[FINAL PROJECT]

THE BETTER

고가용성 글로벌 인프라 및 SOAR 기반
통합 관제 구축과 실전 APT 모의해킹 검증

Project Manager: 이명재

프로젝트 개요

THE BETTER

프로젝트 기간: 2026.02.23. ~ 2026.03.09. (10MD)

프로젝트 목표:

고가용성 네트워크와 안정적인 서버 인프라를 기반으로,
통합 관제·모의해킹·자동화된 시정조치 체계를 구축하여
기업 인프라의 안정성, 보안성, 운영 효율성을 종합적으로 강화

프로젝트 개요

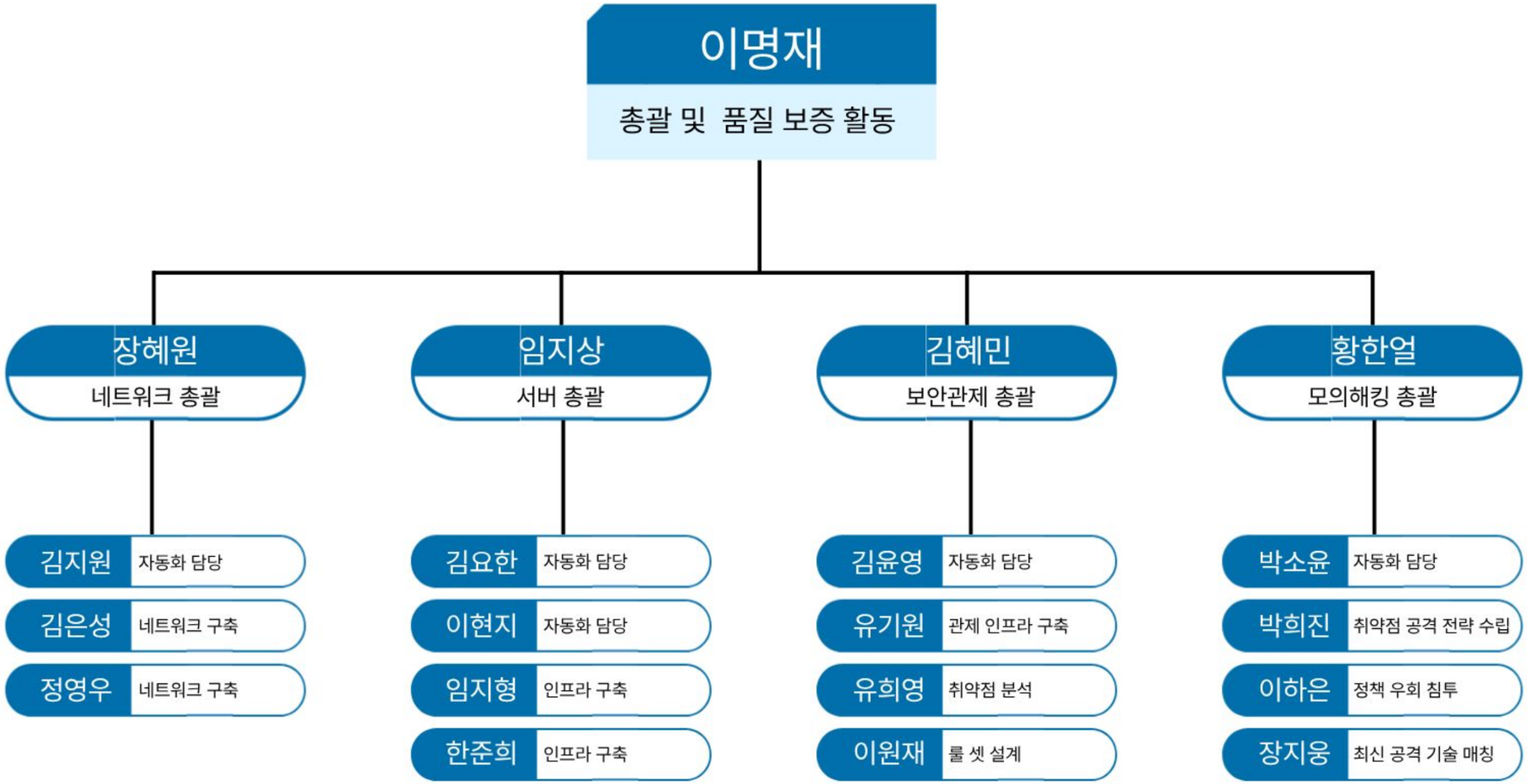
주요 내용

- OSPF, FHRP, EtherChannel, VPN, ASA 기반 네트워크 고도화
- HA, IPS, Zabbix, ELK, Ansible 기반 서버 운영 자동화
- 모의해킹을 통한 취약점 진단 및 보안 검증
- Wazuh·ELK·Scapy 기반 중앙 관제 및 SOAR 체계 구현
- 취약점 패치 및 WAF/방화벽 정책 보완

기대효과

무중단 서비스 보장, 보안 대응 시간 단축, 운영 효율성 향상,
실전형 방어 체계 확보

조직 구성도


이명재
총괄 및 품질 보증 활동
장혜원
네트워크 총괄
김지원 자동화 담당
김은성 네트워크 구축
정영우 네트워크 구축
임지상
서버 총괄
김요한 자동화 담당
이현지 자동화 담당
임지형 인프라 구축
한준희 인프라 구축
김혜민
보안관제 총괄
김윤영 자동화 담당
유기원 관제 인프라 구축
유희영 취약점 분석
이원재 룰 셋 설계
황한얼
모의해킹 총괄
박소윤 자동화 담당
박희진 취약점 공격 전략 수립
이하은 정책 우회 침투
장지웅 최신 공격 기술 매칭

핵심 사용기술

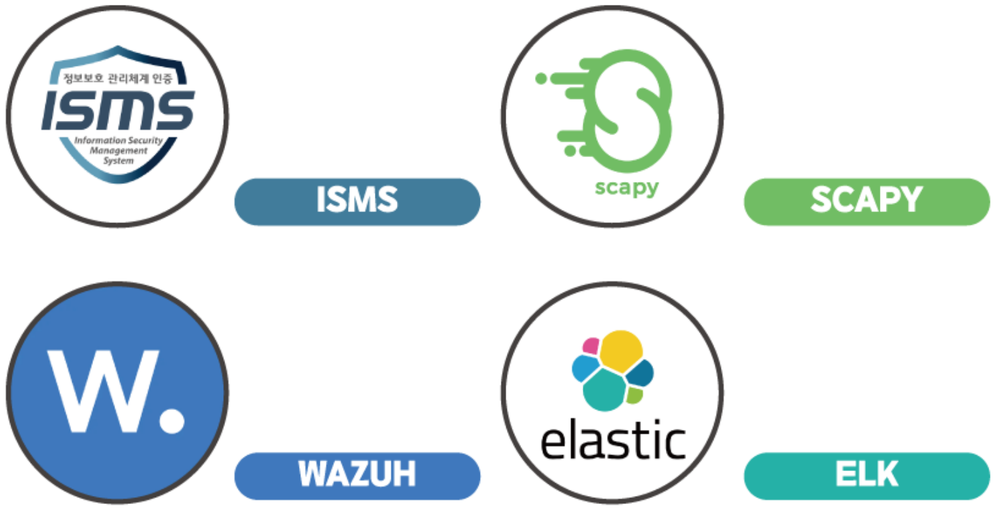
Network Team

핵심 사용기술

Server Team

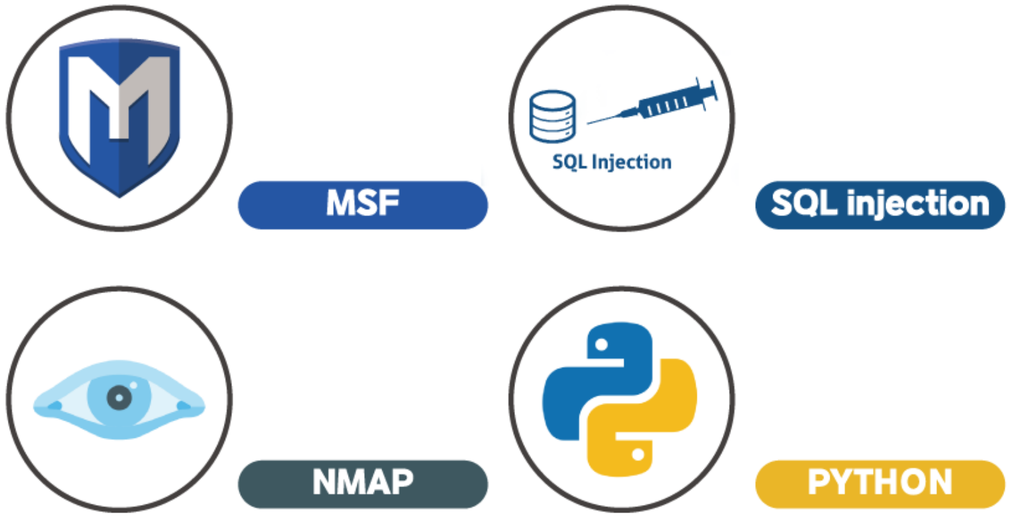
핵심 사용기술

Purple Team



핵심 사용기술

Red Team



핵심 사용기술

Network Team

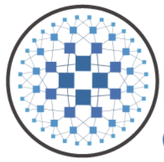
CISCO

GNS3

RSYSLOG

ANSIBLE

Server Team



HAPROXY

SURICATA

ZABBIX

PFSENSE

Purple Team

ISMS

SCAPY

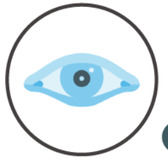
WAZUH

ELK

Red Team

MSF

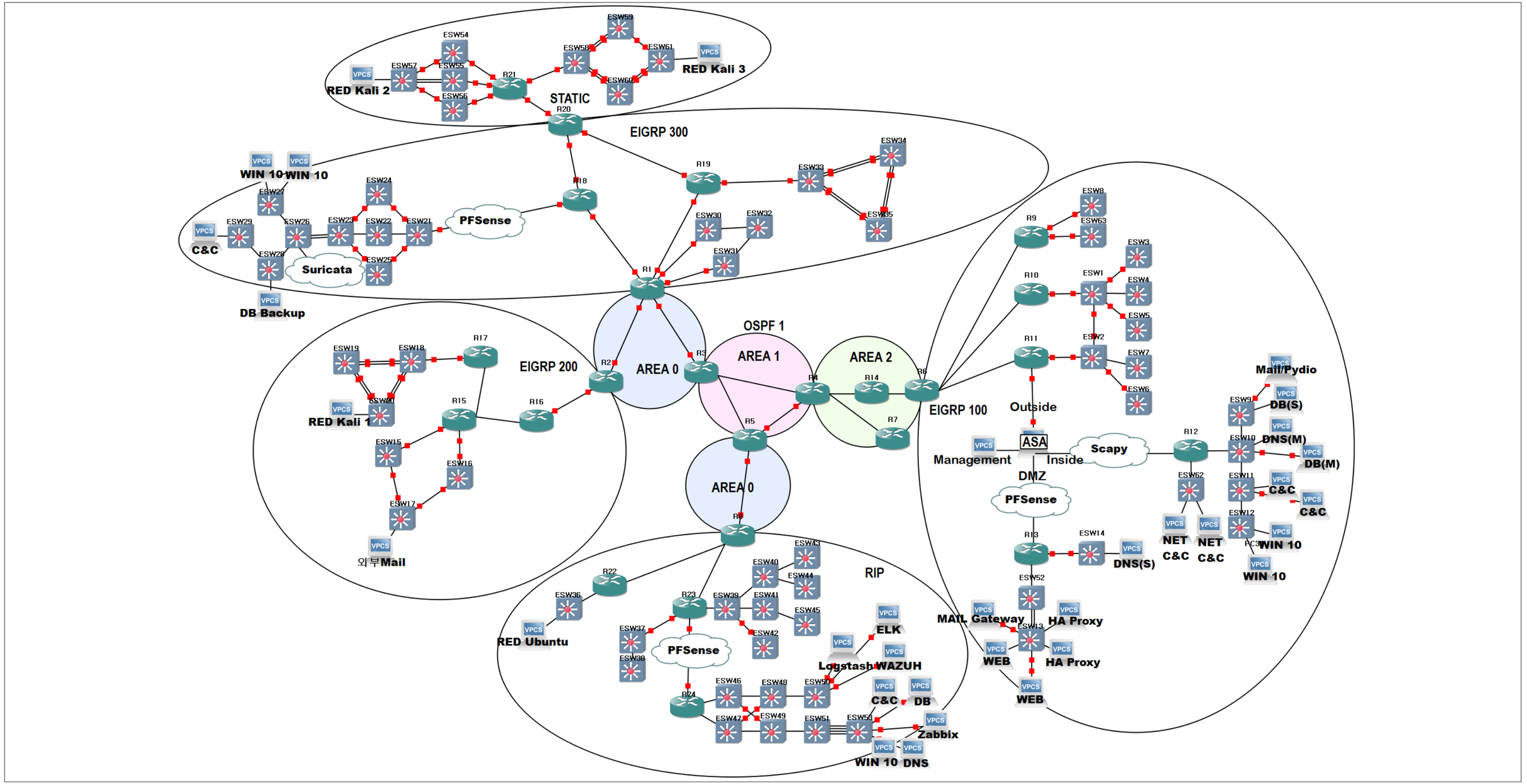
SQL injection



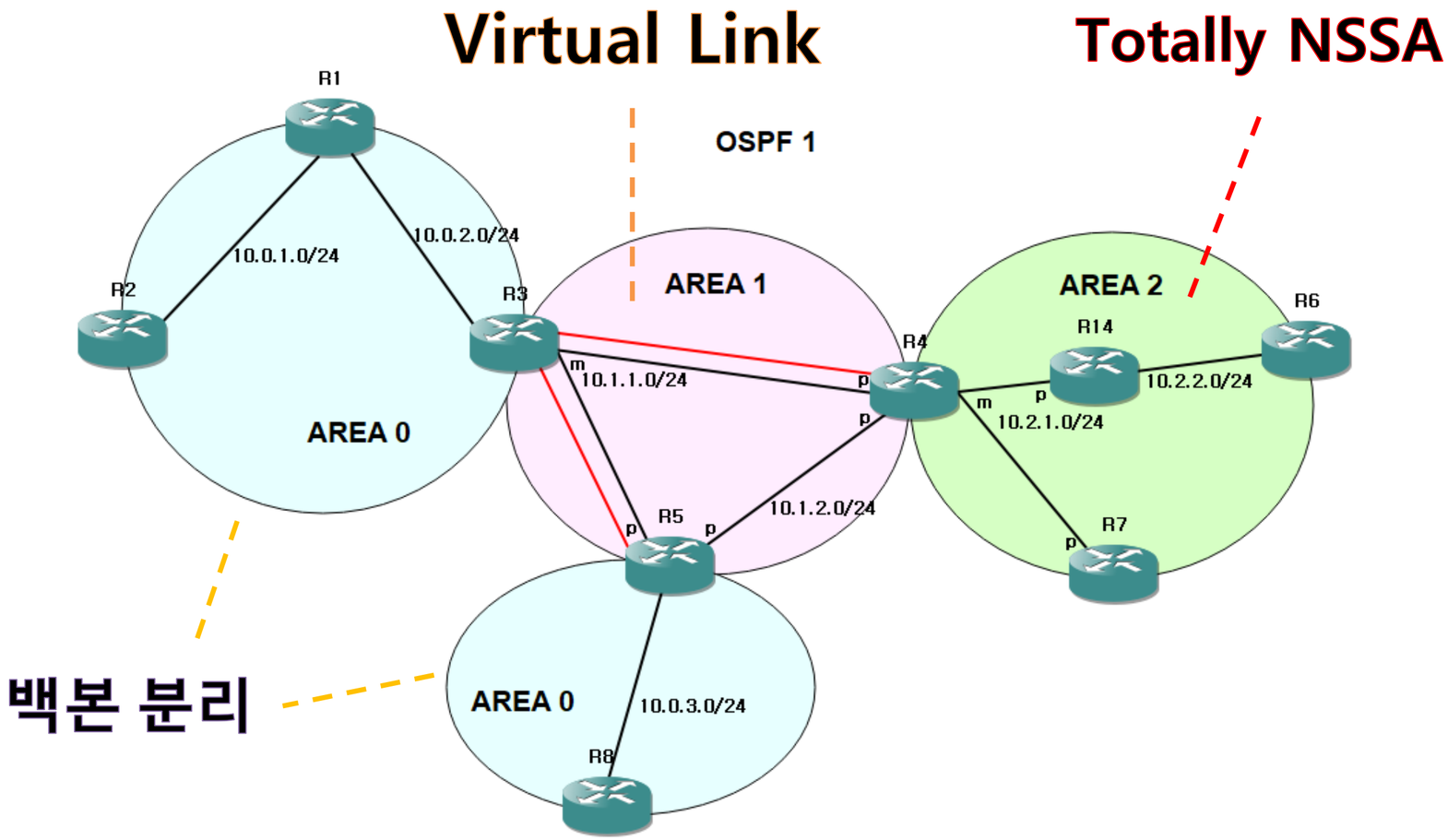
NMAP

PYTHON

네트워크 논리 구성도


RED Kali 2
RED Kali 3
STATIC
EIGRP 300
WIN 10
WIN 10
C&C
PFSense
Suricata
DB Backup
EIGRP 200
RED Kali 1
외부Mail
AREA 0
OSPF 1
AREA 1
AREA 2
AREA 0
RIP
RED Ubuntu
PFSense
ELK
Logstash
WAZUH
C&C
DB
Zabbix
WIN 10
DNS
EIGRP 100
Outside
Management
ASA
Inside
Scapy
DMZ
PFSense
Mail/Pydio
DB(S)
DNS(M)
DB(M)
C&C
C&C
NET
C&C
NET
C&C
WIN 10
WIN 10
DNS(S)
MAIL Gateway
HA Proxy
WEB
HA Proxy
WEB

코어망 (미국 중앙)


Virtual Link
Totally NSSA
OSPF 1
R1
10.0.1.0/24
10.0.2.0/24
R2
R3
AREA 1
AREA 2
R6
R14
R4
m
10.1.1.0/24
p
p
10.2.2.0/24
m
p
10.2.1.0/24
AREA 0
p
R5
p
10.1.2.0/24
R7
p
백본 분리
AREA 0
10.0.3.0/24
R8

코어망 (미국 중앙)

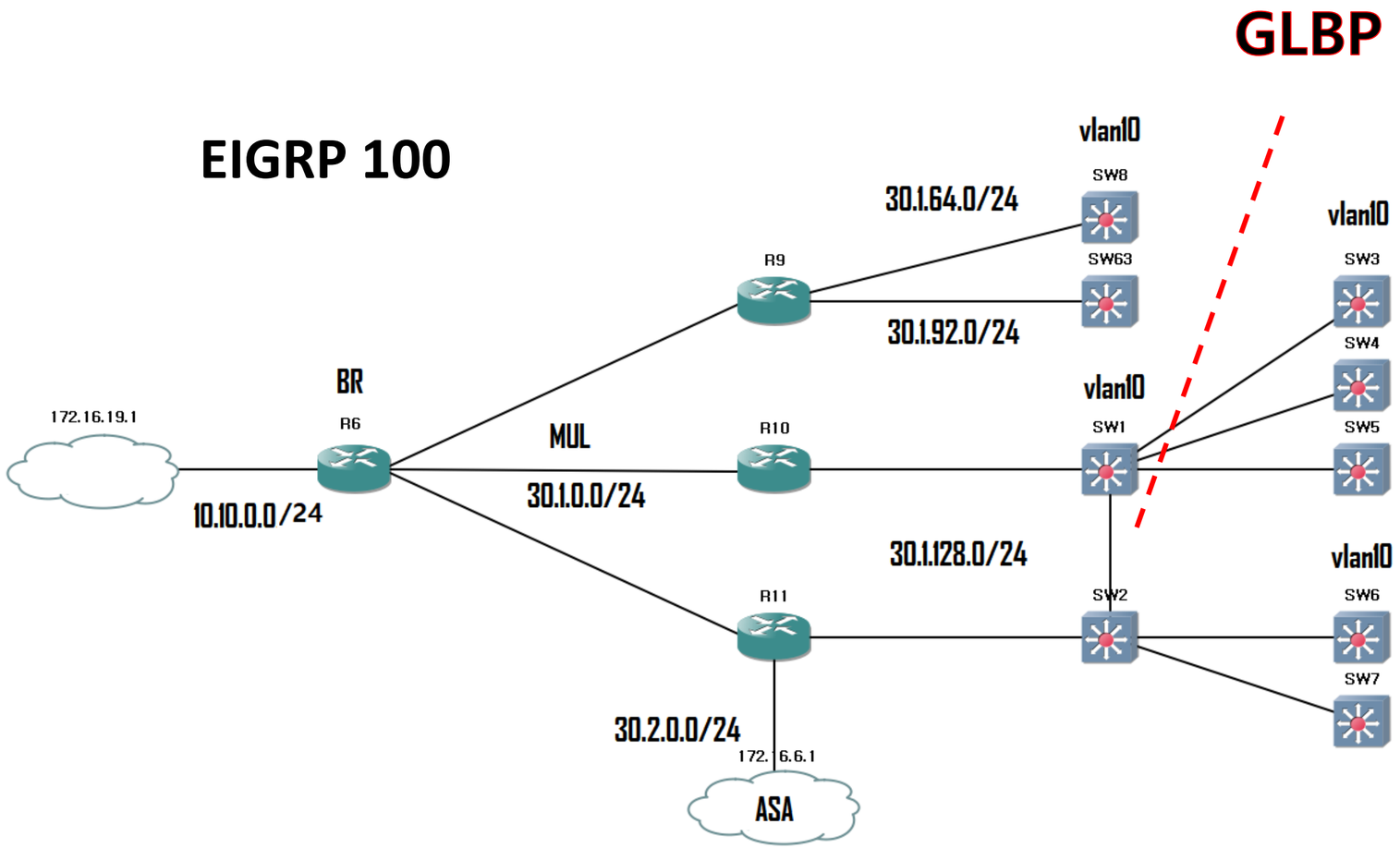
가상 링크

[1]: 백본망과 AREA 2 연결

[2]: 분리된 백본망 연결

```
R3#sh ip ospf virtual-links
Virtual Link OSPF_VL1 to router 4.4.4.4 is up [1]
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 1, via interface Serial1/0.1, Cost of using 128
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
    Adjacency State FULL (Hello suppressed)
    Index 2/4, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
Virtual Link OSPF_VL0 to router 5.5.5.5 is up [2]
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 1, via interface Serial1/0.1, Cost of using 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
    Adjacency State FULL (Hello suppressed)
```

본사(미국동부)1


GLBP
EIGRP 100
vlan10
SW8
30.1.64.0/24
vlan10
SW3
R9
SW63
30.1.92.0/24
SW4
BR
vlan10
172.16.19.1
R6
R10
SW1
SW5
MUL
30.1.0.0/24
10.10.0.0/24
30.1.128.0/24
vlan10
R11
SW2
SW6
SW7
30.2.0.0/24
172. 6.6.1
ASA

본사(미국동부) 1

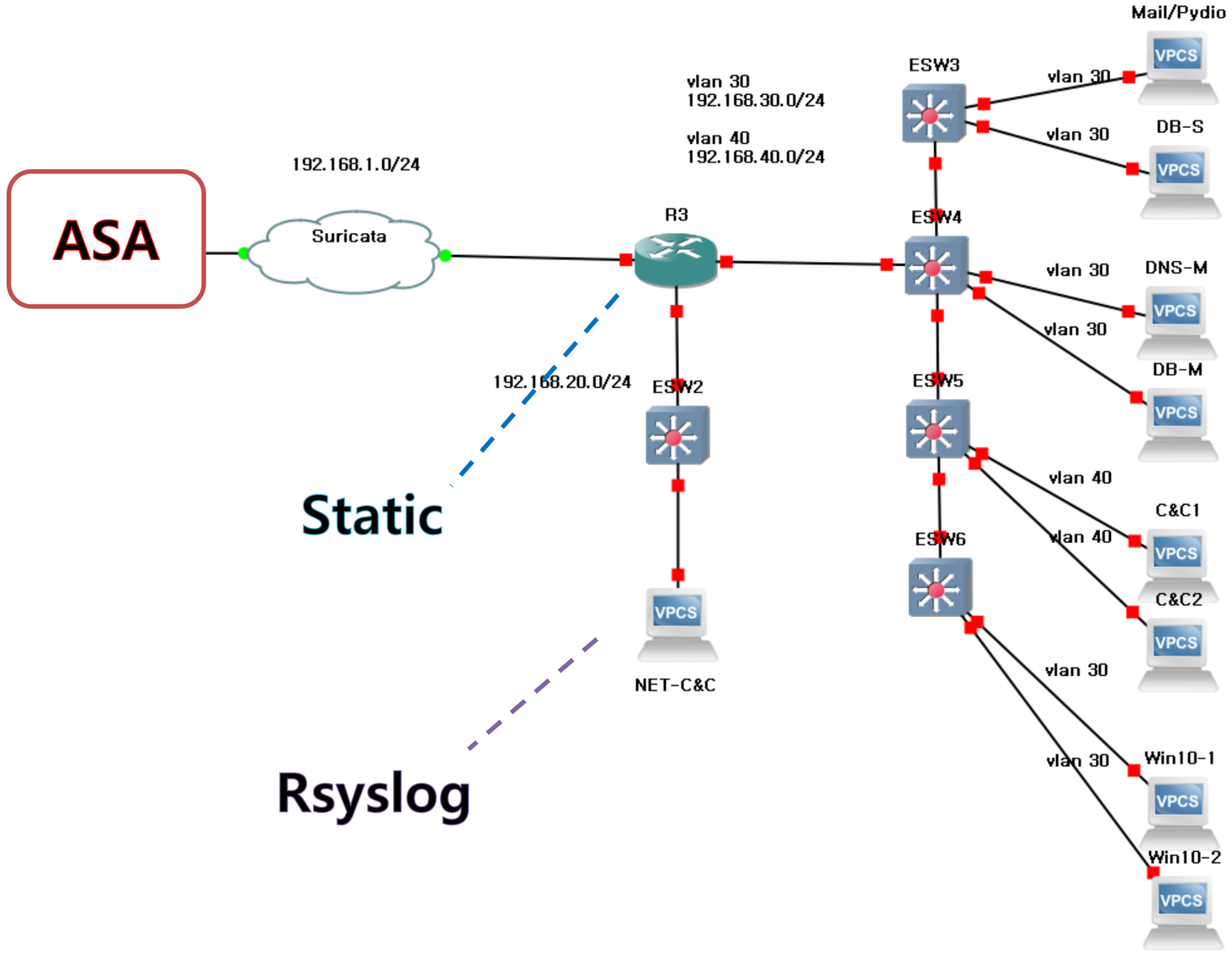
```
SW1# show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Vl10        10   -   120 Active   30.1.128.200    local           30.1.128.253
Vl10        10   1   -   Active   0007.b400.0a01  local           -
Vl10        10   2   -   Listen   0007.b400.0a02  30.1.128.253    -
```

```
SW2#sh glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Vl10        10   -   100 Standby  30.1.128.200    30.1.128.254    local
Vl10        10   1   -   Listen   0007.b400.0a01  30.1.128.254    -
Vl10        10   2   -   Active   0007.b400.0a02  local           -
```

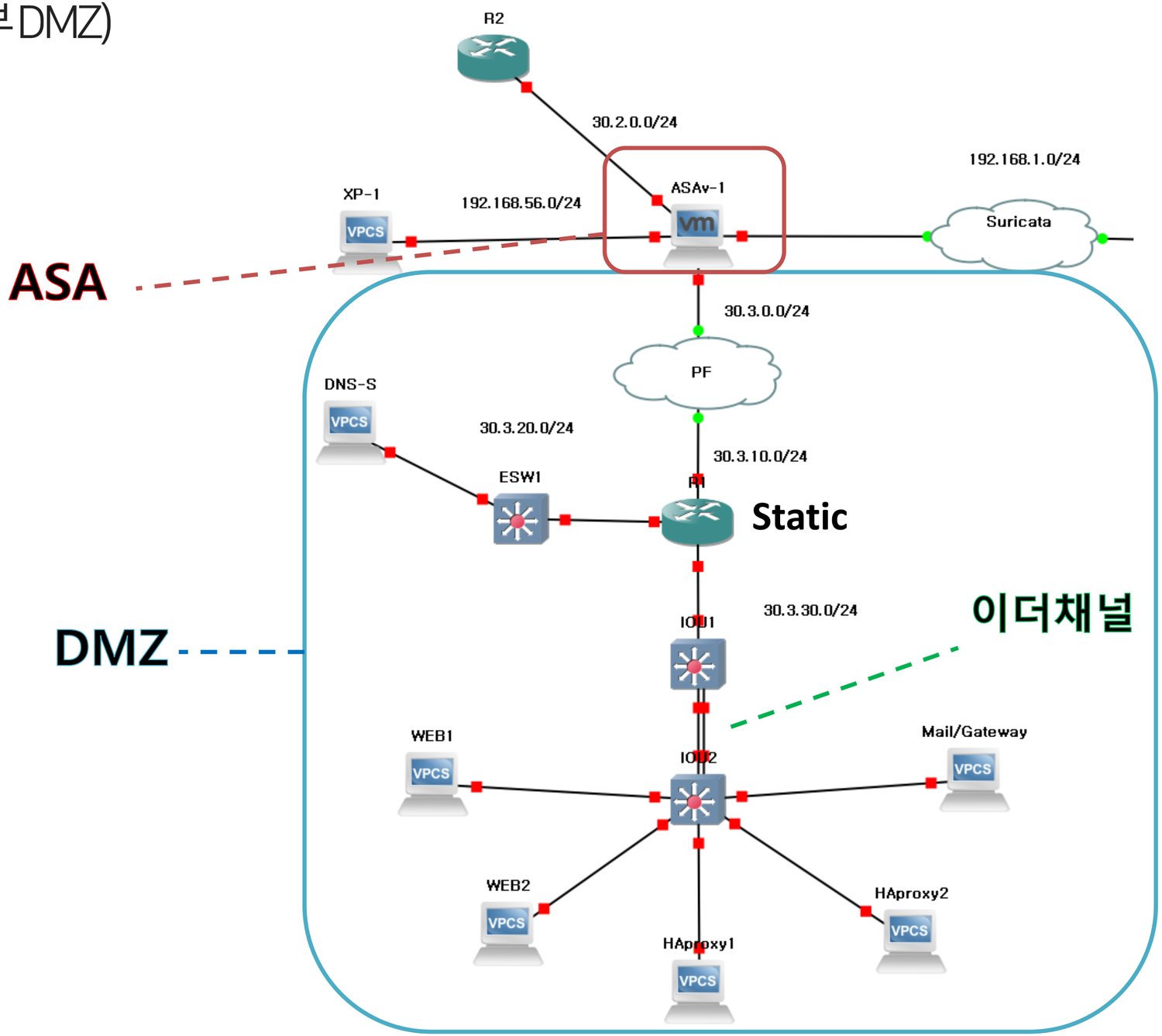
GLBP

AVG(Active), Standby 상태 확인

본사(미국동부사설)


ASA
192.168.1.0/24
Suricata
R3
vlan 30
192.168.30.0/24
vlan 40
192.168.40.0/24
192.168.20.0/24
ESW2
Static
Rsyslog
VPCS
NET-C&C
ESW3
ESW4
ESW5
ESW6
Mail/Pydio
DB-S
DNS-M
DB-M
C&C1
C&C2
Win10-1
Win10-2
vlan 30
vlan 40

본사(미국동부DMZ)


R2
30.2.0.0/24
192.168.1.0/24
XP-1
192.168.56.0/24
ASAv-1
Suricata
ASA
30.3.0.0/24
PF
DNS-S
30.3.20.0/24
30.3.10.0/24
ESW1
R1
Static
30.3.30.0/24
IOU1
이더채널
DMZ
WEB1
IOU2
Mail/Gateway
WEB2
HAproxy2
HAproxy1
VPCS

본사(미국동부사설/DMZ)

ASA

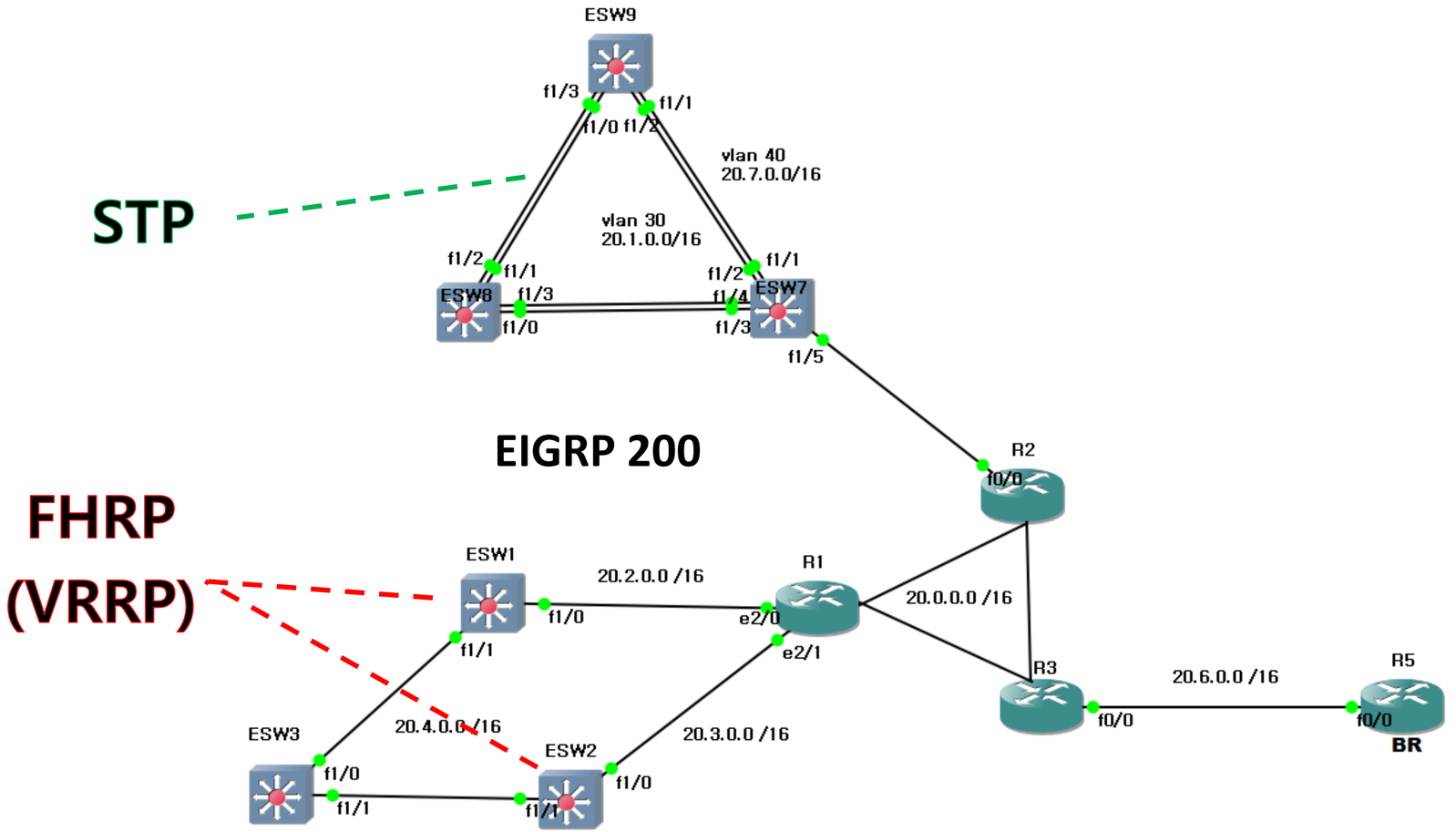
정적 NAT 및 동적 NAT 정책과
트래픽 변환(hit) 현황을 확인가능

각 인터페이스(outside, inside, dmz)에 적용된
ACL 정책과 global 접근 제어 설정을 확인 가능

```
1 (outside) to (inside) source static out1 out1   destination static INSIDE-NET
INSIDE-NET
    translate_hits = 4777, untranslate_hits = 6045
2 (outside) to (inside) source static out2 out2   destination static INSIDE-NET
INSIDE-NET
    translate_hits = 6, untranslate_hits = 6
3 (outside) to (inside) source static out3 out3   destination static INSIDE-NET
INSIDE-NET
    translate_hits = 1064, untranslate_hits = 5087
4 (outside) to (inside) source static out4 out4   destination static INSIDE-NET
INSIDE-NET
    translate_hits = 29, untranslate_hits = 29

Auto NAT Policies (Section 2)
1 (outside) to (inside) source static s4 172.16.8.20
    translate_hits = 0, untranslate_hits = 0
2 (outside) to (inside) source static s1 172.16.254.33
    translate_hits = 2, untranslate_hits = 16
3 (outside) to (inside) source static s2 172.16.254.55
    translate_hits = 0, untranslate_hits = 0
4 (outside) to (inside) source static s3 172.16.254.66
    translate_hits = 21, untranslate_hits = 0
5 (inside) to (outside) source dynamic INSIDE-NET interface
    translate_hits = 217368, untranslate_hits = 12982
ASAV1# _
```

```
ASAV1# sh running-config access-group
access-group OUTSIDE_IN in interface outside
access-group inside_access_in in interface inside
access-group DMZ_access_in in interface dmz
access-group global_access global
ASAV1# _
```

미국서부지사


ESW9
f1/3
f1/1
f1/0 f1/2
vlan 40
20.7.0.0/16
STP
vlan 30
20.1.0.0/16
f1/2
f1/1
f1/2
f1/1
ESW8
f1/3
f1/4
ESW7
f1/0
f1/3
f1/5
EIGRP 200
R2
f0/0
FHRP
(VRRP)
ESW1
20.2.0.0 /16
R1
f1/0
e2/0
20.0.0.0 /16
f1/1
e2/1
R3
20.6.0.0 /16
R5
f0/0
f0/0
BR
ESW3
20.4.0.0 /16
20.3.0.0 /16
ESW2
f1/0
f1/0
f1/1
f1/1

미국서부지사

```
Vlan10 - Group 10
  State is Master
  Virtual IP address is 20.4.0.254
  Virtual MAC address is 0000.5e00.010a
  Advertisement interval is 1.000 sec
  Preemption enabled, delay min 60 secs
  Priority is 150
    Track object 1 state Up decrement 60
  Master Router is 20.4.0.253 (local), priority is 150
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.414 sec
```

```
ESW2#sh vrrp
Vlan10 - Group 10
  State is Backup
  Virtual IP address is 20.4.0.254
  Virtual MAC address is 0000.5e00.010a
  Advertisement interval is 1.000 sec
  Preemption enabled, delay min 60 secs
  Priority is 100
  Master Router is 20.4.0.253, priority is 150
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.609 sec (expires in 2.705 sec)
```

FHRP (VRRP)

Master와 Backup상태 확인

```
ESW1#sh vrrp bri
Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
Vl10               10  150 3414        Y  Master  20.4.0.253      20.4.0.254
```

```
ESW2#show vrrp brief
Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
Vl10               10  100 3609        Y  Backup  20.4.0.253      20.4.0.254
```

```
VLAN30
  Spanning tree enabled protocol ieee
  Root ID     Priority    8192
              Address     c40b.5164.0001
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    8192
              Address     c40b.5164.0001
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                    Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/2      128.43   128    19 BKN     0  8192 c40b.5164.0001 128.43
FastEthernet1/4      128.45   128    19 FWD     0  8192 c40b.5164.0001 128.45
FastEthernet1/5      128.46   128    19 FWD     0  8192 c40b.5164.0001 128.46
```

Root

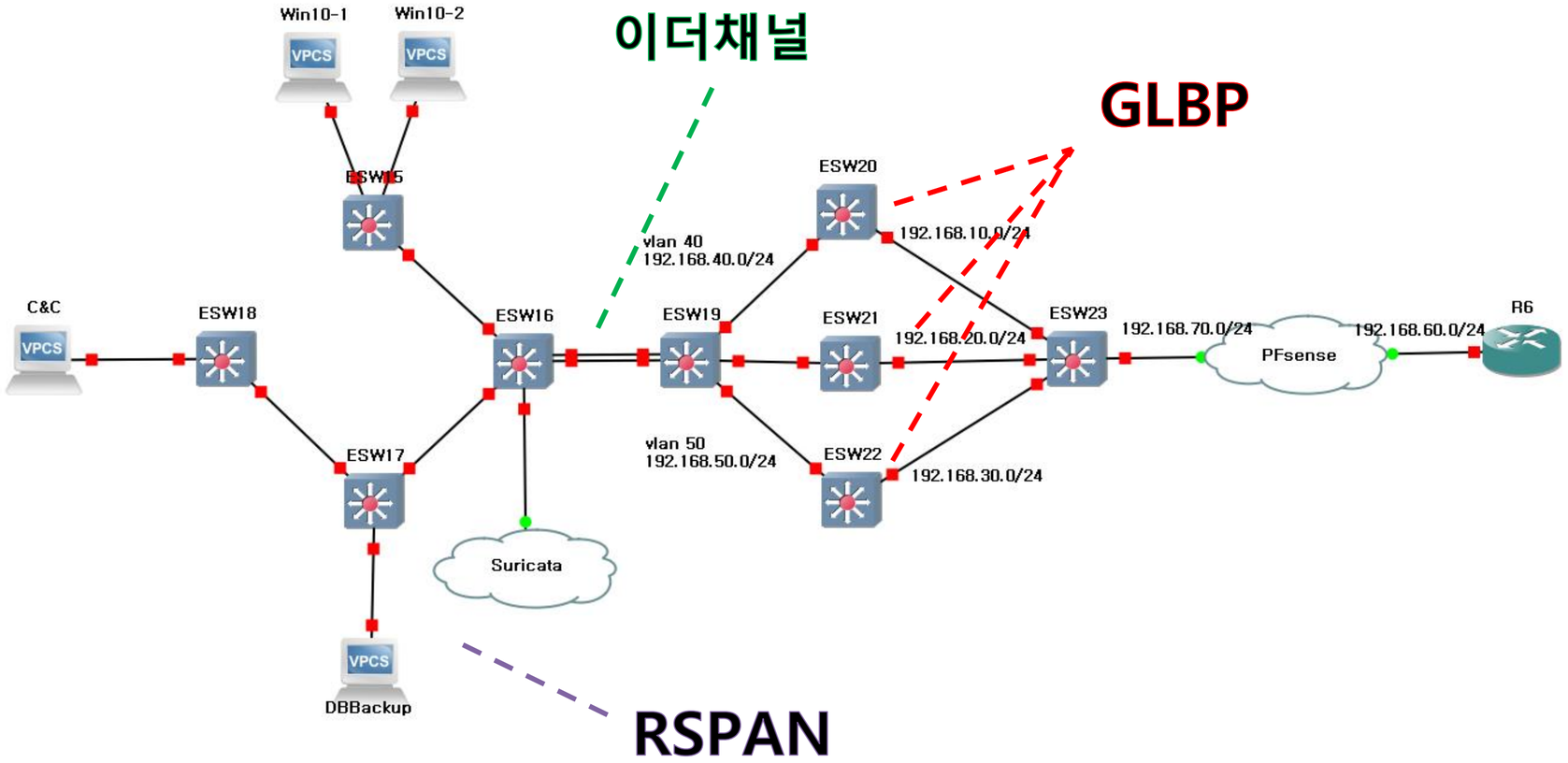
```
SW8#sh spanning-tree bri

VLAN30
  Spanning tree enabled protocol ieee
  Root ID     Priority    8192
              Address     c40b.5164.0001
              Cost        19
              Port        44 (FastEthernet1/3)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    28672
              Address     c40c.1a60.0002
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                    Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/1      128.42   128    19 BKN    19 28672 c40c.1a60.0002 128.42
FastEthernet1/3      128.44   128    19 FWD     0  8192 c40b.5164.0001 128.45
```

Secondary

STP

Root와 Secondary 스위치 확인

IDC(캐나다) 1


Win10-1
Win10-2
VPCS
VPCS
이더채널
GLBP
ESW15
ESW20
vlan 40
192.168.40.0/24
192.168.10.0/24
C&C
VPCS
ESW18
ESW16
ESW19
ESW21
ESW23
192.168.20.0/24
192.168.70.0/24
PFsense
192.168.60.0/24
R6
vlan 50
192.168.50.0/24
ESW17
ESW22
192.168.30.0/24
Suricata
VPCS
DBBackup
RSPAN

GLBP

vlan 40 Active

```
Vl40        1    -   150 Active   192.168.40.3    local           192.168.40.2
Vl40        1    1   -   Listen   0007.b400.0101  192.168.40.2    -
Vl40        1    2   -   Active   0007.b400.0102  local           -
ESW8#
```

vlan 50 Active

```
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Vl50        1    -   150 Active   192.168.50.3    local           192.168.50.2
Vl50        1    1   -   Listen   0007.b400.0101  192.168.50.2    -
Vl50        1    3   -   Active   0007.b400.0103  local           -
ESW10#
```

vlan 40, 50 Standby

```
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Vl40        1    -   120 Standby  192.168.40.3    192.168.40.1    local
Vl40        1    1   -   Active   0007.b400.0101  local           -
Vl40        1    2   -   Listen   0007.b400.0102  192.168.40.1    -
Vl50        1    -   120 Standby  192.168.50.3    192.168.50.1    local
Vl50        1    1   -   Active   0007.b400.0101  local           -
Vl50        1    3   -   Listen   0007.b400.0103  192.168.50.1    -
ESW9#
```

