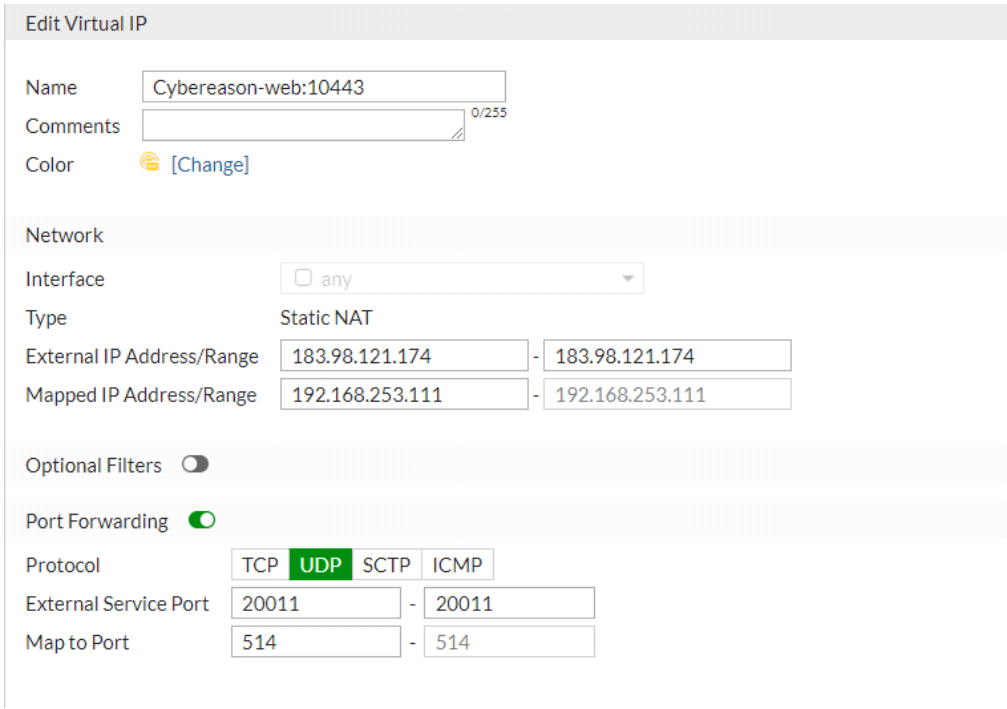
방화벽 로그 수집 테스트시나리오

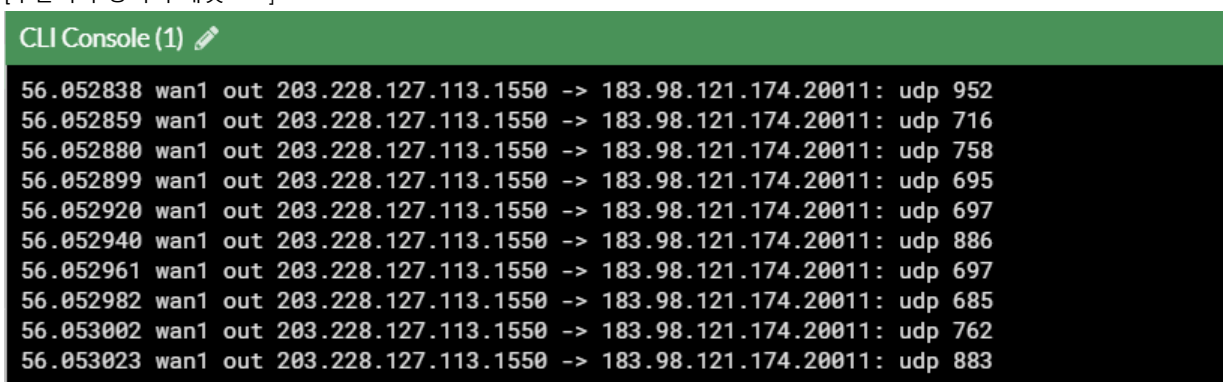
2021년 7월 9일 금요일 오후 12:58

203.228.127.113 : 20011 -> (Virtual IP 포트포워딩) 183.98.121.174 : 514 -> 192.168.253.111 : 514
(rsyslog)

