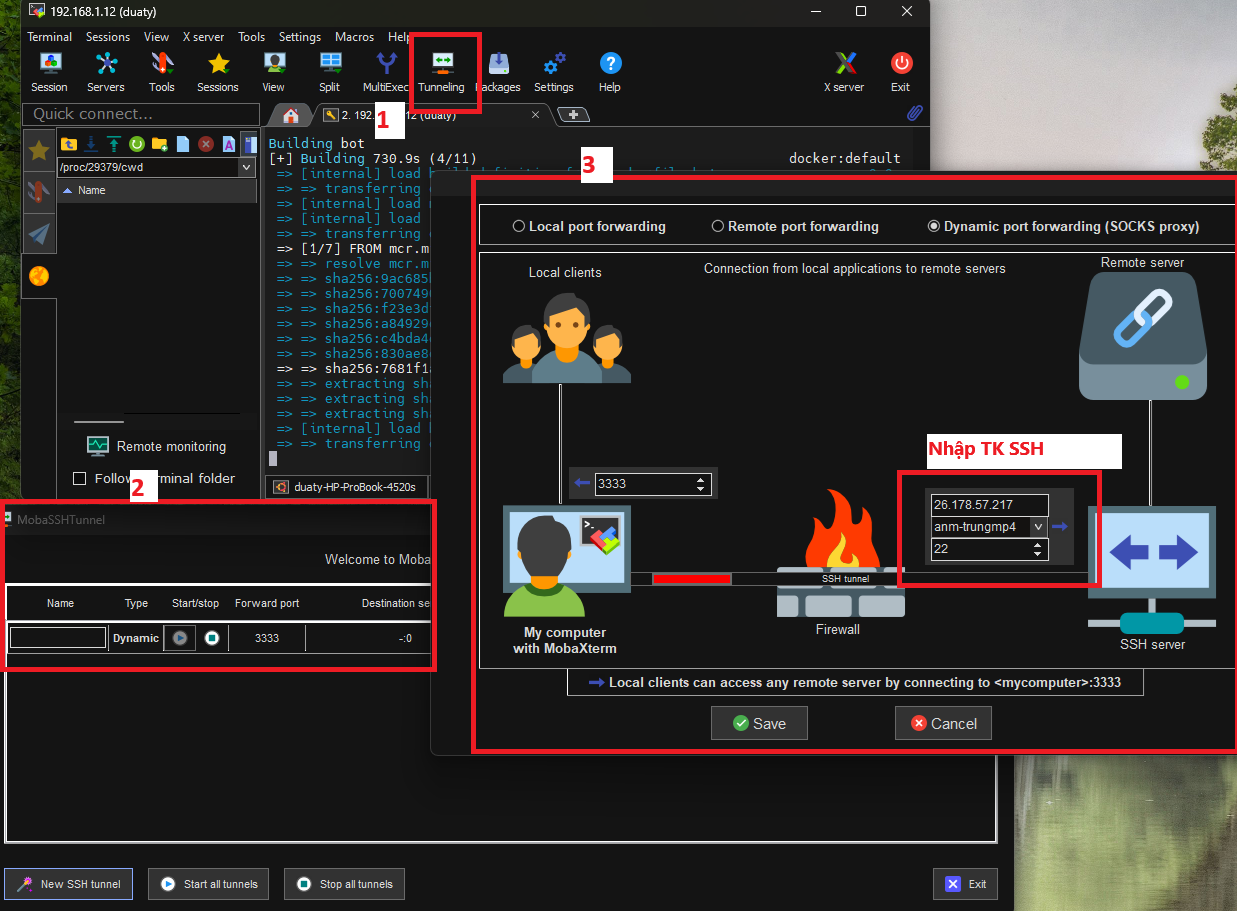


B2: SSH Dynamic portforwarding

Có 2 máy SSH để san tải cho nhau

* anm-trungmp4@26.178.57.217 | password: QAZwsx@123
* tnt2402@26.91.231.39 | password: QAZwsx@123

