Zeek Installation

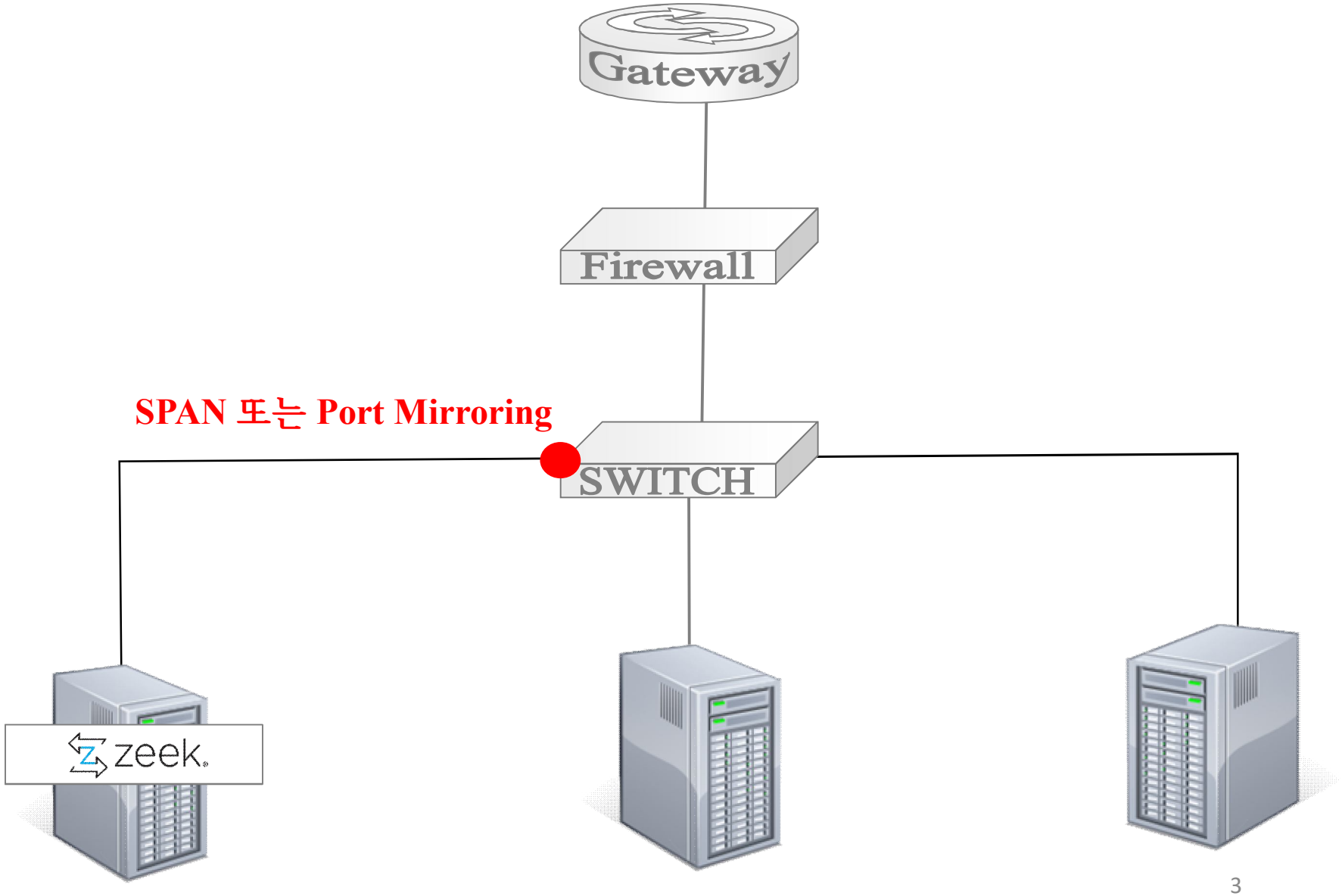
1) [Ubuntu Zeek] Zeek Installation

2) [zeek & Splunk server] scp installation

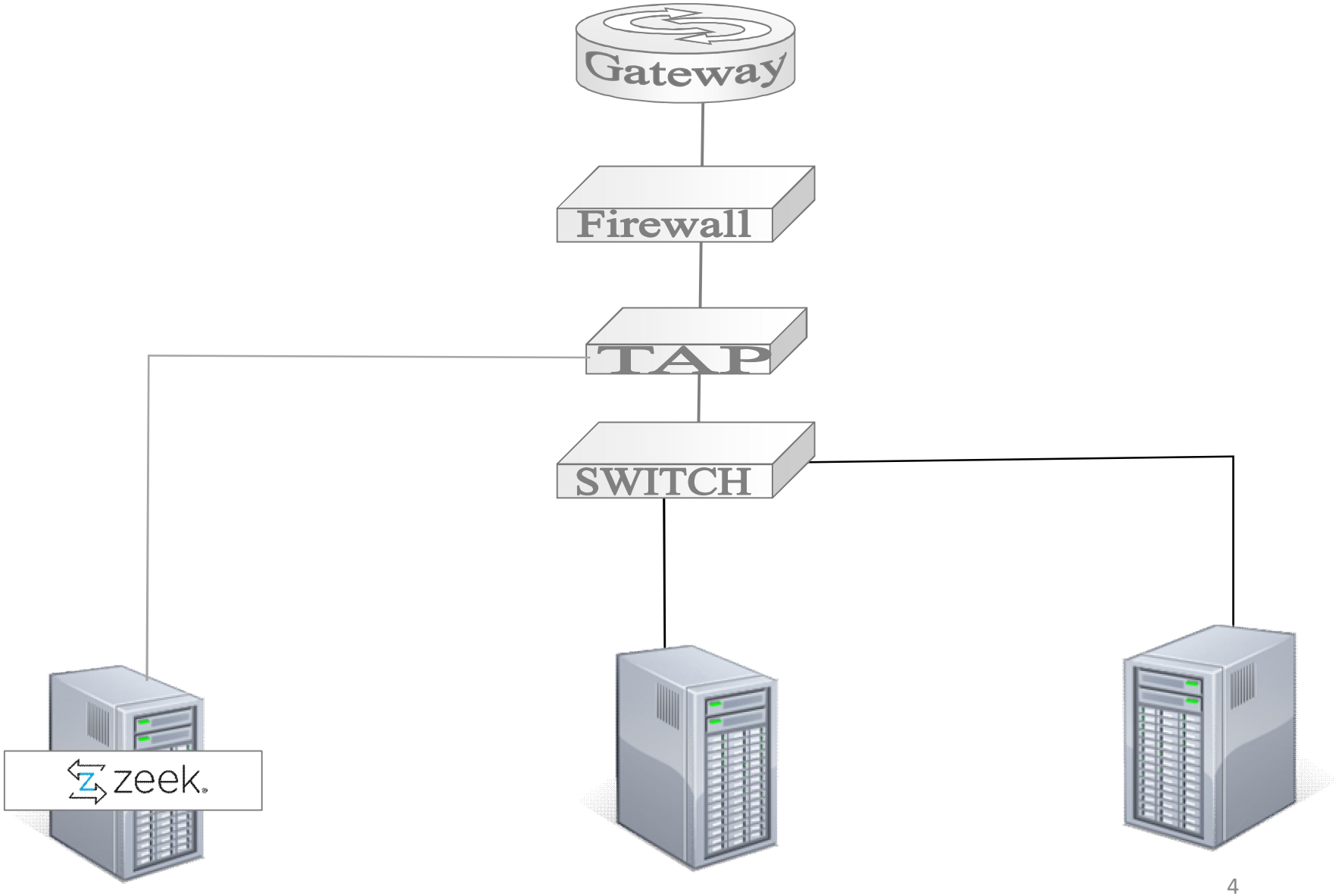
Zeek(p.181)

- 네트워크 침입탐지시스템(NIDS)
  - Bro 또는 프로토콜 분석
  - 네트워크를 모니터링 할 수 있는 오픈 소스 프로그램
- IP헤더와 TCP 헤더를 분석하여 로그 생성
- 응용 프로토콜의 헤더를 분석하여 로그 생성
  - FTP, HTTP, SMTP, X.509 ..

