tcpreplay로 dump데이터 수집

1. 네임서버 설정

/etc/resolv.conf

nameserver 8.8.8.8 (yum repository)

2. tcpreplay 설치

1) install libpcap-devel

yum -y install libpcap-devel

2) download tcpreplay from:

[http://tcpreplay.appneta.com/wiki/installation.htm (http://tcpreplay.appneta.com/wiki/installation.html#downloads](http://tcpreplay.appneta.com/wiki/installation.htm%20(http://tcpreplay.appneta.com/wiki/installation.html#downloads)

구글에서 <https://github.com/appneta/tcpreplay/releases/download/v4.1.0/tcpreplay-4.1.0.tar.gz> 들어가면 gz파일 다운받아짐

3) install tcpreplay

tar xfvz tcpreplay-4.1.0.tar.gz (tcpreplay 설치 할 장비에 접속해서)

cd tcpreplay-4.1.0

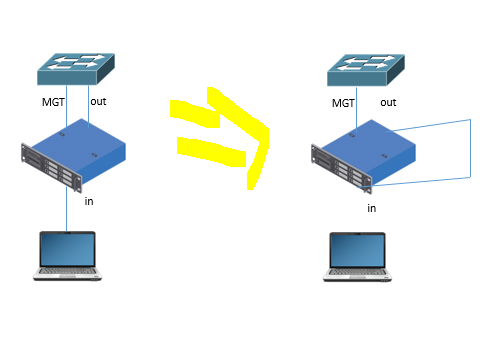
rpm -ivh libpcap-devel-1.5.3-11.el7.x86\_64.rpm ( yum으로 설치)

./configure --enable-dynamic-link

make

make install

- 물리적 선 연결 ( admin은 장비에 연결되어있고 out포트로 잡아줬던 거를 in과 연결 / =? 클라이언트 연결도 되어있지 않아야함

이렇게 구성

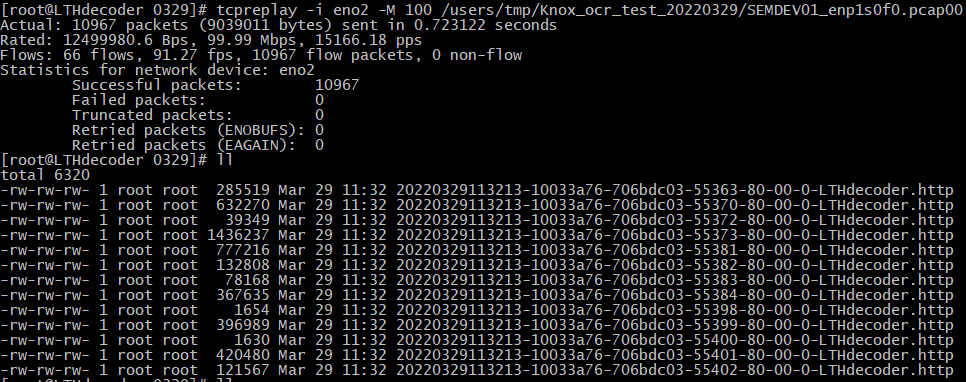
4) test

tcpreplay -i eth0 [file].pcap 파일이 안생긴다면 재기동하고 다시

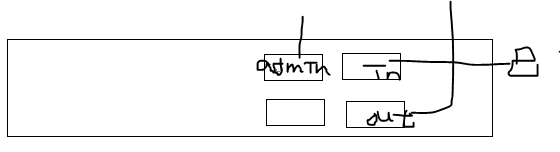
-> 여기서 eth0은 inport랑 연결되어있는 포트명

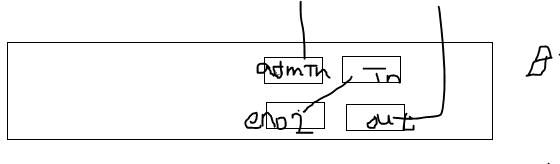
[ \\218.234.36.109\사업본부\06\_사업1그룹기술팀\임시자료\[삼성화재]\_사외보안메일\_패킷덤프 ]

ex)



->이건 어떻게 연결되어있었냐면

였는데

로 연결함