CÁC BƯỚC CÀI ĐẶT TCPDUMP VÀ LẤY LOG.PCAP

\*Nếu firewall chạy trên nền linux hoặc pfsense

Kiển tra xem có cài Tcpdump chưa? (nếu đã có rồi thì tới Bước 3)

# tcpdump -w communication.pcap



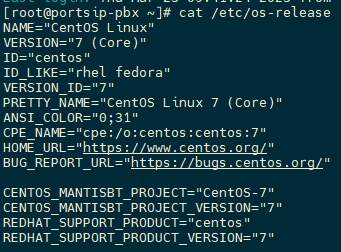
Có hình như trên là đang chạy và hệ thông bên mình đã cài Tcpdump

Chưa có sẽ báo lỗi

Chưa có thì thực hiện các bước dưới đây:

Bước 1: Kiểm tra xem os linux của firewall chạy os nào:

# cat /etc/os-release (kiểm tra OS)



Bước 2: Ví dụ như ở đây OS đang chạy là Centos Linux 7 sẽ chạy lệnh sau để cài gói TCPdump:

# sudo yum install tcpdump

Đối với các trường hợp dùng OS khác, sẽ dùng các câu lệnh khác nhau để cài tùy vào OS

# sudo apt-get install tcpdump [On Debian, Ubuntu and Mint]

# sudo yum install tcpdump [On RHEL/CentOS/Fedora and Rocky Linux/AlmaLinux]

# sudo emerge -a sys-apps/tcpdump [On Gentoo Linux]

# sudo pacman -S tcpdump [On Arch Linux]

# sudo zypper install tcpdump [On OpenSUSE]

Bước 3: dùng câu lệnh :

# tcpdump -w communication.pcap (có thể đặt tên khác như test.pcap; work.pcap)



Có hình này tức là đang chạy

Câu lênh dùng để capture file pcap rồi lưu vào file communication.pcap vào trong server

Khi sử dụng câu lệnh này, log sinh ra realtime > khi muốn dừng lấy log và lưu file thì dùng phím tắt “Ctrl +c”

Bước 4: Lấy file .cap này đưa cho phía bên Vinacis kiểm tra  