RSPAN

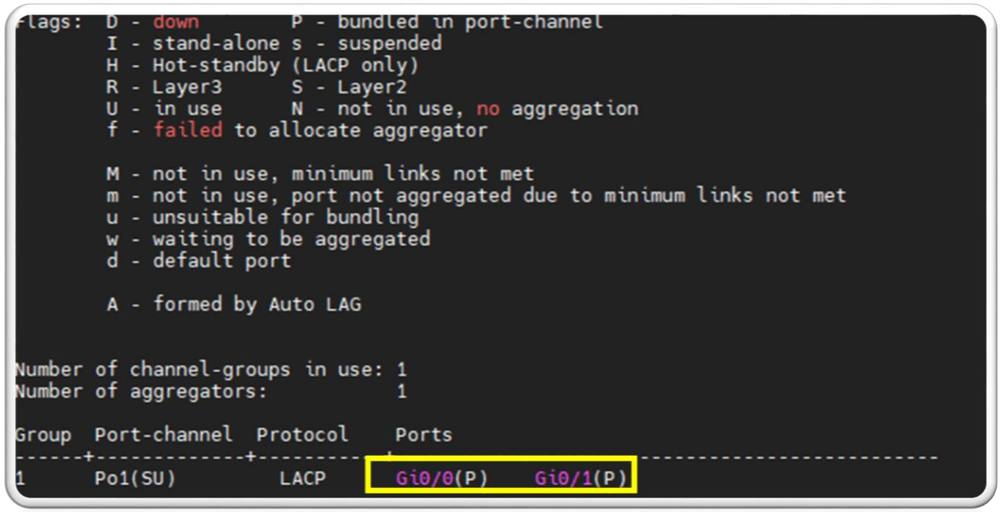
미러링 할 트래픽을 g1/0 포트로 보내기

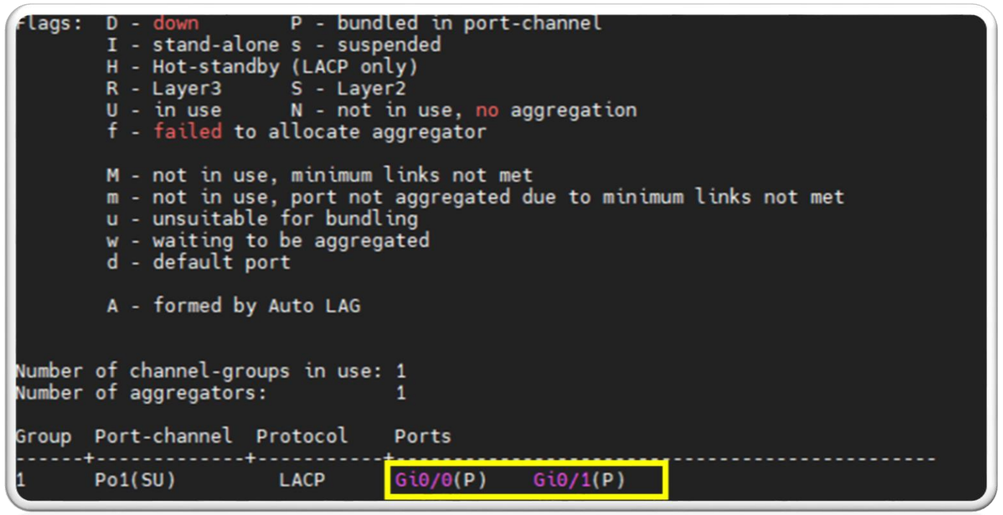
```
Session 1
---------
Type                      : Remote Destination Session
Source RSPAN VLAN         : 100
Destination Ports         : Gi1/0
    Encapsulation         : Native
```

```
Session 1
---------
Type                      : Remote Source Session
Source Ports              :
    Both                  : Gi0/0-1
Dest RSPAN VLAN           : 100
```

```
Session 1
---------
Type                      : Remote Source Session
Source Ports              :
    Both                  : Gi0/0-1
Dest RSPAN VLAN           : 100
```

```
Session 1
---------
Type                      : Remote Source Session
Source Ports              :
    Both                  : Gi0/0
Dest RSPAN VLAN           : 100
```

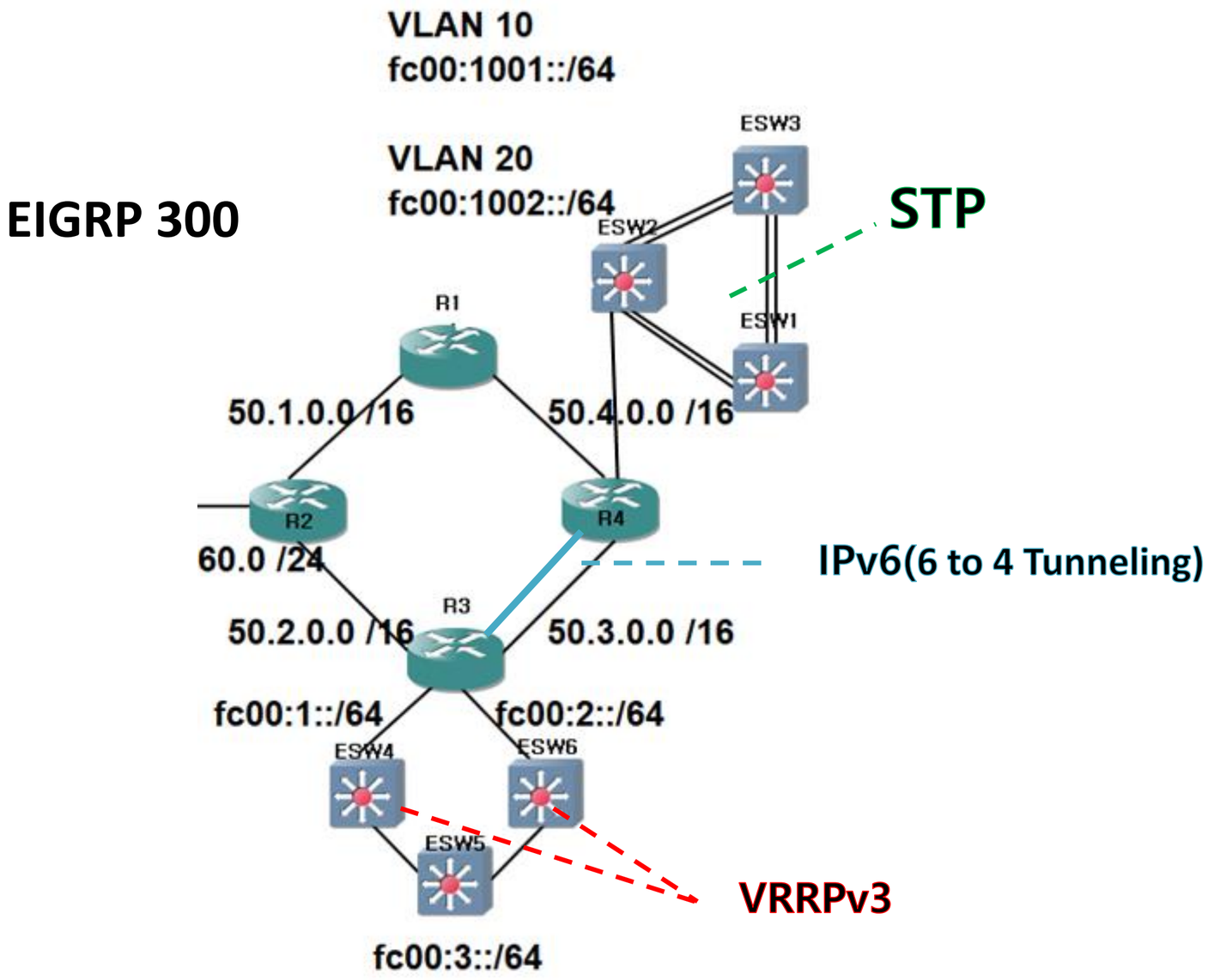




이더채널

스위치간 LACP 연결
포트 채널 (SU)상태 확인

IDC(캐나다) 2


VLAN 10
fc00:1001::/64
VLAN 20
fc00:1002::/64
EIGRP 300
ESW3
ESW2
ESW1
STP
R1
50.1.0.0 /16
50.4.0.0 /16
R2
R4
60.0 /24
IPv6(6 to 4 Tunneling)
R3
50.2.0.0 /16
50.3.0.0 /16
fc00:1::/64
fc00:2::/64
ESW4
ESW6
ESW5
VRRPv3
fc00:3::/64

IPv6
(6 to 4 Tunneling)

IPv6 대역 라우팅 테이블 확인

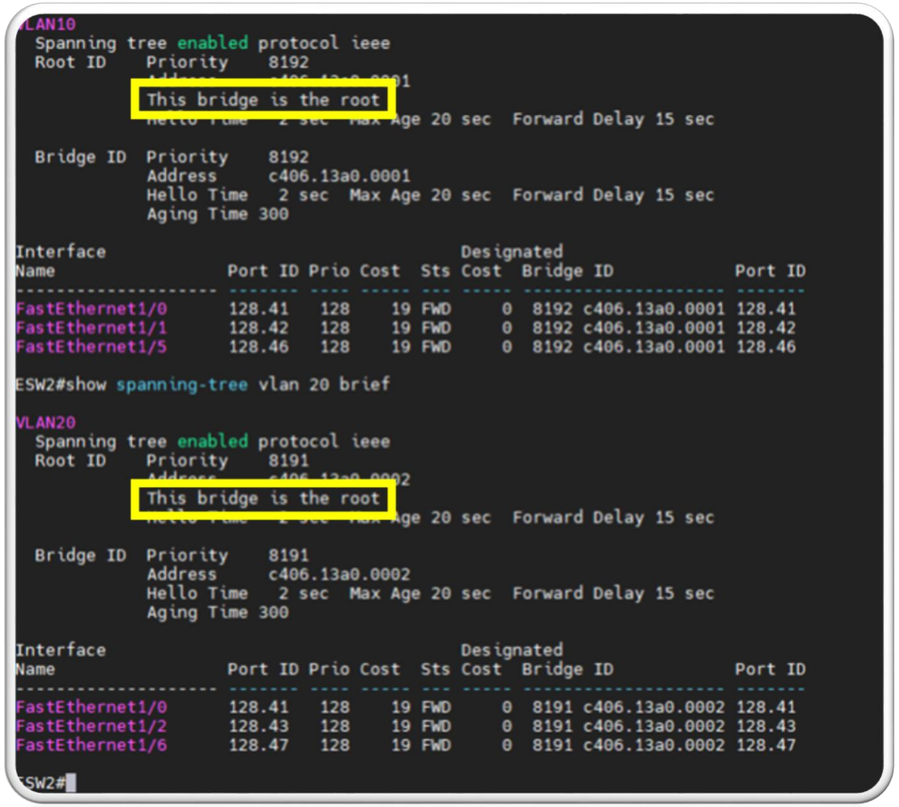
```
IPv6 Routing Table - Default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S   FC00:1::/64 [1/0]
     via Tunnel119, directly connected
S   FC00:2::/64 [1/0]
     via Tunnel119, directly connected
S   FC00:3::/64 [1/0]
     via Tunnel119, directly connected
C   FC00:1001::/64 [0/0]
     via FastEthernet0/0.10, directly connected
L   FC00:1001::1/128 [0/0]
     via FastEthernet0/0.10, receive
C   FC00:1002::/64 [0/0]
     via FastEthernet0/0.20, directly connected
L   FC00:1002::1/128 [0/0]
     via FastEthernet0/0.20, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

VRRPv3

Master와 Backup상태 확인

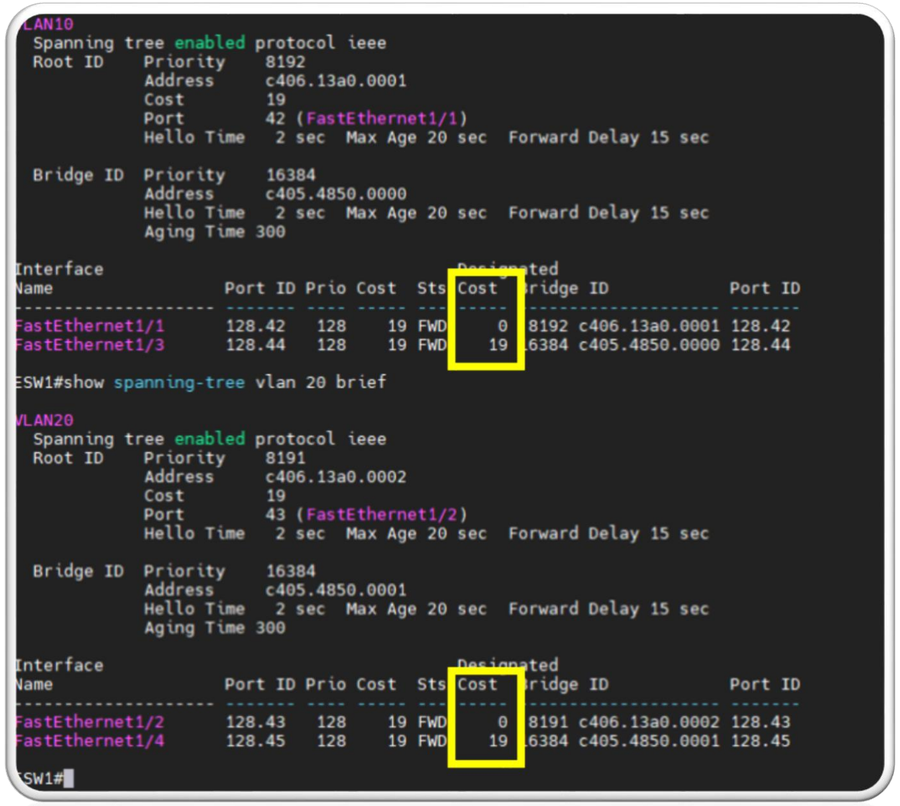
```
GigabitEthernet0/1 - Group 1 - Address-Family IPv6
  State is MASTER
  State duration 20 hours 40 mins 40 secs
  Virtual IP address is FE80::1
  Virtual secondary IP addresses:
    FC00:3::3/64
  Virtual MAC address is 0000.5E00.0201
  Advertisement interval is 1000 msec
  Preemption enabled, delay min 60 secs (0 msec remaining)
  Priority is 150
    Track object 1 state UP decrement 60
  Master Router is FE80::E6A:E8FF:FE4B:1 (local), priority is 150
  Master Advertisement interval is 1000 msec (expires in 39 msec)
  Master Down interval is unknown
```

```
GigabitEthernet0/1 - Group 1 - Address-Family IPv6
  State is BACKUP
  State duration 20 hours 45 mins 2 secs
  Virtual IP address is FE80::1
  Virtual secondary IP addresses:
    FC00:3::3/64
  Virtual MAC address is 0000.5E00.0201
  Advertisement interval is 1000 msec
  Preemption enabled, delay min 60 secs (0 msec remaining)
  Priority is 90
    Track object 1 state UP decrement 60
  Master Router is FE80::E6A:E8FF:FE4B:1, priority is 150
  Master Advertisement interval is 1000 msec (learned)
  Master Down interval is 3648 msec (expires in 2956 msec)
```



```
VLAN10
  Spanning tree enabled protocol ieee
  Root ID     Priority    8192
              Address     c406.13a0.0001
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    8192
              Address     c406.13a0.0001
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                   Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/0      128.41   128     19 FWD     0  8192 c406.13a0.0001 128.41
FastEthernet1/1      128.42   128     19 FWD     0  8192 c406.13a0.0001 128.42
FastEthernet1/5      128.46   128     19 FWD     0  8192 c406.13a0.0001 128.46

ESW2#show spanning-tree vlan 20 brief

VLAN20
  Spanning tree enabled protocol ieee
  Root ID     Priority    8191
              Address     c406.13a0.0002
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    8191
              Address     c406.13a0.0002
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                   Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/0      128.41   128     19 FWD     0  8191 c406.13a0.0002 128.41
FastEthernet1/2      128.43   128     19 FWD     0  8191 c406.13a0.0002 128.43
FastEthernet1/6      128.47   128     19 FWD     0  8191 c406.13a0.0002 128.47

ESW2#
```

Root



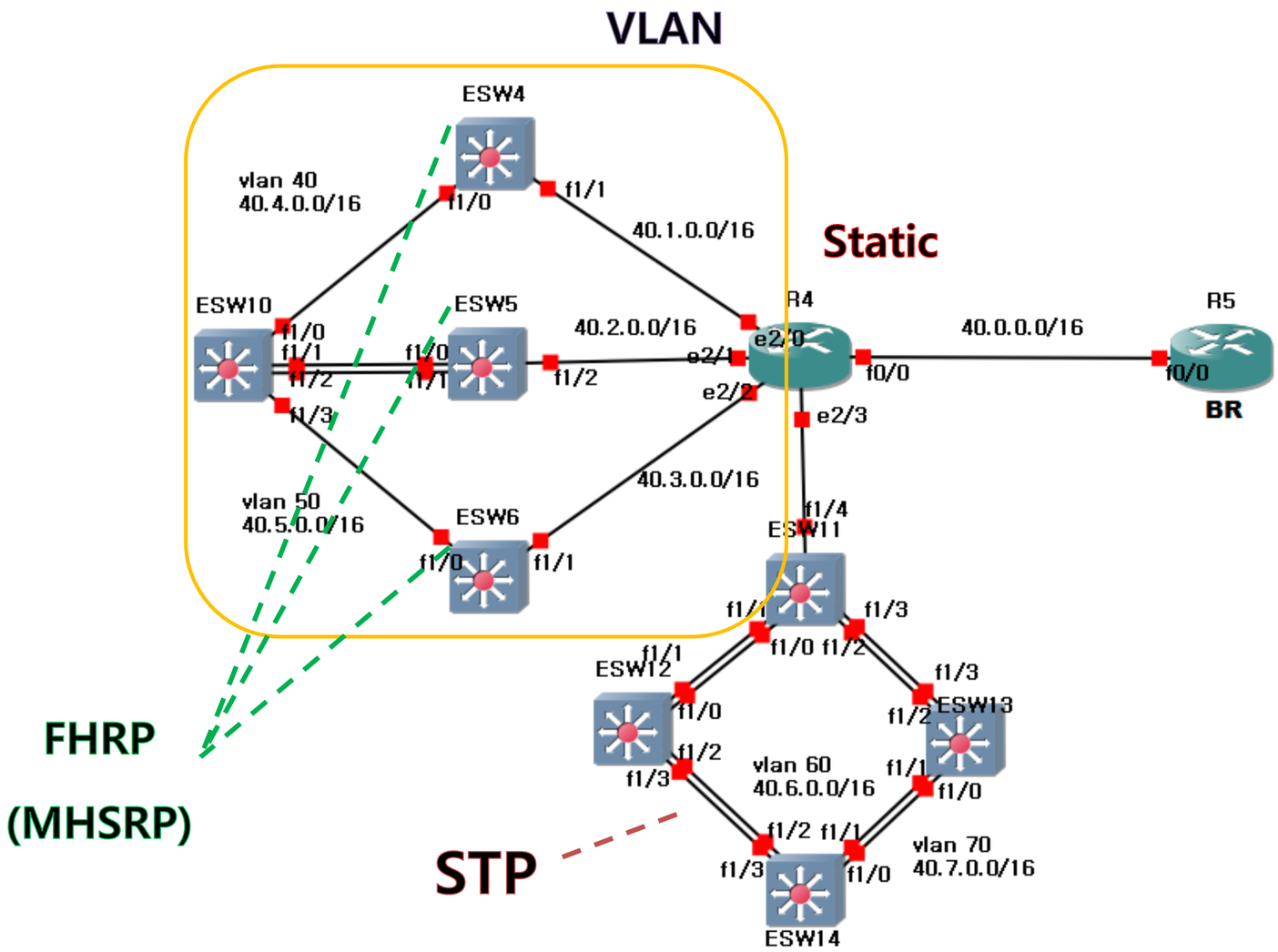
```
VLAN10
  Spanning tree enabled protocol ieee
  Root ID     Priority    8192
              Address     c406.13a0.0001
              Cost        19
              Port        42 (FastEthernet1/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    16384
              Address     c405.4850.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                   Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/1      128.42   128     19 FWD     0  8192 c406.13a0.0001 128.42
FastEthernet1/3      128.44   128     19 FWD    19  6384 c405.4850.0000 128.44

ESW1#show spanning-tree vlan 20 brief

VLAN20
  Spanning tree enabled protocol ieee
  Root ID     Priority    8191
              Address     c406.13a0.0002
              Cost        19
              Port        43 (FastEthernet1/2)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    16384
              Address     c405.4850.0001
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                   Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/2      128.43   128     19 FWD     0  8191 c406.13a0.0002 128.43
FastEthernet1/4      128.45   128     19 FWD    19  6384 c405.4850.0001 128.45

ESW1#
```

Secondary

STP

Root와 Secondary 스위치 확인

알래스카지사


VLAN
ESW4
vlan 40
40.4.0.0/16
f1/0
f1/1
40.1.0.0/16
Static
ESW10
ESW5
R4
R5
f1/0
f1/1
f1/2
f1/3
40.2.0.0/16
e2/0
e2/1
e2/2
e2/3
f0/0
40.0.0.0/16
BR
vlan 50
40.5.0.0/16
ESW6
40.3.0.0/16
f1/4
ESW11
f1/3
ESW12
ESW13
vlan 60
40.6.0.0/16
vlan 70
40.7.0.0/16
ESW14
FHRP
(MHSRP)
STP

FHRP (MHSRP)

액티브-액티브(Active-Active)
로드밸런싱 확인

```
ESW4#sh standby bri
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Vl40        40  110  P Active   local           40.4.0.252      40.4.0.254
Vl50        50  80   P Listen   40.5.0.253      40.5.0.252      40.5.0.254
```

```
ESW5#sh standby bri
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Vl40        40  80   P Standby  40.4.0.253      local           40.4.0.254
Vl50        50  80   P Standby  40.5.0.253      local           40.5.0.254
```

```
ESW6#sh standby bri
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Vl40        40  80   P Listen   40.4.0.253      40.4.0.252      40.4.0.254
Vl50        50  100  P Active   local           40.5.0.252      40.5.0.254
```

```
     21.0.0.0/16 is subnetted, 1 subnets
C       21.21.0.0 is directly connected, Loopback0
     40.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C       40.0.0.0/24 is directly connected, FastEthernet0/0
C       40.1.0.0/16 is directly connected, Ethernet2/0
C       40.2.0.0/16 is directly connected, Ethernet2/1
C       40.3.0.0/16 is directly connected, Ethernet2/2
S       40.4.0.0/16 [1/0] via 40.1.0.2
S       40.5.0.0/16 [1/0] via 40.3.0.2
C       40.6.0.0/16 is directly connected, Ethernet2/3.60
C       40.7.0.0/16 is directly connected, Ethernet2/3.70
S*   0.0.0.0/0 [1/0] via 40.0.0.1
R4#
```

Static Routing

외부 대역을 향한
Default Static Routing

```
C       40.7.0.0/16 is directly con
S*   0.0.0.0/0 [1/0] via 40.0.0.1
R4#
```

```
VLAN60
  Spanning tree enabled protocol ieee
  Root ID     Priority    4096
              Address     c40f.1a14.0001
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4096
              Address     c40f.1a14.0001
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                   Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/0      128.41   128    19 BKN     0  4096 c40f.1a14.0001 128.41
FastEthernet1/2      128.43   128    19 FWD     0  4096 c40f.1a14.0001 128.43
FastEthernet1/4      128.45   128    19 FWD     0  4096 c40f.1a14.0001 128.45
```

Root

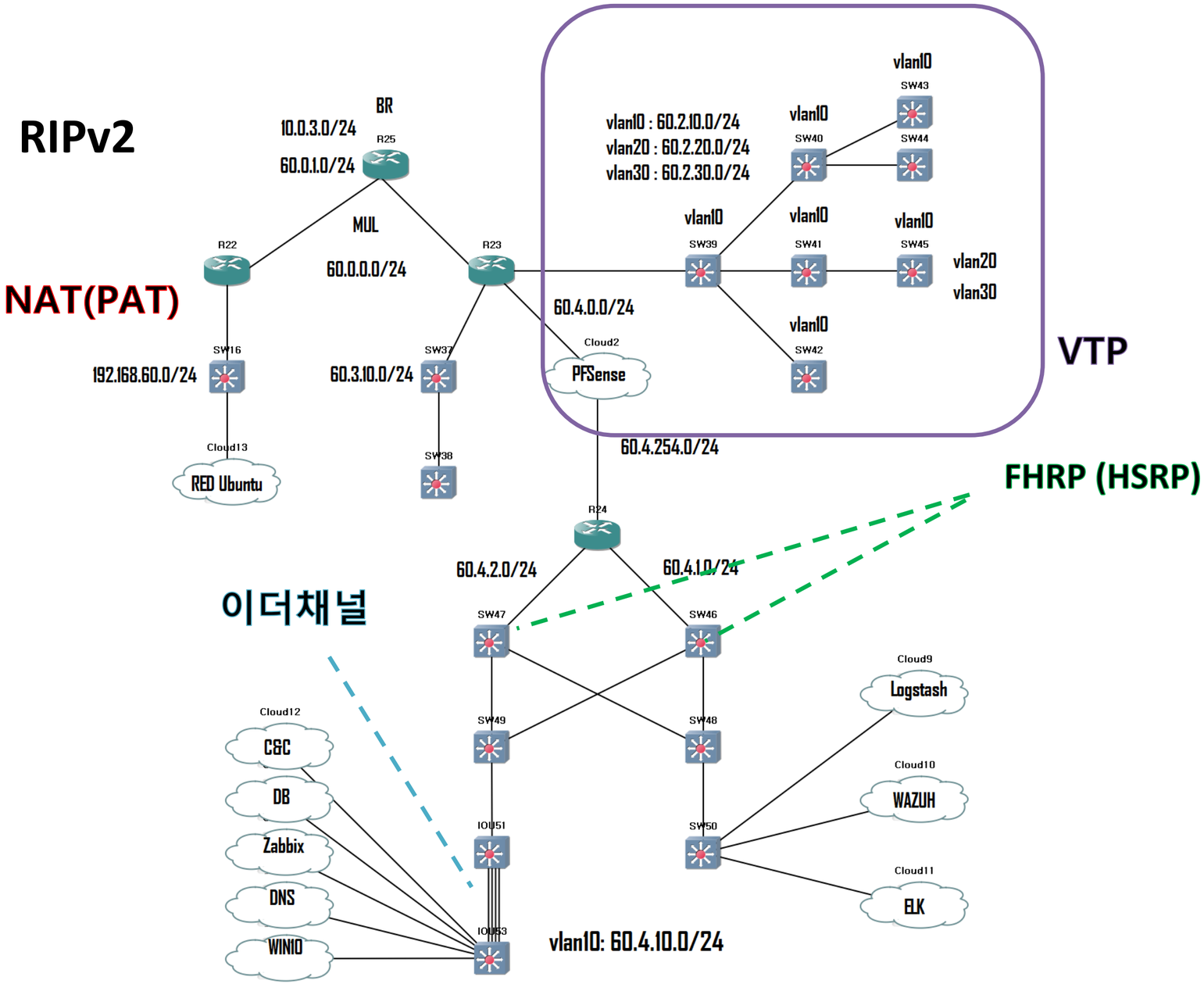
```
VLAN60
  Spanning tree enabled protocol ieee
  Root ID     Priority    4096
              Address     c40f.1a14.0001
              Cost        19
              Port        43 (FastEthernet1/2)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    8192
              Address     c411.72b4.0001
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                   Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/1      128.42   128    19 BKN    19  8192 c411.72b4.0001 128.42
FastEthernet1/2      128.43   128    19 FWD     0  4096 c40f.1a14.0001 128.43
```

Secondary

STP

Root와 Secondary 스위치 확인

관제 센터 (멕시코)


RIPv2
NAT(PAT)
BR
10.0.3.0/24
R25
60.0.1.0/24
MUL
60.0.0.0/24
R22
R23
SW16
192.168.60.0/24
Cloud13
RED Ubuntu
SW37
60.3.10.0/24
SW38
60.4.0.0/24
Cloud2
PFSense
60.4.254.0/24
vlan10 : 60.2.10.0/24
vlan20 : 60.2.20.0/24
vlan30 : 60.2.30.0/24
vlan10
SW43
SW40
SW44
SW39
SW41
SW45
SW42
vlan20
vlan30
VTP
FHRP (HSRP)
이더채널
R24
60.4.2.0/24
60.4.1.0/24
SW47
SW46
SW49
SW48
IOU51
IOU53
SW50
Cloud12
C&C
DB
Zabbix
DNS
WIN10
Cloud9
Logstash
Cloud10
WAZUH
Cloud11
ELK
vlan10: 60.4.10.0/24

FHRP (HSRP)

Active, Standby 상태 확인

```
SW46#sh standby bri
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Vl10        10  120    Active   local           60.4.10.253     60.4.10.200
SW46#sh standby
Vlan10 - Group 10 (version 2)
  State is Active
    2 state changes, last state change 02:59:30
  Virtual IP address is 60.4.10.200
  Active virtual MAC address is 0000.0c9f.f00a
    Local virtual MAC address is 0000.0c9f.f00a (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.780 secs
  Preemption disabled
  Active router is local
  Standby router is 60.4.10.253, priority 100 (expires in 8.552 sec)
  Priority 120 (configured 120)
  IP redundancy name is "hsrp-Vl10-10" (default)
```

```
SW47#sh standby bri
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Vl10        10  100  P Standby  60.4.10.254     local           60.4.10.200
SW47#sh standby
Vlan10 - Group 10 (version 2)
  State is Standby
    1 state change, last state change 03:02:24
  Virtual IP address is 60.4.10.200
  Active virtual MAC address is 0000.0c9f.f00a
    Local virtual MAC address is 0000.0c9f.f00a (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.520 secs
  Preemption enabled
  Active router is 60.4.10.254, priority 120 (expires in 7.268 sec)
  Standby router is local
  Priority 100 (default 100)
  IP redundancy name is "hsrp-Vl10-10" (default)
```

VTP

서버 역할과 상태 확인

```
SW39#sh vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 68
Number of existing VLANs        : 8
VTP Operating Mode              : Server
VTP Domain Name                 : cisco
```

VTP Server

```
SW44#sh vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 68
Number of existing VLANs        : 8
VTP Operating Mode              : Client
VTP Domain Name                 : cisco
```

VTP Client

```
SW45#sh vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 68
Number of existing VLANs        : 8
VTP Operating Mode              : Transparent
VTP Domain Name                 : cisco
```

VTP Transparent

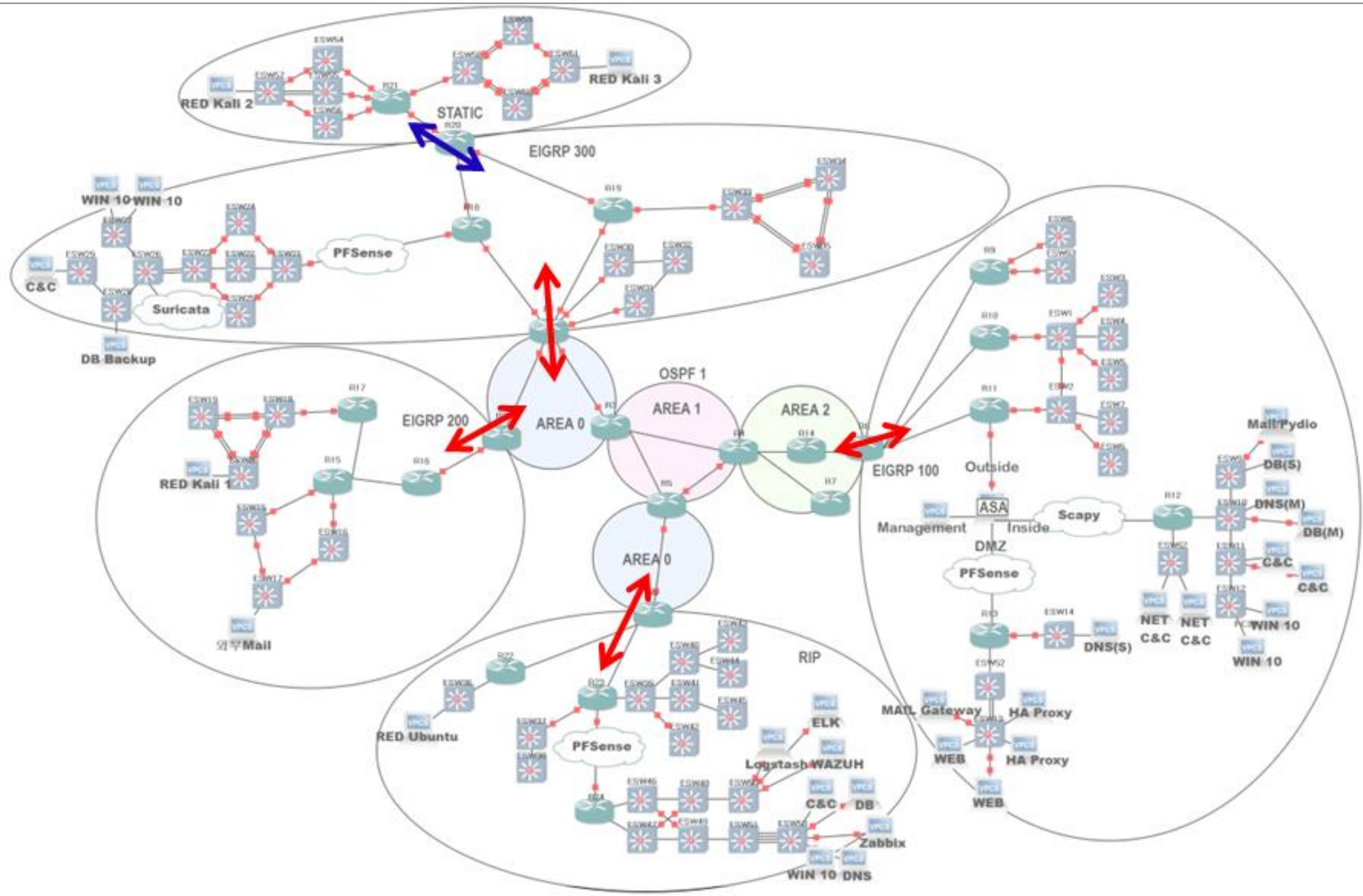
이더채널

스위치간 LACP 연결
포트 채널 (SU)상태 확인

```
Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Et0/0(P)    Et0/1(P)    Et0/2(P)
                                 Et0/3(P)
```