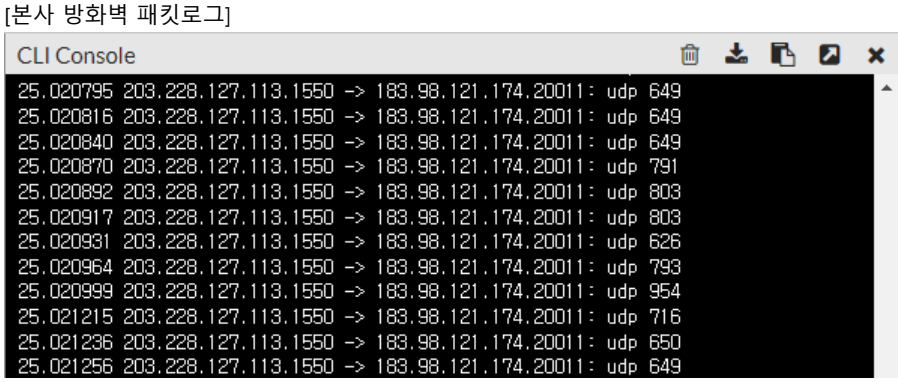
[포워딩 설정]



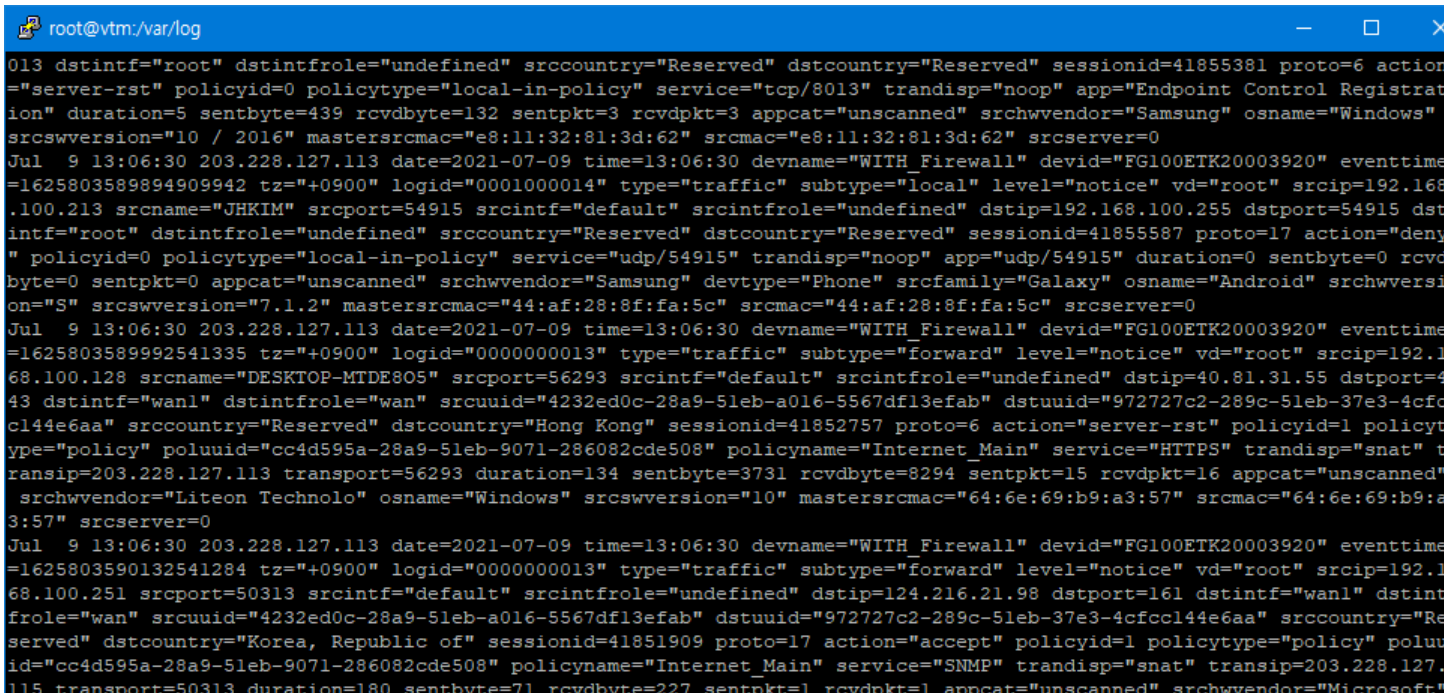
[부산지사 방화벽 패킷로그]