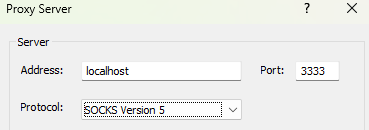
Thực hiện cấu hình SSH Dynamic Forwarding

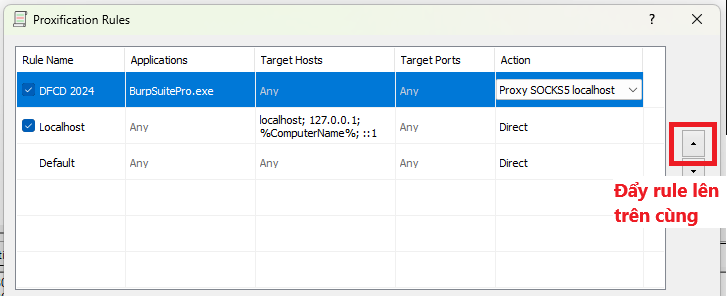
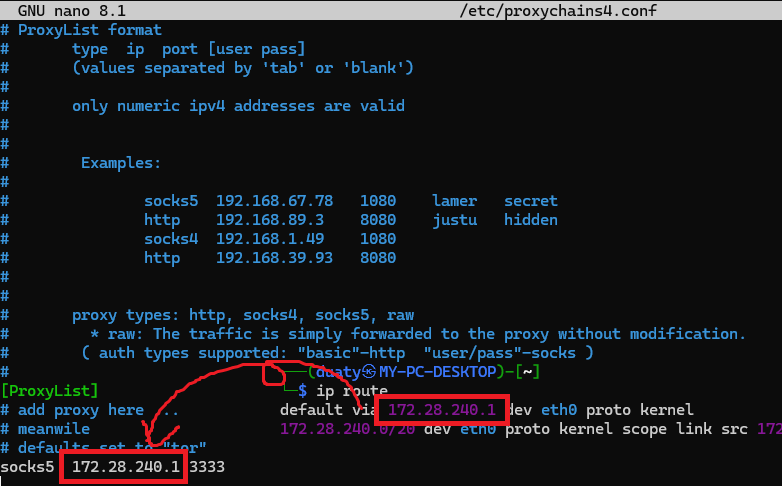


Sau khi setup dynamic forwarding thì mọi traffic đẩy vào SOCKS5 proxy sẽ tunnel sang mạng attack

B3: Routing traffic qua SOCKS5 proxy

Vì đây là SOCKS5 proxy nên không thể cấu hình BurpSuite upstream proxy (burp chỉ hỗ trợ HTTP proxy) nên phải cần thêm 1 ứng dụng routing để có thể route traffic từ burp & wsl vào sock5 proxy

* Đối với windows: Tải proxifier portable: <https://www.proxifier.com/download/ProxifierPE.zip>.   
  Chạy và nhập key P6Z3T-UYJC9-YAK3F-APN9M-6ZDSD để activate  
  Hướng dẫn cấu hình: B1 Profile -> Proxy Servers -> Add, sau đó điền SOCKS5 proxy trong mobaxterm ở bước 2  
    
  B2: Profile -> Proxification Rules -> Add, sau đó thêm rule mới để route traffic từ những app cần dùng sang SOCKS5 proxy. Trong ảnh là đang cấu hình tạm BurpSuitePro.exe nhưng ae muốn add gì cũng được. Có thể cấu hình qua target host nếu cần  
  A screenshot of a computer

  Description automatically generated  
  
* Đối với WSL: Sử dụng Proxychains: sudo apt install proxychains4  
  Cấu hình proxychains4 trỏ tới SOCKS5 proxy bằng cách sửa file /etc/proxychains4.conf. Do WSL sử dụng virtual network (vNIC) của Window Hypervisor Platform nên localhost máy ngoài sẽ có thể truy cập trong qua default gateway của WSL (sử dụng IP route để check default gateway)  
    
  Chạy các tool khác bằng proxychains4 sẽ tự động được đẩy về proxy này (ví dụ proxychains curl ipinfo.io/ip)