```
Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Et0/0(P)    Et0/1(P)    Et0/2(P)
                                 Et0/3(P)
```

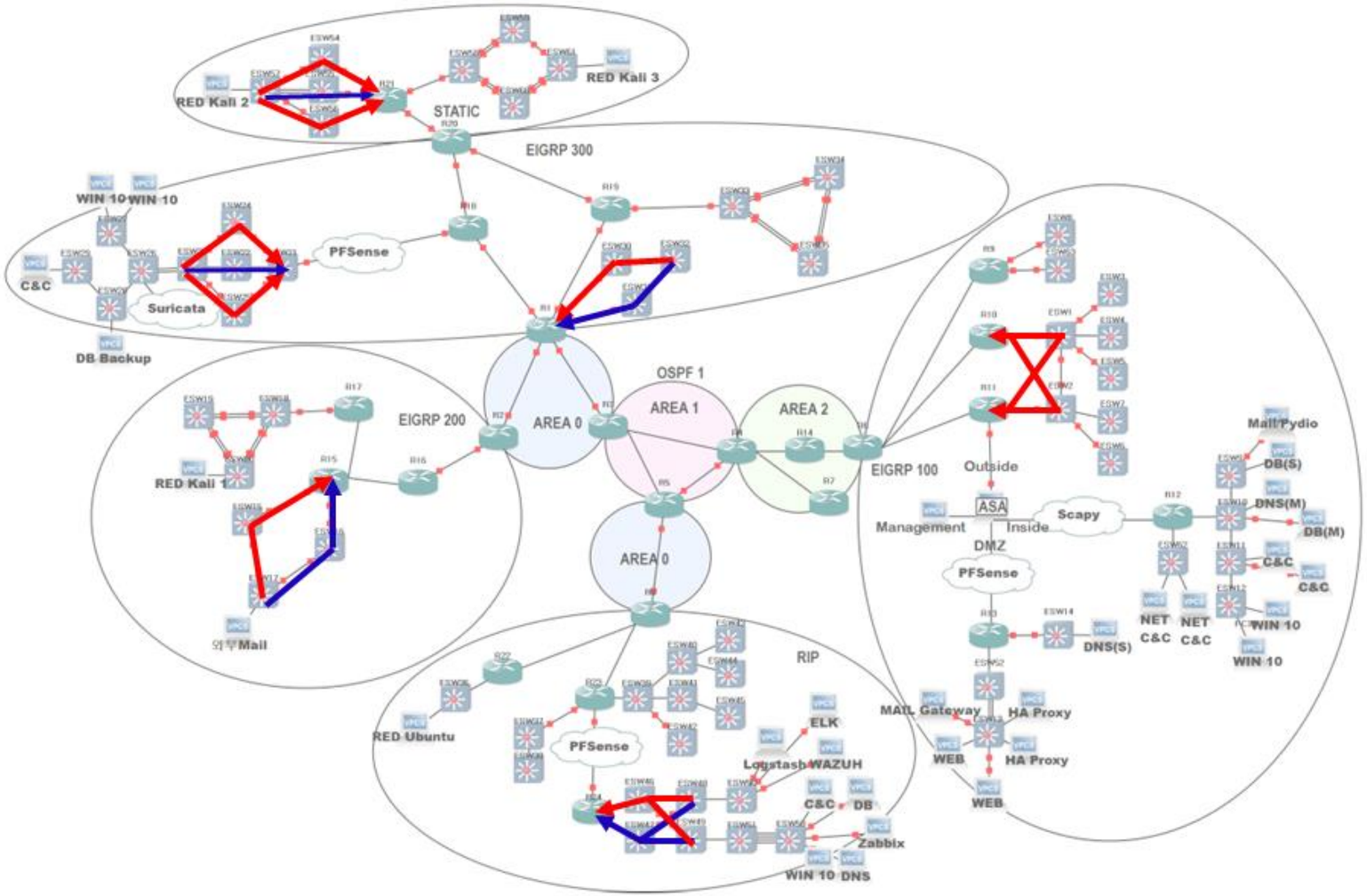
글로벌 네트워크 토폴로지: 서로 다른 라우팅 프로토콜 간 라우팅 정보 공유 경로



빨강: 동적 라우팅 프로토콜에서 라우팅 정보를 서로 재분배

파랑: 정적 라우팅

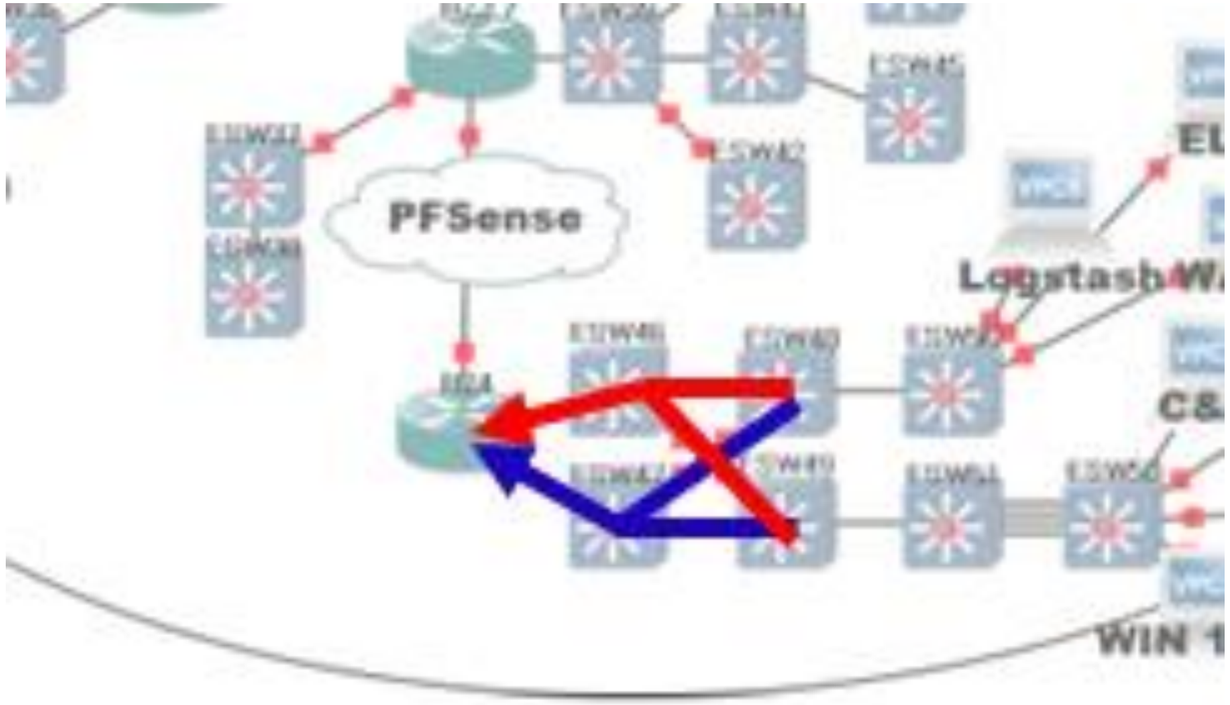
글로벌 네트워크 토폴로지: 게이트웨이 이중화(FHRP) 트래픽 흐름도



빨강: Active 경로

파랑: Backup 경로

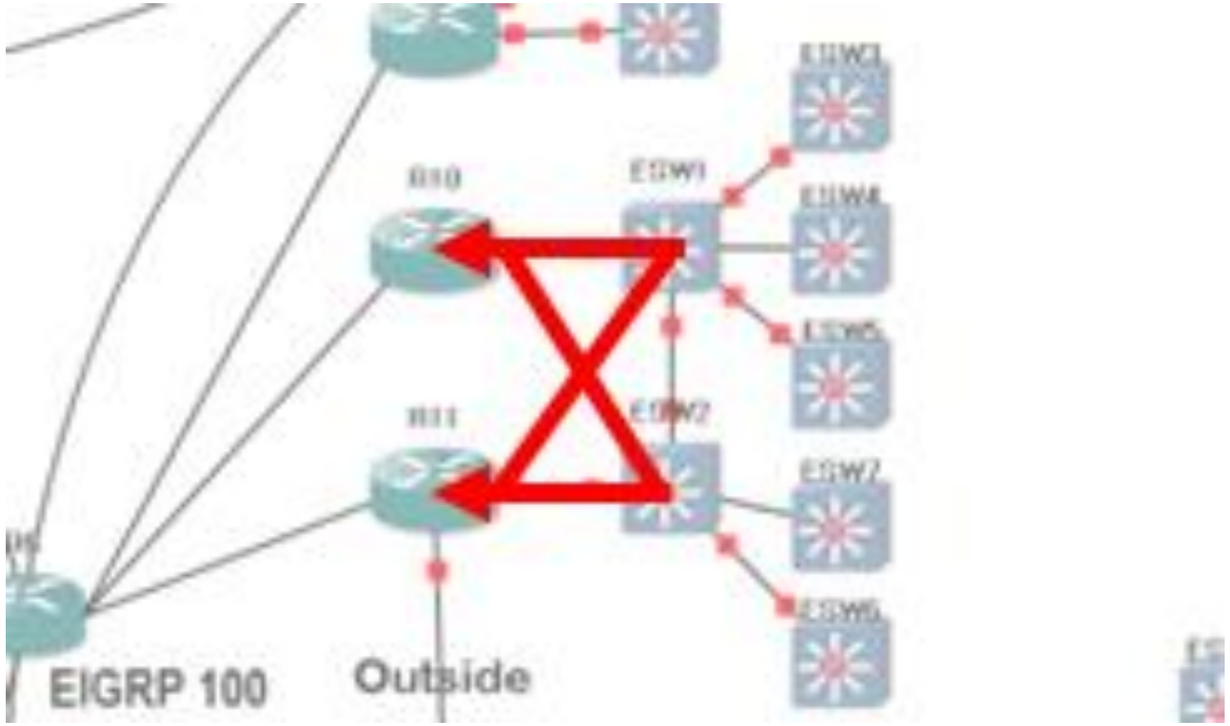
글로벌 네트워크 토폴로지: 게이트웨이 이중화(FHRP) 트래픽 흐름도



빨강: Active 경로

파랑: Backup 경로

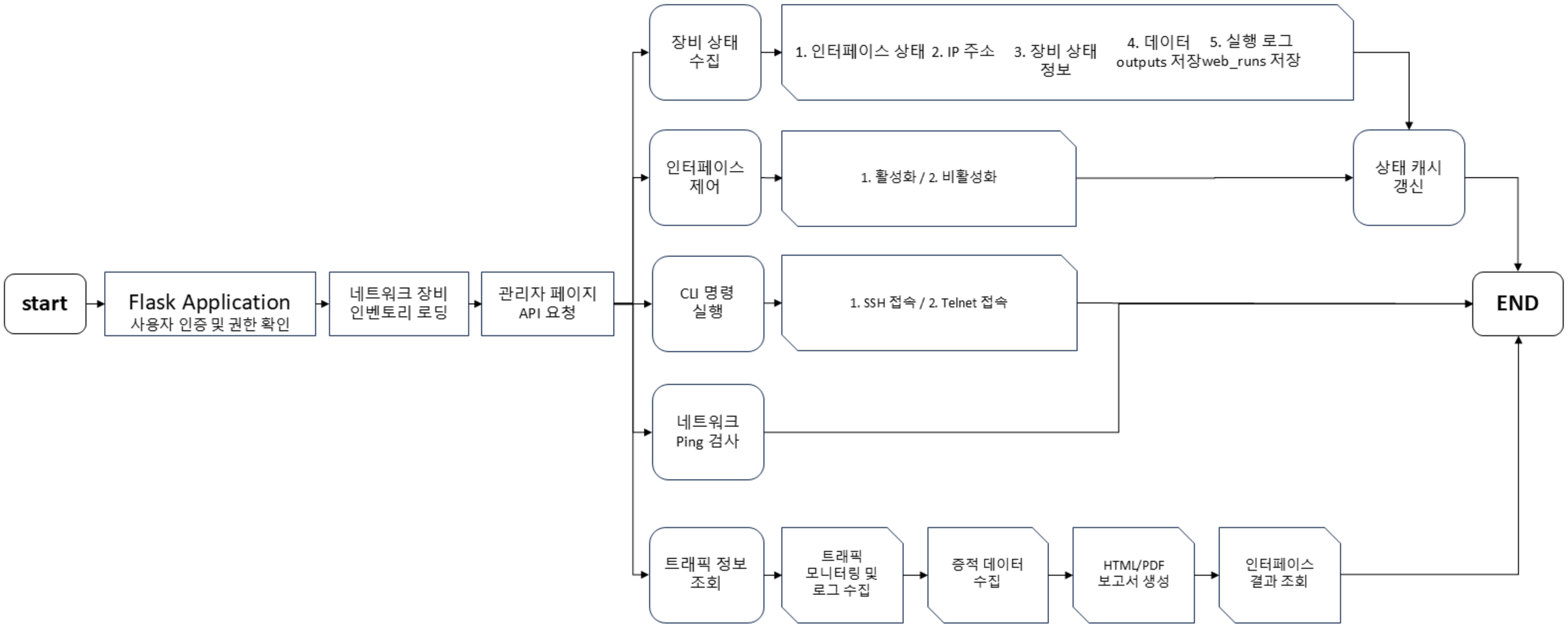
글로벌 네트워크 토폴로지: 게이트웨이 이중화(FHRP) 트래픽 흐름도



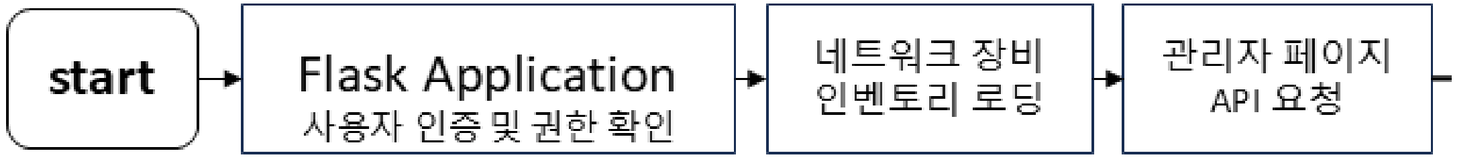
빨강: Active 경로

파랑: Backup 경로

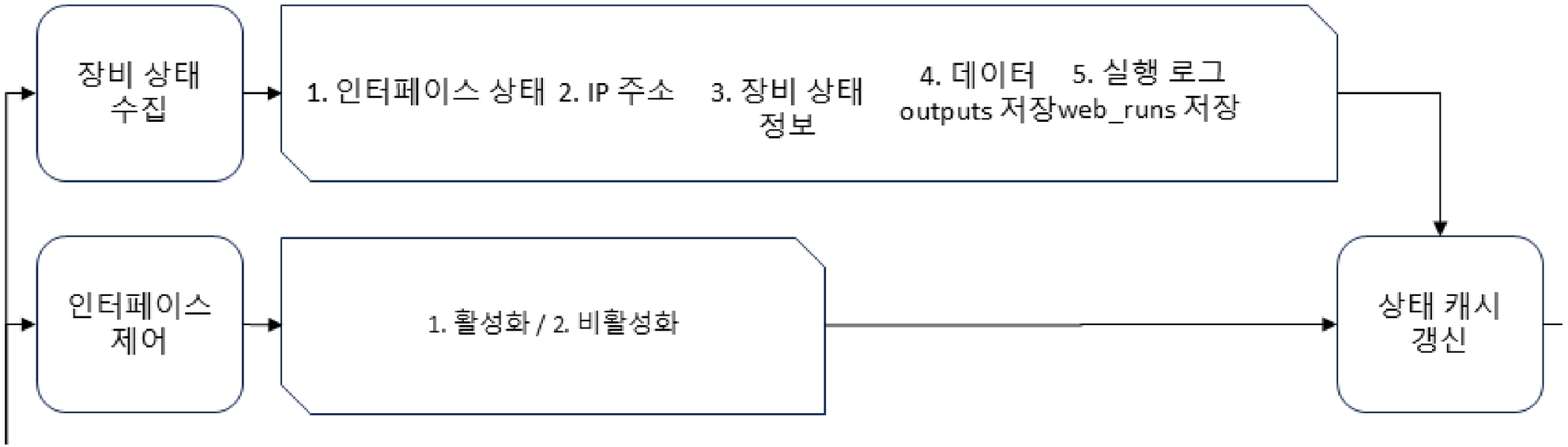
자동화 코드 흐름도


start
Flask Application
사용자 인증 및 권한 확인
네트워크 장비
인벤토리 로딩
관리자 페이지
API 요청
장비 상태
수집
1. 인터페이스 상태 2. IP 주소 3. 장비 상태
정보
4. 데이터
outputs 저장
5. 실행 로그
web_runs 저장
인터페이스
제어
1. 활성화 / 2. 비활성화
CLI 명령
실행
1. SSH 접속 / 2. Telnet 접속
네트워크
Ping 검사
트래픽 정보
조회
트래픽
모니터링 및
로그 수집
증적 데이터
수집
HTML/PDF
보고서 생성
인터페이스
결과 조회
상태 캐시
갱신
END

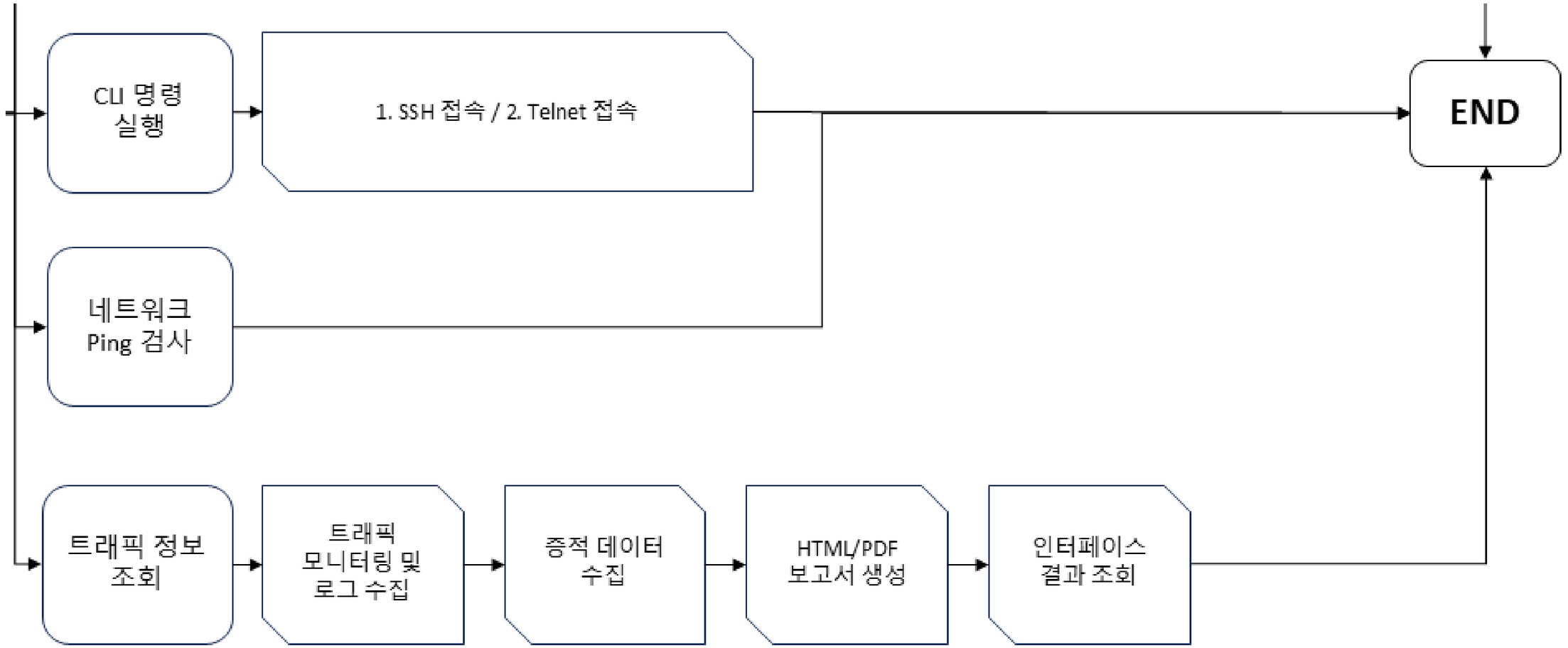
자동화 코드 흐름도


start
Flask Application
사용자 인증 및 권한 확인
네트워크 장비
인벤토리 로딩
관리자 페이지
API 요청

자동화 코드 흐름도


장비 상태 수집
1. 인터페이스 상태 2. IP 주소 3. 장비 상태 정보 4. 데이터 outputs 저장 5. 실행 로그 web_runs 저장
인터페이스 제어
1. 활성화 / 2. 비활성화
상태 캐시 갱신

자동화 코드 흐름도


CLI 명령
실행
1. SSH 접속 / 2. Telnet 접속
END
네트워크
Ping 검사
트래픽 정보
조회
트래픽
모니터링 및
로그 수집
증적 데이터
수집
HTML/PDF
보고서 생성
인터페이스
결과 조회

메인페이지

Router Monitor
Logged in as: admin (admin)

online

Command Center
Overview · CCP / MRTG 느낌

Navigation shortcuts

Overview
Device Dashboard
Run Logs
Outputs Explorer

outputs: /root/ansible/outputs
logs: /root/ansible/web_runs

Auto Refresh status

Overview 자동 갱신

* 장비 온라인/다운/트래픽 수치만 갱신

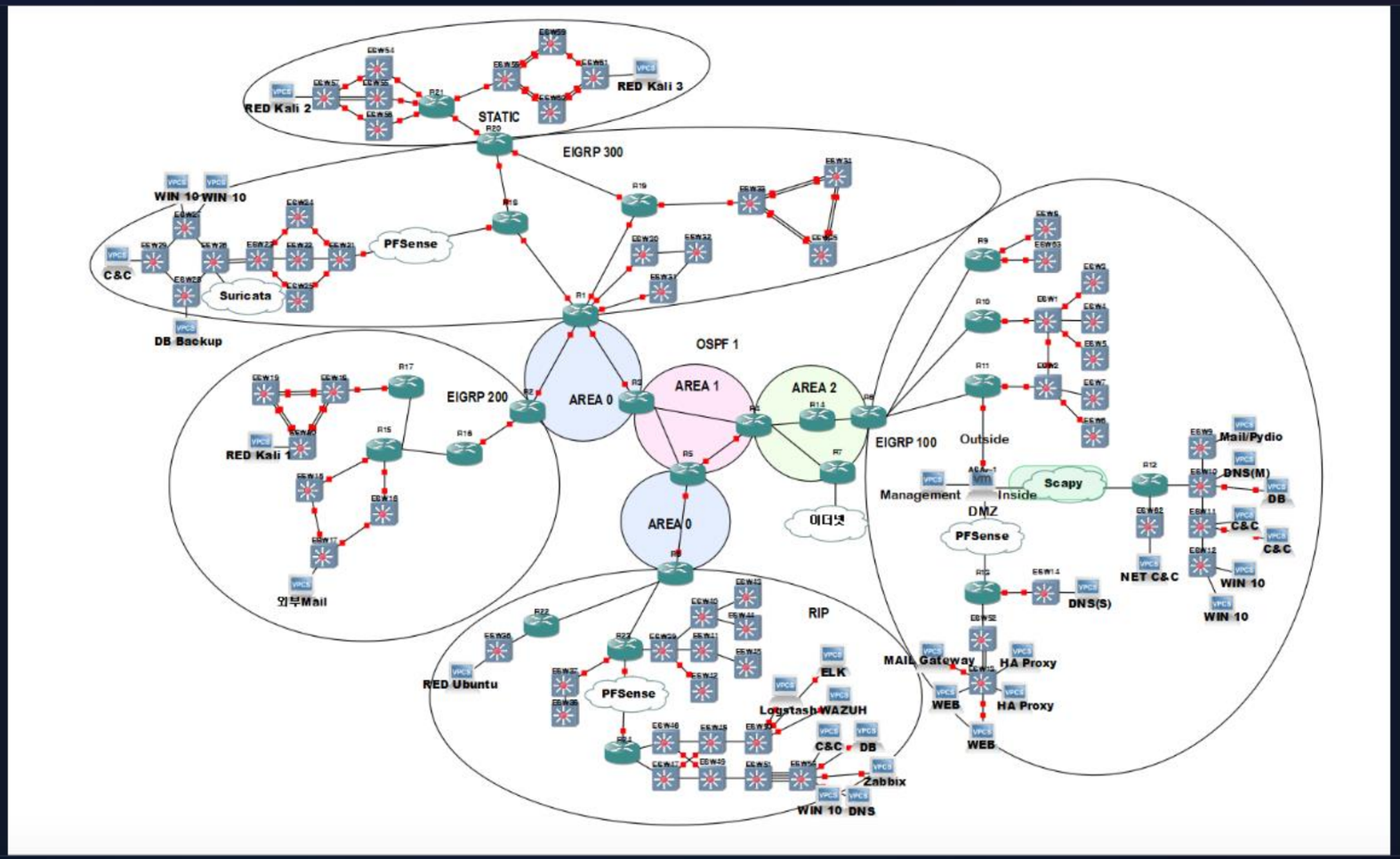
Logged in: admin (admin)

전체 라우터 상태 · 인터페이스 Down · 트래픽(IN/OUT)

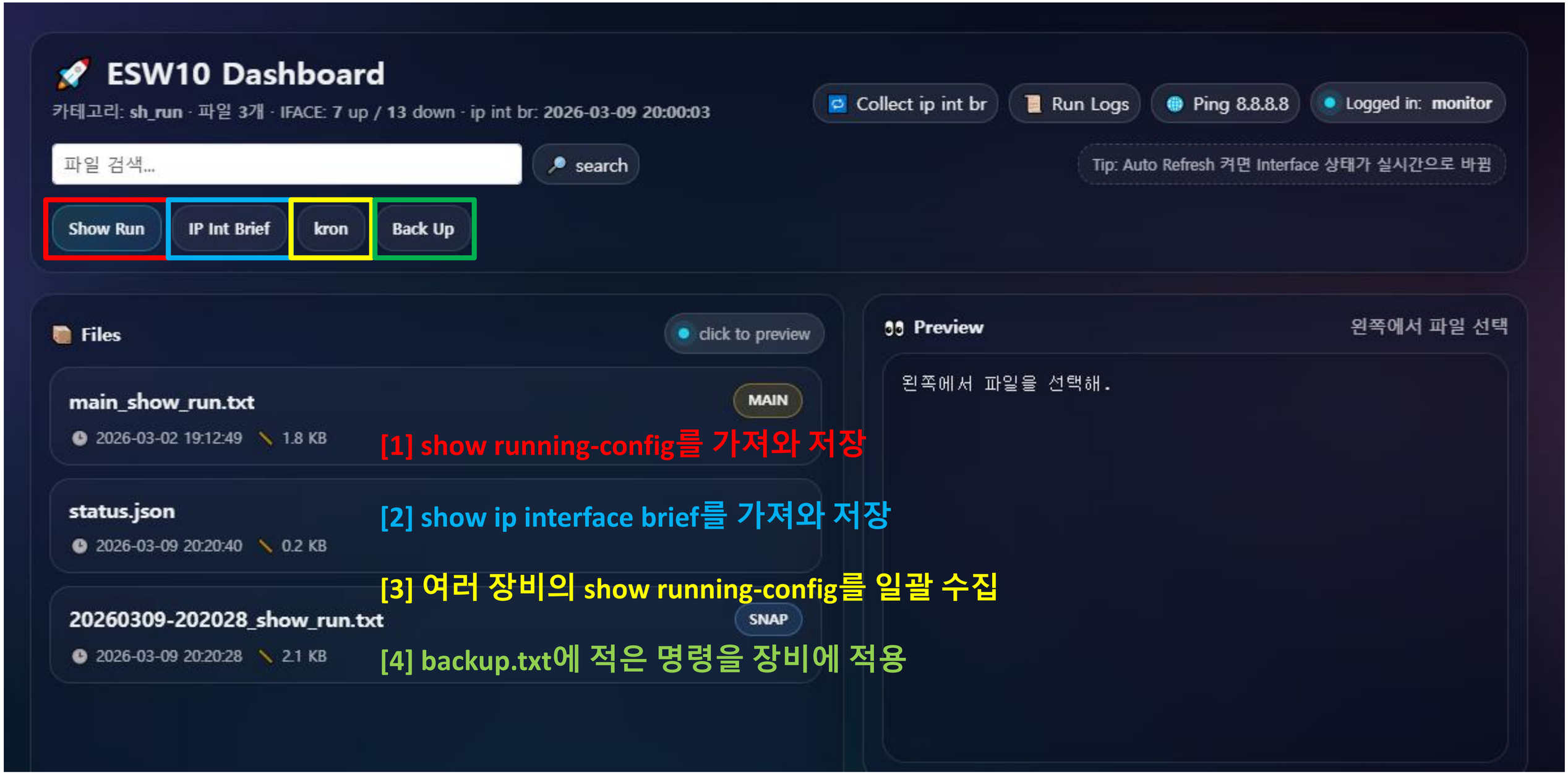
poll: 5s | ping all | logs

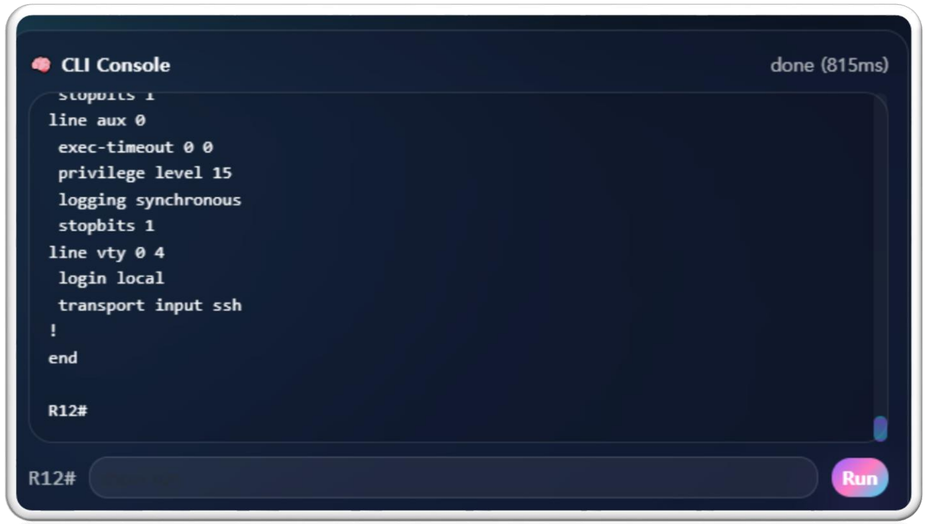
GNS3 Map

project: 0dd503c9-f39c-4312-8393-596f5a2bbe8c | refresh canvas | ↗ interactive map



대시보드


ESW10 Dashboard
카테고리: sh_run · 파일 3개 · IFACE: 7 up / 13 down · ip int br: 2026-03-09 20:00:03
Collect ip int br
Run Logs
Ping 8.8.8.8
Logged in: monitor
파일 검색...
search
Tip: Auto Refresh 켜면 Interface 상태가 실시간으로 바뀜
Show Run
IP Int Brief
kron
Back Up
Files
click to preview
Preview
왼쪽에서 파일 선택
왼쪽에서 파일을 선택해.
main_show_run.txt
MAIN
2026-03-02 19:12:49
1.8 KB
[1] show running-config를 가져와 저장
status.json
2026-03-09 20:20:40
0.2 KB
[2] show ip interface brief를 가져와 저장
[3] 여러 장비의 show running-config를 일괄 수집
20260309-202028_show_run.txt
SNAP
2026-03-09 20:20:28
2.1 KB
[4] backup.txt에 적은 명령을 장비에 적용

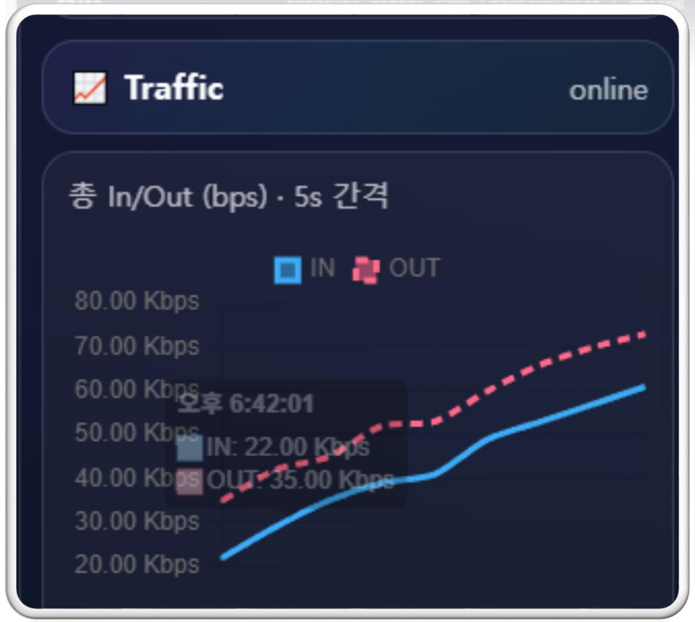


CLI 호출

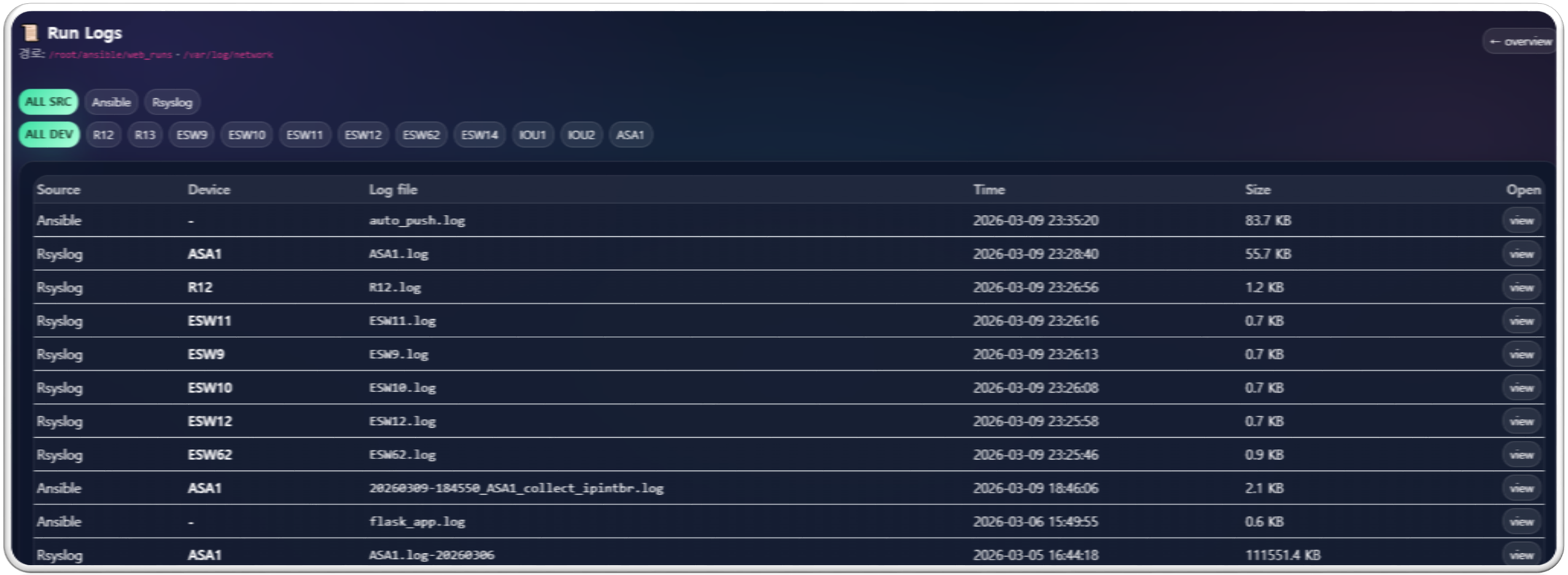
SSH / Telnet

인터페이스 상태 / 조정

장비별 LOG 파일 수집



네트워크 트래픽 통계



RSYSLOG 파일 생성 목록

서버 안정성 목표

서버 장애 예방을 위한 5가지 핵심 목표

1) 고가용성

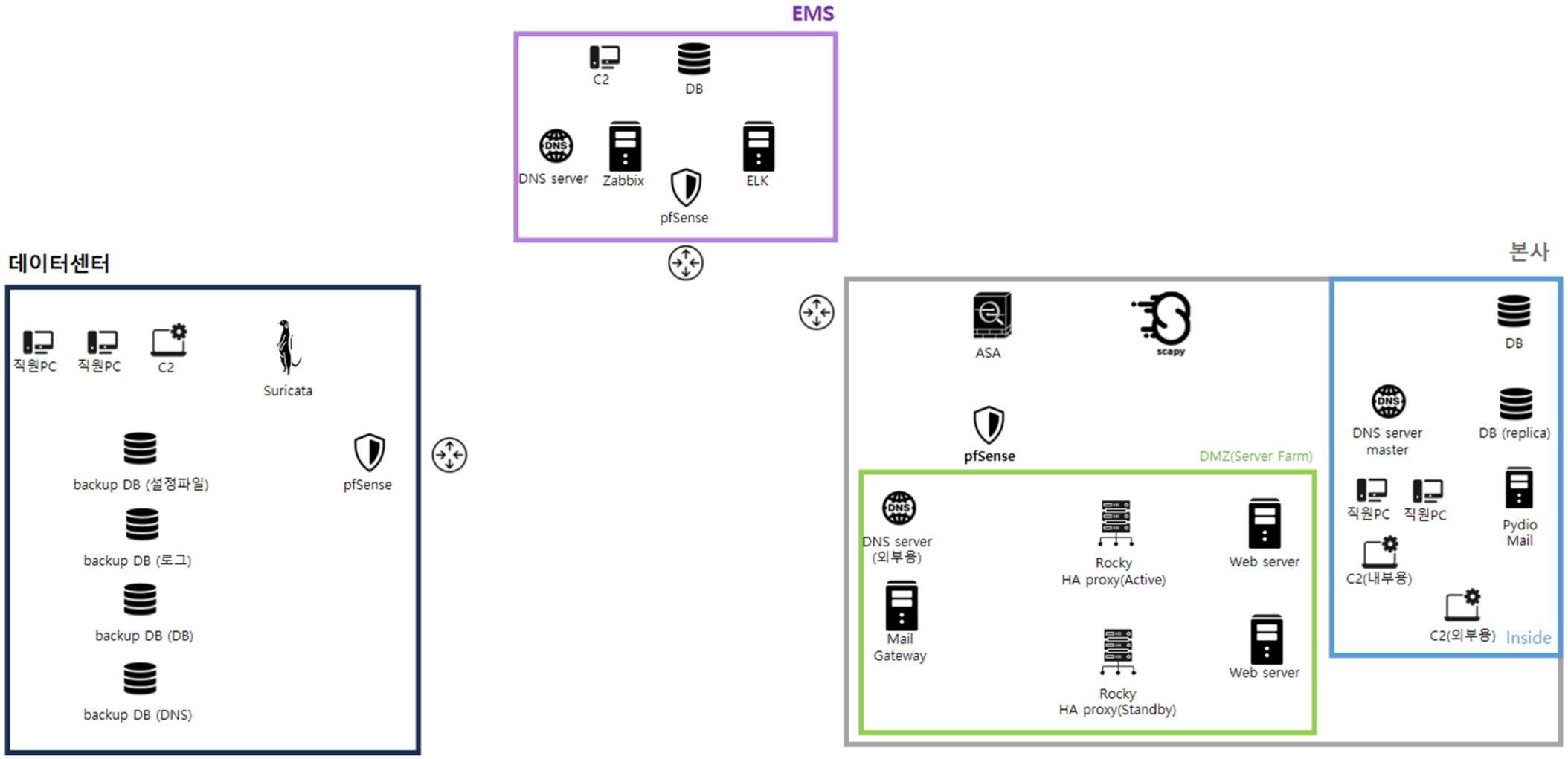
2) 복구

3) 보안

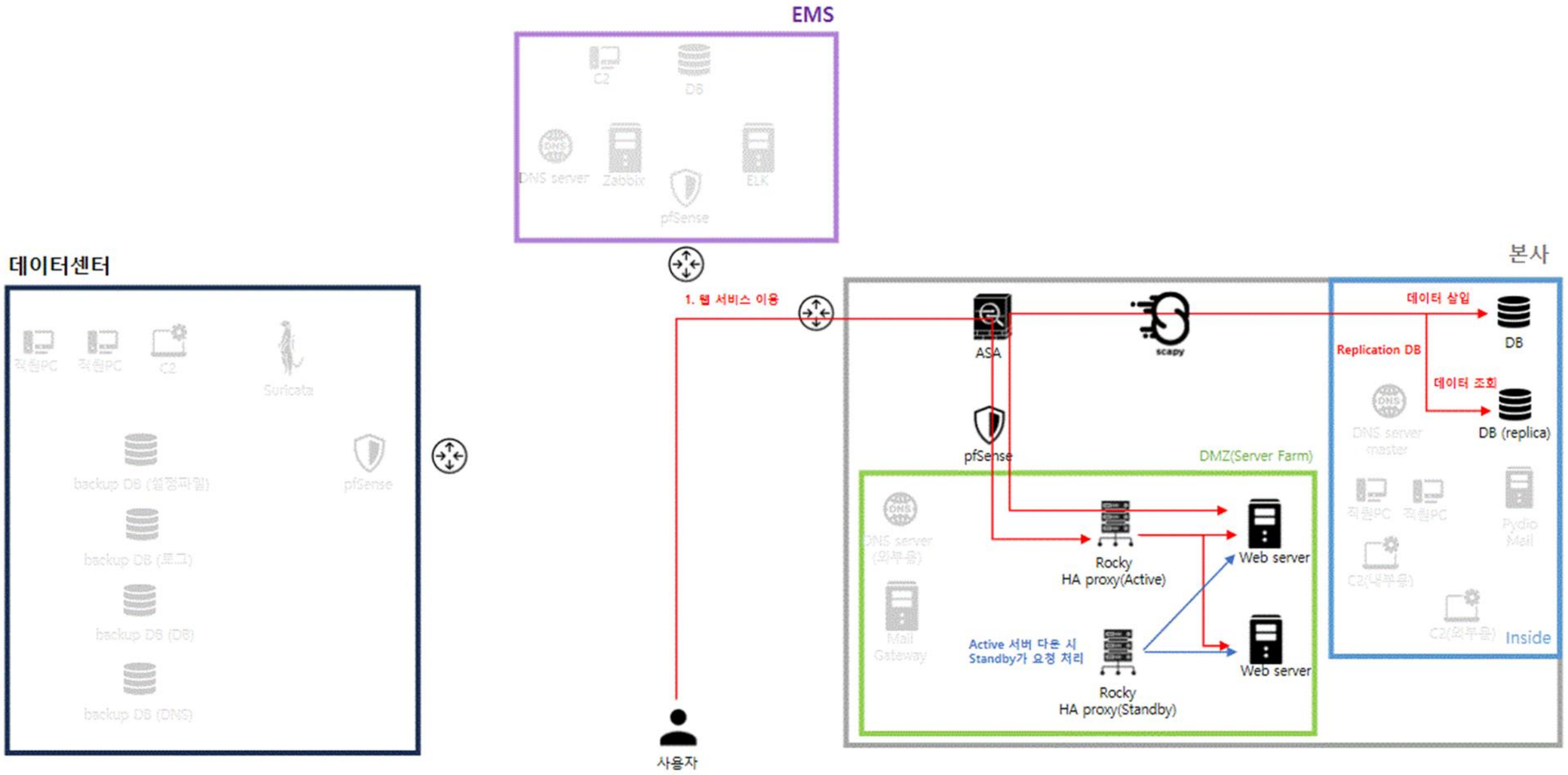
4) 자동화

5) 관제

전체 인프라 구성도

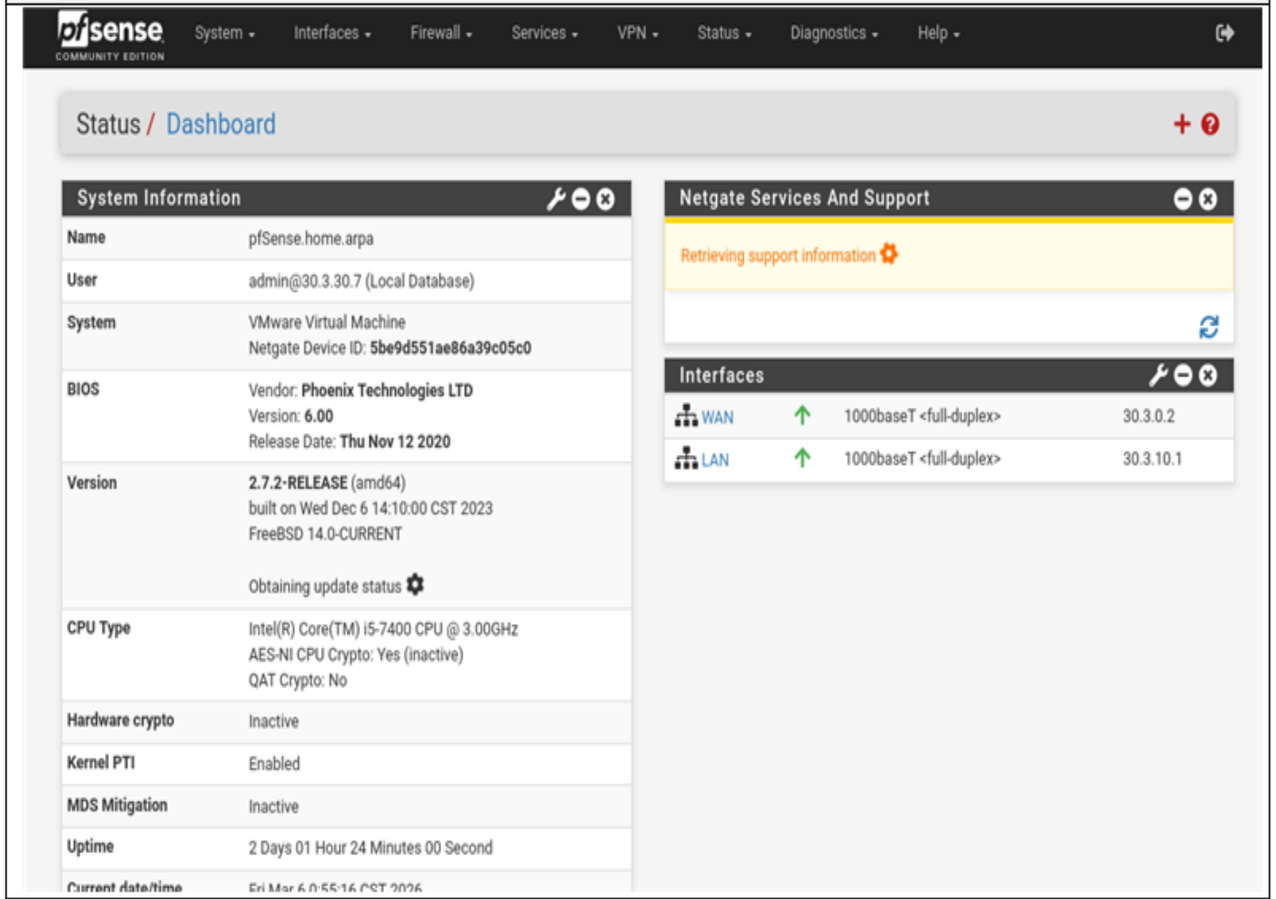

EMS
C2
DB
DNS server
Zabbix
ELK
pfSense
데이터센터
직원PC
직원PC
C2
Suricata
backup DB (설정파일)
pfSense
backup DB (로그)
backup DB (DB)
backup DB (DNS)
본사
ASA
scapy
pfSense
DMZ(Server Farm)
DNS server
(외부용)
Rocky
HA proxy(Active)
Web server
Mail
Gateway
Rocky
HA proxy(Standby)
Web server
DB
DNS server
master
DB (replica)
직원PC
직원PC
Pydio
Mail
C2(내부용)
C2(외부용)
Inside

웹 서비스 흐름도


EMS
C2
DB
DNS server
Zabbix
ELK
pfSense
데이터센터
직원PC
직원PC
C2
Suricata
backup DB (설정파일)
pfSense
backup DB (로그)
backup DB (DB)
backup DB (DNS)
본사
1. 웹 서비스 이용
ASA
scapy
데이터 삽입
DB
Replication DB
데이터 조회
DB (replica)
DNS server
master
pfSense
DMZ(Server Farm)
DNS server
(외부용)
Rocky
HA proxy(Active)
Web server
Mail
Gateway
Active 서버 다운 시
Standby가 요청 처리
Rocky
HA proxy(Standby)
Web server
직원PC
직원PC
Pydio
Mail
C2(내부용)
C2(외부용)
Inside
사용자

Pfsense 구축 결과

pfSense 홈페이지 접속



pfsense blacklist 설정

290 Matched Firewall Log Entries. (Maximum 500) Pause ■

Action	Time	Interface	Source	Destination	Protocol
X	Mar 6 07:53:38	WAN	172.16.28.140	30.3.10.1	ICMP
X	Mar 6 07:53:39	WAN	172.16.28.140	30.3.10.1	ICMP
X	Mar 6 07:53:41	WAN	172.16.28.140	30.3.10.1	ICMP
X	Mar 6 07:53:42	WAN	172.16.28.140	30.3.10.1	ICMP
X	Mar 6 07:53:43	WAN	172.16.28.140	30.3.10.1	ICMP

HA Proxy 구축 결과

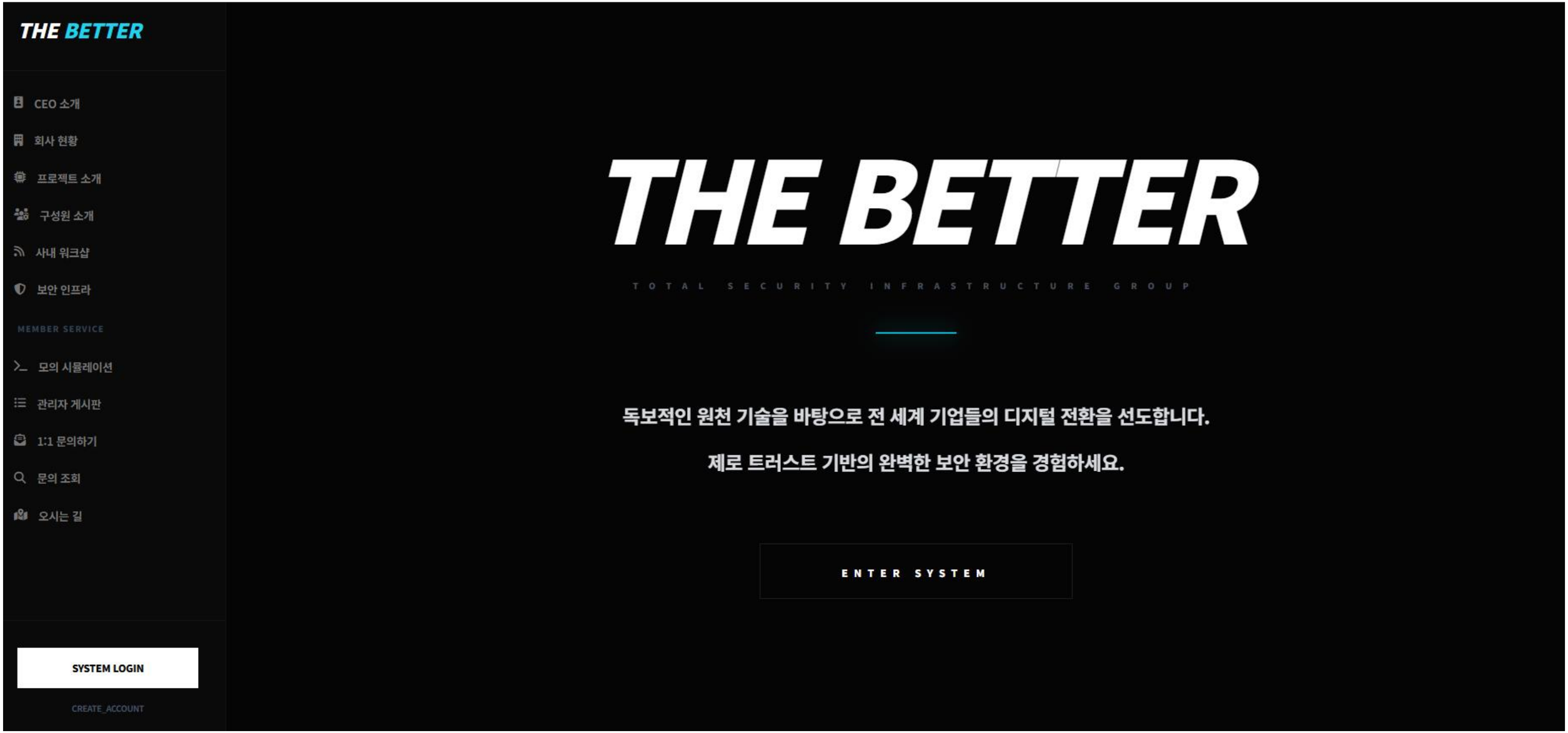
Active

```
[root@US-ha1-Rocky-wz haproxy]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0c:29:6e:75:66 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 30.3.30.4/24 brd 30.3.30.255 scope global noprefixroute ens160
       valid_lft forever preferred_lft forever
    inet 30.3.30.9/24 scope global secondary ens160
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe6e:7566/64 scope link noprefixroute
```

Stanby

```
[root@US-ha2-Rocky-wz ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0c:29:8f:72:d3 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 30.3.30.5/24 brd 30.3.30.255 scope global noprefixroute ens160
       valid_lft forever preferred_lft forever
    inet 30.3.30.9/24 scope global secondary ens160
       valid_lft forever preferred_lft forever
```

Web 구축 결과


THE BETTER
CEO 소개
회사 현황
프로젝트 소개
구성원 소개
사내 워크샵
보안 인프라
MEMBER SERVICE
모의 시뮬레이션
관리자 게시판
1:1 문의하기
문의 조회
오시는 길
SYSTEM LOGIN
CREATE_ACCOUNT
THE BETTER
TOTAL SECURITY INFRASTRUCTURE GROUP
독보적인 원천 기술을 바탕으로 전 세계 기업들의 디지털 전환을 선도합니다.
제로 트러스트 기반의 완벽한 보안 환경을 경험하세요.
ENTER SYSTEM

DB Replica 구축 결과

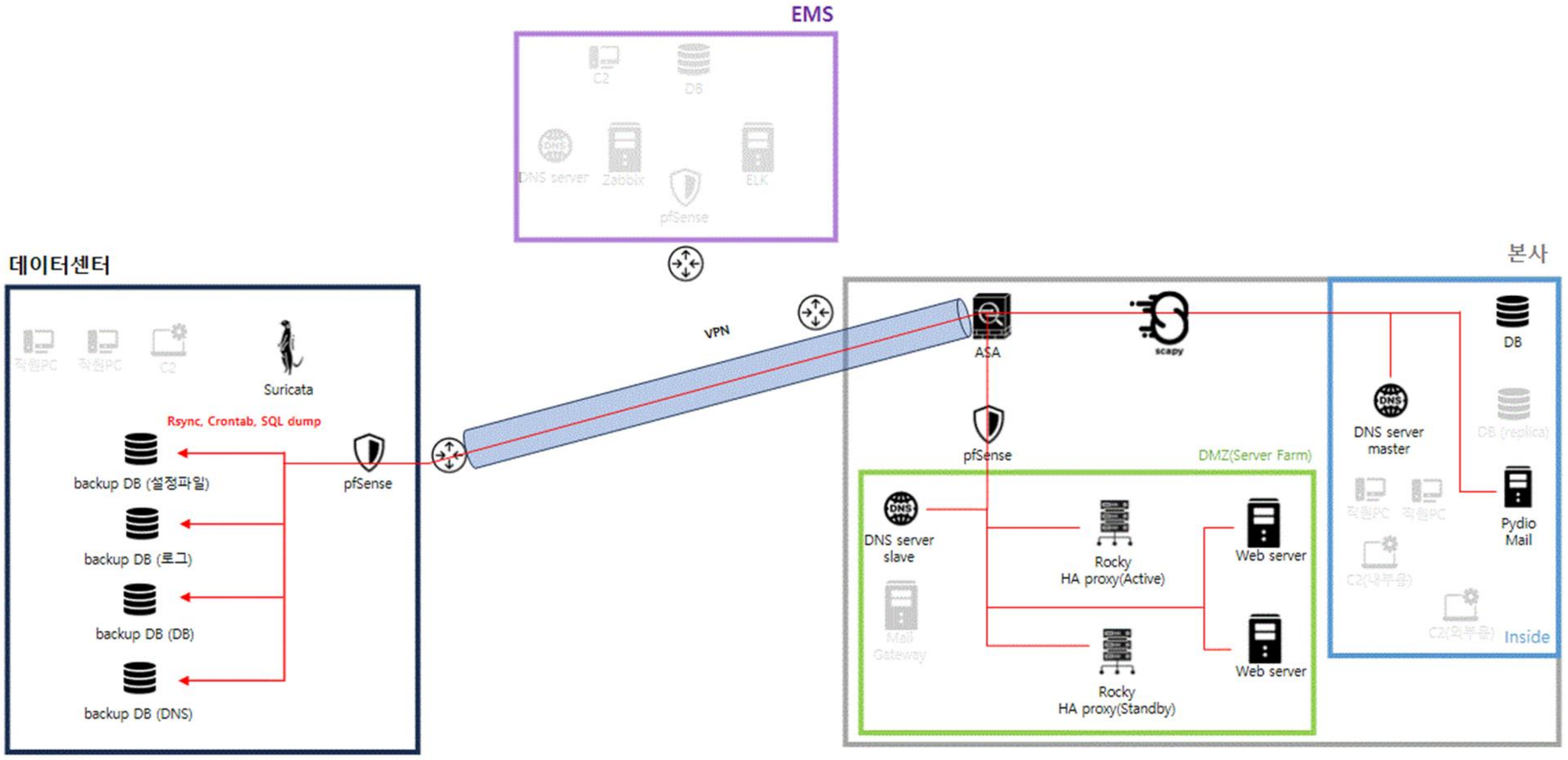
Master DB에서 Slave 확인