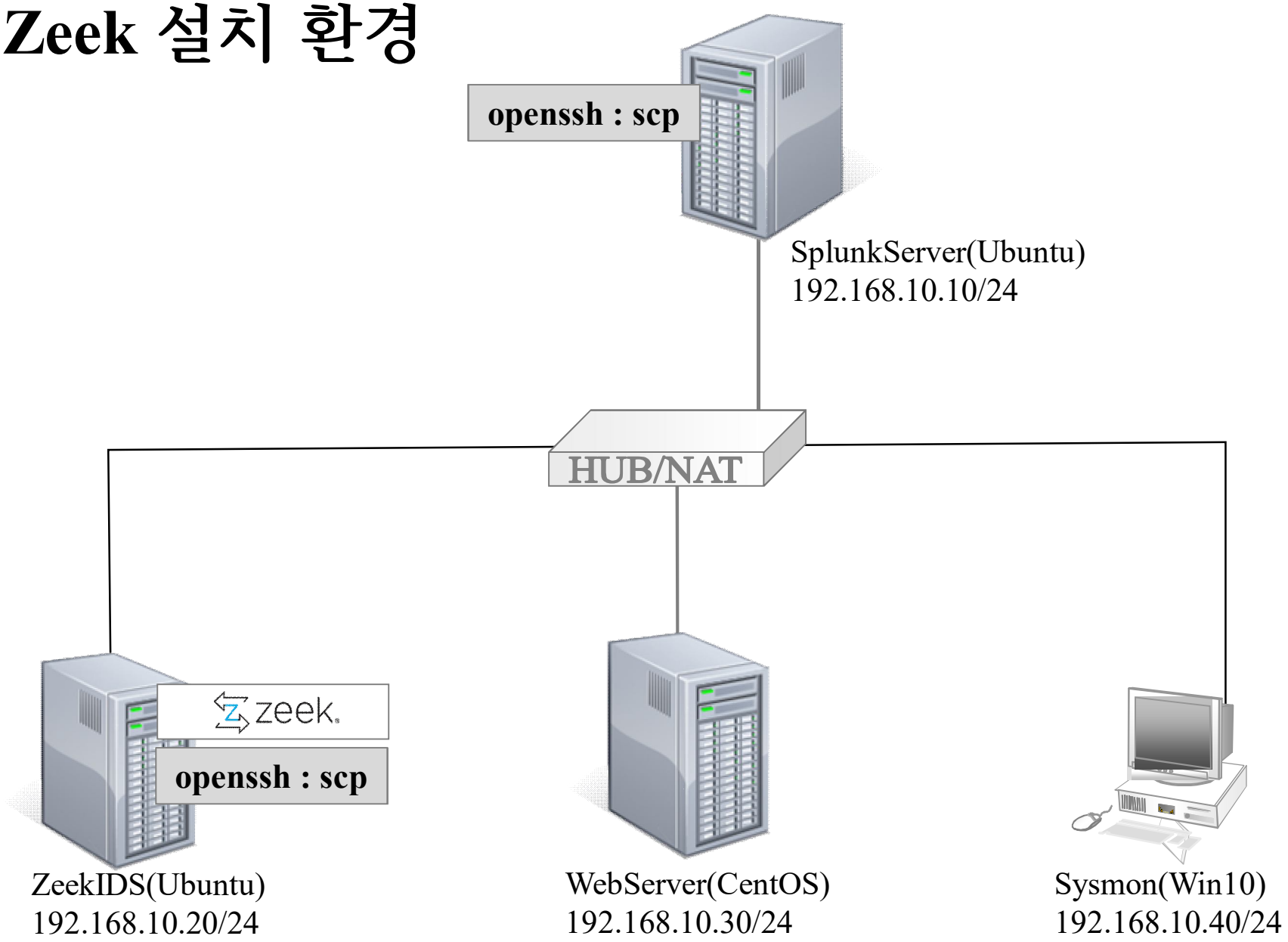
Zeek 설치 방법(p.182)



Zeek 설치 방법(p.182)



Zeek 설치 환경


openssh : scp
SplunkServer(Ubuntu)
192.168.10.10/24
HUB/NAT
zeek
openssh : scp
ZeekIDS(Ubuntu)
192.168.10.20/24
WebServer(CentOS)
192.168.10.30/24
Sysmon(Win10)
192.168.10.40/24