[본사 방화벽 패킷로그]



[111 서버 패킷 로그]


root@vtm:/var/log
013 dstintf="root" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved" sessionid=41855381 proto=6 action
="server-rst" policyid=0 policytype="local-in-policy" service="tcp/8013" trandisp="noop" app="Endpoint Control Registrat
ion" duration=5 sentbyte=439 rcvdbyte=132 sentpkt=3 rcvdpkt=3 appcat="unscanned" srchwvendor="Samsung" osname="Windows"
srcswversion="10 / 2016" mastersrcmac="e8:11:32:81:3d:62" srcmac="e8:11:32:81:3d:62" srcserver=0
Jul 9 13:06:30 203.228.127.113 date=2021-07-09 time=13:06:30 devname="WITH_Firewall" devid="FG100ETK20003920" eventtime
=1625803589894909942 tz="+0900" logid="0001000014" type="traffic" subtype="local" level="notice" vd="root" srcip=192.168
.100.213 srcname="JHKIM" srcport=54915 srcintf="default" srcintfrole="undefined" dstip=192.168.100.255 dstport=54915 dst
intf="root" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved" sessionid=41855587 proto=17 action="deny
" policyid=0 policytype="local-in-policy" service="udp/54915" trandisp="noop" app="udp/54915" duration=0 sentbyte=0 rcvd
byte=0 sentpkt=0 appcat="unscanned" srchwvendor="Samsung" devtype="Phone" srcfamily="Galaxy" osname="Android" srchwversi
on="S" srcswversion="7.1.2" mastersrcmac="44:af:28:8f:fa:5c" srcmac="44:af:28:8f:fa:5c" srcserver=0
Jul 9 13:06:30 203.228.127.113 date=2021-07-09 time=13:06:30 devname="WITH_Firewall" devid="FG100ETK20003920" eventtime
=1625803589992541335 tz="+0900" logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root" srcip=192.1
68.100.128 srcname="DESKTOP-MTDE8O5" srcport=56293 srcintf="default" srcintfrole="undefined" dstip=40.81.31.55 dstport=4
43 dstintf="wan1" dstintfrole="wan" srcuuid="4232ed0c-28a9-51eb-a016-5567df13efab" dstuuid="972727c2-289c-51eb-37e3-4cfc
c144e6aa" srccountry="Reserved" dstcountry="Hong Kong" sessionid=41852757 proto=6 action="server-rst" policyid=1 policyt
ype="policy" poluuid="cc4d595a-28a9-51eb-9071-286082cde508" policyname="Internet_Main" service="HTTPS" trandisp="snat" t
ransip=203.228.127.113 transport=56293 duration=134 sentbyte=3731 rcvdbyte=8294 sentpkt=15 rcvdpkt=16 appcat="unscanned"
srchwvendor="Liteon Technolo" osname="Windows" srcswversion="10" mastersrcmac="64:6e:69:b9:a3:57" srcmac="64:6e:69:b9:a
3:57" srcserver=0
Jul 9 13:06:30 203.228.127.113 date=2021-07-09 time=13:06:30 devname="WITH_Firewall" devid="FG100ETK20003920" eventtime
=1625803590132541284 tz="+0900" logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root" srcip=192.1
68.100.251 srcport=50313 srcintf="default" srcintfrole="undefined" dstip=124.216.21.98 dstport=161 dstintf="wan1" dstint
frole="wan" srcuuid="4232ed0c-28a9-51eb-a016-5567df13efab" dstuuid="972727c2-289c-51eb-37e3-4cfcc144e6aa" srccountry="Re
served" dstcountry="Korea, Republic of" sessionid=41851909 proto=17 action="accept" policyid=1 policytype="policy" poluu
id="cc4d595a-28a9-51eb-9071-286082cde508" policyname="Internet_Main" service="SNMP" trandisp="snat" transip=203.228.127.
115 transport=50313 duration=180 sentbyte=71 rcvdbyte=227 sentpkt=1 rcvdpkt=1 appcat="unscanned" srchwvendor="Microsoft"
mastersrcmac="00:15:5d:64:fa:12" srcmac="00:15:5d:64:fa:12" srcserver=0