```
MariaDB [(none)]> show processlist;
+----+----------+---------------------+------+
| Id | User     | Host                | db   |
+----+----------+---------------------+------+
|  6 | repuser  | 192.168.30.3:49758  | NULL |
```

Slave에서 Master 요청 대기 상태

```
MariaDB [(none)]> show processlist;
+----+-------------+----------+------+-----------+------+-----------------------------------
| Id | User        | Host     | db   | Command   | Time | State
+----+-------------+----------+------+-----------+------+-----------------------------------
|  5 | system user |          | NULL | Slave_IO  | 39972 | Waiting for master to send event
|  6 | system user |          | NULL | Slave_SQL | 35021 | Slave has read all relay log; wait
```

백업 서비스 흐름도

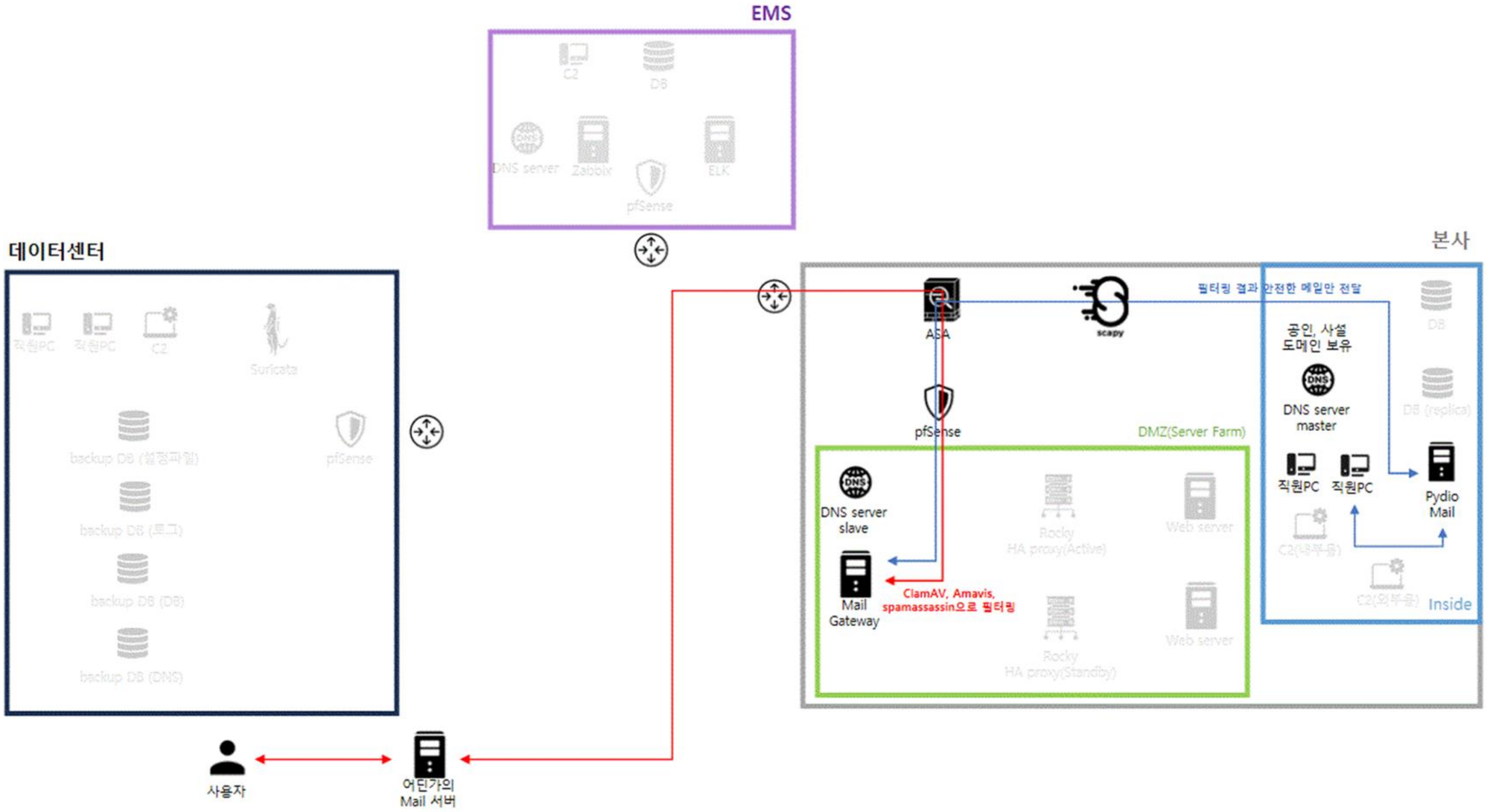

EMS
C2
DB
DNS server
Zabbix
ELK
pfSense
데이터센터
본사
VPN
작업PC
작업PC
C2
Suricata
Rsync, Crontab, SQL dump
backup DB (설정파일)
backup DB (로그)
backup DB (DB)
backup DB (DNS)
pfSense
ASA
scapy
pfSense
DMZ(Server Farm)
DNS server slave
Rocky HA proxy(Active)
Web server
Mail Gateway
Rocky HA proxy(Standby)
Web server
DB
DNS server master
DB (replica)
작업PC
작업PC
Pydio Mail
C2(내부용)
C2(외부용)
Inside

백업 서비스 구축 결과

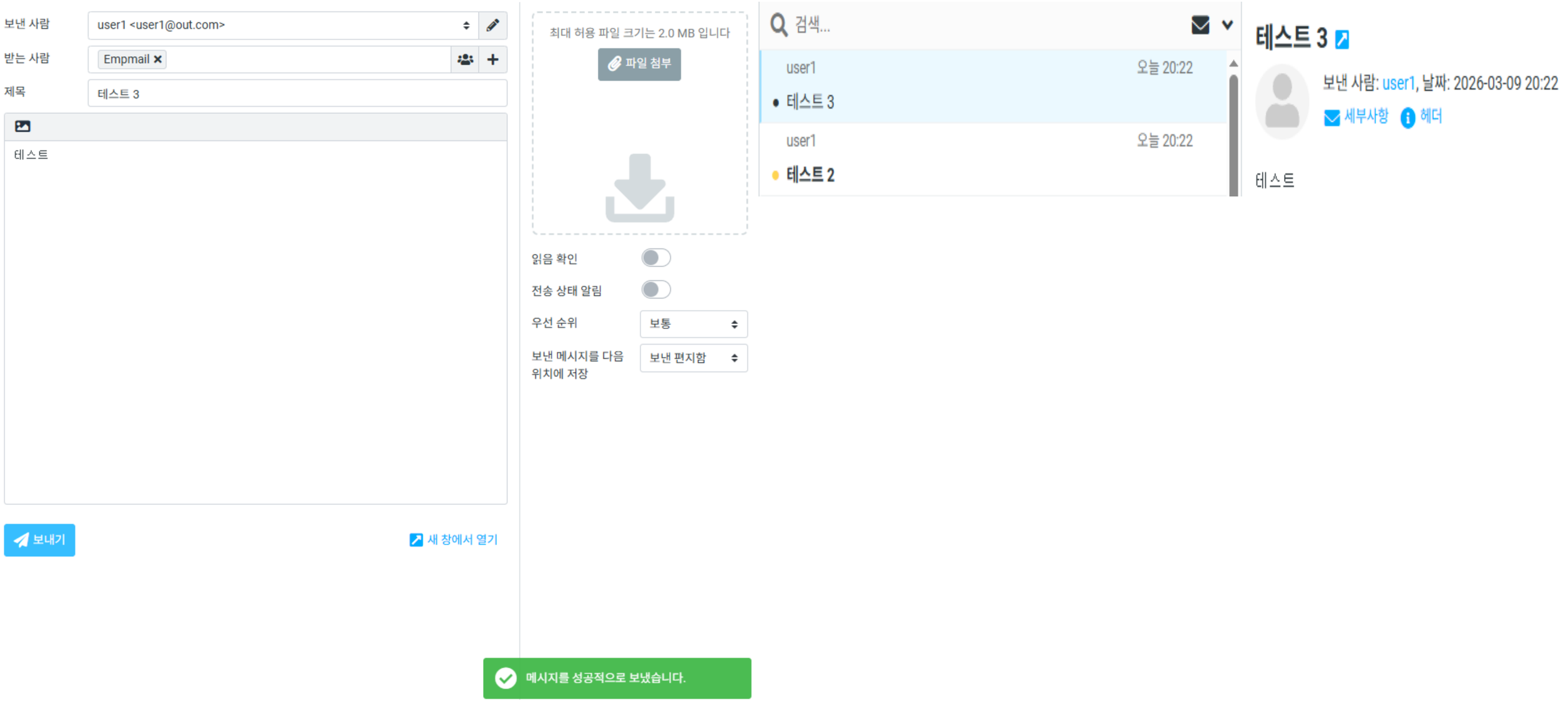
백업 결과

```
root@CA-bb-Ubuntu:/backup# ls
2026-02-23  2026-02-24
root@CA-bb-Ubuntu:/backup# cd 2026-02-23
root@CA-bb-Ubuntu:/backup/2026-02-23# ls
CA-cc-Rocky  US-cc1-Rocky  US-gm-Rocky   US-ha2-Rocky  US-md-Rocky  US-sb-Ubuntu  US-su-Rocky
CA-su-Rocky  US-cc2-Rocky  US-ha1-Rocky  US-mb-Ubuntu  US-pm-Rocky  US-sd-Rocky
root@CA-bb-Ubuntu:/backup/2026-02-23# cd ..
root@CA-bb-Ubuntu:/backup# cd 2026-02-24
root@CA-bb-Ubuntu:/backup/2026-02-24# ls
CA-cc-Rocky   US-cc2-Rocky  US-ha2-Rocky  US-pm-Rocky   US-su-Rocky
CA-su-Rocky   US-gm-Rocky   US-mb-Ubuntu  US-sb-Ubuntu  US-wp1-Ubuntu
US-cc1-Rocky  US-ha1-Rocky  US-md-Rocky   US-sd-Rocky   US-wp2-Ubuntu
```

메일 서비스 / Pydio 흐름도



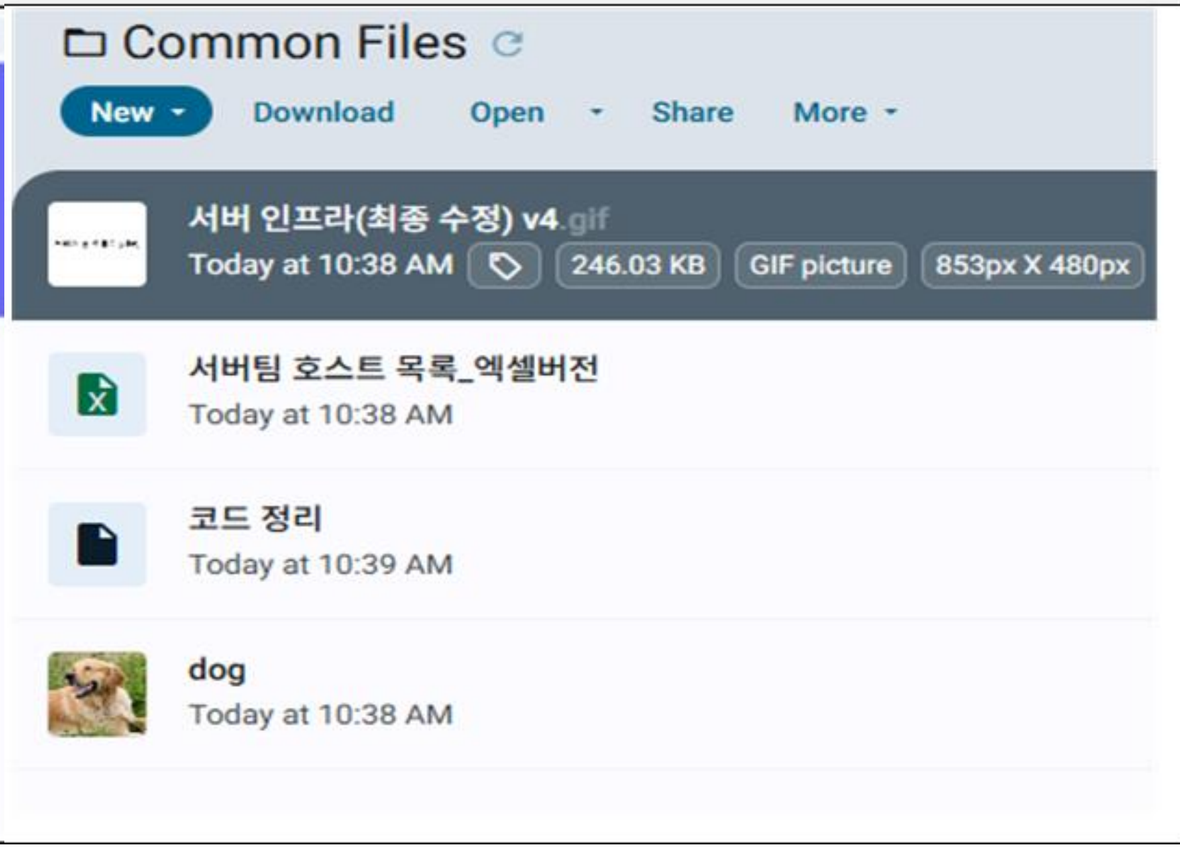
메일 서비스 구축 결과


보낸 사람
user1 <user1@out.com>
받는 사람
Empmail
제목
테스트 3
테스트
보내기
새 창에서 열기
최대 허용 파일 크기는 2.0 MB 입니다
파일 첨부
읽음 확인
전송 상태 알림
우선 순위
보통
보낸 메시지를 다음 위치에 저장
보낸 편지함
검색...
user1
오늘 20:22
테스트 3
user1
오늘 20:22
테스트 2
테스트 3
보낸 사람: user1, 날짜: 2026-03-09 20:22
세부사항
헤더
테스트
메시지를 성공적으로 보냈습니다.

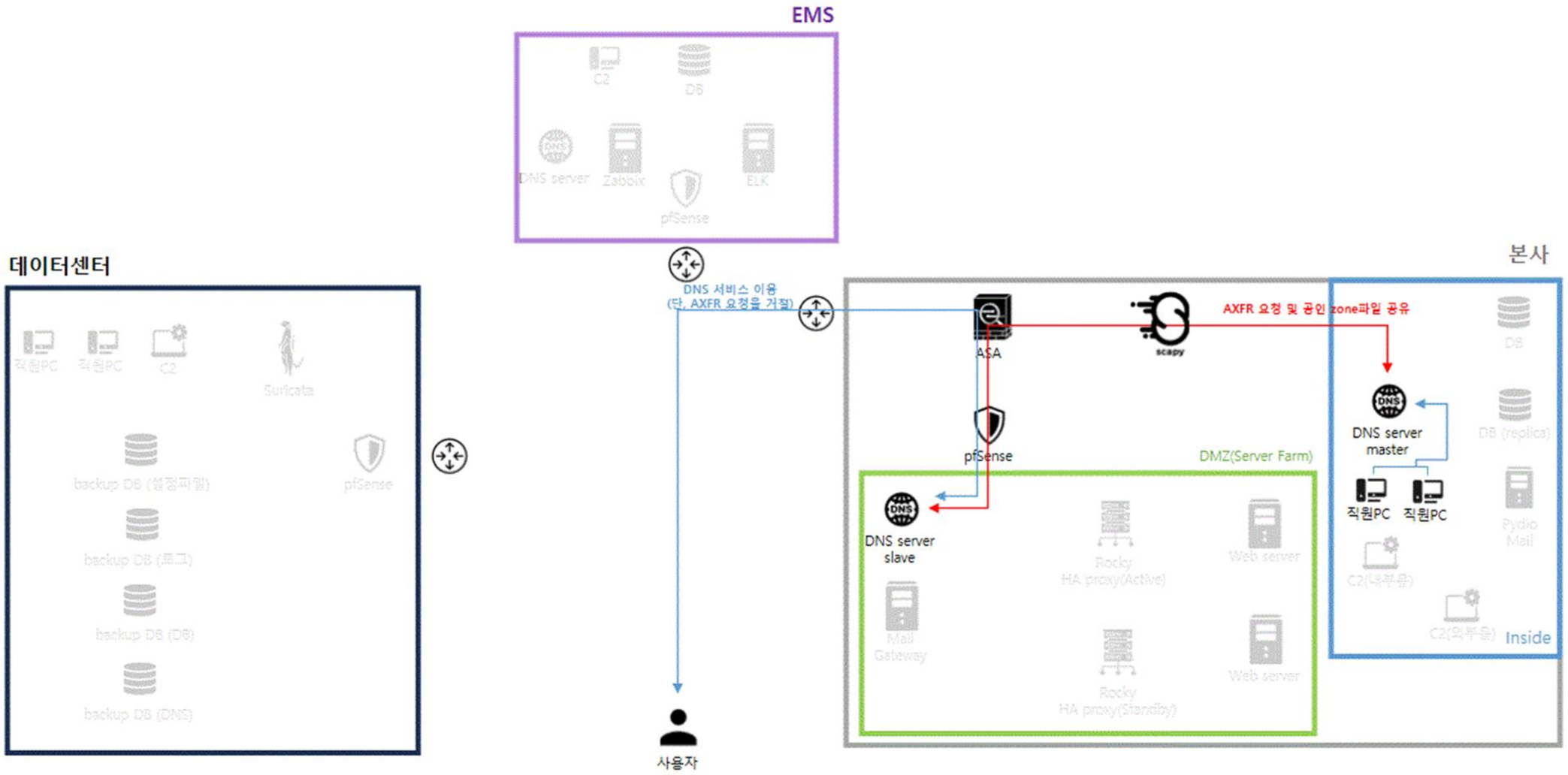
Pydio 서비스 구축 결과

Pydio 홈페이지 접속

Pydio 업로드 사진



DNS 서버 흐름도

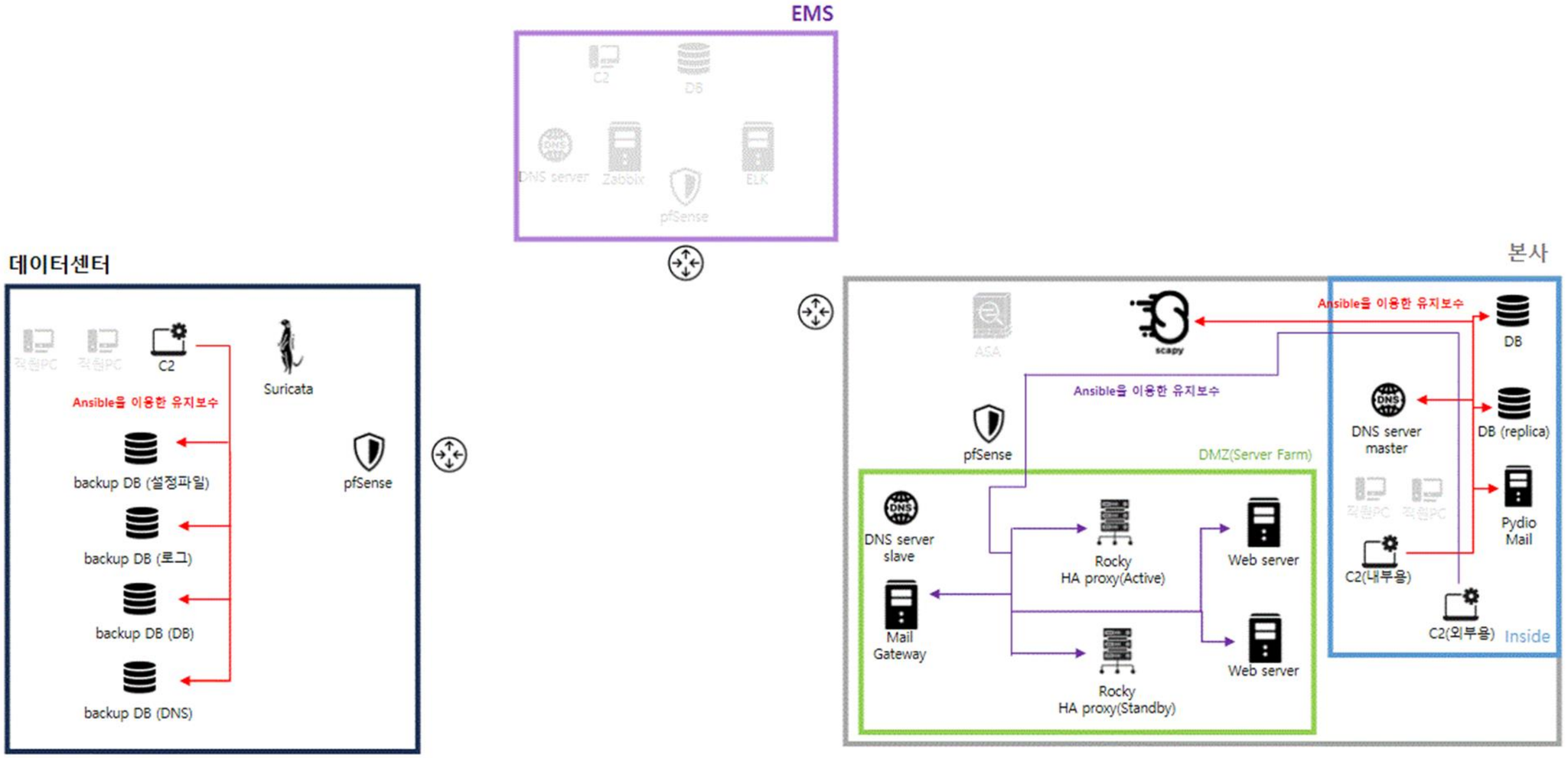

EMS
C2
DB
DNS server
Zabbix
ELK
pfSense
데이터센터
직원PC
직원PC
C2
Suricata
backup DB (설정파일)
pfSense
backup DB (로그)
backup DB (DB)
backup DB (DNS)
DNS 서비스 이용
(단, AXFR 요청을 거절)
사용자
본사
ASA
scapy
AXFR 요청 및 공인 zone파일 공유
DB
DNS server
master
DB (replica)
pfSense
DMZ(Server Farm)
직원PC
직원PC
Pydio
Mail
DNS server
slave
Rocky
HA proxy(Active)
Web server
C2(내부용)
Mail
Gateway
Rocky
HA proxy(Standby)
Web server
C2(외부용)
Inside

DNS 서버 구축 결과

Slave에 better.com.zone 생성 확인

```
[root@US-sd-Rocky ~]# ls /var/named/
better.com.zone  data  dynamic  named.ca  named.empty  named.localhost  named.loopback  slaves
[root@US-sd-Rocky ~]#
```

C2 관리 흐름도

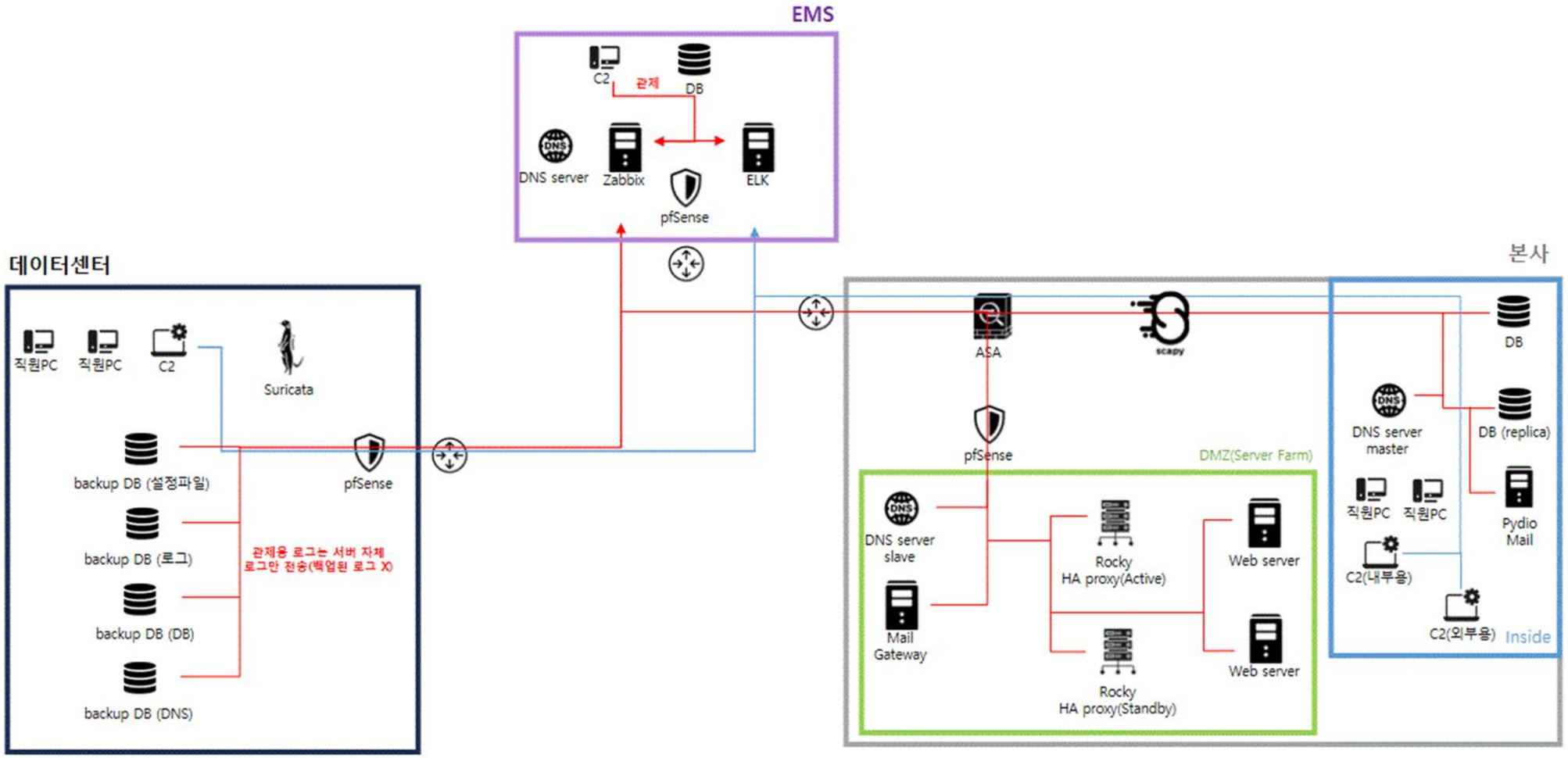

EMS
C2
DB
DNS server
Zabbix
ELK
pfSense
데이터센터
작업PC
작업PC
C2
Suricata
Ansible을 이용한 유지보수
backup DB (설정파일)
backup DB (로그)
backup DB (DB)
backup DB (DNS)
pfSense
본사
ACA
scapy
Ansible을 이용한 유지보수
Ansible을 이용한 유지보수
DB
DB (replica)
DNS server master
Pydio Mail
pfSense
DMZ(Server Farm)
DNS server slave
Rocky HA proxy(Active)
Web server
Mail Gateway
Rocky HA proxy(Standby)
Web server
작업PC
작업PC
C2(내부용)
C2(외부용)
Inside

Guacamole 구축 결과

Guacamole 접속

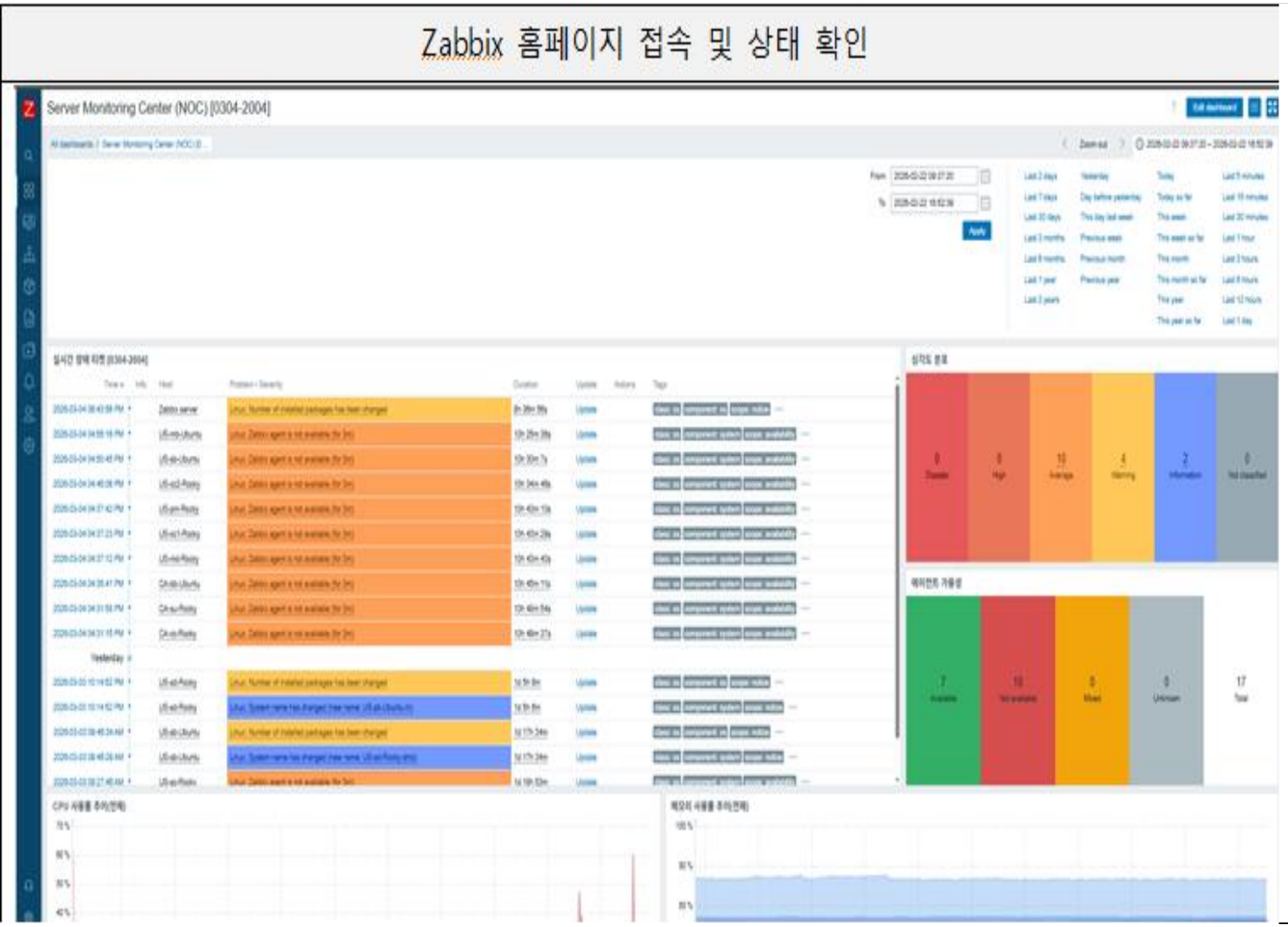

```
← TERMINATE SESSION
Welcome to Ubuntu 24.04.4 LTS (GNU/Linux 6.8.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Fri Mar  6 10:52:47 AM KST 2026

  System load:  0.36               Processes:             206
  Usage of /:   31.5% of 33.17GB   Users logged in:       2
  Memory usage: 25%                IPv4 address for ens32: 172.16.28.4
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

1 update can be applied immediately.
To see these additional updates run: apt list --upgradable

28 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm
```

관제 서비스 흐름도


EMS
C2
관제
DB
DNS server
Zabbix
ELK
pfSense
데이터센터
직원PC
직원PC
C2
Suricata
backup DB (설정파일)
pfSense
backup DB (로그)
관제용 로그는 서버 자체
로그만 전송(백업된 로그 X)
backup DB (DB)
backup DB (DNS)
본사
ASA
scapy
DB
pfSense
DMZ(Server Farm)
DNS server
master
DB (replica)
DNS server
slave
Rocky
HA proxy(Active)
Web server
직원PC
직원PC
Pydio
Mail
C2(내부용)
Mail
Gateway
Rocky
HA proxy(Standby)
Web server
C2(외부용)
Inside

Zabbix 구축 결과

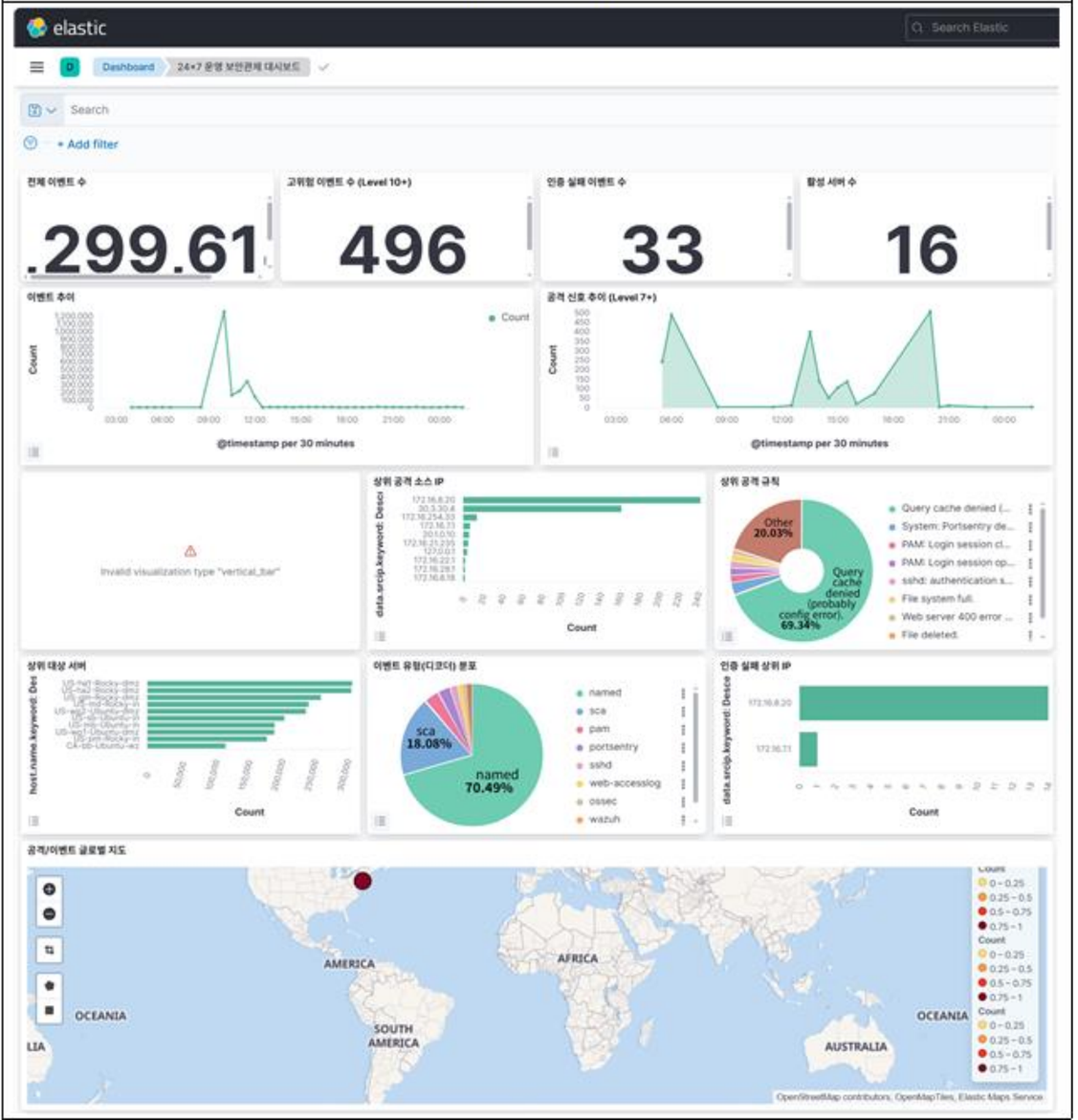
Zabbix 홈페이지 접속 및 상태 확인



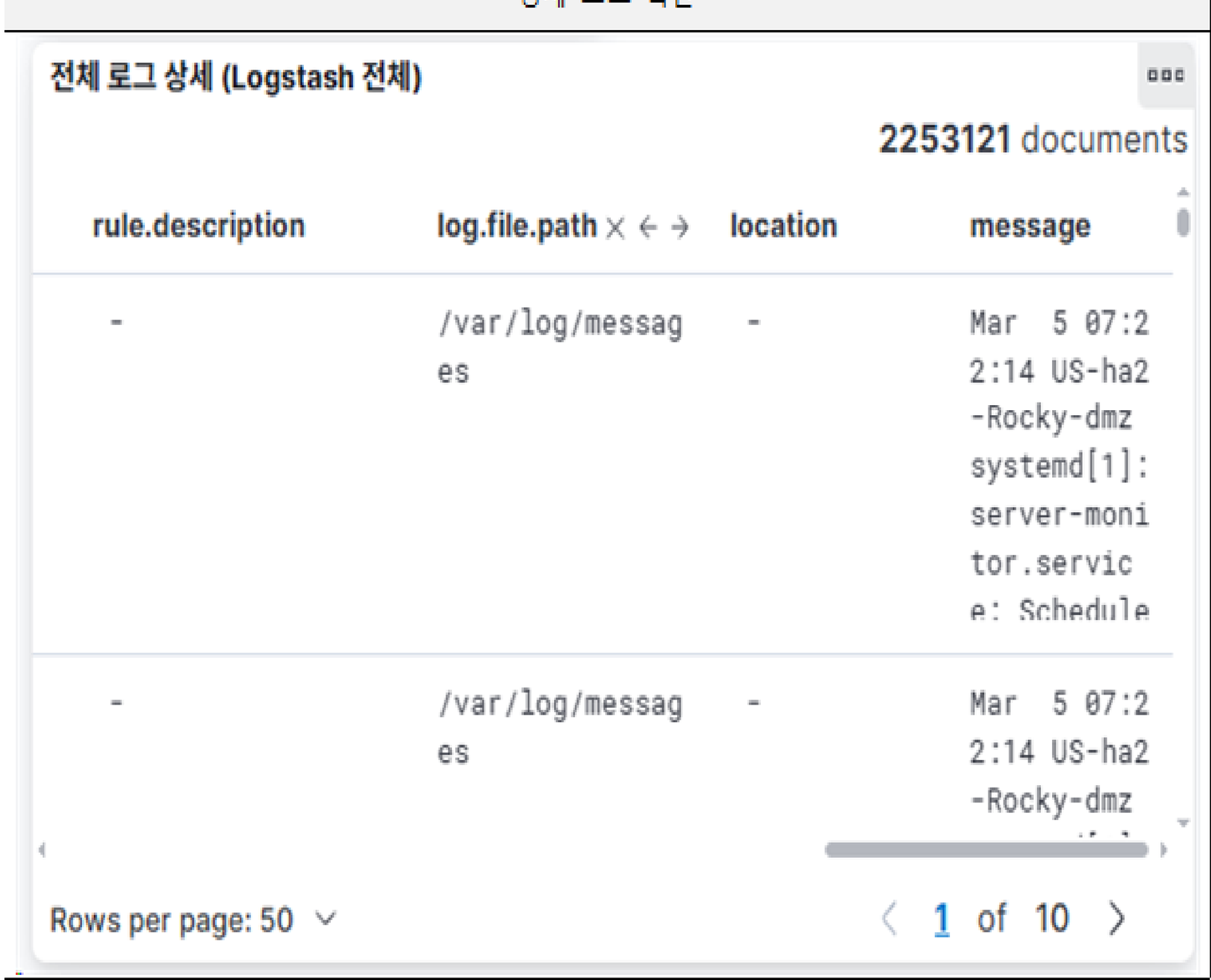
Name ▲	Interface	Availab
CA-bb-Ubuntu	192.168.50.6:10050	ZBX
CA-cc-Rocky	192.168.50.4:10050	ZBX
CA-su-Rocky	192.168.50.5:10050	ZBX
US-cc1-Rocky	192.168.40.2:10050	ZBX
US-cc2-Rocky	192.168.40.3:10050	ZBX
US-gm-Rocky	30.3.30.6:10050	ZBX
US-ha1-Rocky	30.3.30.4:10050	ZBX
US-ha2-Rocky	30.3.30.5:10050	ZBX
US-mb-Ubuntu	192.168.30.5:10050	ZBX
US-md-Rocky	192.168.30.4:10050	ZBX
US-pm-Rocky	192.168.30.2:10050	ZBX
US-sb-Ubuntu	192.168.30.3:10050	ZBX
US-sc-Rocky	172.16.23.110:10050	ZBX
US-sd-Rocky	30.3.20.2:10050	ZBX
US-wp1-Ubuntu	30.3.30.2:10050	ZBX
US-wp2-Ubuntu	30.3.30.3:10050	ZBX

ELK 구축 결과

ELK 홈페이지 접속



상세 로그 확인



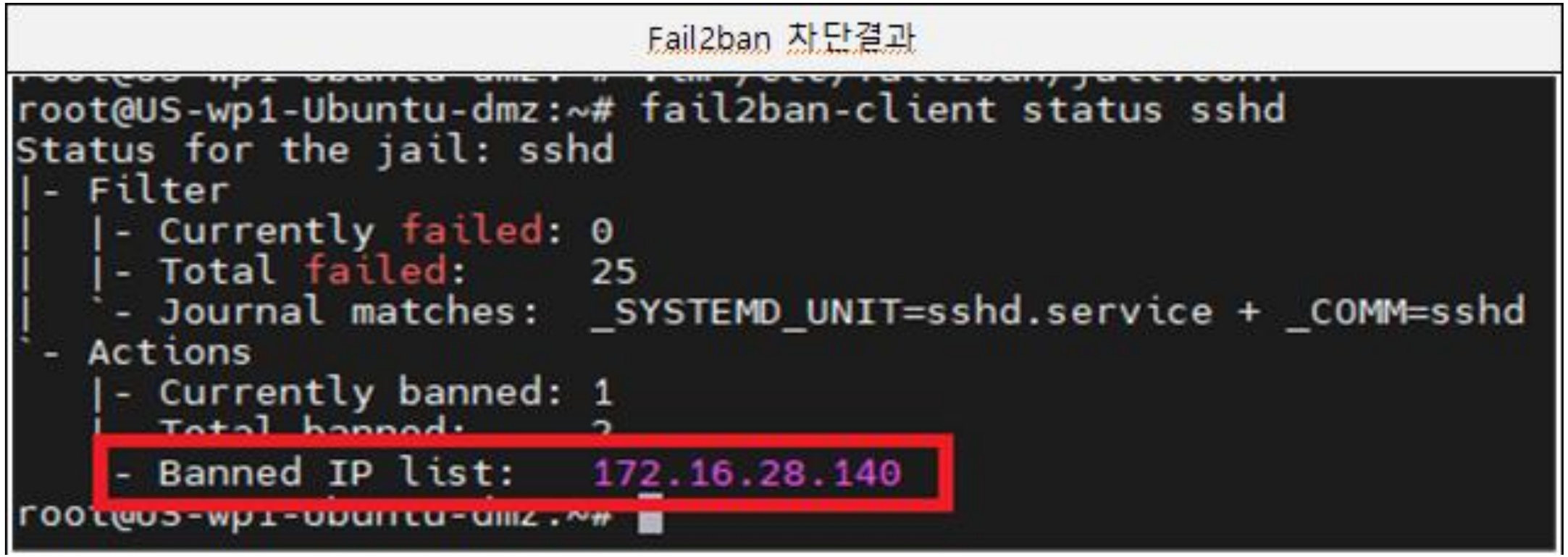
보안 및 자동화 도구

자동화와 보안의 완벽한 조화 구현

보안)

Fail2Ban

Fail2ban 차단결과



보안)

Portsentry

Portsentry 결과