1) [Ubuntu Zeek] Zeek Installation

❶ 설치 전 환경 설정

#apt update

#apt-get install curl gnupg2 wget –y

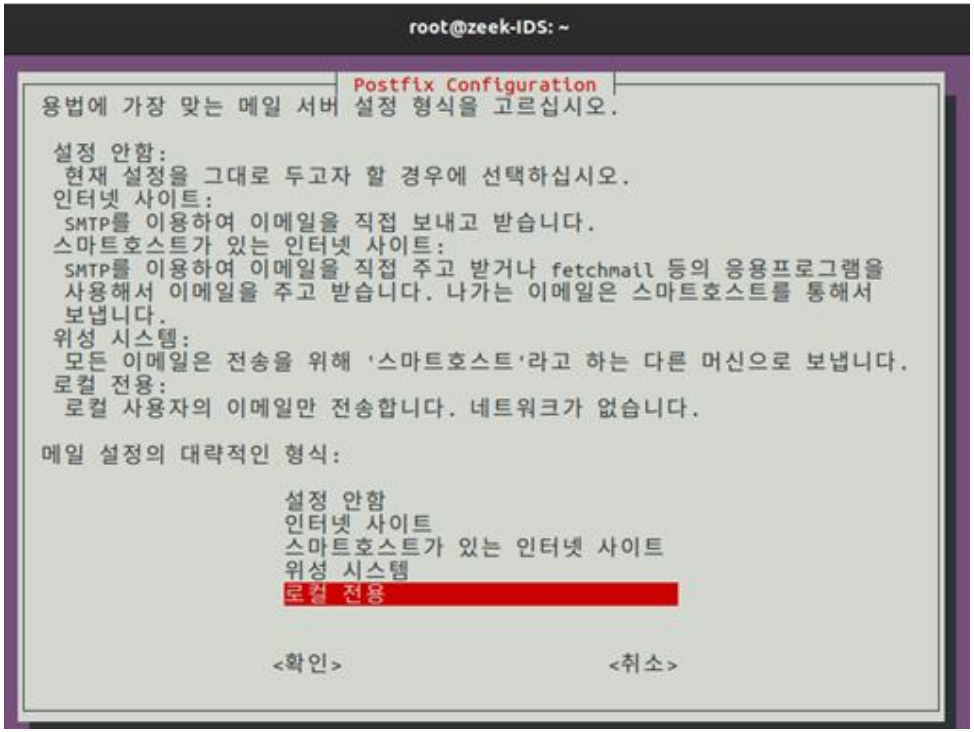
#curl -fsSL
https://download.opensuse.org/repositories/security:zeek/xUbuntu_20.04/Release.key | gpg --dearmor | tee /etc/apt/trusted.gpg.d/security_zeek.gpg

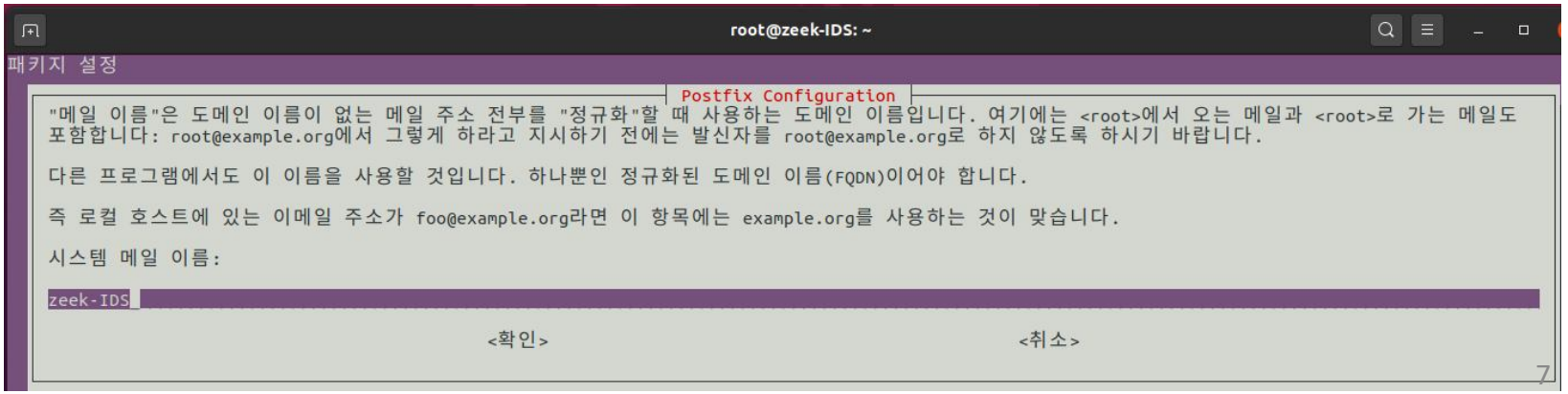
#echo 'deb
http://download.opensuse.org/repositories/security:/zeek/xUbuntu_20.04/ /' | tee /etc/apt/sources.list.d/security:zeek.list