```
2026-03-05T04:58:32.061902-05:00 US-wp1-Ubuntu-wz portsentry[1151]: attackalert: ERROR: Could not block host 30.3.30
2026-03-05T04:58:32.155525-05:00 US-wp1-Ubuntu-wz portsentry[1151]: attackalert: TCP SYN/Normal scan from host: 30.3
2026-03-05T04:58:32.155773-05:00 US-wp1-Ubuntu-wz portsentry[1151]: attackalert: Host 30.3.30.4 has been blocked via
2026-03-05T04:58:32.156103-05:00 US-wp1-Ubuntu-wz portsentry[1151]: adminalert: No target variable specified in KILL
2026-03-05T04:58:32.156267-05:00 US-wp1-Ubuntu-wz portsentry[1151]: attackalert: ERROR: Could not block host 30.3.30
2026-03-05T04:58:42.167162-05:00 US-wp1-Ubuntu-wz portsentry[1151]: attackalert: TCP SYN/Normal scan from host: 30.3
2026-03-05T04:58:42.167756-05:00 US-wp1-Ubuntu-wz portsentry[1151]: attackalert: Host 30.3.30.4 has been blocked via
2026-03-05T04:58:42.168035-05:00 US-wp1-Ubuntu-wz portsentry[1151]: adminalert: No target variable specified in KILL
```

보안)

ModSecurity

Modsecurity 결과

```
2026/03/05 06:05:40 [error] 1173170#1173170: *55 access forbidden by rule,
 "www.better.com"
2026/03/05 06:05:41 [error] 1173170#1173170: *55 access forbidden by rule,
 better.com"
2026/03/05 06:05:41 [error] 1173171#1173171: *54 access forbidden by rule
 "www.better.com"
2026/03/05 06:18:32 [error] 1173171#1173171: *110 directory index of "/var/
est: "GET /uploads/ HTTP/1.1", host: "www.better.com"
2026/03/05 06:25:17 [error] 1173171#1173171: *155 FastCGI sent in stderr: "
 on false in /var/www/html/main/upload_proc.php:46
Stack trace:
#0 {main}
  thrown in /var/www/html/main/upload_proc.php on line 46" while reading up
TP/1.1", upstream: "fastcgi://unix:/var/run/php/php8.3-fpm.sock:", host: "
2026/03/05 06:28:57 [error] 1184710#1184710: *1 access forbidden by rule, c
better.com"
2026/03/05 06:28:57 [error] 1184710#1184710: *1 access forbidden by rule, c
"www.better.com"
```

보안)

pfSense

pfsense blacklist 설정

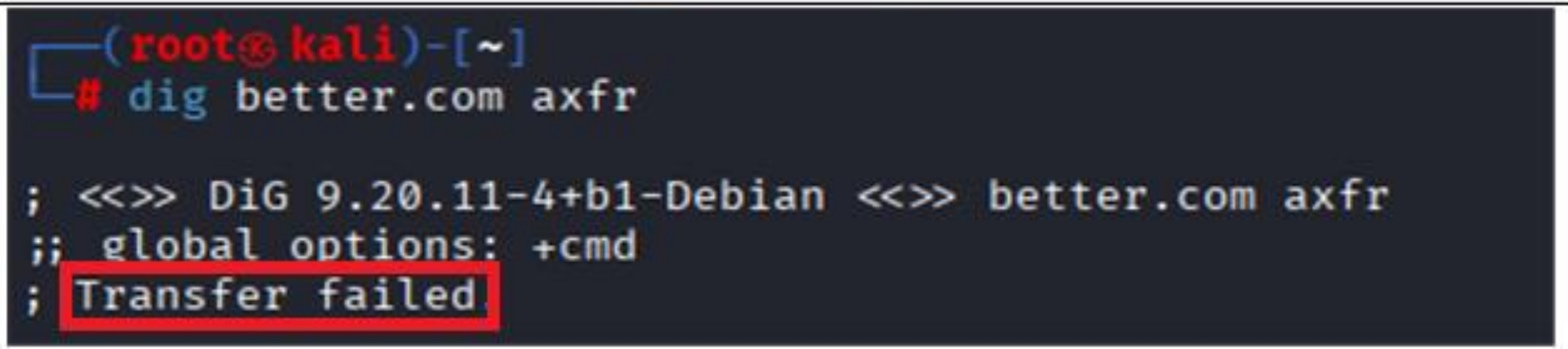
290 Matched Firewall Log Entries. (Maximum 500) Pause ■

Action	Time	Interface	Source	Destination	Protocol
✗	Mar 6 07:53:38	WAN	172.16.28.140	30.3.10.1	ICMP
✗	Mar 6 07:53:39	WAN	172.16.28.140	30.3.10.1	ICMP
✗	Mar 6 07:53:41	WAN	172.16.28.140	30.3.10.1	ICMP
✗	Mar 6 07:53:42	WAN	172.16.28.140	30.3.10.1	ICMP
✗	Mar 6 07:53:43	WAN	172.16.28.140	30.3.10.1	ICMP

보안)

DNS Key

AXFR 공격 방어 성공



자동화)

Ansible

```
PLAY RECAP ************************************************************************************************
[redacted] : ok=0  changed=0  unreachable=1  failed=0  skipped=0  rescued=0  ignored=0
[redacted] : ok=3  changed=1  unreachable=0  failed=0  skipped=0  rescued=0  ignored=0
[redacted] : ok=3  changed=1  unreachable=0  failed=0  skipped=0  rescued=0  ignored=0
[redacted] : ok=3  changed=1  unreachable=0  failed=0  skipped=0  rescued=0  ignored=0
[redacted] : ok=0  changed=0  unreachable=1  failed=0  skipped=0  rescued=0  ignored=0
[redacted] : ok=3  changed=1  unreachable=0  failed=0  skipped=0  rescued=0  ignored=0
[redacted] : ok=3  changed=1  unreachable=0  failed=0  skipped=0  rescued=0  ignored=0
[redacted] : ok=3  changed=1  unreachable=0  failed=0  skipped=0  rescued=0  ignored=0
[redacted] : ok=3  changed=1  unreachable=0  failed=0  skipped=0  rescued=0  ignored=0
[redacted] : ok=3  changed=1  unreachable=0  failed=0  skipped=0  rescued=0  ignored=0
[redacted] : ok=3  changed=1  unreachable=0  failed=0  skipped=0  rescued=0  ignored=0
[redacted] : ok=3  changed=1  unreachable=0  failed=0  skipped=0  rescued=0  ignored=0
[redacted] : ok=3  changed=1  unreachable=0  failed=0  skipped=0  rescued=0  ignored=0
[redacted] : ok=3  changed=1  unreachable=0  failed=0  skipped=0  rescued=0  ignored=0
```

서버 총 정리

가용성, 연속성, 복구
HA Proxy, DNS, Replica, Backup

보안
Fail2Ban, Portsentry, ModSecurity, pfSense

서비스
Pydio, Mail, Guacamole, Zabbix, ELK

자동화
Ansible

한 줄 요약

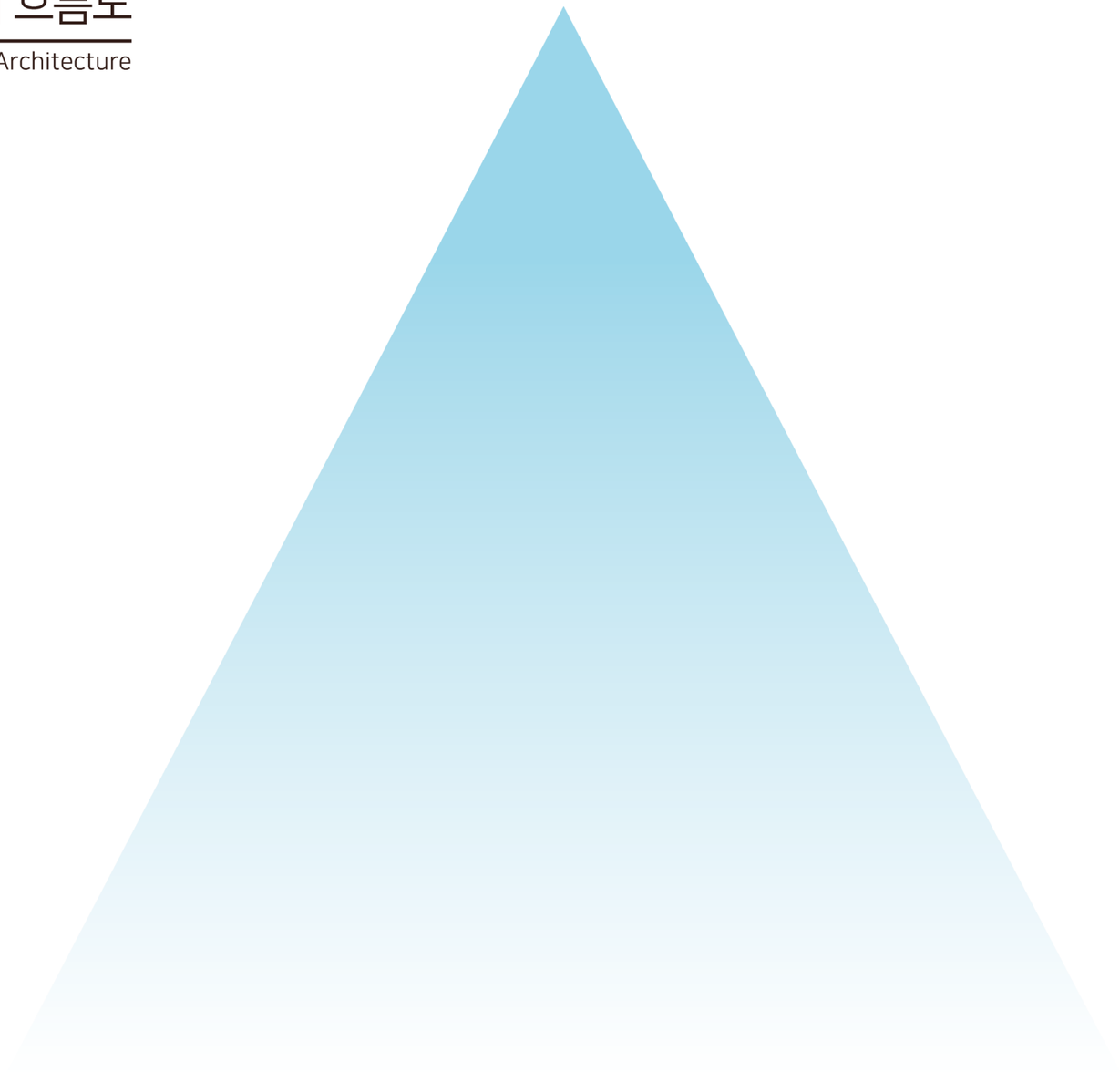
서버가 고장나도 서비스가 이어지고,

사고가 나도 복구가 가능하며,

공격은 초기에 줄일 수 있는 인프라를 구축

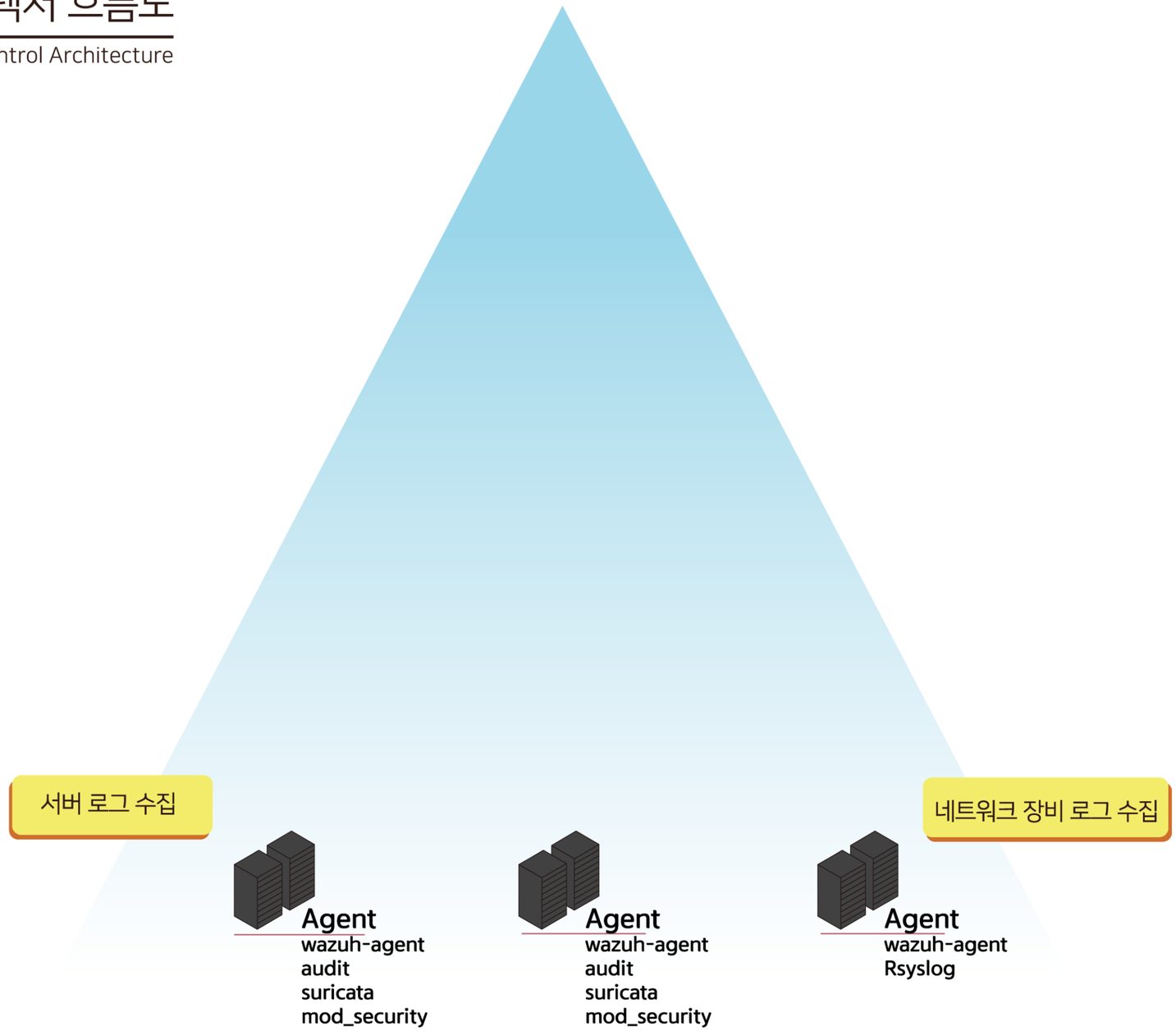
관제 아키텍처 흐름도

Monitoring & Control Architecture



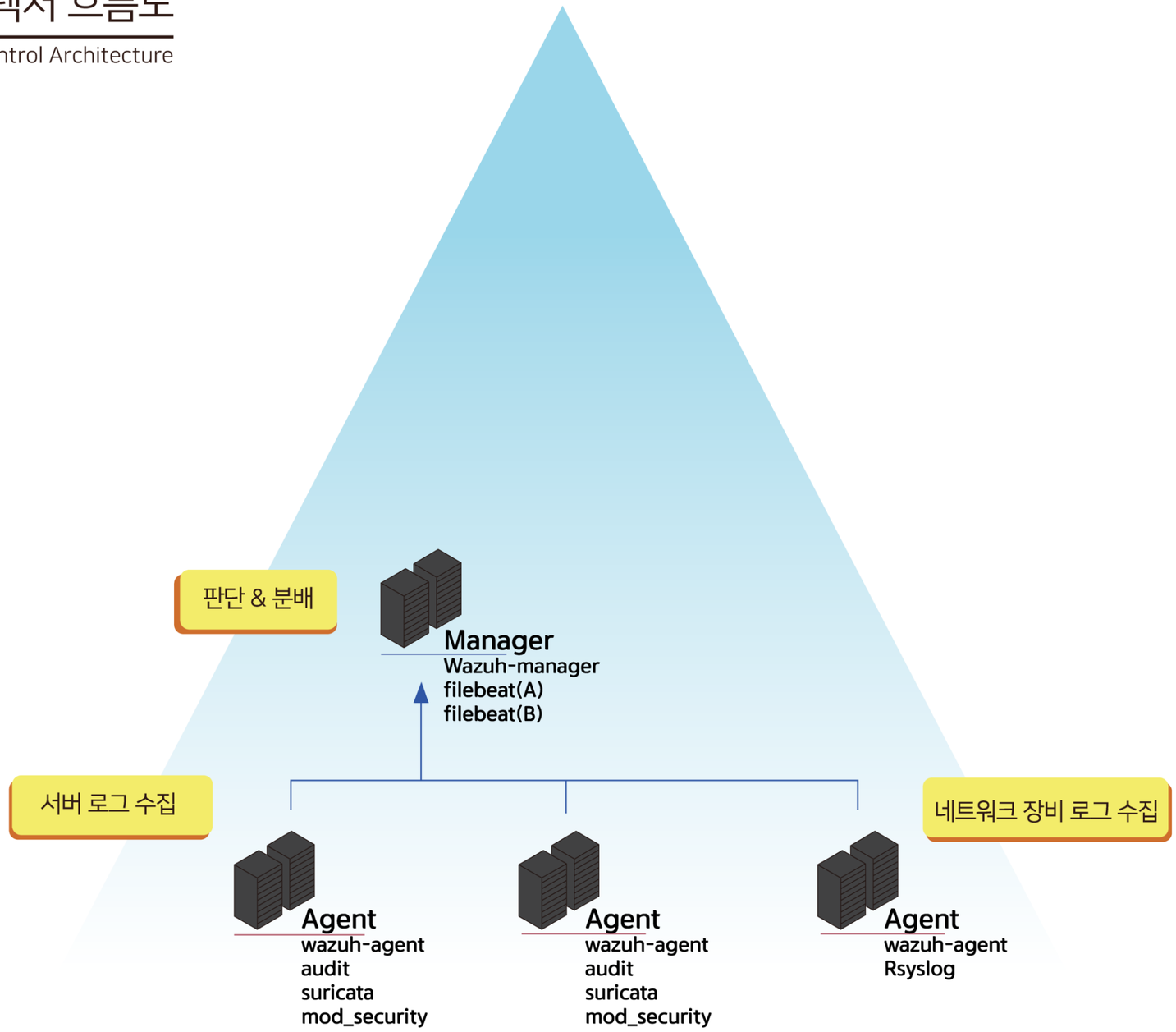
관제 아키텍처 흐름도

Monitoring & Control Architecture



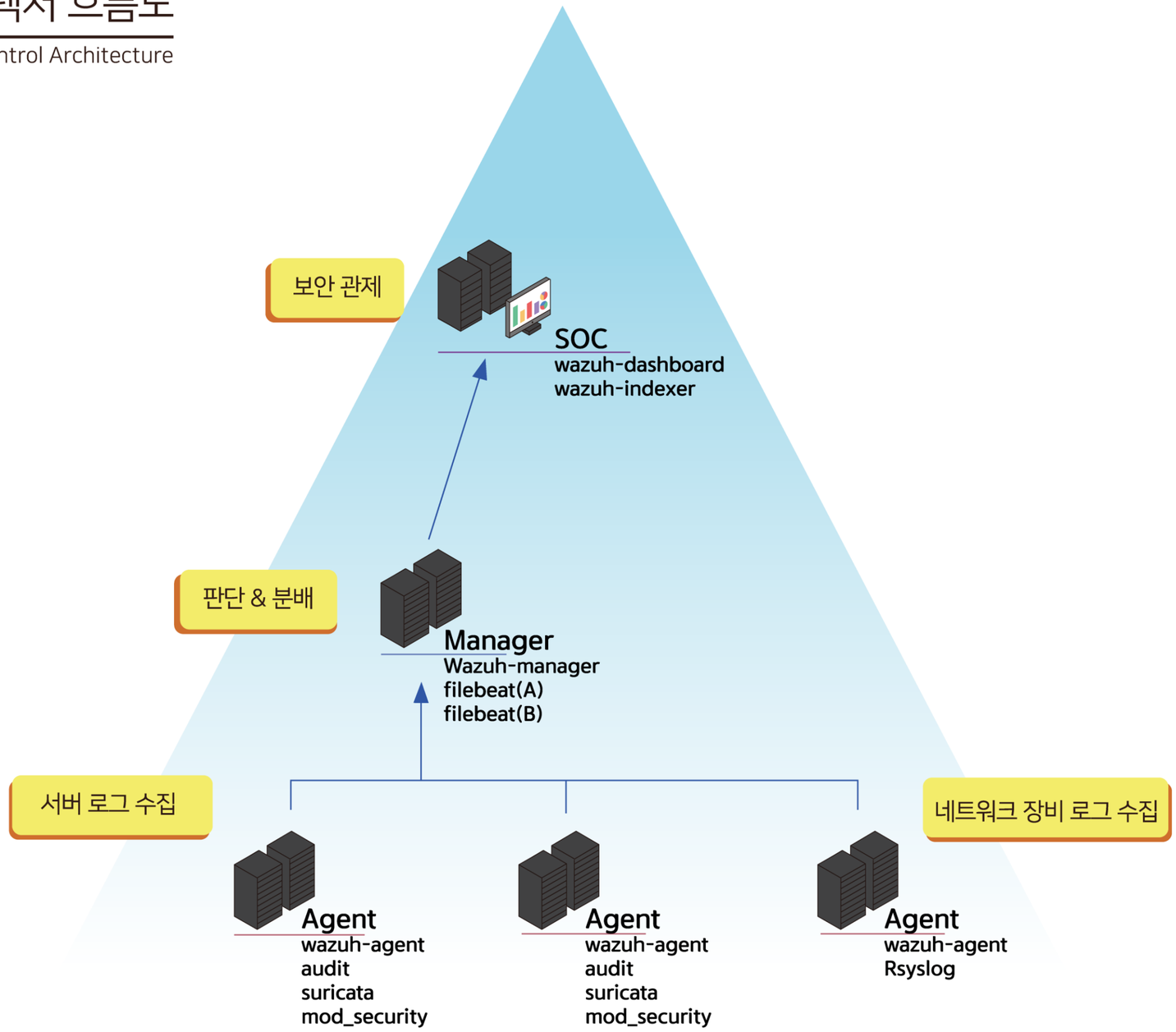
관제 아키텍처 흐름도

Monitoring & Control Architecture



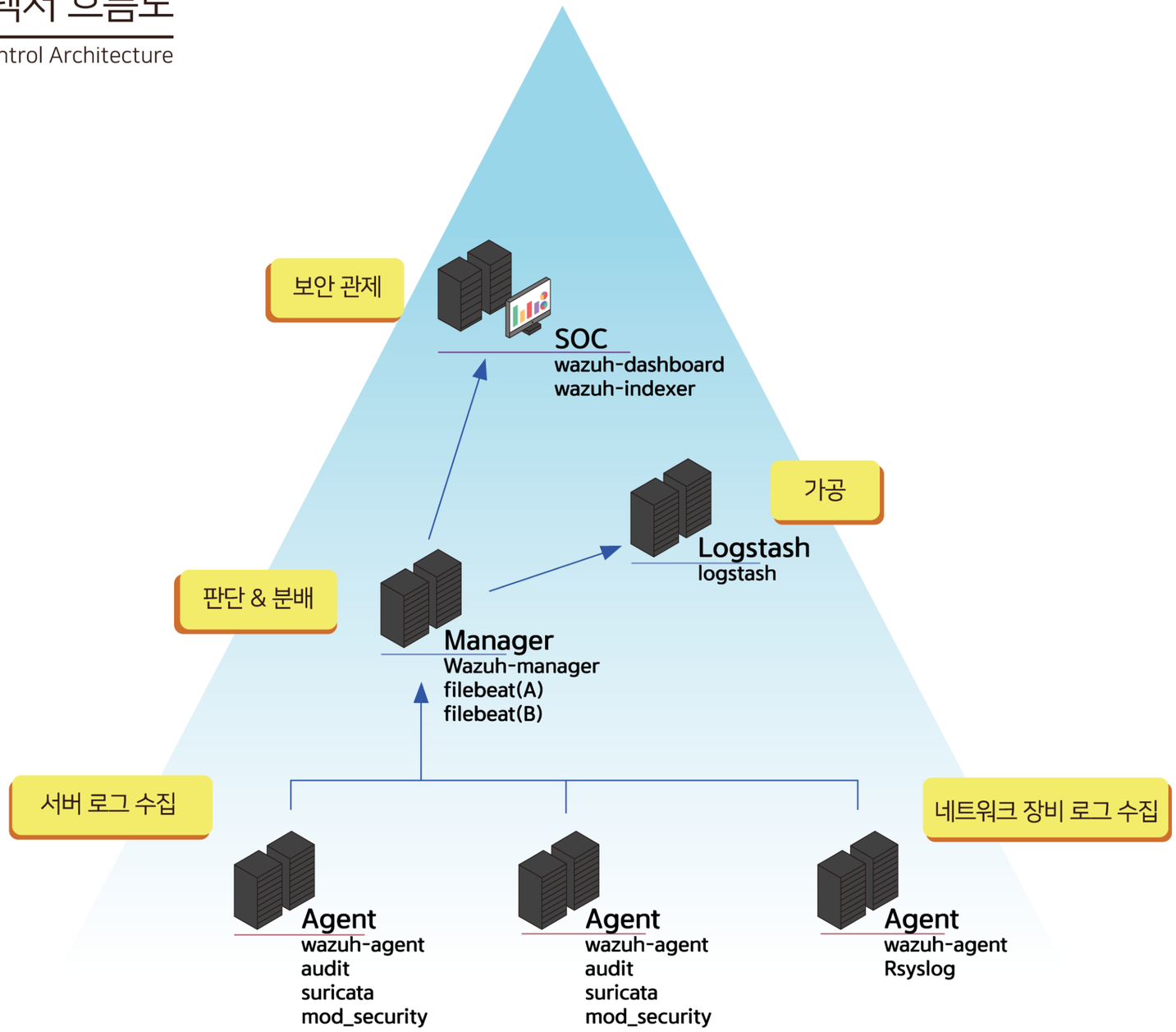
관제 아키텍처 흐름도

Monitoring & Control Architecture



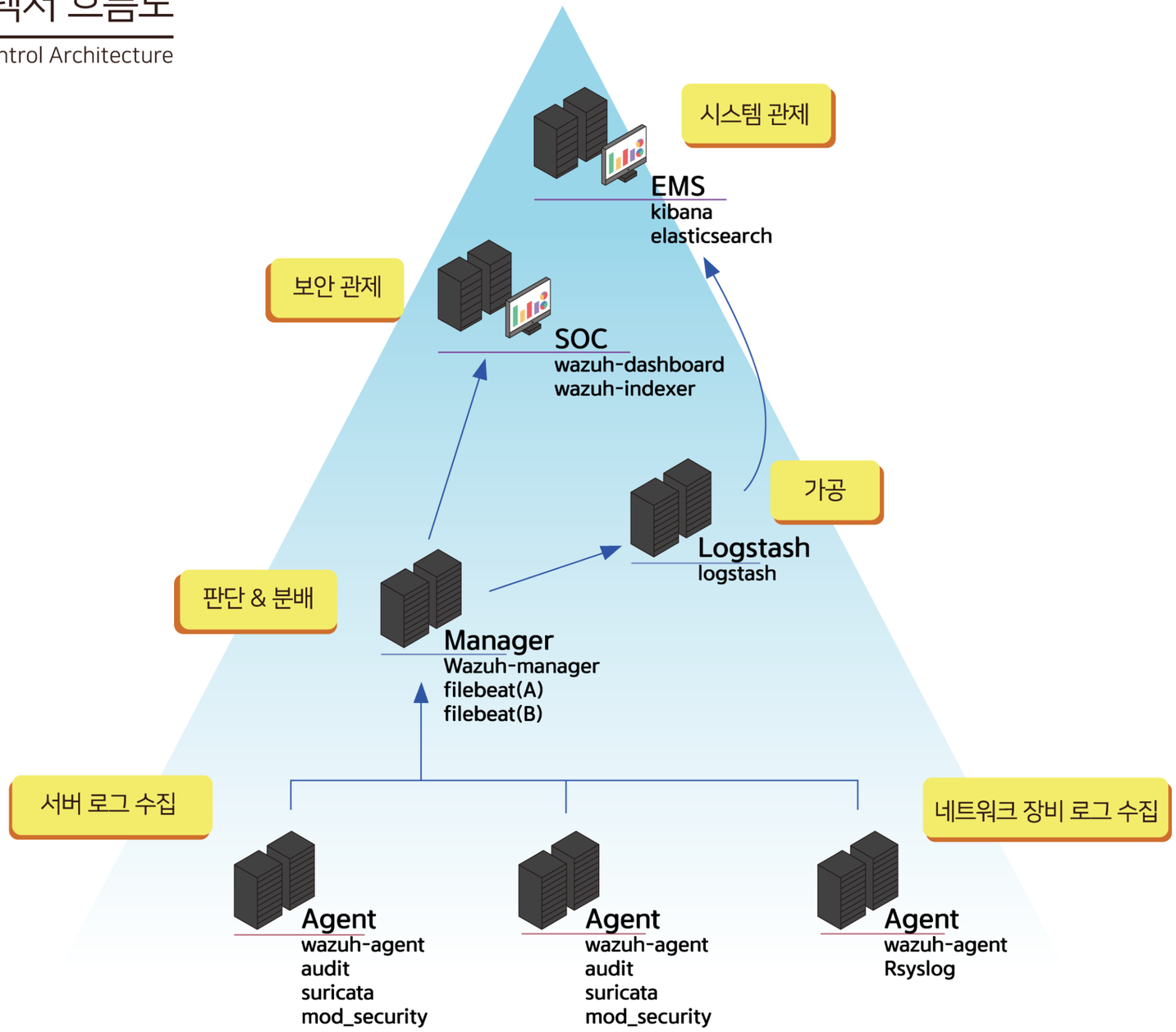
관제 아키텍처 흐름도

Monitoring & Control Architecture



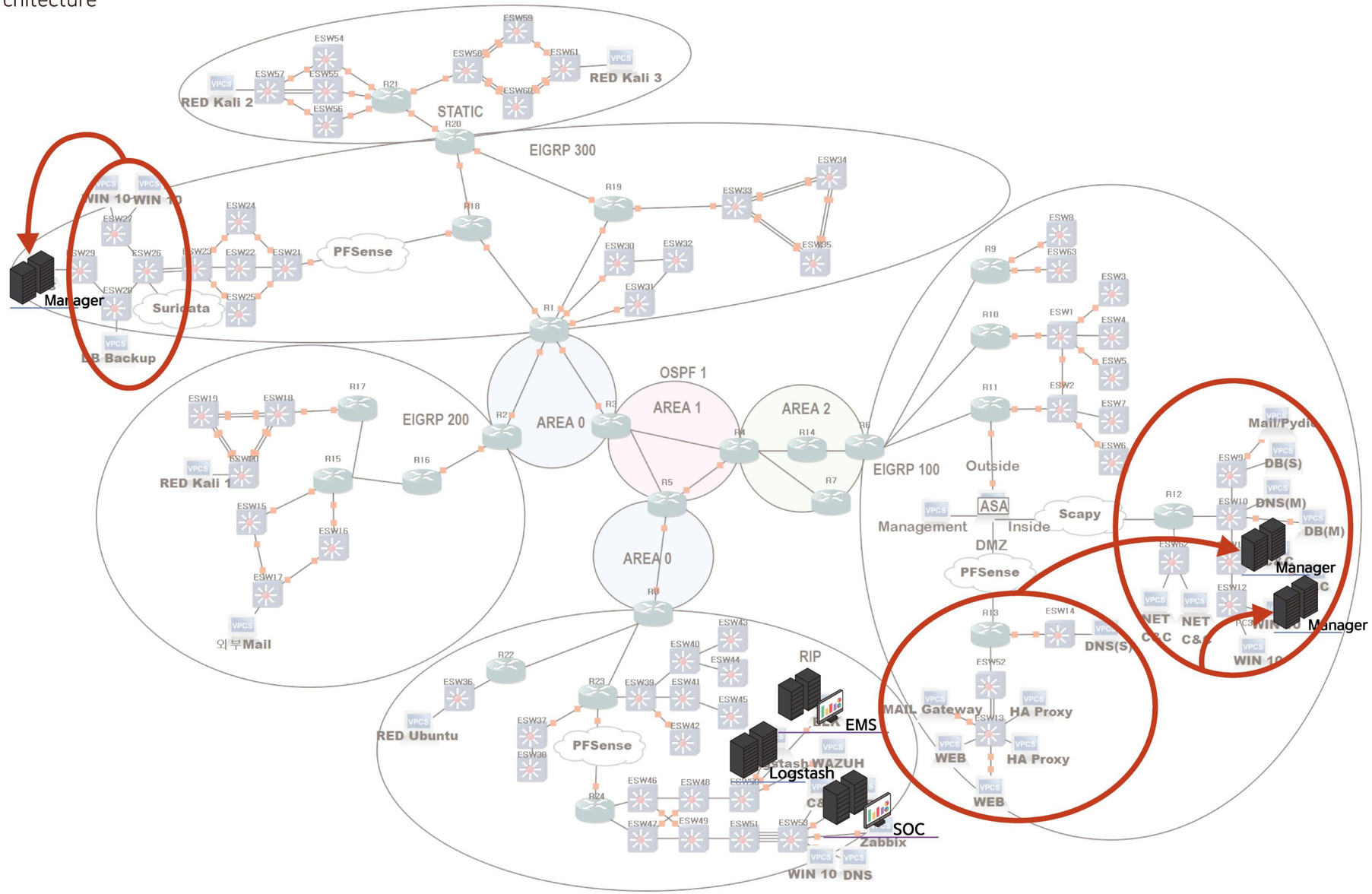
관제 아키텍처 흐름도

Monitoring & Control Architecture



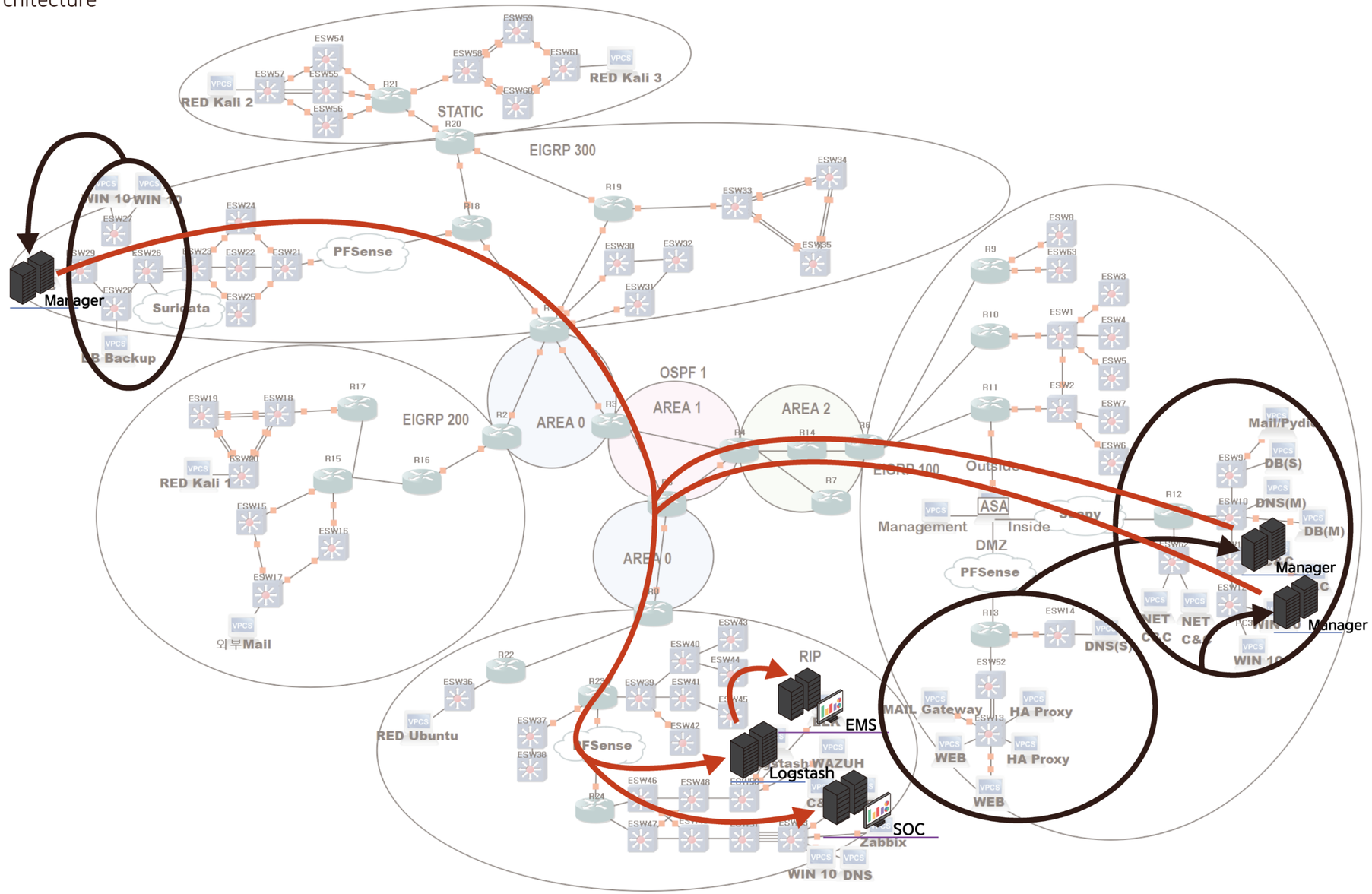
관제 아키텍처 흐름도

Monitoring & Control Architecture



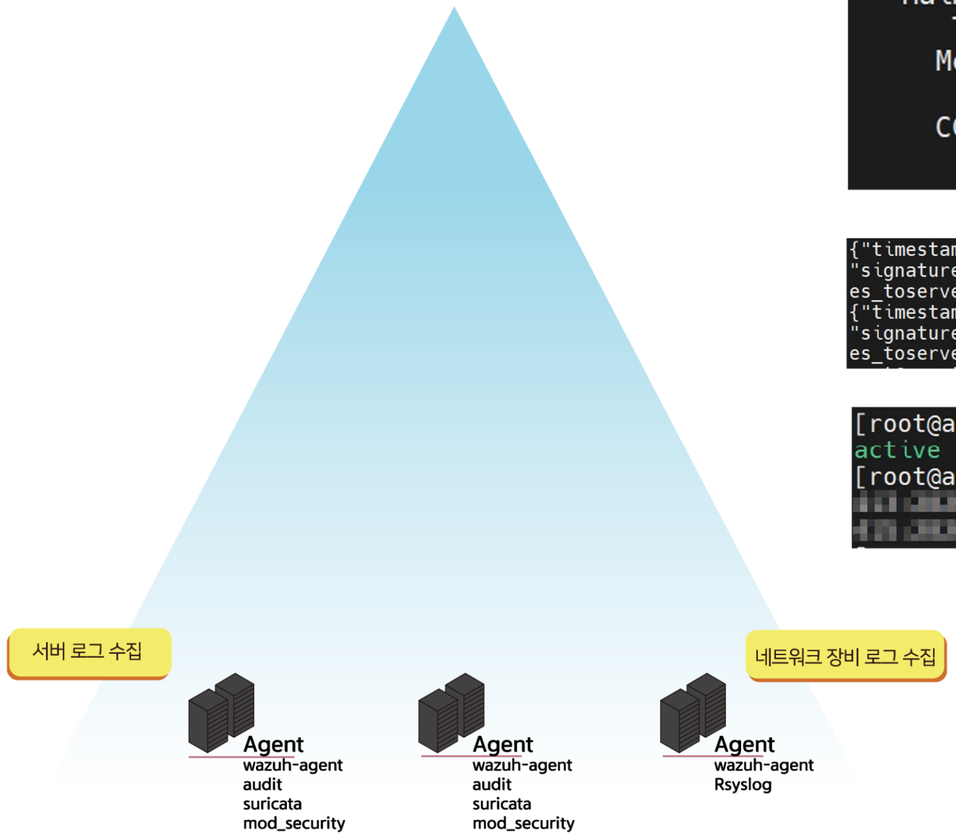
관제 아키텍처 흐름도

Monitoring & Control Architecture



관제 아키텍처 흐름도

Monitoring & Control Architecture




```
root@agent                                                    ls
suricata.rules
root@agent-                                                  systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; preset: enabled)
     Active: active (running) since Mon 2026-03-09 15:13:28 UTC; 1min 19s ago
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata.io/documentation/
    Process: 3559 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.ya
   Main PID: 3560 (Suricata-Main)
      Tasks: 8 (limit: 4543)
     Memory: 46.8M (peak: 47.1M)
        CPU: 801ms
     CGroup: /system.slice/suricata.service
             └─3560 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pid
```

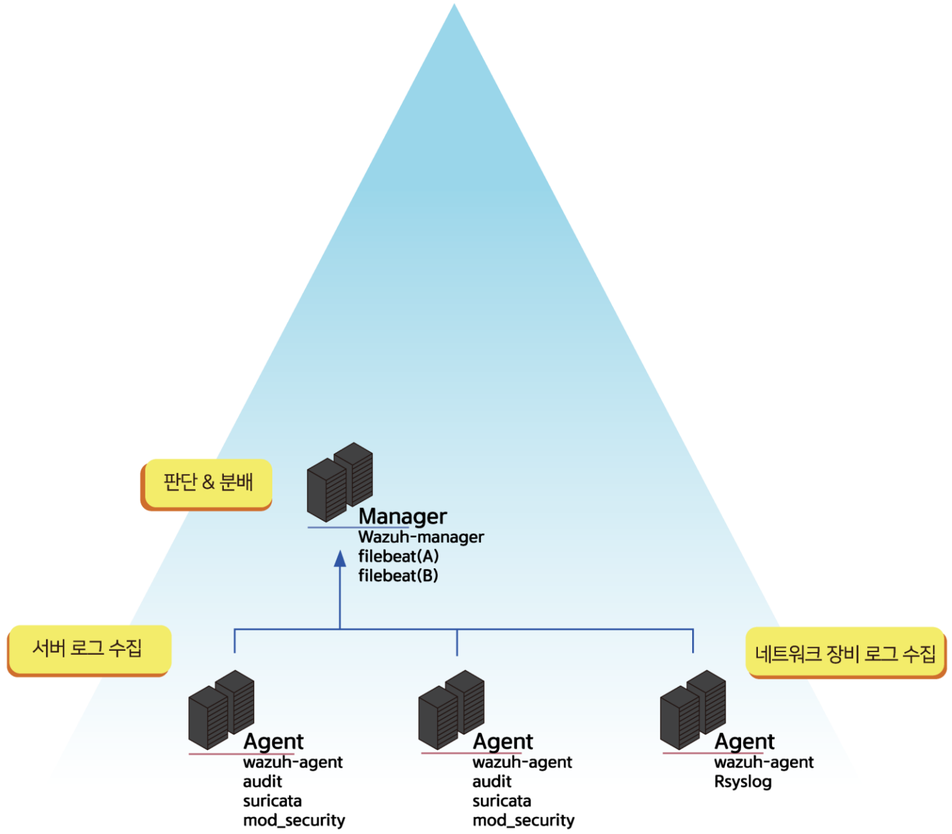

{"timestamp":"[redacted]","flow_id":2224311968768711,"in_iface":"ens33","event_type":"alert","src_ip":"[redacted]
"signature_id":[redacted],"rev":1,"signature":"Blind SQLi - High Frequency Requests","category":"Attempted Information Leak","severity"
es_toserver":391,"bytes_toclient":423,"start":"[redacted]","src_ip":"[redacted]","dest_ip":"[redacted]","src_
{"timestamp":"[redacted]","flow_id":2224311968768711,"in_iface":"ens33","event_type":"alert","src_ip":"[redacted]
"signature_id":[redacted],"rev":1,"signature":"Blind SQLi - High Frequency Requests","category":"Attempted Information Leak","severity"
es_toserver":457,"bytes_toclient":489,"start":"[redacted]","src_ip":"[redacted]","dest_ip":"[redacted]","src_