❷ Zeek Installation

#apt update -y

#apt-get install zeek -y





❸ PATH 설정

#echo "export PATH=$PATH:/opt/zeek/bin" >> ~/.bashrc

#source ~/.bashrc

#zeek --version

```
root@zeek-IDS:~# zeek --version
zeek version 5.0.0
root@zeek-IDS:~#
```

❹ Zeek Configuration

#cd /opt/zeek/etc

#cat /opt/zeek/etc/networks.cfg

```
root@zeek-IDS:/opt/zeek/etc# pwd
/opt/zeek/etc
root@zeek-IDS:/opt/zeek/etc# ls -l
합계 16
-rw-rw-r-- 1 root zeek  262  1월 29  2015 networks.cfg
-rw-rw-r-- 1 root zeek  651  1월 29  2015 node.cfg
-rw-rw-r-- 1 root zeek 3052  1월 29  2015 zeekctl.cfg
drwxr-xr-x 2 root zeek 4096  7월 30 14:14 zkg
root@zeek-IDS:/opt/zeek/etc# cat networks.cfg
# List of local networks in CIDR notation, optionally followed by a
# descriptive tag.
# For example, "10.0.0.0/8" or "fe80::/64" are valid prefixes.

10.0.0.0/8          Private IP space
172.16.0.0/12       Private IP space
192.168.0.0/16      Private IP space
```

#ifconfig

```
root@zeek-IDS:/opt/zeek/etc# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.12  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::ac48:a451:53cf:9cea  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:d0:3a:96  txqueuelen 1000  (Ethernet)
        RX packets 61699  bytes 91719964 (91.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3675  bytes 250798 (250.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

#nano /opt/zeek/etc/node.cfg

[zeek]

type=standalone

host=localhost

interface=ens33

```
  GNU nano 4.8                                                node.cfg
# Example ZeekControl node configuration.
#
# This example has a standalone node ready to go except for possibly changing
# the sniffing interface.

# This is a complete standalone configuration.  Most likely you will
# only need to change the interface.
[zeek]
type=standalone
host=localhost
interface=ens33
```

❹ Zeek 활성화

#zeekctl check

#zeekctl deploy

#zeekctl status

#ls –l /opt/zeek/spool/zeek

```
root@zeek-IDS:/opt/zeek/etc#
root@zeek-IDS:/opt/zeek/etc# ls -l /opt/zeek/spool/zeek
합계 144
-rw-r--r-- 1 root zeek   252  7월 30 14:49 capture_loss.log
-rw-r--r-- 1 root zeek 23532  7월 30 14:58 conn.log
-rw-r--r-- 1 root zeek 22305  7월 30 14:58 dns.log
-rw-r--r-- 1 root zeek  2363  7월 30 14:55 http.log
-rw-r--r-- 1 root zeek   210  7월 30 14:49 known_hosts.log
-rw-r--r-- 1 root zeek   241  7월 30 14:48 known_services.log
-rw-r--r-- 1 root zeek 30777  7월 30 14:48 loaded_scripts.log
-rw-r--r-- 1 root zeek   763  7월 30 14:49 notice.log
-rw-r--r-- 1 root zeek   989  7월 30 14:52 ntp.log
-rw-r--r-- 1 root zeek   227  7월 30 14:48 packet_filter.log
-rw-r--r-- 1 root zeek   674  7월 30 14:48 reporter.log
-rw-r--r-- 1 root zeek   508  7월 30 14:55 software.log
-rw-r--r-- 1 root zeek  5886  7월 30 14:58 ssl.log
-rw-r--r-- 1 root zeek   888  7월 30 14:58 stats.log
-rw-r--r-- 1 root zeek    20  7월 30 14:48 stderr.log
-rw-r--r-- 1 root zeek   188  7월 30 14:48 stdout.log
-rw-r--r-- 1 root zeek   903  7월 30 14:54 weird.log
```

#tail /opt/zeek/spool/zeek/conn.log

```
root@zeek-IDS:/opt/zeek/etc# tail /opt/zeek/spool/zeek/conn.log
1659161491.671335       CJ9lye2SHkkcH4c9Q       192.168.10.1    65198   239.255.255.250 1900    udp     -       3.02985
6  700      0       S0      T       F       0       D       4       812     0       0       -
1659161491.686111       CHqNVR1cDyLwBRdFUj      192.168.10.1    65200   239.255.255.250 1900    udp     -       3.02997
9  700      0       S0      T       F       0       D       4       812     0       0       -
1659161544.850382       CmsBcA2VwUCJboRMm9      192.168.10.11   50552   192.168.10.2    53      udp     dns     0.00662
2  47       108     SF      T       T       0       Dd      1       75      1       136     -
1659161544.857948       CrJhuH2EM3k8EJqxWe      192.168.10.11   38605   192.168.10.2    53      udp     dns     0.00599
5  47       108     SF      T       T       0       Dd      1       75      1       136     -
1659161548.567765       C6waTA1ECI7D1dUtXd      192.168.10.11   52843   192.168.10.2    53      udp     dns     0.04779
6  37       101     SF      T       T       0       Dd      1       65      1       129     -
1659161548.568343       CQD9erMWE323xC8n6       192.168.10.11   53625   192.168.10.2    53      udp     dns     0.01165
3  37       111     SF      T       T       0       Dd      1       65      1       139     -
```

2) [zeek & Splunk server] scp installation

- SCP를 이용하기 위해서는 SSH 서비스가 활성화 되어있어야 함

#apt-get install –y openssh-server

#ufw allow 22/tcp

*scp [전송파일명] [서버계정명]@[전송받을 서버]:[전송받을 서버 디렉터리]

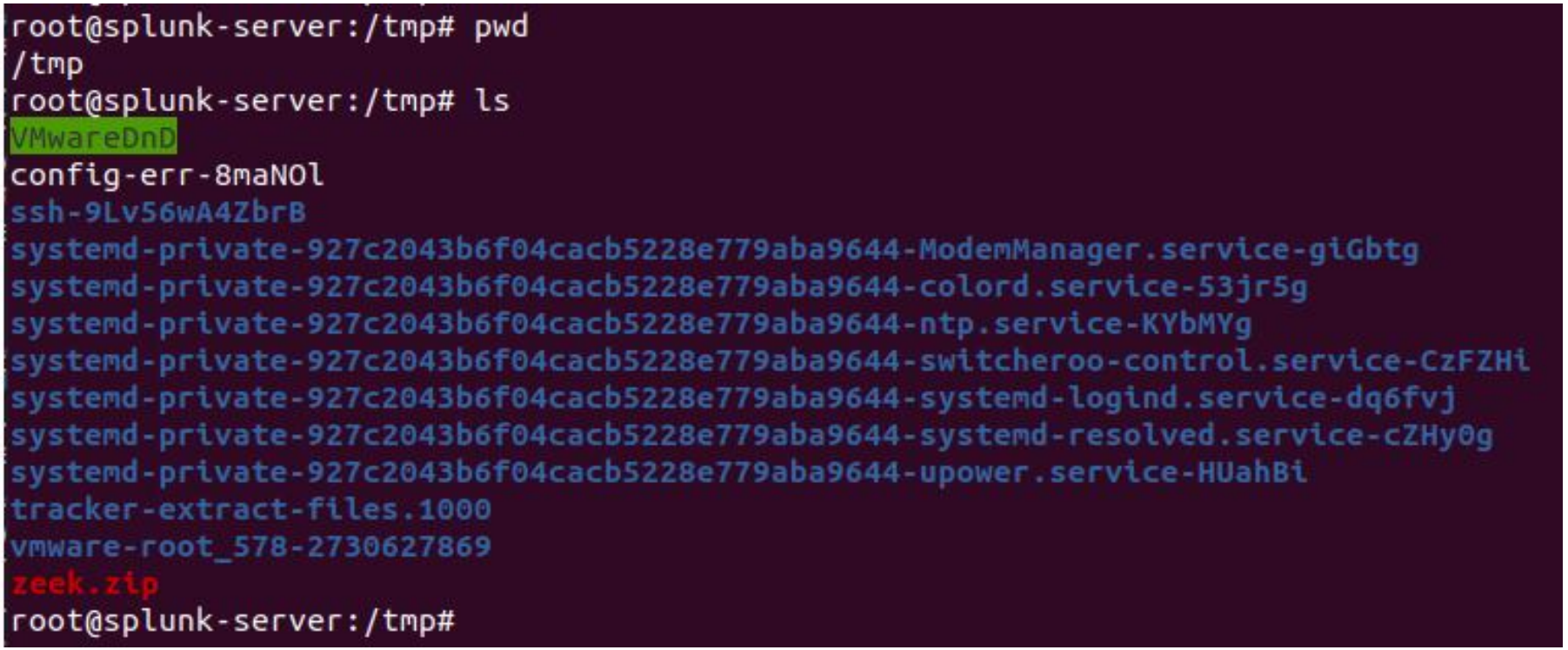
```
root@zeek-IDS:/opt/zeek/spool/zeek# scp conn.log splunk@192.168.10.11:/tmp
The authenticity of host '192.168.10.11 (192.168.10.11)' can't be established.
ECDSA key fingerprint is SHA256:Da7Ed6sOXjDNpogWae2zGXj87qM6QqVwlkwmLLDbjjw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.10.11' (ECDSA) to the list of known hosts.
splunk@192.168.10.11's password:
conn.log                                      100%  169KB  35.5MB/s   00:00
root@zeek-IDS:/opt/zeek/spool/zeek#
```

SCP를 이용해 Zeek log file을 Splunk Server 전송

#scp zeek.zip splunk@192.168.10.10:/tmp