```
[root@agent                ~]# systemctl is-active wazuh-agent
active
[root@agent                ~]#
                           wazuh-agentd: INFO: Using AES as encryption method.
                           wazuh-agentd: INFO: (4102): Connected to the server (          :1514/tcp).
```

관제 아키텍처 흐름도

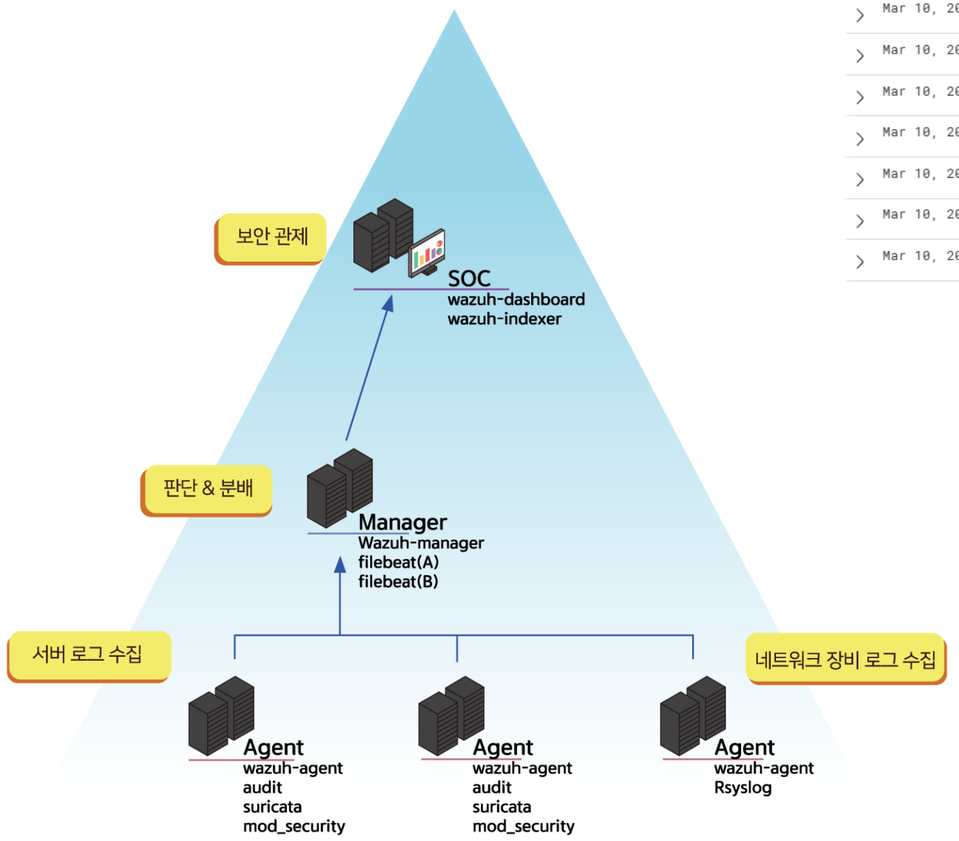
Monitoring & Control Architecture

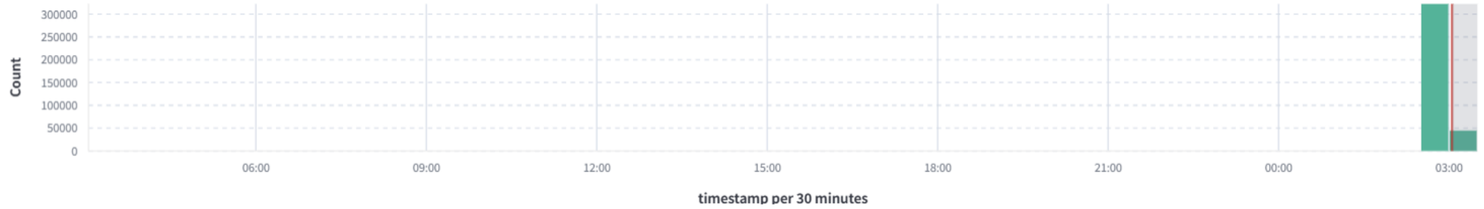
```
root@manager# systemctl is-active filebeat-a filebeat-b
active
active
root@manager
/etc/filebeat-a/filebeat.yml:19:output.elasticsearch:
/etc/filebeat-a/filebeat.yml:20:  hosts: ["https://172.16.254.33:9200"]
/etc/filebeat-a/filebeat.yml:24:  ssl.certificate_authorities: ["/etc/filebeat-a/certs/indexer-root-ca.pem"]
/etc/filebeat-a/filebeat.yml:25:  ssl.verification_mode: full
/etc/filebeat-b/filebeat.yml:16:output.logstash:
/etc/filebeat-b/filebeat.yml:17:  hosts: ["172.16.254.66:5044"]
/etc/filebeat-b/filebeat.yml:18:  ssl.enabled: true
/etc/filebeat-b/filebeat.yml:19:  ssl.certificate_authorities: ["/etc/filebeat-b/certs/logstash-ca.crt"]
/etc/filebeat-b/filebeat.yml:20:  ssl.verification_mode: full
```



관제 아키텍처 흐름도

Monitoring & Control Architecture

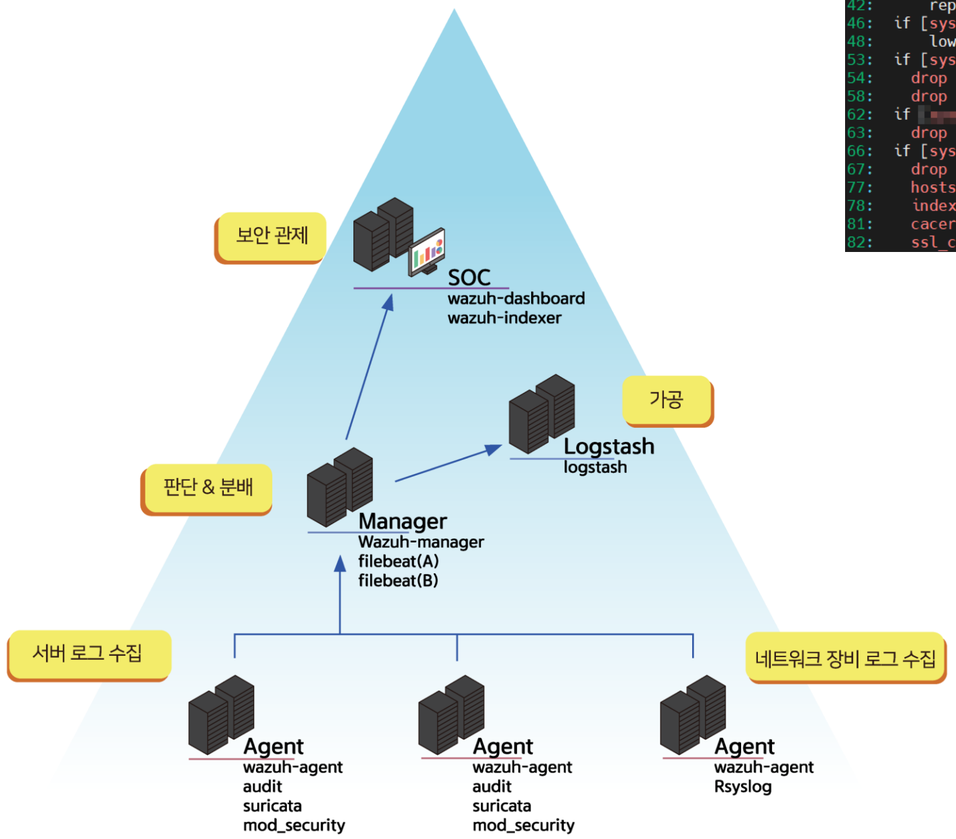




Time	agent.hostname	rule.level	rule.groups	rule.description
Mar 10, 2026 @ 03:03:13.092	manager-u-test	3	ids, suricata	Suricata: Alert - Blind SQLi - High Frequency Requests
Mar 10, 2026 @ 03:03:13.091	manager-u-test	3	ids, suricata	Suricata: Alert - Blind SQLi - High Frequency Requests
Mar 10, 2026 @ 03:03:12.677	manager-u-test	3	ids, suricata	Suricata: Alert - Blind SQLi - High Frequency Requests
Mar 10, 2026 @ 03:03:12.676	manager-u-test	3	ids, suricata	Suricata: Alert - Blind SQLi - High Frequency Requests
Mar 10, 2026 @ 03:03:12.003	manager-u-test	3	ids, suricata	Suricata: Alert - Blind SQLi - High Frequency Requests
Mar 10, 2026 @ 03:03:11.631	manager-u-test	3	ids, suricata	Suricata: Alert - Blind SQLi - High Frequency Requests
Mar 10, 2026 @ 03:03:11.628	manager-u-test	3	ids, suricata	Suricata: Alert - Blind SQLi - High Frequency Requests
Mar 10, 2026 @ 03:03:11.625	manager-u-test	3	ids, suricata	Suricata: Alert - Blind SQLi - High Frequency Requests
Mar 10, 2026 @ 03:03:11.623	manager-u-test	3	ids, suricata	Suricata: Alert - Blind SQLi - High Frequency Requests

관제 아키텍처 흐름도

Monitoring & Control Architecture

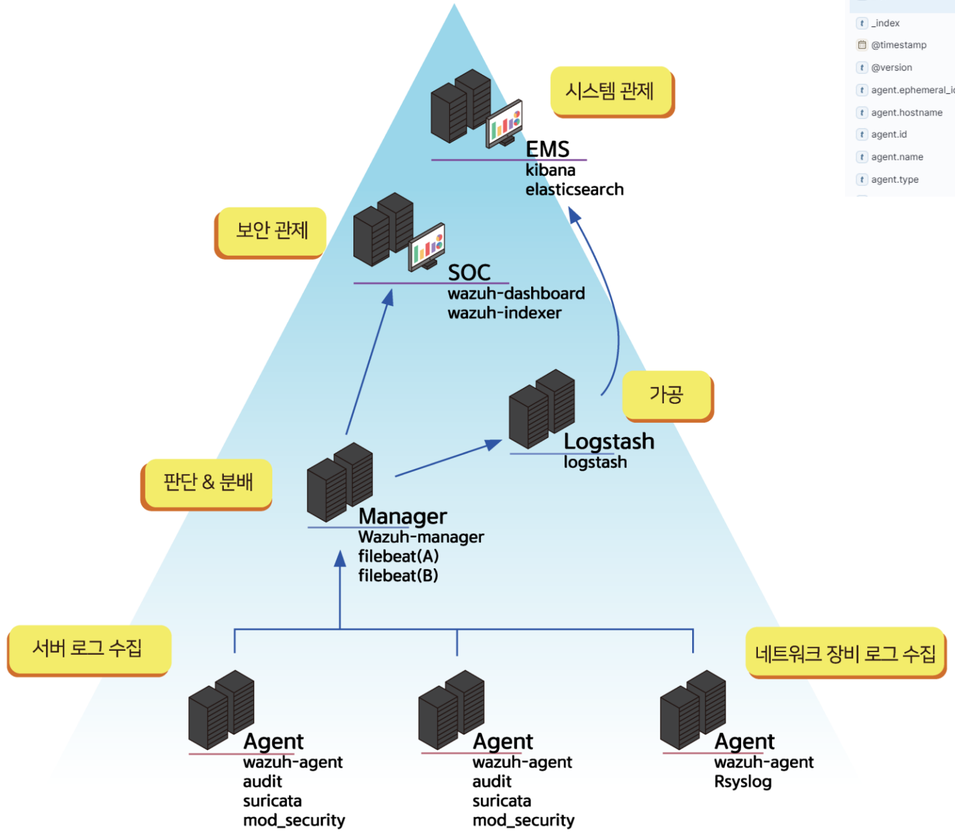


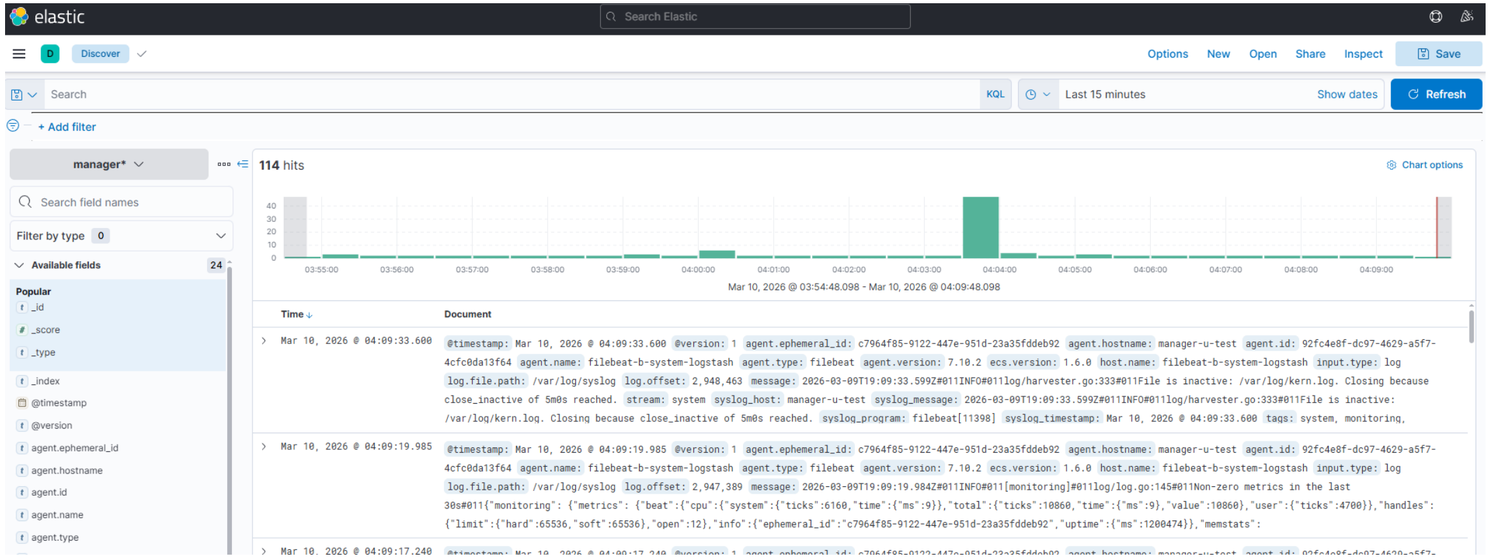

```
[root@logstash-r ~]# grep -n "hosts =>" /etc/logstash/conf.d/11-filebeat-b-to-ems.conf
13:     hosts => ["https://172.16.254.55:9443"]
```

```
[root@logstash
12:   # Keep only system stream from filebeat-b.
13:   if
14:     drop {}
18:   if [log][f
19:     drop {}
25:         "^%{
26:         "^%{
27:         "^%{
30:     tag_on
33:   if [syslog_timestamp] {
35:       match => ["syslog_timestamp", "ISO8601", "MMM d HH:mm:ss", "MMM dd HH:mm:ss"]
40:   if [syslog_message] {
42:       replace => { "message" => "%{syslog_message}" }
46:   if [syslog_program] {
48:       lowercase => ["syslog_program"]
53:   if [syslog
54:     drop {}
58:     drop {}
62:   if
63:     drop {}
66:   if [syslog
67:     drop {}
77:     hosts => ["https://172.16.254.55:9443"]
78:     index => "manager-system-ems-%{+YYYY.MM.dd}"
81:     cacert => "/etc/logstash/certs/es-proxy-ca.crt"
82:     ssl_certificate_verification => true
```

관제 아키텍처 흐름도

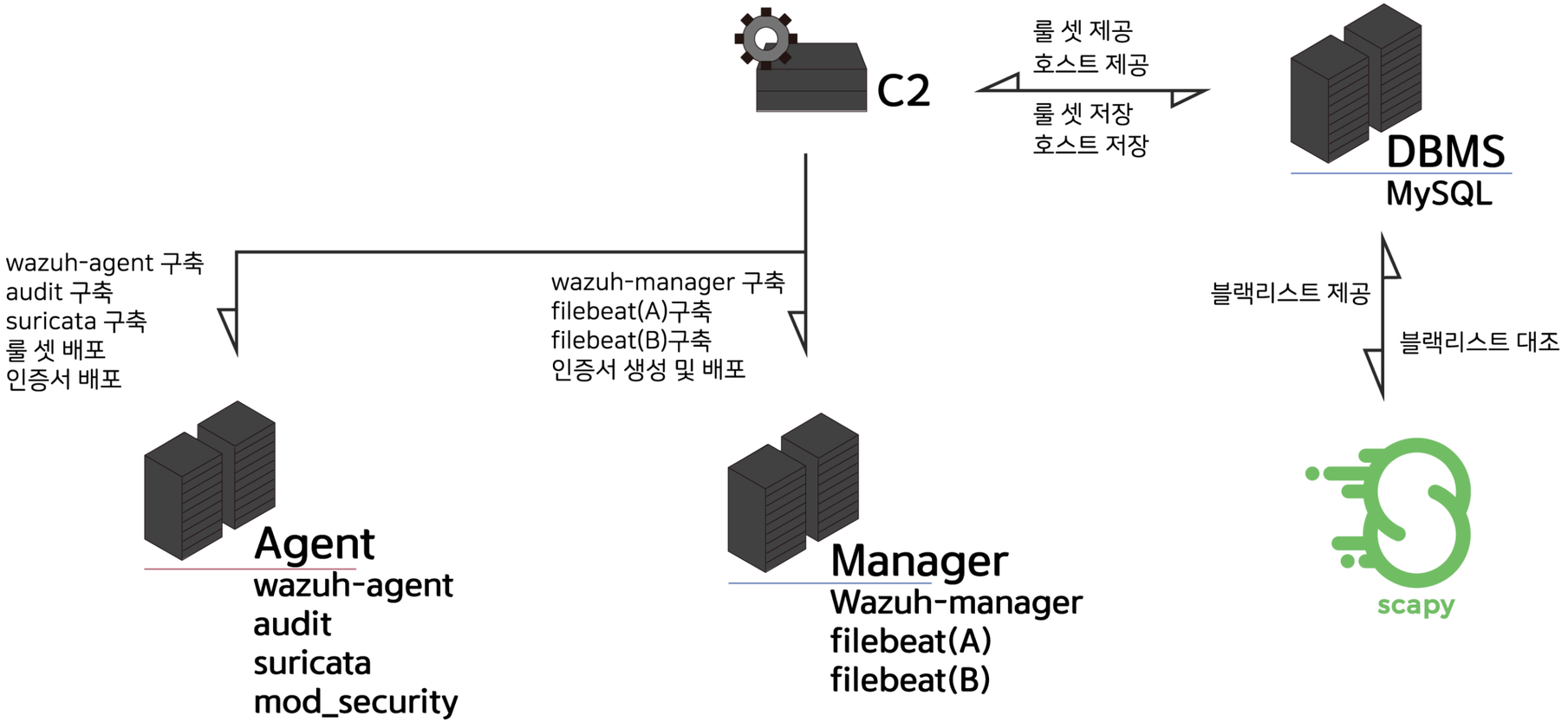
Monitoring & Control Architecture





자동화 아키텍처 흐름도

Automation Architecture Diagram

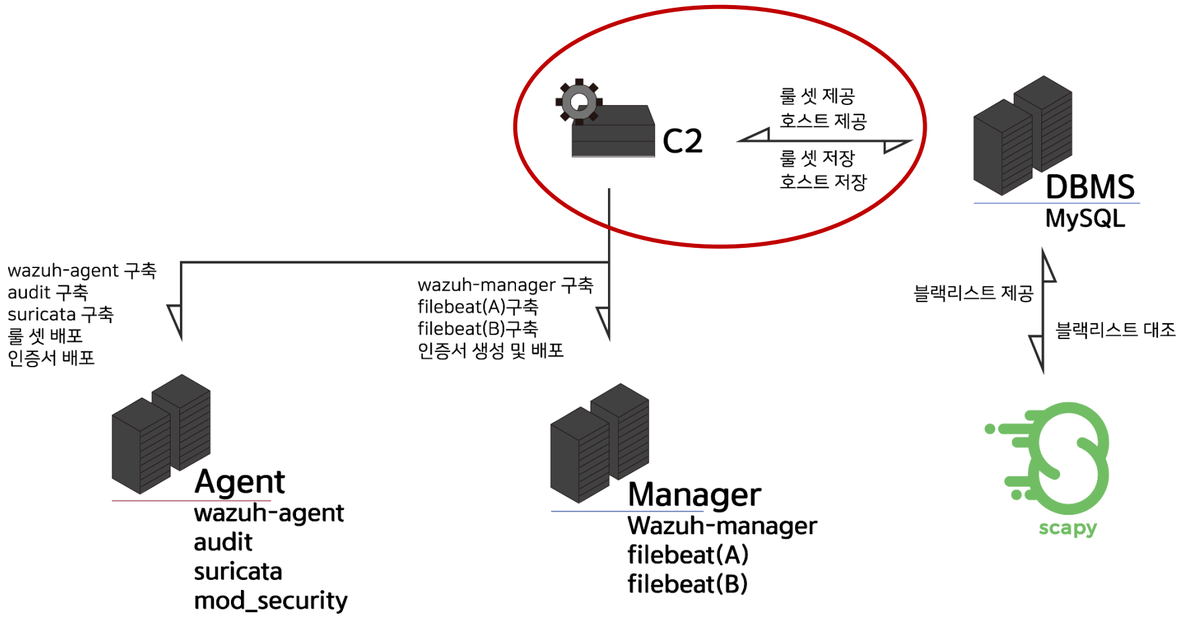


자동화 아키텍처 흐름도

Automation Architecture Diagram

```
TASK [DB 룰  파일 생성] ********************************************************
changed: [localhost] => (item=suricata)
changed: [localhost] => (item=audit)
changed: [localhost] => (item=wazuh)
changed: [localhost] => (item=modsecurity)

TASK [생성된 파일 확인] ********************************************************
changed: [localhost]

TASK [debug] *******************************************************************
ok: [localhost] => {
    "msg": [
        "-rw-r--r-- 1 root root    0 Mar 10 04:19 /root/audit_rules.conf",
        "-rw-r--r-- 1 root root 4.8K Mar 10 04:19 /root/modsecurity_rules.conf",
        "-rw-r--r-- 1 root root  16K Mar 10 04:19 /root/suricata_rules.conf",
        "-rw-r--r-- 1 root root 3.7K Mar 10 04:19 /root/wazuh_rules.conf"
    ]
}

PLAY RECAP *********************************************************************
localhost                  : ok=3    changed=2    unreachable=0    failed=0    sk
```

```
[root@localhost rules]# ls
audit_rules.conf  modsecurity_rules.conf  suricata_rules.conf  wazuh_rules.conf
```



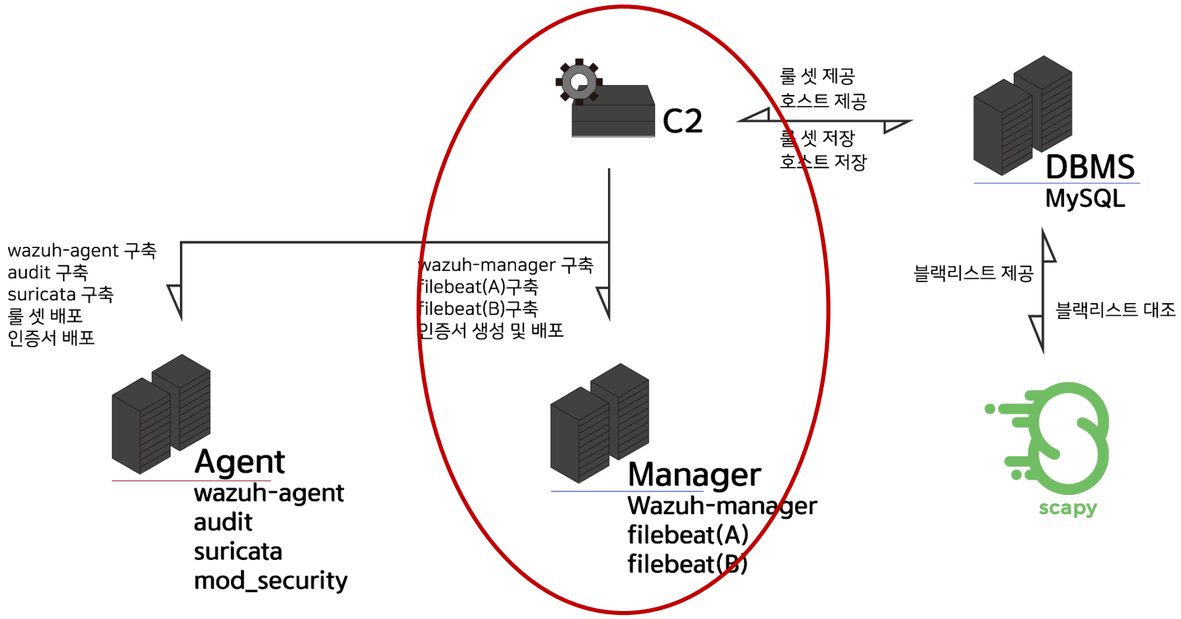
자동화 아키텍처 흐름도

Automation Architecture Diagram

```
TASK [[Ubuntu] 필수 패키지 설치] ************************************
TASK [[Ubuntu] Wazuh GPG Key 다운로드 및 아머 해제] ***********
TASK [[Ubuntu] Elastic GPG Key 다운로드 및 아머 해제] *********
TASK [[Ubuntu] Wazuh 저장소 추가] ************************************
TASK [[Ubuntu] Elastic 저장소 추가 (Filebeat용)] ***************
TASK [[Rocky] Wazuh 저장소 추가] ************************************
TASK [[Rocky] Elastic 저장소 추가 (Filebeat용)] ***************
TASK [Wazuh Manager 및 Filebeat 패키지 설치] ******************
                => (item=wazuh-manager)
                => (item=filebeat)
PLAY RECAP *********************************************************
                          : ok=7    changed=0    unreachable=0
```

```
TASK [Filebeat(B) 전용 디렉토리 생성] ************************
changed:  => (item=/etc/filebeat-b)
ok:  => (item=/etc/filebeat-b)
changed:  => (item=/var/lib/filebeat-b)
ok:  => (item=/var/lib/filebeat-b)
changed:  => (item=/var/log/filebeat-b)
ok:  => (item=/var/log/filebeat-b)

TASK [Filebeat(B) 전용 설정 파일 생성] ************************
ok:
changed:

TASK [Filebeat(B) 전용 Systemd 서비스 등록] ******************
changed:
ok:

TASK [Systemd 데몬 재로드] ************************************
ok:
ok:

TASK [Filebeat(B) 서비스 활성화 및 시작] ********************
changed:
changed:

TASK [Filebeat(B) 프로세스 확인] ******************************
ok:
ok:

TASK [debug] ***************************************************
ok:  => {
    "ps_result.stdout_lines": [
        "root        9701       1  8 04:38 ?        00:00:00 /us
eat -path.config /etc/filebeat-b -path.data /var/lib/filebeat-b
    ]
}
ok:  => {
    "ps_result.stdout_lines": [
        "root       13652       1 99 19:38 ?        00:00:00 /us
eat -path.config /etc/filebeat-b -path.data /var/lib/filebeat-b
    ]
}

PLAY RECAP *****************************************************
                          : ok=8    changed=1    unreachable=0
                          : ok=8    changed=4    unreachable=0
```

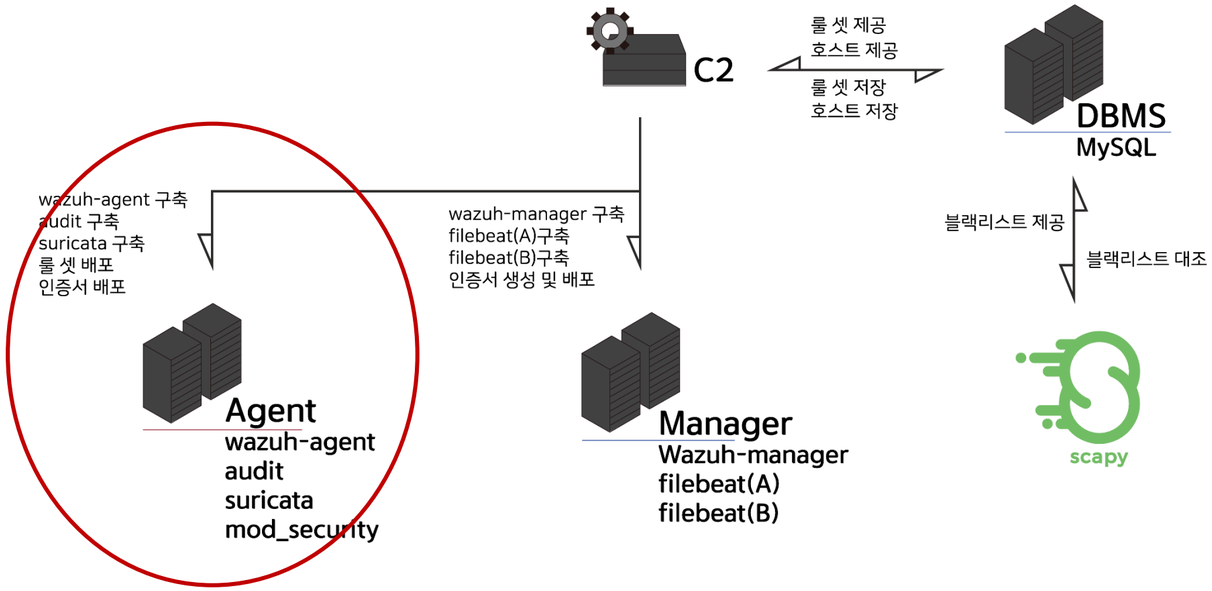
```
TASK [1. 인증서 디렉토리 생성
ok:

TASK [2. Root CA 개인키 생성]
ok:

TASK [3. Root CA용 CSR 생성]
ok:

TASK [4. Root CA 자체 서명] *
ok:

TASK [5. Manager 개인키 생성]
changed:

TASK [6. Manager CSR 생성] **
ok:

TASK [7. Manager 인증서 서명
ok:

TASK [8. 파일 권한 및 소유권
ok:                    => (item=/e
ok:                    => (item=/e
changed:                => (it

TASK [9. ossec.conf 설정 업데
changed:
```




```
TASK [Gathering Facts] *****************************
ok:
ok:

TASK [(Debian/Ubuntu) Filebeat 설치] **********
skipping:
ok:

TASK [(RedHat/CentOS) Filebeat 설치] **********
skipping:
ok:

TASK [Wazuh Filebeat 설정 템플릿 다운로드] ****
changed:
changed:

TASK [Filebeat 설정 수정 (Indexer 정보 입력)] *
changed:
changed:

TASK [Wazuh Filebeat 모듈 설치] ***************
ok:
changed:

TASK [Filebeat 서비스 시작] *******************
changed:
changed:

PLAY RECAP *************************************
                          : ok=6    changed=3
                          : ok=6    changed=4
```

자동화 아키텍처 흐름도

Automation Architecture Diagram




```
TASK [(Debian/Ubuntu) Suricata 패키지 설치] ***
skipping:
ok:

TASK [(RedHat/CentOS) Suricata 패키지 설치] ***
skipping:
ok:

TASK [Suricata 룰 디렉토리 생성] **************
ok:
ok:

TASK [사용자 정의 룰 파일 복사] ***************
ok:
changed:

TASK [suricata.yaml에 커스텀 룰 경로 추가] ****
changed:
ok:

TASK [Suricata 서비스 시작] *******************
ok:
changed:

RUNNING HANDLER [restart suricata] ************
changed:

PLAY RECAP *************************************
                    : ok=6    changed=1
                    : ok=7    changed=3
```

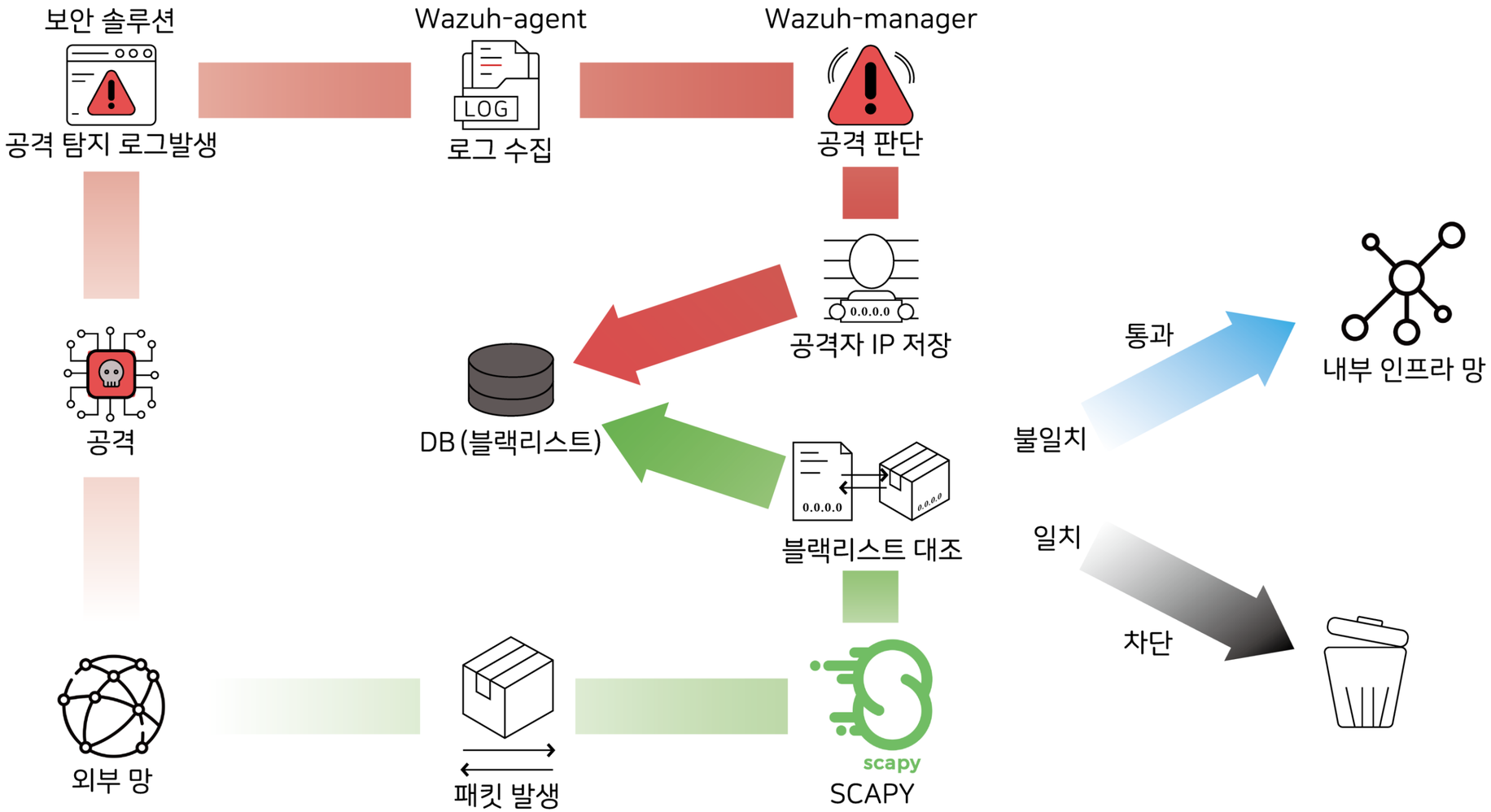
```
TASK [(Debian/Ubuntu) Auditd 패키지 설치] *******
skipping:
ok:

TASK [(RedHat/CentOS) Auditd 패키지 설치] *******
skipping:
ok:

TASK [기존 audit.rules 파일 백업] ***************
changed:
changed:

TASK [사용자 정의 룰 파일 복사] *****************
changed:
ok:

TASK [Auditd 서비스 활성화 및 시작] *************
ok:
ok:

RUNNING HANDLER [restart auditd] ****************
changed:

PLAY RECAP *************************************
                    : ok=5    changed=1
                    : ok=6    changed=3
```

```
TASK [[Ubuntu] 필수 패키지 설치] ****
skipping:
changed:

TASK [[Ubuntu] Wazuh GPG Key 다운로드
skipping:
ok:

TASK [[Ubuntu] Wazuh 저장소 추가 (메뉴
skipping:
ok:

TASK [[Rocky] Wazuh 저장소 추가] ****
skipping:
ok:

TASK [Wazuh Agent 패키지 설치] ******
ok:
ok:

TASK [Wazuh Agent 설정 파일(ossec.con
ok:
ok:
```

```
TASK [Manager 서버에서 Root CA 파일 가져오기] **
ok:

PLAY [Wazuh Agent 서버들에 인증서 배포 및 설정]

TASK [Gathering Facts] *************************
ok:
ok:

TASK [Agent 인증서 디렉토리 생성] **************
ok:
changed:

TASK [Root CA 인증서 배포] *********************
ok:
changed:

TASK [ossec.conf에 Root CA 경로 등록] **********
changed:
changed:
```

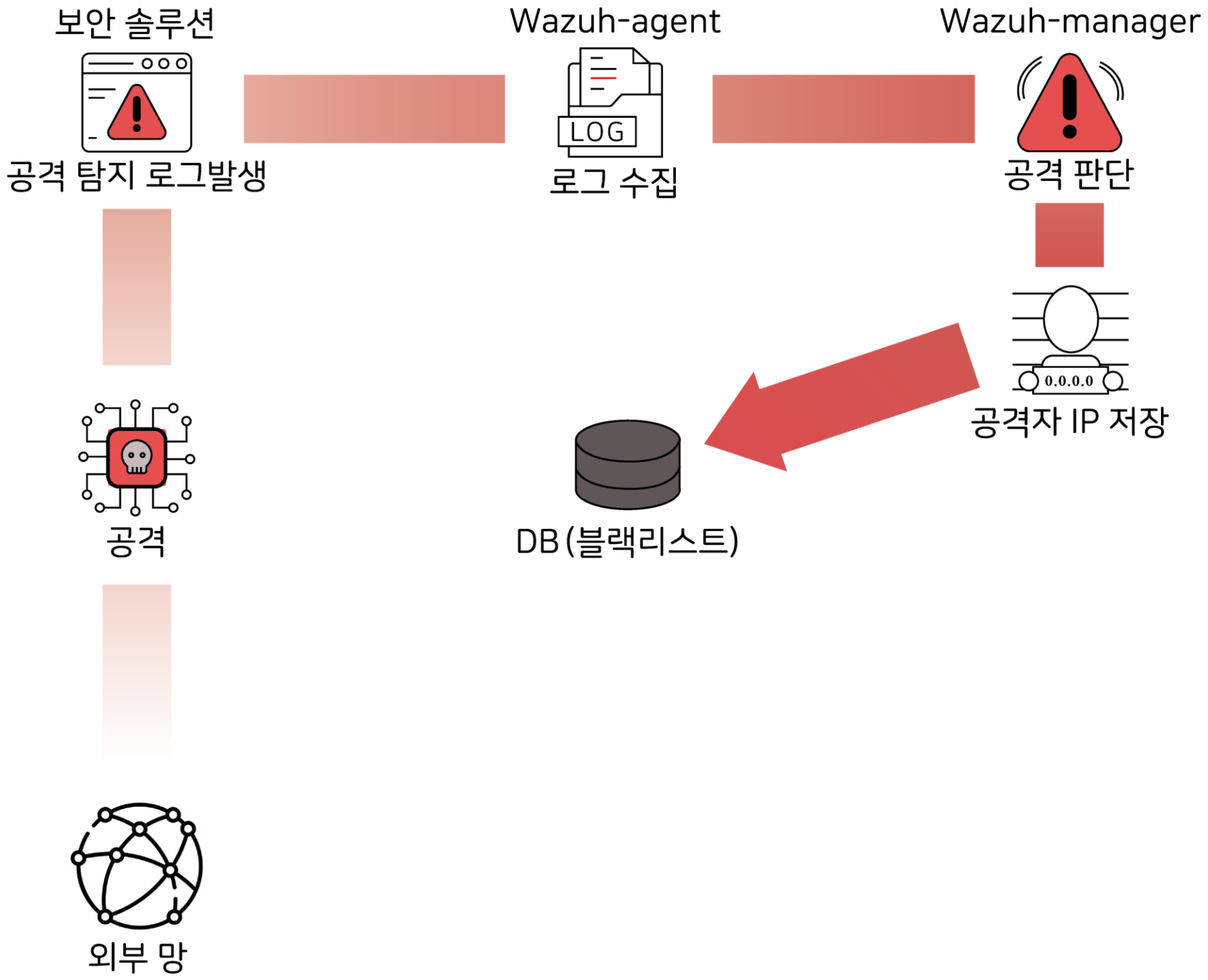
SOAR 아키텍처 흐름도

Automated Incident Response Framework



SOAR 아키텍처 흐름도

Automated Incident Response Framework




```
root@manager
  314      <disabled>yes</disabled>
  315    </cluster>
  316
  317    <integration>
  318      <name>custom-hackerdb</name>
  319      <alert_format>json</alert_format>
  320    </integration>
  321
  322  </ossec_config>
```

```
SELECT * FROM `hackerTABLE`
```

프로파일링 [한줄 편집] [수정] [SQL 분석]

모두 보기 | 행 개수: 25 행

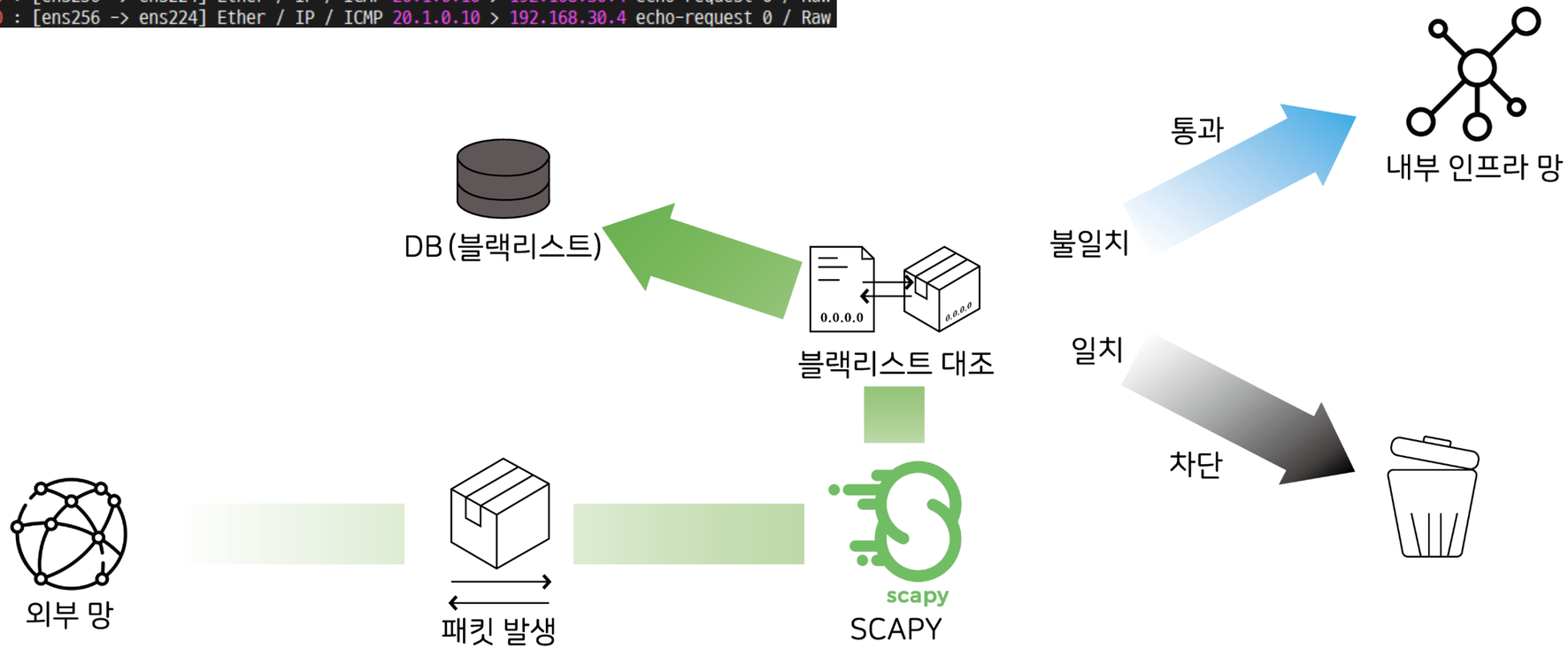
추가 옵션

	ip
수정 복사 삭제	20.1.0.10
수정 복사 삭제	40.1.0.10

SOAR 아키텍처 흐름도

Automated Incident Response Framework

```
--- scapy ips 시작 ---
필터 조건: inbound
현재 블랙리스트 : [40.1.0.10, 20.1.0.10]
DENIED : [ens256 -> ens224] Ether / IP / ICMP 20.1.0.10 > 192.168.30.4 echo-request 0 / Raw
DENIED : [ens256 -> ens224] Ether / IP / ICMP 20.1.0.10 > 192.168.30.4 echo-request 0 / Raw
DENIED : [ens256 -> ens224] Ether / IP / ICMP 20.1.0.10 > 192.168.30.4 echo-request 0 / Raw
DENIED : [ens256 -> ens224] Ether / IP / ICMP 20.1.0.10 > 192.168.30.4 echo-request 0 / Raw
DENIED : [ens256 -> ens224] Ether / IP / ICMP 20.1.0.10 > 192.168.30.4 echo-request 0 / Raw
```

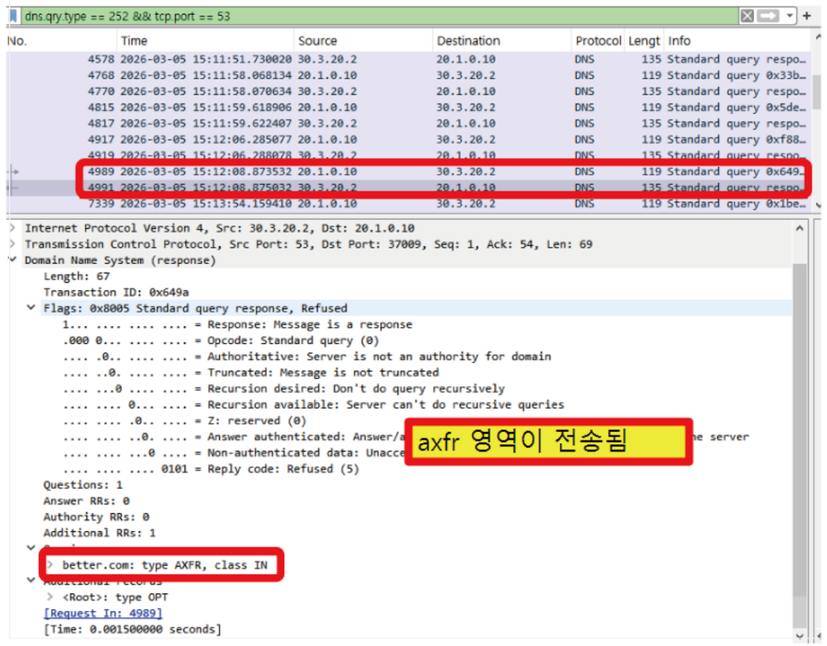


취약점 식별 및 재검증

Vulnerability Identification and Validation

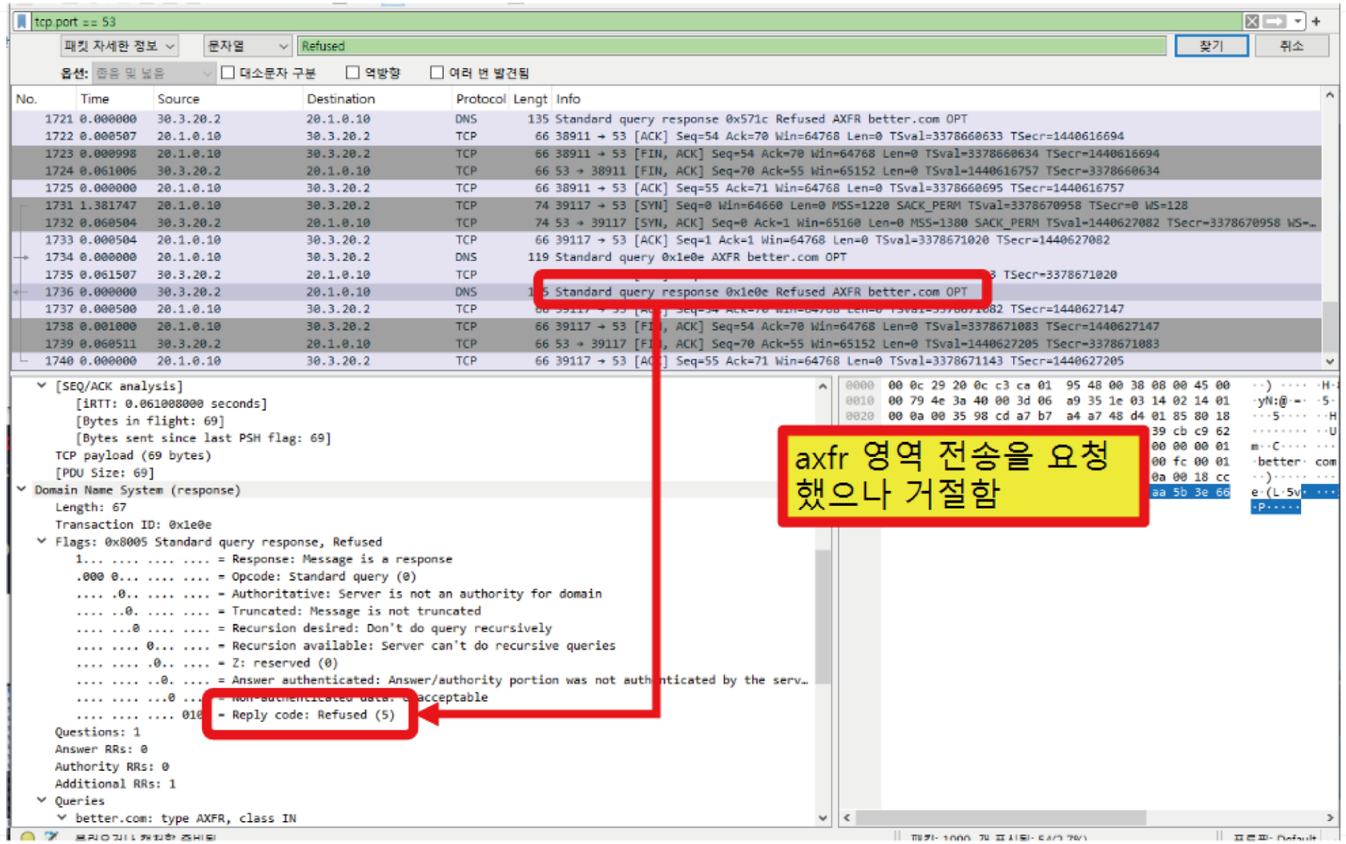
DNS 정보 탈취 취약점

취약점 탐지 및 분석



비인가 사용자에게도 axfr 영역 전송이 가능한 DNS 정보 노출 취약점

취약점 보완 및 재검증



서버에서 DNS axfr 영역 전송 가능 서버 제한하도록 보안 정책 수립

주요 정보통신 점검 가이드 준수

Compliance with Major ICT Inspection Guidelines

분류	점검 항목
계정 관리	root 계정 원격 접속 제한
	패스워드 복잡성 설정
	계정 잠금 임계값 설정
	패스워드 파일 보호
	root 이외의 UID가 '0' 금지
	root 계정 su 제한
	패스워드 최소 길이 설정
	패스워드 최대 사용기간 설정
	패스워드 최소 사용기간 설정
	불필요한 계정 제거
	관리자 그룹에 최소한의 계정 포함
	계정이 존재하지 않는 GID 금지
	동일한 UID 금지
	사용자 shell 점검
	Session Timeout 설정

분류	점검 항목
파일 및 디렉터리 관리	root 홈, 패스 디렉터리 권한 및 패스 설정
	파일 및 디렉터리 소유자 설정
	/etc/passwd 파일 소유자 및 권한 설정
	/etc/shadow 파일 소유자 및 권한 설정
	/etc/hosts 파일 소유자 및 권한 설정
	/etc/(x)inetd.conf 파일 소유자 및 권한 설정
	/etc/syslog.conf 파일 소유자 및 권한 설정
	/etc/services 파일 소유자 및 권한 설정
	SUID,SGID,Sticky bit 설정 파일 점검
	사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정
	world writable 파일 점검
	/dev에 존재하지 않는 device 파일 점검
	$HOME/.rhosts, hosts.equiv 사용 금지
	접속 IP 및 포트 제한
	hosts.lpd 파일 소유자 및 권한 설정
	UMASK 설정 관리
	홈디렉토리 소유자 및 권한 설정
	홈디렉토리로 지정한 디렉토리의 존재 관리
	숨겨진 파일 및 디렉토리 검색 및 제거

호스트 리포트

▶ 172.16.254.33 | PASS=19 | 취약/수동=25

▶ 172.16.254.55 | PASS=19 | 취약/수동=25

▼ 172.16.254.66 | PASS=23 | 취약/수동=22

▼ 계정 관리 | 상태=정상 수집 | PASS=14 | 취약/수동=16

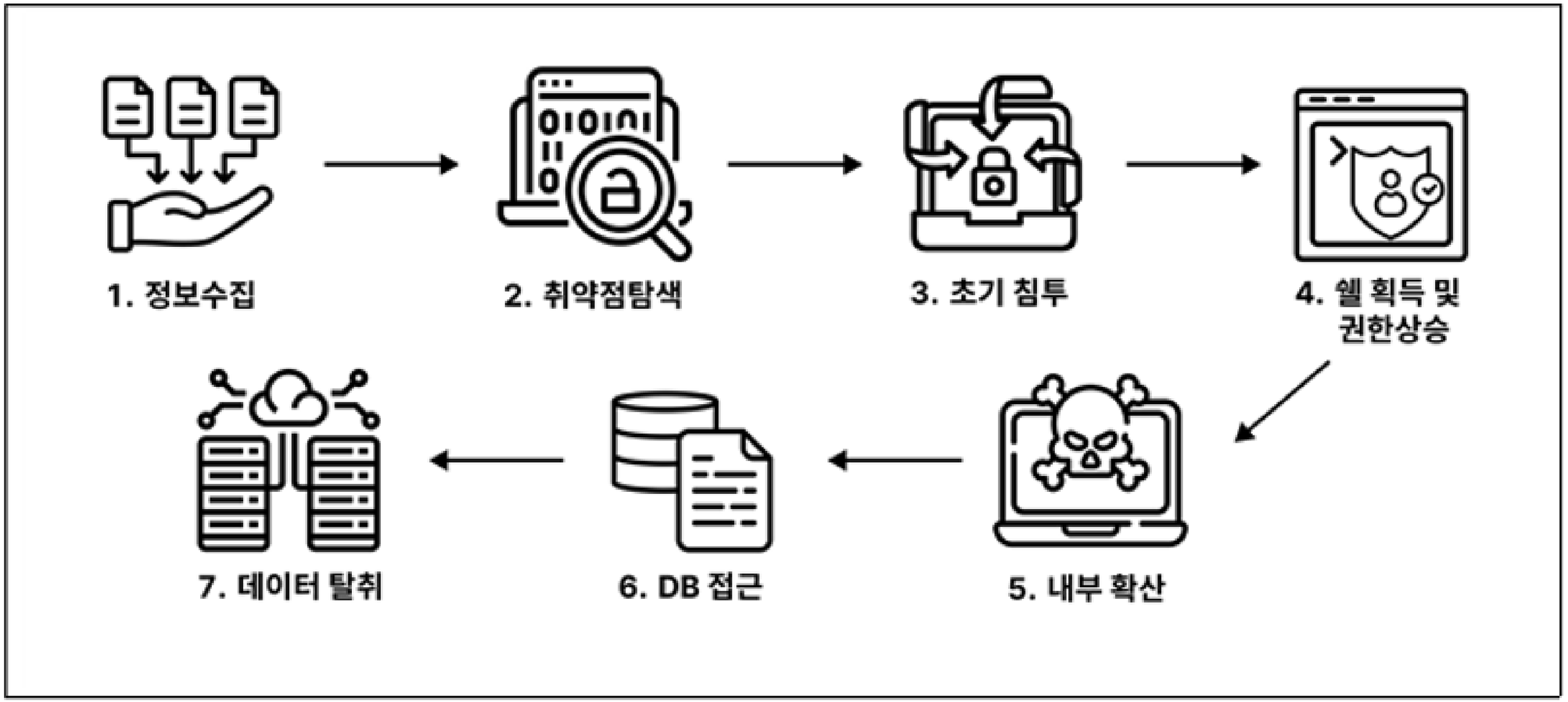
```
================================================
[ 계정 관리 보안 점검 리포트 - 2026-03-10 06:17:59 ]
대상 호스트: 172.16.254.66
================================================
[U-01] root 원격 접속 제한: VULNERABLE
[U-01] root 원격 접속 제한: VULNERABLE
[U-02] 패스워드 복잡성 설정: PASS
[U-02] 패스워드 복잡성 설정: PASS
[U-03] 계정 잠금 임계값 설정: VULNERABLE
[U-03] 계정 잠금 임계값 설정: VULNERABLE
[U-04] 패스워드 파일 보호: PASS
[U-04] 패스워드 파일 보호: PASS
[U-05] root 이외 UID 0 계정 존재: PASS
[U-05] root 이외 UID 0 계정 존재: PASS
[U-06] su 제한 설정(pam_wheel): VULNERABLE
[U-06] su 제한 설정(pam_wheel): VULNERABLE
[U-44] 패스워드 최소 길이(8자): VULNERABLE
[U-44] 패스워드 최소 길이(8자): VULNERABLE
```

ISMS(정보보호 관리 체계) 인증 기준 반영

Compliance with ISMS Certification Criteria

분류	점검 항목	
사고 예방 및 대응체계 구축	**침해사고를 예방하고 사고 발생 시 신속하고 효과적으로 대응할 수 있도록 내,외부 침해시도의 탐지,대응,분석 및 공유를 위한 체계와 절차를 수립하고, 관련 외부기관 및 전문가들과 협조 체계를 구축하여야 한다.**	
	사고 발생 시 신속하고 효과적으로 대응하기 위한 체계와 절차를 마련하고 있는가?	O
	침해사고의 모니터링, 대응 및 처리를 위하여 외부전문가와의 협조체계를 수립하고 있는가?	O
취약점 점검 및 조치	**정기적으로 취약점 점검을 수행하고 발견된 취약점에 대해서는 신속하게 조치하여야 한다. 또한 최신 보안취약점의 발생 여부를 지속적으로 파악하고 정보시스템에 미치는 영향을 분석하여 조치하여야 한다.**	
	정보시스템 취약점 점검 절차를 수립하고 정기적으로 점검을 수행하고 있는가?	O
	발견된 취약점에 대한 조치를 수행하고 그 결과를 책임자에게 보고하고 있는가?	O
	최신 보안취약점 발생 여부를 지속적으로 파악하고 정보시스템에 미치는 영향을 분석하여 조치하고 있는가?	O
이상행위 분석 및 모니터링	**내,외부에 의한 침해시도, 개인정보유출 시도, 부정행위 등을 신속하게 탐지,대응할 수 있도록 네트워크 및 데이터 흐름 등을 수집하여 분석하며, 모니터링 및 점검 결과에 따른 사후조치는 적시에 이루어져야 한다.**	
	이상행위를 탐지할 수 있도록 주요 정보시스템, 응용프로그램, 네트워크, 보안시스템 등에서 발생한 네트워크 트래픽, 데이터 흐름, 이벤트 로그 등을 수집하여 분석 및 모니터링하고 있는가?	O
	침해시도, 개인정보유출시도, 부정행위 등의 여부를 판단하기 위한 기준 및 임계치를 정의하고 이에 따라 이상행위의 판단 및 조사 등 후속 조치가 적시에 이루어지고 있는가?	O
사고 대응 및 복구	**침해사고 및 개인정보 유출 징후나 발생을 인지한 때에는 법적 통지 및 신고 의무를 준수하여야 하며, 절차에따라 신속하게 대응 및 복구하고 사고분석 후 재발방지 대책을 수립하여 대응체계에 반영하여야한다.**	
	침해사고 및 개인정보 유출의 징후 또는 발생을 인지한 경우 정의된 침해사고 대응절차에 따라 신속하게 대응 및 보고가 이루어지고 있는가?	O
	개인정보 침해사고 발생 시 관련 법령에 따라 정보주체(이용자) 통지 및 관계기관 신고 절차를 이행하고 있는가?	O
	침해사고가 종결된 후 사고의 원인을 분석하여 그 결과를 보고하고 관련 조직 및 인력과 공유하고 있는가?	O
	유사사고가 재발하지 않도록 대책을 수립하고 필요한 경우 침해사고 대응절차 등을 변경하고 있는가?	O

공격 수행 프로세스



개요 및 점검 범위

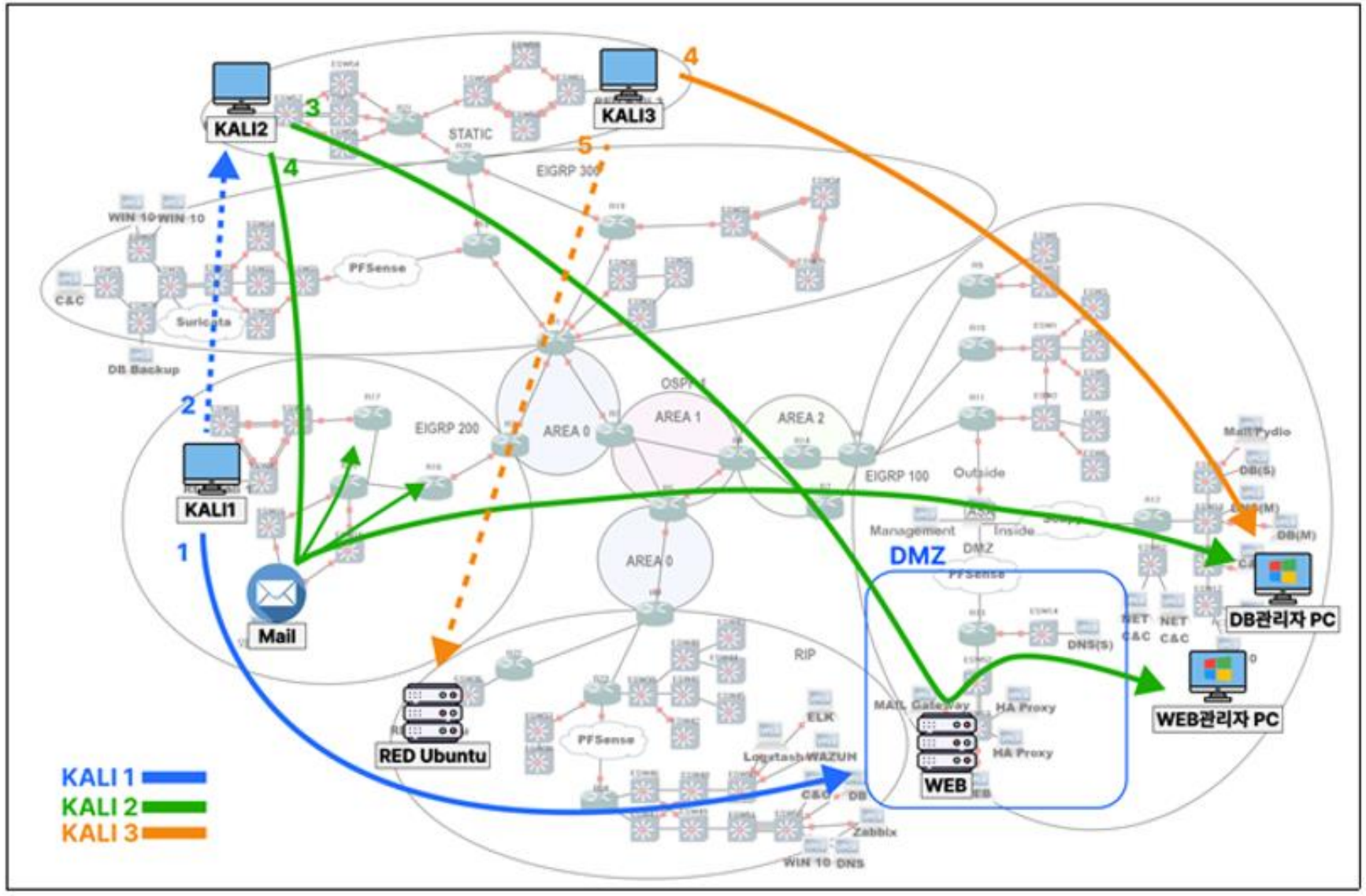
구 분	항 목	내 용
점검 대상	외부 웹 서비스	www.better.com
	내부 관리망	내부 IP대역
	핵심 서버	Web, DB server
핵심 타겟	중요 데이터	고객 및 파트너사 데이터
	관리자 자산	내부 관리자 PC 및 관리 시스템
점검 방식	수행 유형	모의 침투 테스트
수행 기간	테스트 기간	2026.03.02. ~ 2026.03.06

본 점검은 외부 공격자가 인터넷 환경에서 접근 가능한 대외 웹 서비스를 시작점으로,
취약점 악용을 통해 내부 관리망 및 핵심 데이터베이스(DB) 자산까지
단계적으로 침투 가능한지를 검증하는 것을 목표로 수행되었다.

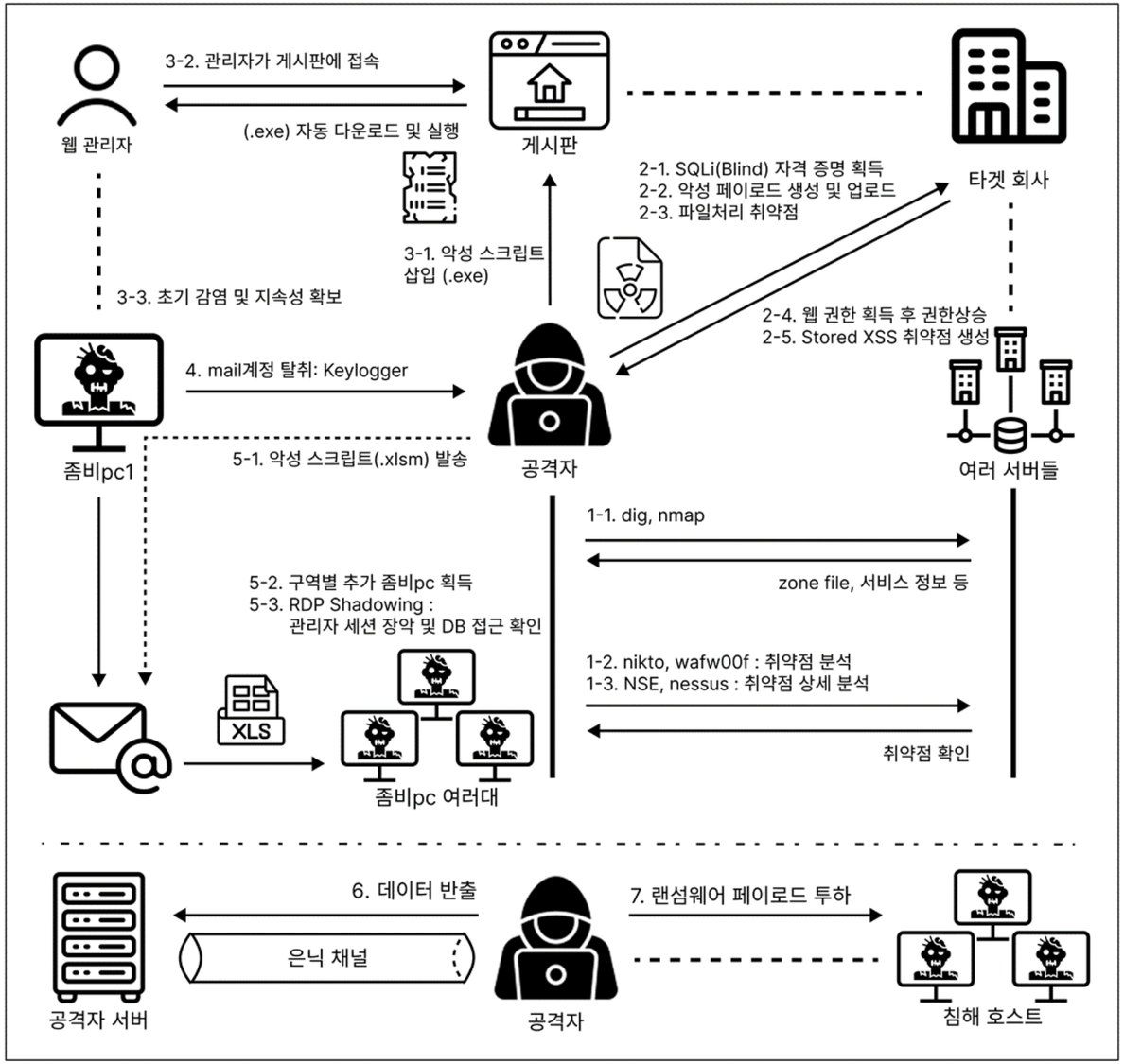
점검 수행 체계

구분	세부 항목	상세 내용 및 기술적 요건
전략	공격 모델	Cyber Kill-Chain: 단계적 침투 모델 적용
	화이트박스 협업	인프라·시나리오 공유 기반 '정보 공유형' 실효성 검증
대상	인프라 자산	DMZ(Web), 내부망(Admin PC), 핵심 DB 서버 및 네트워크 장비
	공격 벡터	OWASP Top 10(SQLi, XSS 등), 시스템 CVE, 권한 상승 기법
규칙	시스템 가용성 보장	CPU 80% / 응답 300ms 지연 시 즉시 중단
	데이터 무결성	Snapshot 기반 복구 및 실제 데이터 파괴·수정 엄격 금지
	운영 가이드	업무시간(09~18시) 준수 및 범위 외 자산 침투 제한
지표	시나리오 완수	전 단계 킬체인 완수 및 핵심 DB 접근 권한 확보
	보안 공백 식별	방어 기전(WAF/IDS/SOAR) 우회 및 개선 권고안 도출

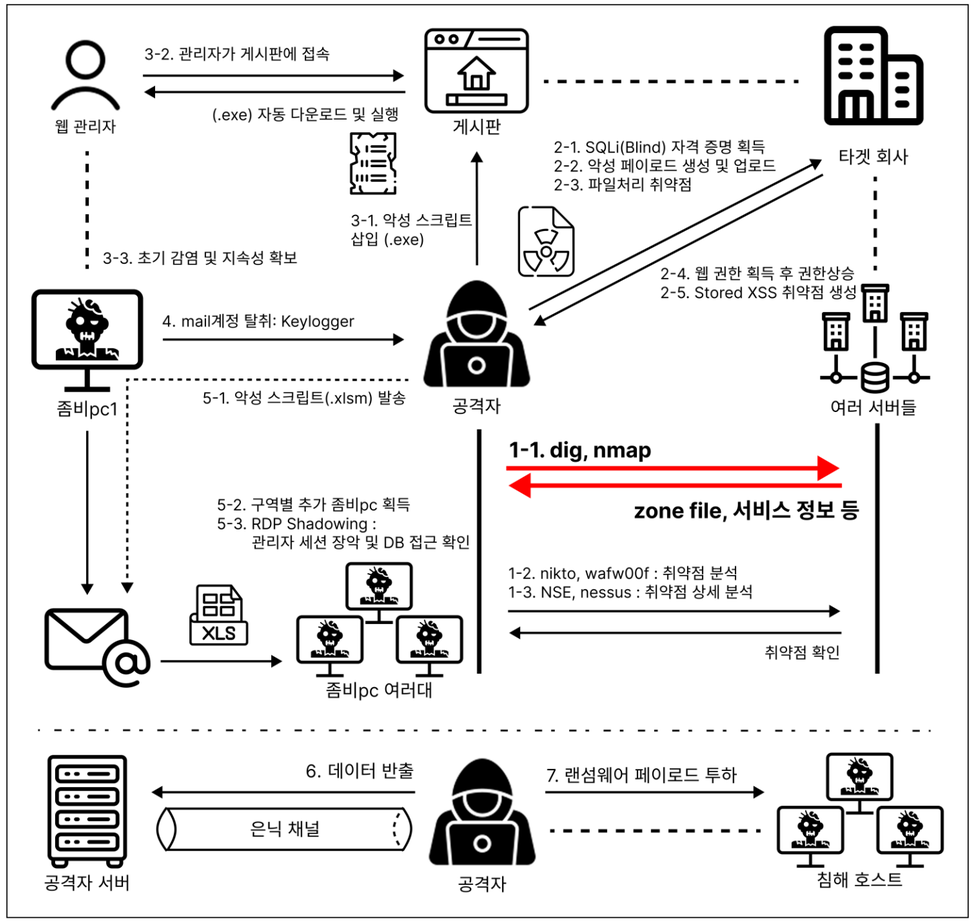
공격 경로


KALI2
KALI3
KALI1
Mail
RED Ubuntu
WEB
DB관리자 PC
WEB관리자 PC
STATIC
EIGRP 300
EIGRP 200
EIGRP 100
AREA 0
AREA 1
AREA 2
OSPF 1
RIP
PFSense
Suricata
C&C
DB Backup
WIN 10
WIN 10
DMZ
Management
Outside
Inside
MAIL Gateway
HA Proxy
HA Proxy
DNS(S)
ELK
Logstash
WAZUH
Zabbix
WIN 10 DNS
Mail Pydio
DB(S)
DB(M)
NET
C&C
1
2
3
4
4
5
KALI 1
KALI 2
KALI 3

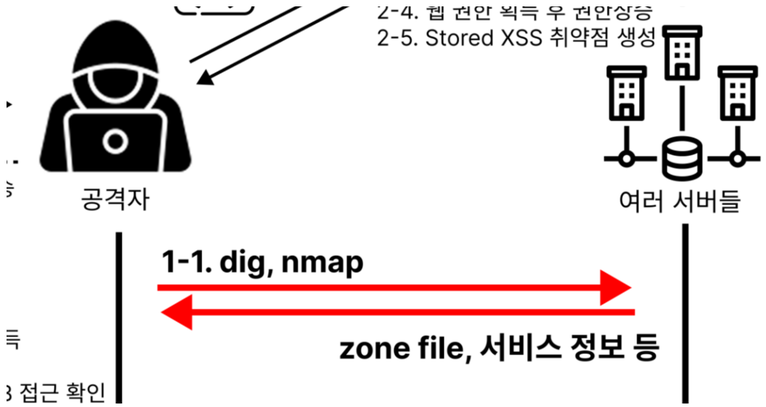
시나리오


3-2. 관리자가 게시판에 접속
(.exe) 자동 다운로드 및 실행
웹 관리자
게시판
타겟 회사
2-1. SQLi(Blind) 자격 증명 획득
2-2. 악성 페이로드 생성 및 업로드
2-3. 파일처리 취약점
3-1. 악성 스크립트
삽입 (.exe)
3-3. 초기 감염 및 지속성 확보
2-4. 웹 권한 획득 후 권한상승
2-5. Stored XSS 취약점 생성
4. mail계정 탈취: Keylogger
좀비pc1
5-1. 악성 스크립트(.xlsm) 발송
공격자
여러 서버들
1-1. dig, nmap
zone file, 서비스 정보 등
5-2. 구역별 추가 좀비pc 획득
5-3. RDP Shadowing :
관리자 세션 장악 및 DB 접근 확인
1-2. nikto, wafw00f : 취약점 분석
1-3. NSE, nessus : 취약점 상세 분석
취약점 확인
XLS
좀비pc 여러대
6. 데이터 반출
은닉 채널
7. 랜섬웨어 페이로드 투하
공격자 서버
공격자
침해 호스트

시나리오


웹 관리자
3-2. 관리자가 게시판에 접속
(.exe) 자동 다운로드 및 실행
게시판
타겟 회사
2-1. SQLi(Blind) 자격 증명 획득
2-2. 악성 페이로드 생성 및 업로드
2-3. 파일처리 취약점
3-1. 악성 스크립트
삽입 (.exe)
3-3. 초기 감염 및 지속성 확보
2-4. 웹 권한 획득 후 권한상승
2-5. Stored XSS 취약점 생성
4. mail계정 탈취: Keylogger
좀비pc1
5-1. 악성 스크립트(.xlsm) 발송
공격자
여러 서버들
1-1. dig, nmap
zone file, 서비스 정보 등
5-2. 구역별 추가 좀비pc 획득
5-3. RDP Shadowing :
관리자 세션 장악 및 DB 접근 확인
XLS
1-2. nikto, wafw00f : 취약점 분석
1-3. NSE, nessus : 취약점 상세 분석
취약점 확인
좀비pc 여러대
6. 데이터 반출
은닉 채널
7. 랜섬웨어 페이로드 투하
공격자 서버
공격자
침해 호스트

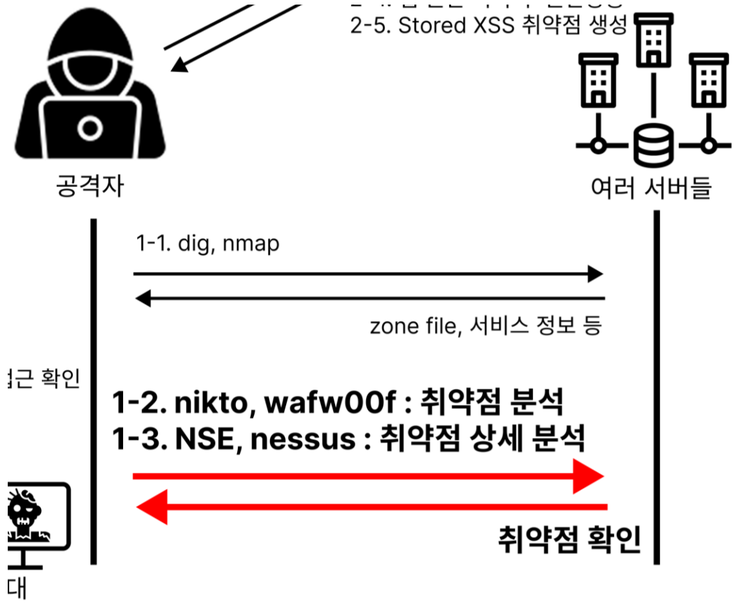
시나리오




```
; <<>> DiG 9.20.11-4+b1-Debian <<>> better.com axfr
;; global options: +cmd
better.com.             604800  IN      SOA
com. 5 3600 1800 604800 86400
better.com.             604800  IN      NS
better.com.             604800  IN      A
better.com.             604800  IN      AAAA
mail.better.com.        604800  IN      A
ns1.better.com.         604800  IN      A
web1.better.com.        604800  IN      A
www.better.com.         604800  IN      A
better.com.             604800  IN      SOA
com. 5 3600 1800 604800 86400
;; Query time: 28 msec
;; SERVER: 30.3.20.2#53(30.3.20.2) (TCP)
;; WHEN: Wed Mar 04 17:18:24 KST 2026
;; XFR size: 9 records (messages 1, bytes 295)
```

```
Nmap scan report for
Host is up (0.025s latency).

PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

시나리오




```
|       NGINX:CVE-2025-53859    6.3     https://vulners.com/nginx/NGINX:CVE-2
025-53859
|       NGINX:CVE-2024-7347     5.7     https://vulners.com/nginx/NGINX:CVE-2
024-7347
|_      NGINX:CVE-2025-23419    5.3     https://vulners.com/nginx/NGINX:CVE-2
025-23419
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-cookie-flags:
|   /login.php:
|     PHPSESSID:
|       httponly flag not set
| http-enum:
|   /login.php: Possible admin folder
|_  /uploads/: Potentially interesting folder w/ directory listing
|_http-server-header: nginx/1.26.3 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

HIGH **CGI Generic SQL Injection (blind)**

Description

By sending specially crafted parameters to one or more CGI scripts hosted on the remote web server, Nessus was able to get a very different response, which suggests that it may have been able to modify the behavior of the application and directly access the underlying database.

An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.

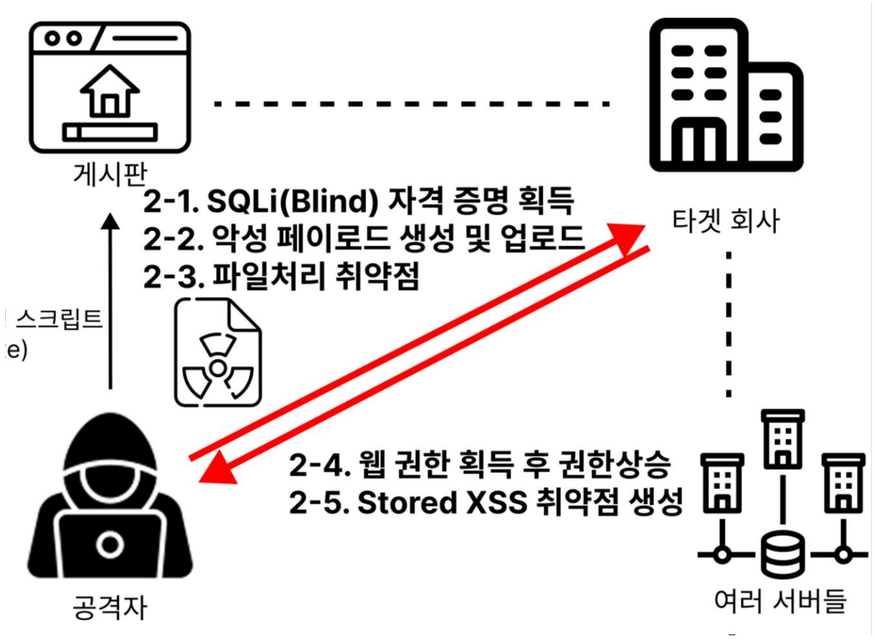
Solution

Modify the affected CGI scripts so that they properly escape arguments.

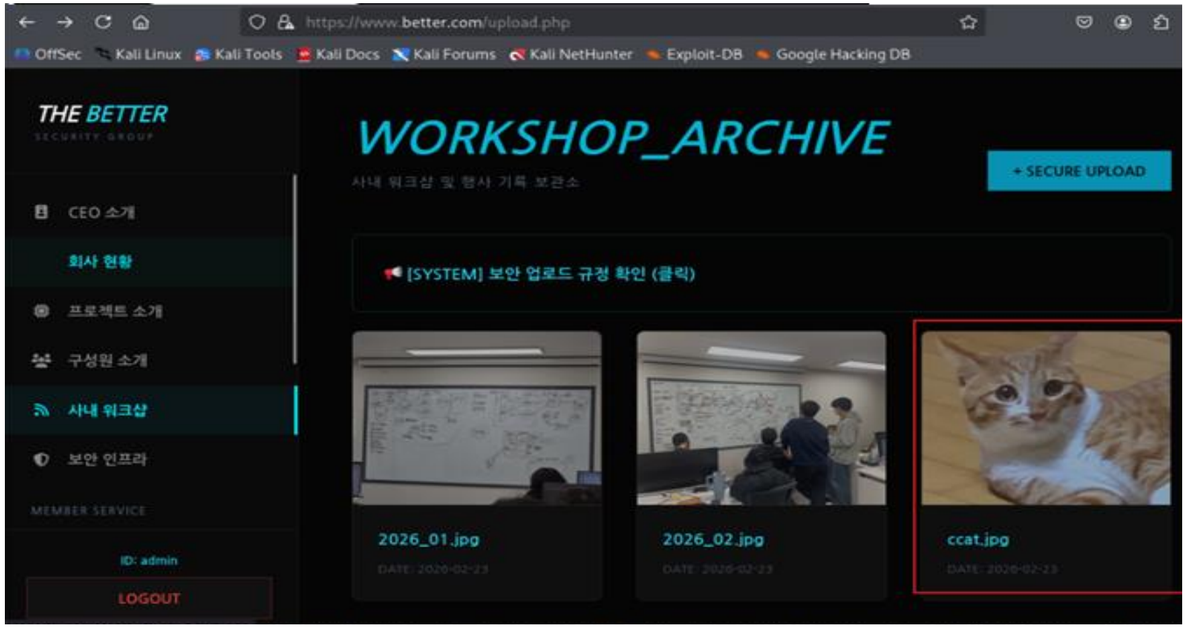
See Also

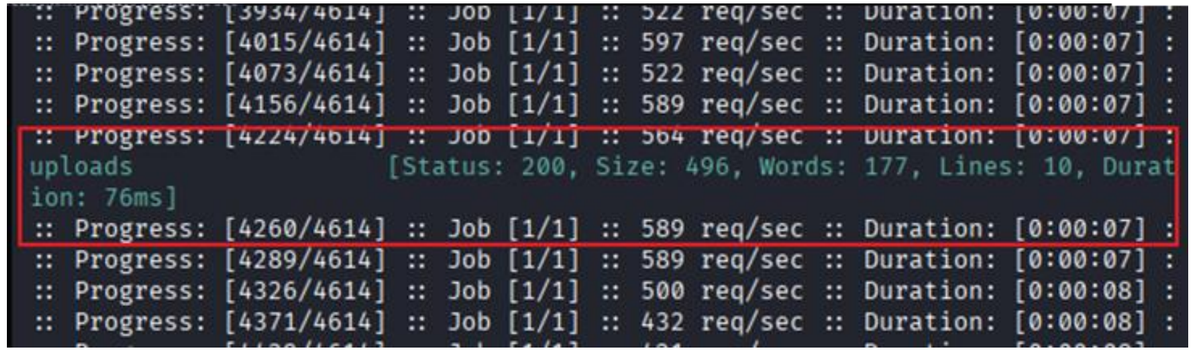
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://www.nessus.org/u?ed792cf5
http://www.nessus.org/u?11ab1866

시나리오

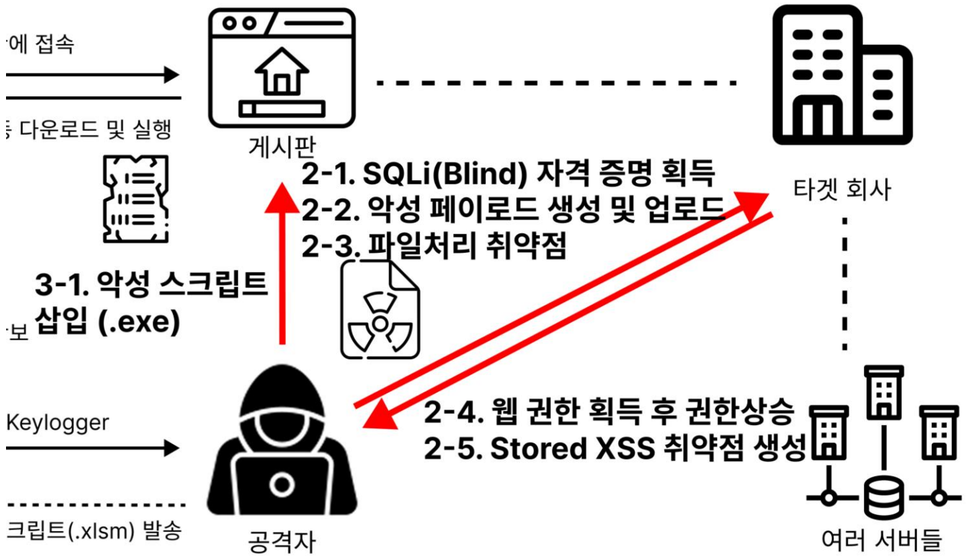

게시판
타겟 회사
2-1. SQLi(Blind) 자격 증명 획득
2-2. 악성 페이로드 생성 및 업로드
2-3. 파일처리 취약점
스크립트
e)
2-4. 웹 권한 획득 후 권한상승
2-5. Stored XSS 취약점 생성
공격자
여러 서버들


=== Dumping Data from users ===
[Searching Admin ID]
[Searching Admin Password]
[!] 최종 탈취 성공
ID:
PW:


https://www.better.com/upload.php
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
THE BETTER
SECURITY GROUP
WORKSHOP_ARCHIVE
사내 워크샵 및 행사 기록 보관소
+ SECURE UPLOAD
CEO 소개
회사 현황
프로젝트 소개
구성원 소개
사내 워크샵
보안 인프라
MEMBER SERVICE
ID: admin
LOGOUT
[SYSTEM] 보안 업로드 규정 확인 (클릭)
2026_01.jpg
2026_02.jpg
ccat.jpg


:: Progress: [4015/4614] :: Job [1/1] :: 597 req/sec :: Duration: [0:00:07] :
:: Progress: [4073/4614] :: Job [1/1] :: 522 req/sec :: Duration: [0:00:07] :
:: Progress: [4156/4614] :: Job [1/1] :: 589 req/sec :: Duration: [0:00:07] :
uploads [Status: 200, Size: 496, Words: 177, Lines: 10, Durat
ion: 76ms]
:: Progress: [4260/4614] :: Job [1/1] :: 589 req/sec :: Duration: [0:00:07] :
:: Progress: [4289/4614] :: Job [1/1] :: 589 req/sec :: Duration: [0:00:07] :
:: Progress: [4326/4614] :: Job [1/1] :: 500 req/sec :: Duration: [0:00:08] :
:: Progress: [4371/4614] :: Job [1/1] :: 432 req/sec :: Duration: [0:00:08] :

시나리오



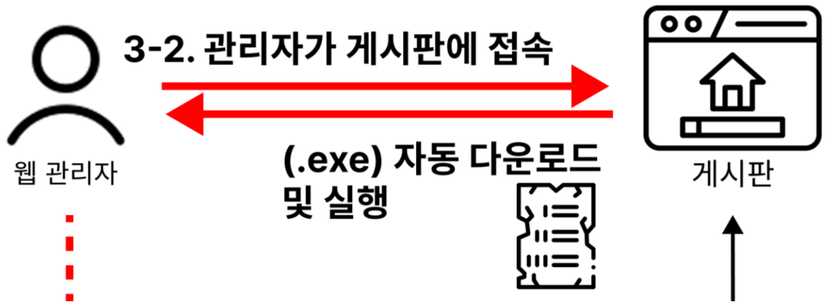

```
Active sessions
==============

  Id  Name  Type                   Information       Connection
  --  ----  ----                   -----------       ----------
  1         meterpreter php/linux  www-data @ [redacted]
```

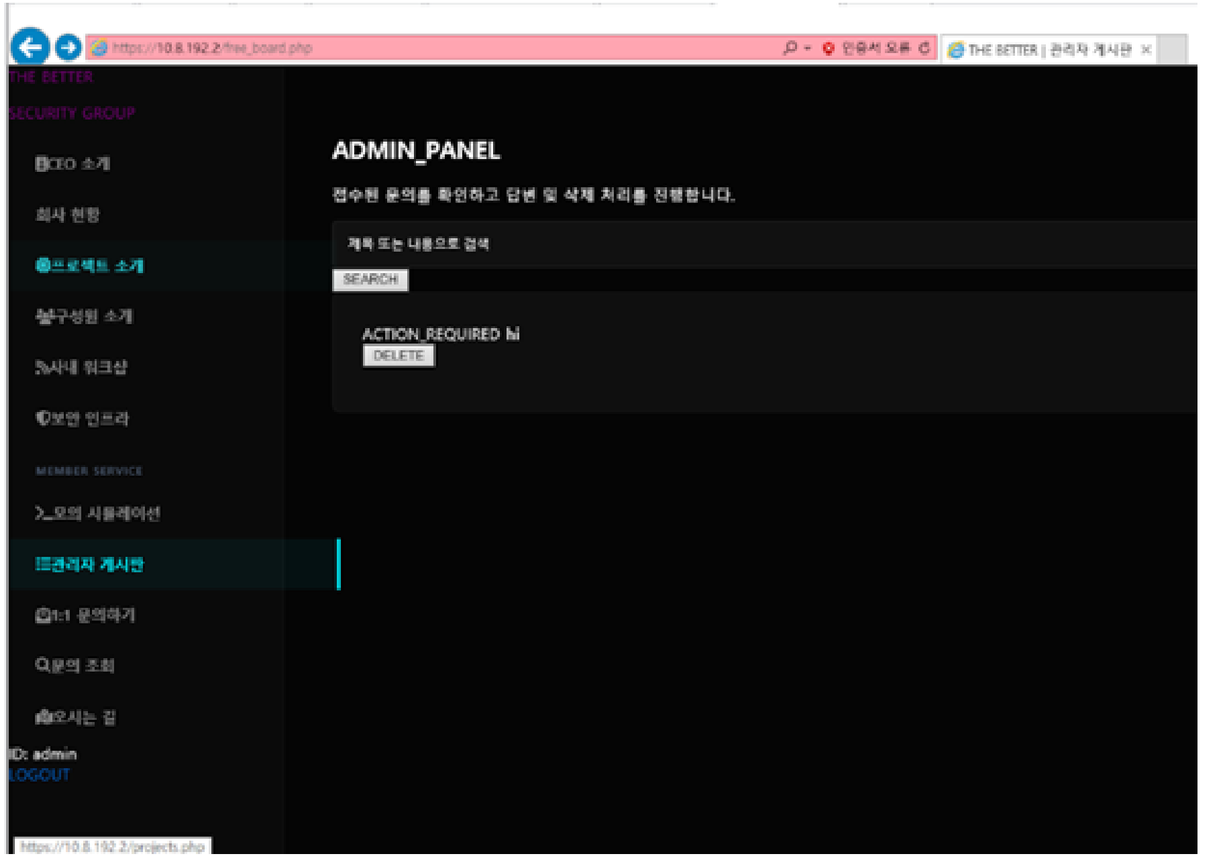
```
whoami
www-data
```

권한 상승