```
root@zeek-IDS:/opt/zeek/spool/zeek# scp conn.log splunk@192.168.10.11:/tmp
The authenticity of host '192.168.10.11 (192.168.10.11)' can't be established.
ECDSA key fingerprint is SHA256:Da7Ed6sOXjDNpogWae2zGXj87qM6QqVwlkwmLLDbjjw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.10.11' (ECDSA) to the list of known hosts.
splunk@192.168.10.11's password:
conn.log                                      100%  169KB  35.5MB/s   00:00
root@zeek-IDS:/opt/zeek/spool/zeek#
```

```
root@zeek-IDS:/opt/zeek/spool#
root@zeek-IDS:/opt/zeek/spool# scp zeek.zip splunk@192.168.10.10:/tmp
splunk@192.168.10.10's password:
zeek.zip                                      100%   37KB  13.5MB/s   00:00
root@zeek-IDS:/opt/zeek/spool#
```


root@splunk-server:/tmp# pwd
/tmp
root@splunk-server:/tmp# ls
VMwareDnD
config-err-8maNOl
ssh-9Lv56wA4ZbrB
systemd-private-927c2043b6f04cacb5228e779aba9644-ModemManager.service-giGbtg
systemd-private-927c2043b6f04cacb5228e779aba9644-colord.service-53jr5g
systemd-private-927c2043b6f04cacb5228e779aba9644-ntp.service-KYbMYg
systemd-private-927c2043b6f04cacb5228e779aba9644-switcheroo-control.service-CzFZHi
systemd-private-927c2043b6f04cacb5228e779aba9644-systemd-logind.service-dq6fvj
systemd-private-927c2043b6f04cacb5228e779aba9644-systemd-resolved.service-cZHy0g
systemd-private-927c2043b6f04cacb5228e779aba9644-upower.service-HUahBi
tracker-extract-files.1000
vmware-root_578-2730627869
zeek.zip
root@splunk-server:/tmp#