```
whoami
root
```

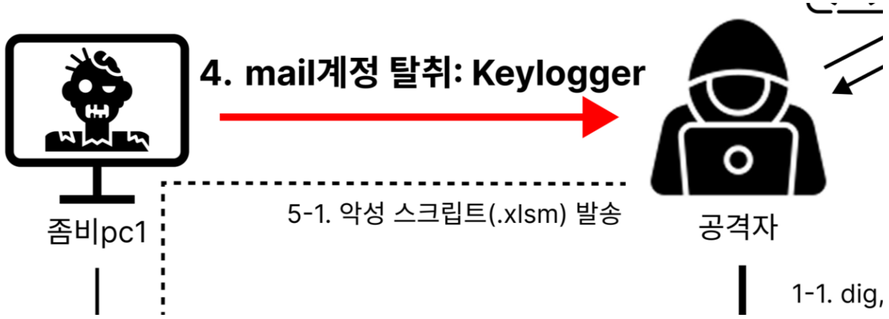
시나리오

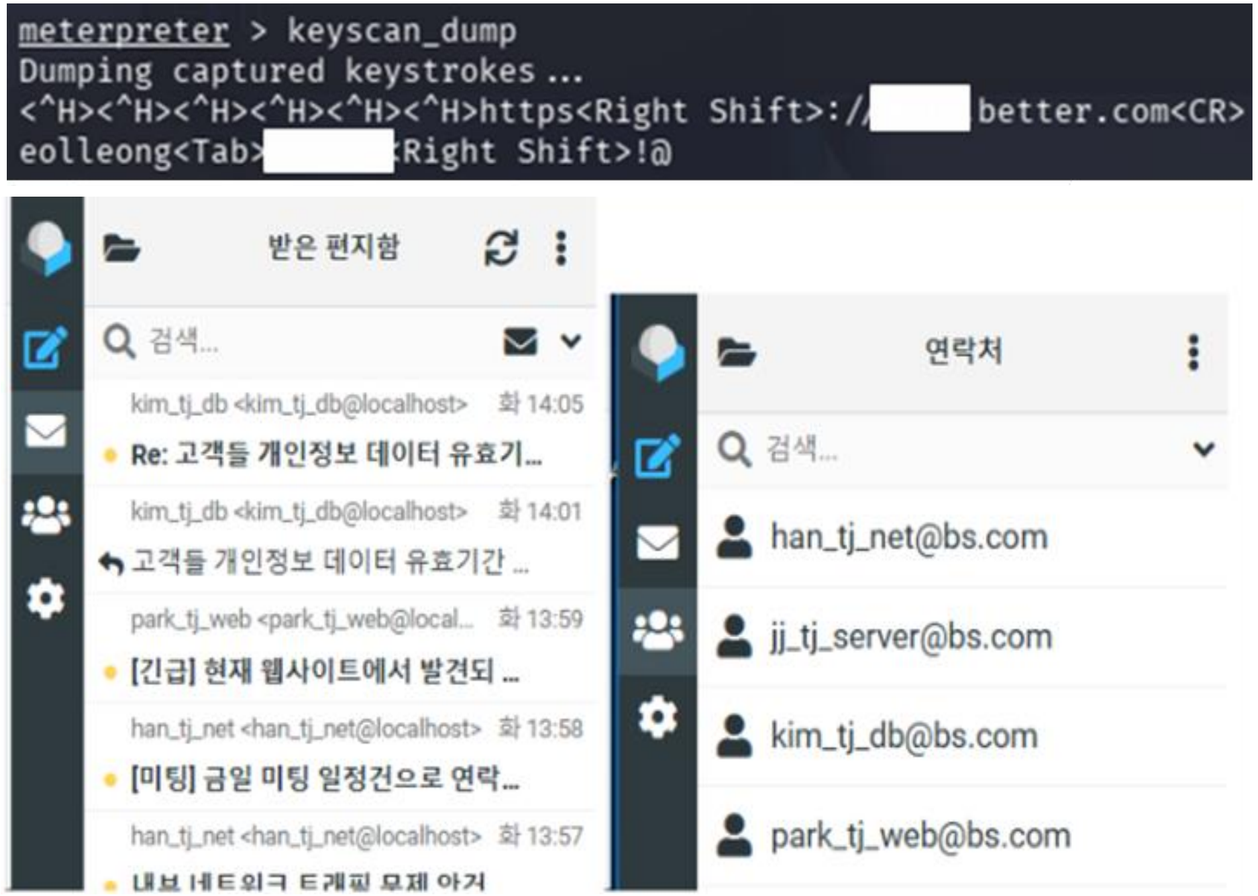

3-2. 관리자가 게시판에 접속
(.exe) 자동 다운로드
및 실행
웹 관리자
게시판


THE BETTER
SECURITY GROUP
CEO 소개
회사 현황
프로젝트 소개
팀구성원 소개
사내 워크샵
보안 인프라
MEMBER SERVICE
모의 시뮬레이션
관리자 게시판
1:1 문의하기
문의 조회
오시는 길
ID: admin
LOGOUT
ADMIN_PANEL
접수된 문의를 확인하고 답변 및 삭제 처리를 진행합니다.
제목 또는 내용으로 검색
SEARCH
ACTION_REQUIRED hi
DELETE

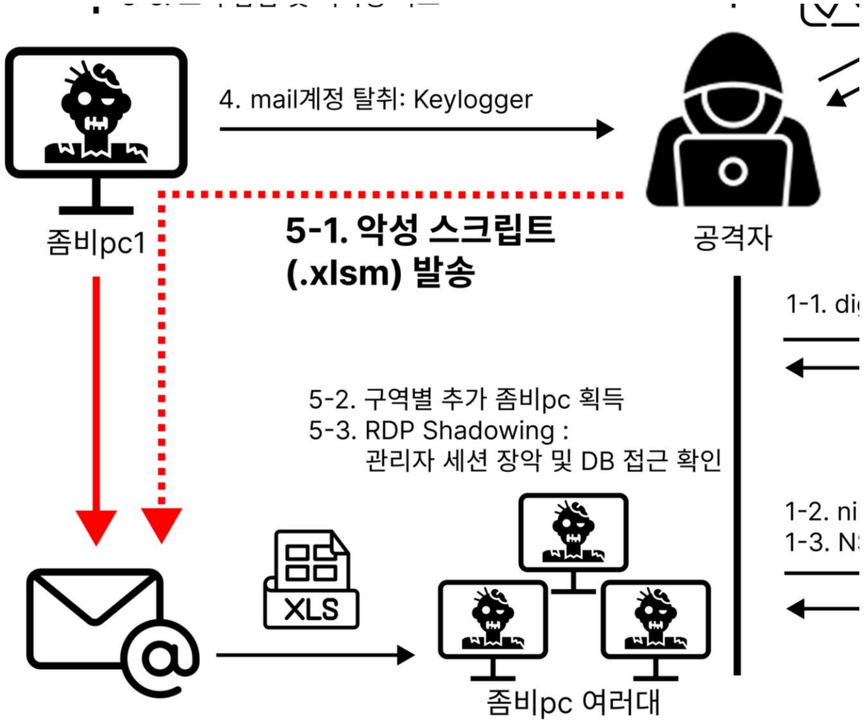

Active sessions
Id Name Type Information Connection
2 meterpreter x86/windows

시나리오

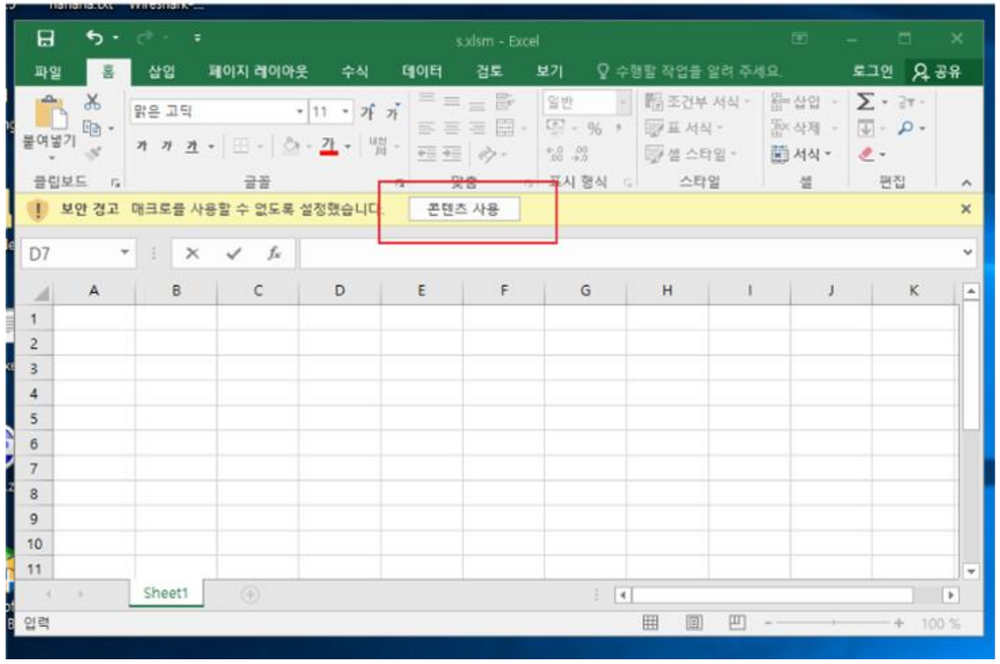

4. mail계정 탈취: Keylogger
좀비pc1
5-1. 악성 스크립트(.xlsm) 발송
공격자
1-1. dig,


meterpreter > keyscan_dump
Dumping captured keystrokes ...
<^H><^H><^H><^H><^H><^H>https<Right Shift>:/ better.com<CR>
eolleong<Tab> <Right Shift>!@
받은 편지함
검색...
kim_tj_db <kim_tj_db@localhost> 화 14:05
Re: 고객들 개인정보 데이터 유효기...
kim_tj_db <kim_tj_db@localhost> 화 14:01
고객들 개인정보 데이터 유효기간 ...
park_tj_web <park_tj_web@local... 화 13:59
[긴급] 현재 웹사이트에서 발견되 ...
han_tj_net <han_tj_net@localhost> 화 13:58
[미팅] 금일 미팅 일정건으로 연락...
han_tj_net <han_tj_net@localhost> 화 13:57
연락처
검색...
han_tj_net@bs.com
jj_tj_server@bs.com
kim_tj_db@bs.com
park_tj_web@bs.com

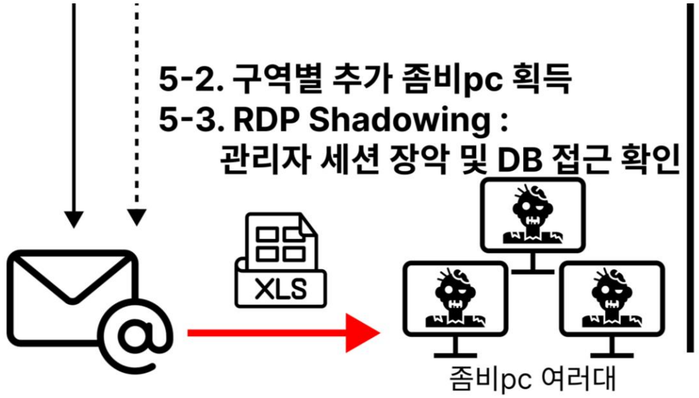
시나리오

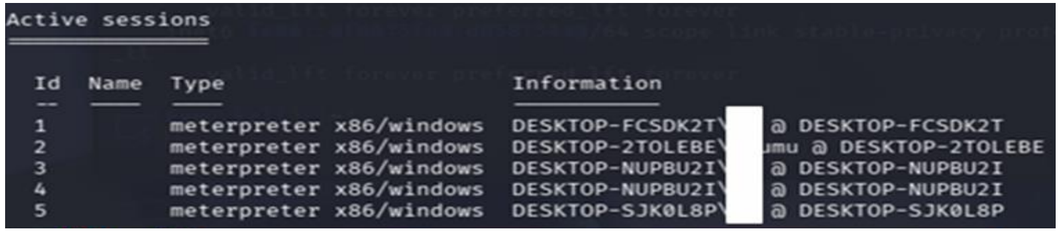

4. mail계정 탈취: Keylogger
좀비pc1
5-1. 악성 스크립트
(.xlsm) 발송
공격자
1-1. di
5-2. 구역별 추가 좀비pc 획득
5-3. RDP Shadowing :
관리자 세션 장악 및 DB 접근 확인
1-2. ni
1-3. N
XLS
좀비pc 여러대

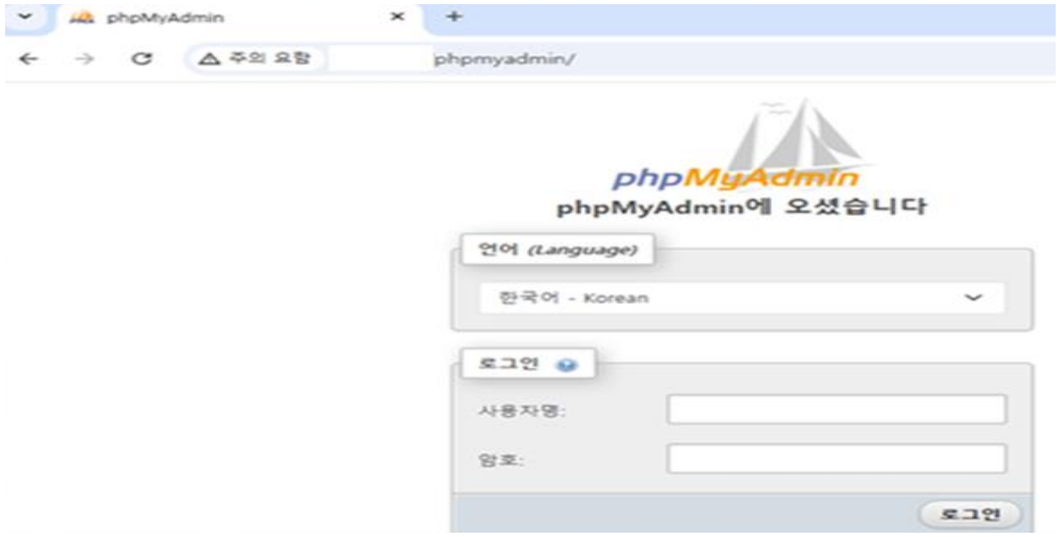

받은 편지함
회신
전체 회신
전달
삭제
표시
더 보기
검색...
eolleong <eolleong@localhost> 오늘 13:50
[공지] 2026년도 서비스 구역별 인프라 ...
kim_tj_db <kim_tj_db@localhost> 화 14:03
ㅇㅇ데이터베이스 보관에 따른 서버 이...
han_tj_net <han_tj_net@localhost> 화 13:58
[미팅] 금일 미팅 일정건으로 연락드립...
han_tj_net <han_tj_net@localhost> 화 13:57
내부 네트워크 트래픽 문제 안건
eolleong <eolleong@localhost> 화 13:55
[서버] 신규 서버 구성 관련 회의일정
eolleong <eolleong@localhost> 화 13:53
[공지] 2026년도 TJ그룹 전체 공지
[공지] 2026년도 서비스 구역별 인프라 자산 실사 및 예산 편성안
보낸 사람
날짜: 2026-02-22 13:50
세부사항
헤더
2026년 구역별 예산안.xlsm (~3 KB)
안녕하십니까, 웹서버 관리자입니다.
2026년도 통합 인프라 고도화 사업과 관련하여, 각 서비스 구역별 서버, DB, 보안 장비에 대한 예산 할당안이 취합되었습니다.
모든 관리자께서는 첨부된 '2026년 구역별 예산안.xlsm' 파일을 확인하시어, 본인 담당 영역의 장비 리스트와 예산 산출 내역에 이상이 없는지 회신 검토 부탁드립니다.
본 파일은 실시간 자산 관리 시스템과 연동되어 있어, 실행 시 상단의 [콘텐츠 사용]을 클릭하셔야 최신 단가 및 자산 정보가 로딩됩니다.
감사합니다.

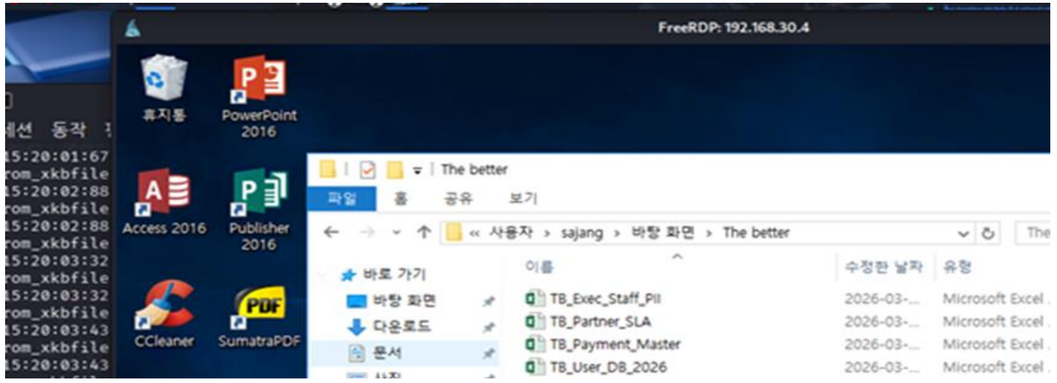

s.xlsm - Excel
파일
홈
삽입
페이지 레이아웃
수식
데이터
검토
보기
로그인
공유
붙여넣기
맑은 고딕
보안 경고 매크로를 사용할 수 없도록 설정했습니다.
콘텐츠 사용
D7
Sheet1
입력

시나리오

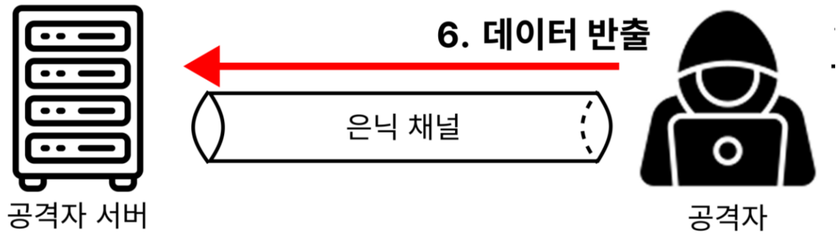

5-2. 구역별 추가 좀비pc 획득
5-3. RDP Shadowing :
관리자 세션 장악 및 DB 접근 확인
XLS
좀비pc 여러대


Active sessions
Id Name Type Information
1 meterpreter x86/windows DESKTOP-FCSDK2T @ DESKTOP-FCSDK2T
2 meterpreter x86/windows DESKTOP-2TOLEBE @ DESKTOP-2TOLEBE
3 meterpreter x86/windows DESKTOP-NUPBU2I @ DESKTOP-NUPBU2I
4 meterpreter x86/windows DESKTOP-NUPBU2I @ DESKTOP-NUPBU2I
5 meterpreter x86/windows DESKTOP-SJK0L8P @ DESKTOP-SJK0L8P


phpMyAdmin
주의 요함
phpmyadmin/
phpMyAdmin
phpMyAdmin에 오셨습니다
언어 (Language)
한국어 - Korean
로그인
사용자명:
암호:
로그인


FreeRDP: 192.168.30.4
휴지통
PowerPoint 2016
Access 2016
Publisher 2016
CCleaner
SumatraPDF
The better
파일 홈 공유 보기
« 사용자 › sajang › 바탕 화면 › The better
바로 가기
바탕 화면
다운로드
문서
이름
수정한 날짜
유형
TB_Exec_Staff_PII
TB_Partner_SLA
TB_Payment_Master
TB_User_DB_2026
Microsoft Excel

시나리오

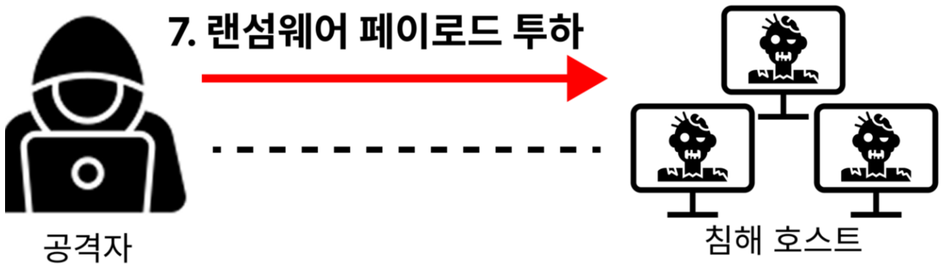


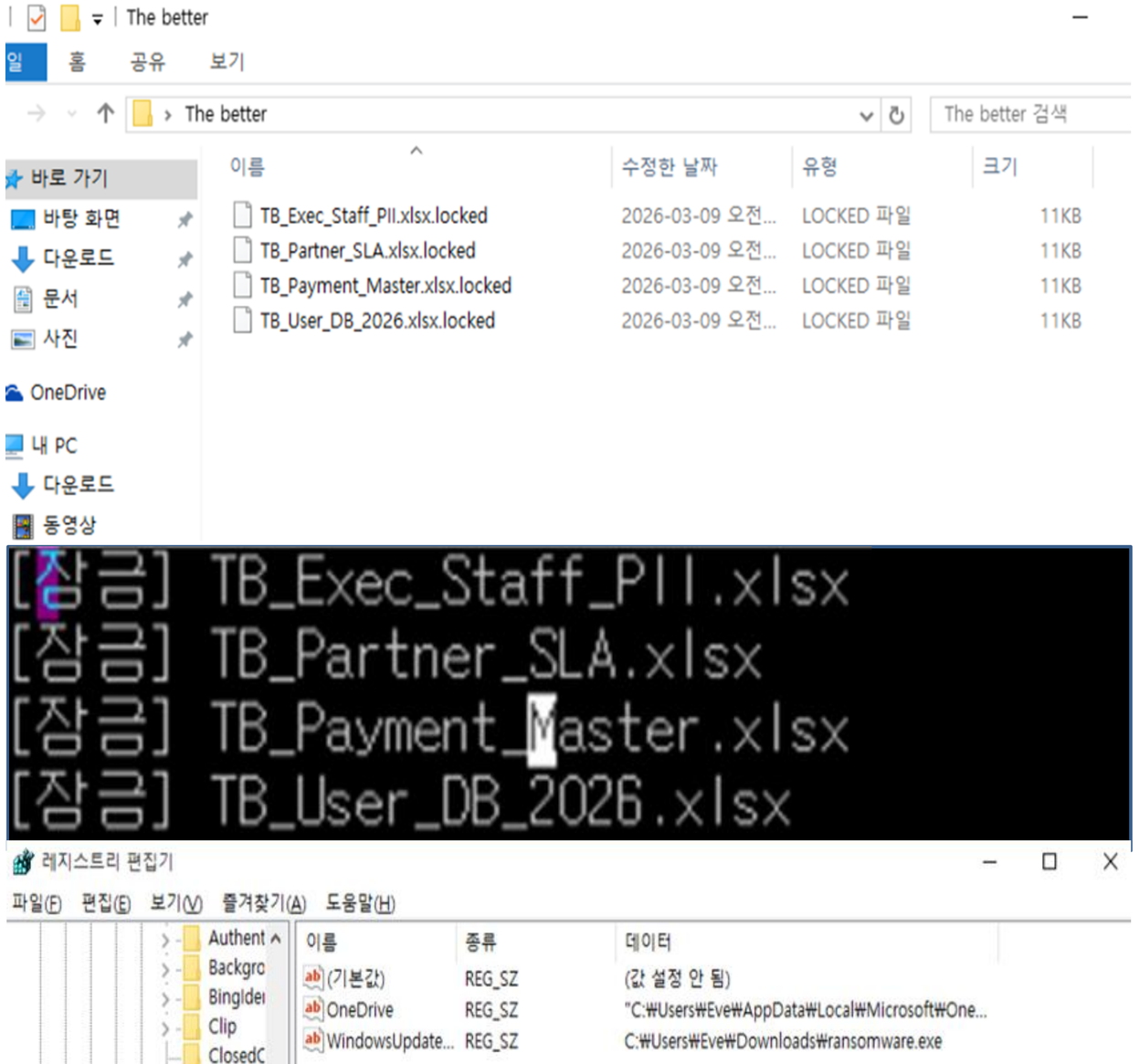

```
meterpreter > [redacted]
[*] downloading: C:/Users/sajang/Desktop/The better\TB_Exec_Staff_PII.xlsx → /home/Eve/
[*] Completed  : C:/Users/sajang/Desktop/The better\TB_Exec_Staff_PII.xlsx → /home/Eve/
[*] downloading: C:/Users/sajang/Desktop/The better\TB_Partner_SLA.xlsx → /home/Eve/TB
[*] Completed  : C:/Users/sajang/Desktop/The better\TB_Partner_SLA.xlsx → /home/Eve/TB
[*] downloading: C:/Users/sajang/Desktop/The better\TB_Payment_Master.xlsx → /home/Eve/
[*] Completed  : C:/Users/sajang/Desktop/The better\TB_Payment_Master.xlsx → /home/Eve/
[*] downloading: C:/Users/sajang/Desktop/The better\TB_User_DB_2026.xlsx → /home/Eve/T
[*] Completed  : C:/Users/sajang/Desktop/The better\TB_User_DB_2026.xlsx → /home/Eve/T
```

MACHINE	ADDRESSES	VERSION	LAST SEEN
kali [redacted]	100.117.246.7	1.94.2 Linux 6.17.10+kali-amd64	Connected
[redacted]			
ubuntus [redacted]	100.88.84.69	1.94.1 Linux 6.14.0-37-generic	Connected

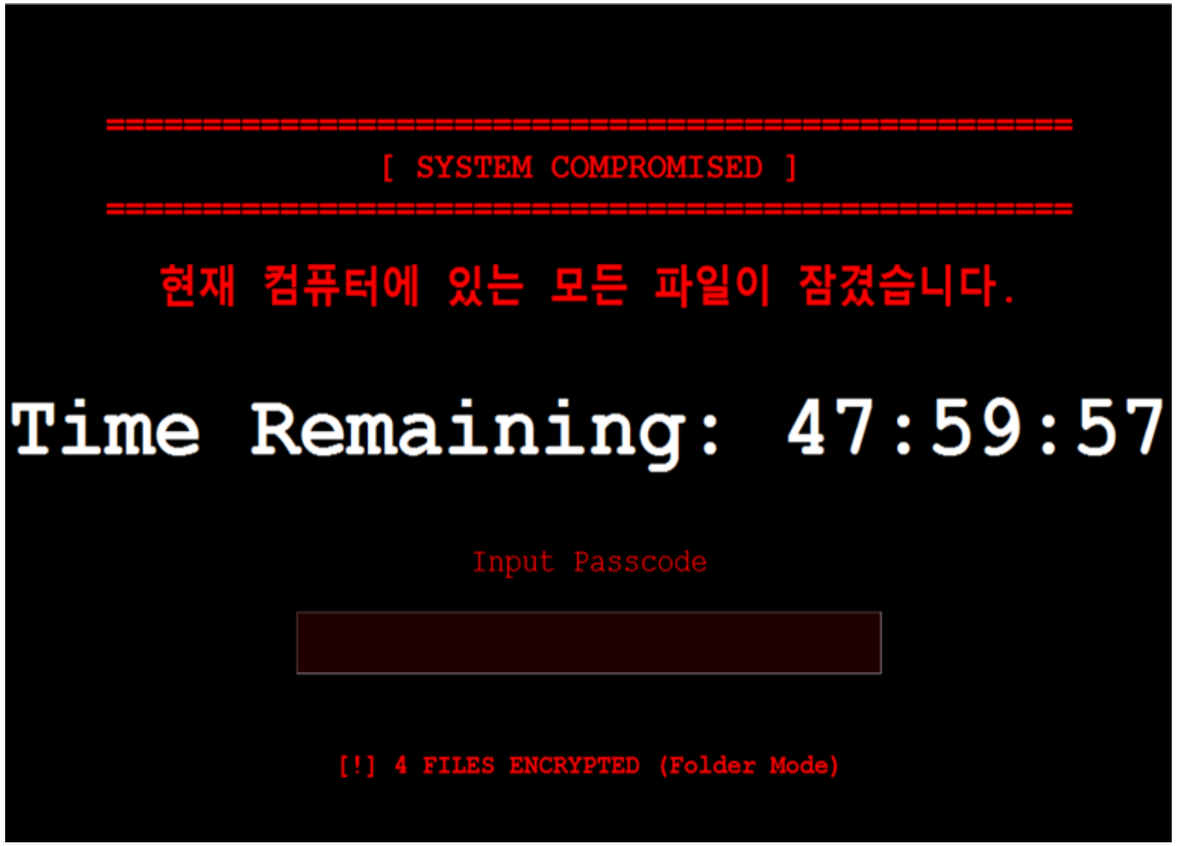
```
root@Team-Red:~#
better/
better/TB_Exec_Staff_PII.xlsx
better/TB_Payment_Master.xlsx
better/TB_User_DB_2026.xlsx
better/TB_Partner_SLA.xlsx
```

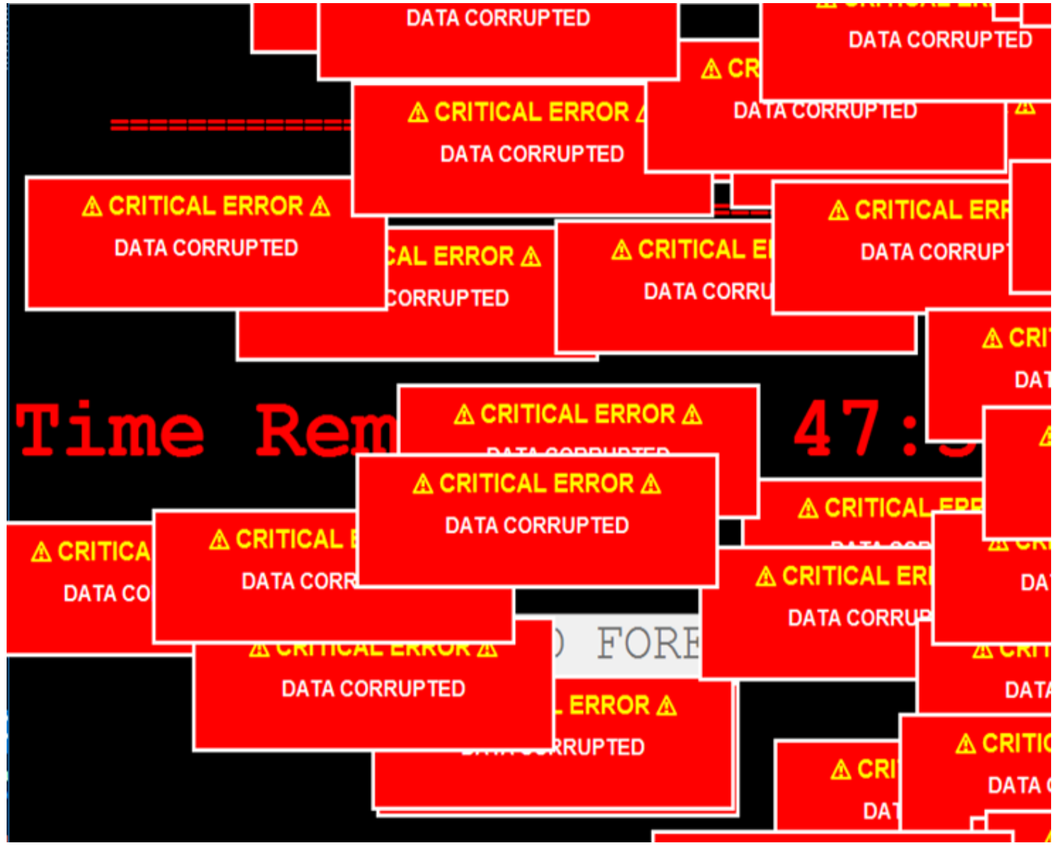
시나리오


7. 랜섬웨어 페이로드 투하
공격자
침해 호스트


The better
일
홈
공유
보기
The better
The better 검색
바로 가기
바탕 화면
다운로드
문서
사진
OneDrive
내 PC
다운로드
동영상
이름
수정한 날짜
유형
크기
TB_Exec_Staff_PII.xlsx.locked 2026-03-09 오전... LOCKED 파일 11KB
TB_Partner_SLA.xlsx.locked 2026-03-09 오전... LOCKED 파일 11KB
TB_Payment_Master.xlsx.locked 2026-03-09 오전... LOCKED 파일 11KB
TB_User_DB_2026.xlsx.locked 2026-03-09 오전... LOCKED 파일 11KB
[잠금] TB_Exec_Staff_PII.xlsx
[잠금] TB_Partner_SLA.xlsx
[잠금] TB_Payment_Master.xlsx
[잠금] TB_User_DB_2026.xlsx
레지스트리 편집기
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H)
Authent
Backgro
BingIdei
Clip
ClosedC
이름
종류
데이터
(기본값) REG_SZ (값 설정 안 됨)
OneDrive REG_SZ "C:₩Users₩Eve₩AppData₩Local₩Microsoft₩One...
WindowsUpdate... REG_SZ C:₩Users₩Eve₩Downloads₩ransomware.exe

시나리오

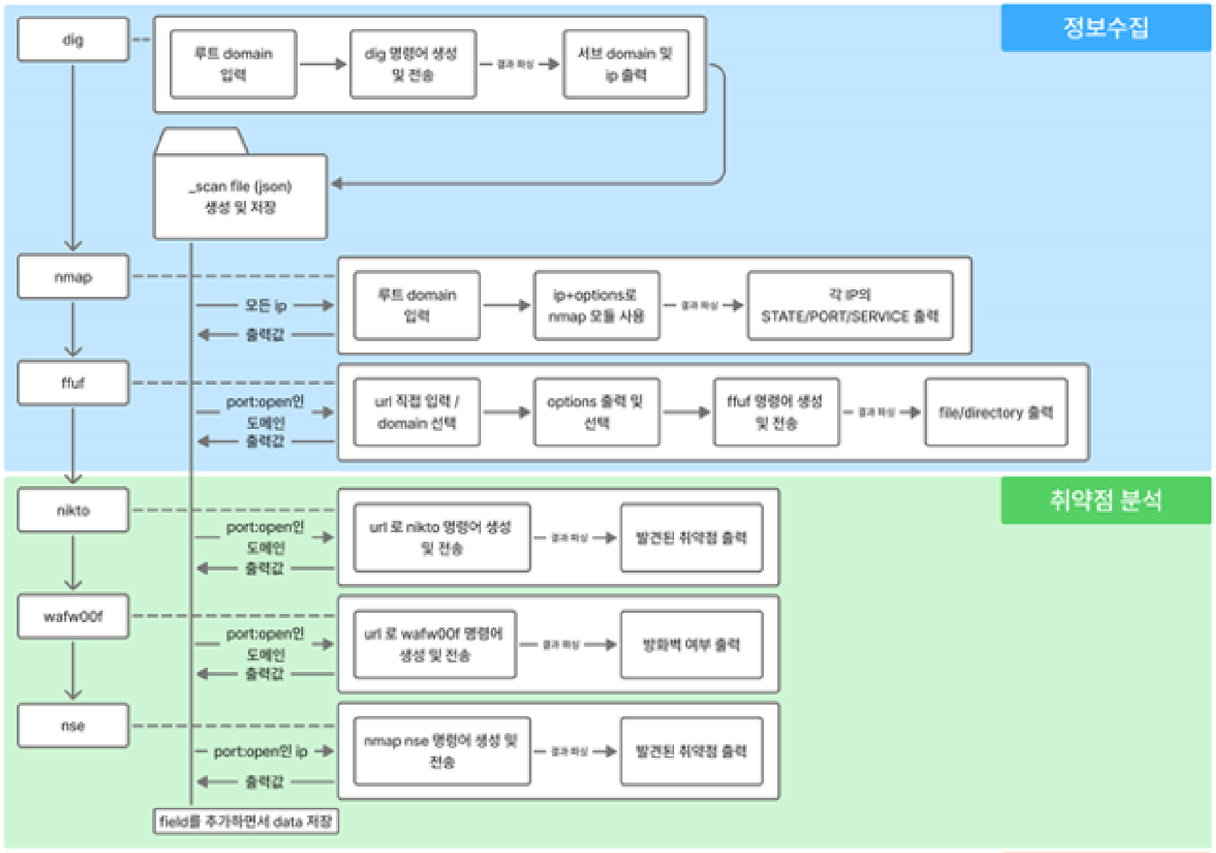

[SYSTEM COMPROMISED]
현재 컴퓨터에 있는 모든 파일이 잠겼습니다.
Time Remaining: 47:59:57
Input Passcode
[!] 4 FILES ENCRYPTED (Folder Mode)

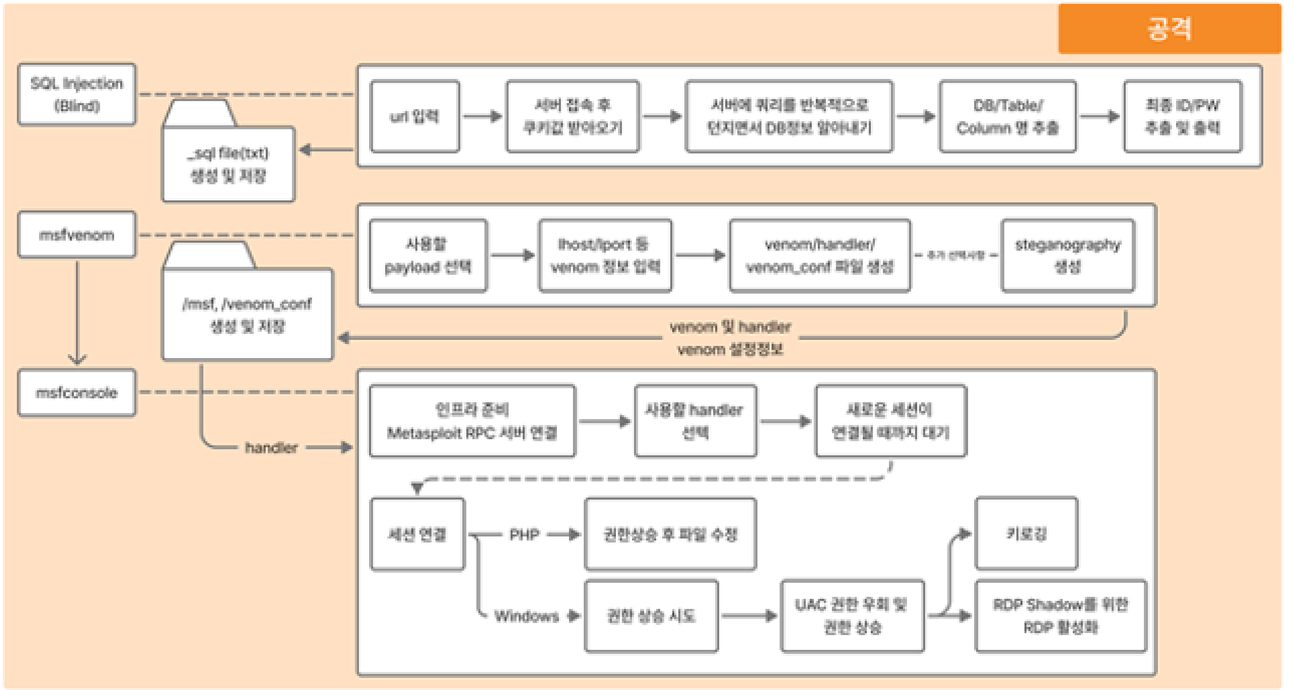

⚠ CRITICAL ERROR ⚠
DATA CORRUPTED

취약점 분석

침투 단계	취약점 항목	OWASP 2021	CVE / CWE	CVSS	위험도	핵심 영향
STEP 1	DNS Zone Transfer	A05:2021	CVE-1999-0532	5.3	Medium	인프라 구조 및 IP대역 전체 노출
STEP 2-1	Blind SQL Injection	A03:2021	CWE-89	9.8	**Critical**	DB계정 및 자격 증명 탈취
STEP 2-2	Steganography	A04:2021	CVE-2016-3714	8.4	High	이미지 내 악성 페이로드 은닉 후 업로드
STEP 02-4	LFI	A01:2021	CWE-98	8.1	High	서버 내 민감 파일 열람 및 원격 스크립트 실행
STEP 02-6	SUID 권한 상승	A01:2021	CVE-2021-4034/ CWE-269	7.8	**Critical**	일반 웹 서버 권한에서 시스템 최상위(Root) 권한 획득
STEP 02-7	Stored XSS	A03:2021	CWE-79	7.5	High	관리자 페이지 변조 및 악성코드 유포 거점 확보
STEP 03	ActiveX 기반 실행	A03:2021	CVE-2021-40444 / CWE-494	8.8	High	관리자 PC 내 악성코드(.exe) 자동 다운로드 및 감염
STEP 04	RDP Shadowing & UAC 우회	A01:2021	CVE-2019-0708 / CWE-284	9.8	**Critical**	관리자 세션 직접 제어 및 내부망 측면 이동(Lateral)
STEP 04	보안 정책 무력화	A05:2021	CWE-693	5.0	Medium	방화벽/디펜더 중지로 실시간 공격 탐지 체계 무력화
STEP 05	오피스 문서 RCE	A06:2021	CVE-2023-36884 / CVE-2022-30190	8.8	High	"2026 예산안" 문서를 통한 추가 좀비 PC 대량 확보
STEP 06	은닉 채널 데이터 반출	A05:2021	CWE-668 / CWE-284	5.3	Medium	Tailscale 암호화 터널을 이용한 기밀 데이터 외부 유출
STEP 07	랜섬웨어 페이로드 투하	Impact	CWE-732 / CWE-778	10.0	**Critical**	침해 호스트 전체 데이터 암호화 및 가용성 완전 파괴

자동화


정보수집
dig
루트 domain 입력
dig 명령어 생성 및 전송
결과 파일
서브 domain 및 ip 출력
_scan file (json) 생성 및 저장
nmap
오든 ip
출력값
루트 domain 입력
ip+options로 nmap 모듈 사용
결과 파일
각 IP의 STATE/PORT/SERVICE 출력
ffuf
port:open인 도메인
출력값
url 직접 입력 / domain 선택
options 출력 및 선택
ffuf 명령어 생성 및 전송
결과 파일
file/directory 출력
취약점 분석
nikto
port:open인 도메인
출력값
url 로 nikto 명령어 생성 및 전송
결과 파일
발견된 취약점 출력
wafw00f
port:open인 도메인
출력값
url 로 wafw00f 명령어 생성 및 전송
결과 파일
방화벽 여부 출력
nse
port:open인 ip
출력값
nmap nse 명령어 생성 및 전송
결과 파일
발견된 취약점 출력
field를 추가하면서 data 저장


공격
SQL Injection (Blind)
_sql file(txt) 생성 및 저장
url 입력
서버 접속 후 쿠키값 받아오기
서버에 쿼리를 반복적으로 던지면서 DB정보 알아내기
DB/Table/Column 명 추출
최종 ID/PW 추출 및 출력
msfvenom
/msf, /venom_conf 생성 및 저장
사용할 payload 선택
lhost/lport 등 venom 정보 입력
venom/handler/venom_conf 파일 생성
추가 선택사항
steganography 생성
venom 및 handler
venom 설정정보
msfconsole
handler
인프라 준비 Metasploit RPC 서버 연결
사용할 handler 선택
새로운 세션이 연결될 때까지 대기
세션 연결
PHP
권한상승 후 파일 수정
키로깅
Windows
권한 상승 시도
UAC 권한 우회 및 권한 상승
RDP Shadow를 위한 RDP 활성화

프로젝트 종합 리뷰 및 성과

프로젝트 종합 리뷰 및 성과

Foundation / Architecture

1. SPOF 제로화 및 무중단 인프라(HA) 아키텍처 완성

서버 고가용성(HA) 구축 100%
네트워크 관제 및 보안 100% 달성

프로젝트 종합 리뷰 및 성과

Foundation / Architecture

1. SPOF 제로화 및 무중단 인프라(HA) 아키텍처 완성

서버 고가용성(HA) 구축 100%
네트워크 관제 및 보안 100% 달성

Operations / Automation

2. SOAR 기반 통합 관제 및 자동 대응 체계(MTTR 단축) 확립

중앙 관제 및 자동화
SOAR 구축 100% 달성

프로젝트 종합 리뷰 및 성과

Foundation / Architecture

1. SPOF 제로화 및 무중단 인프라(HA) 아키텍처 완성

서버 고가용성(HA) 구축 100%
네트워크 관제 및 보안 100% 달성

Operations / Automation

2. SOAR 기반 통합 관제 및 자동 대응 체계(MTTR 단축) 확립

중앙 관제 및 자동화
SOAR 구축 100% 달성

Validation / Testing

3. 실전 APT 공방 시뮬레이션을 통한 엔터프라이즈 방어력 검증

APT 킬체인 시나리오 구현 및
취약점 분석 100% 달성

감사합니다.