대우능력개발원
DAEWOO DEVELOPMENT OF ABILITY

F/W 프로젝트

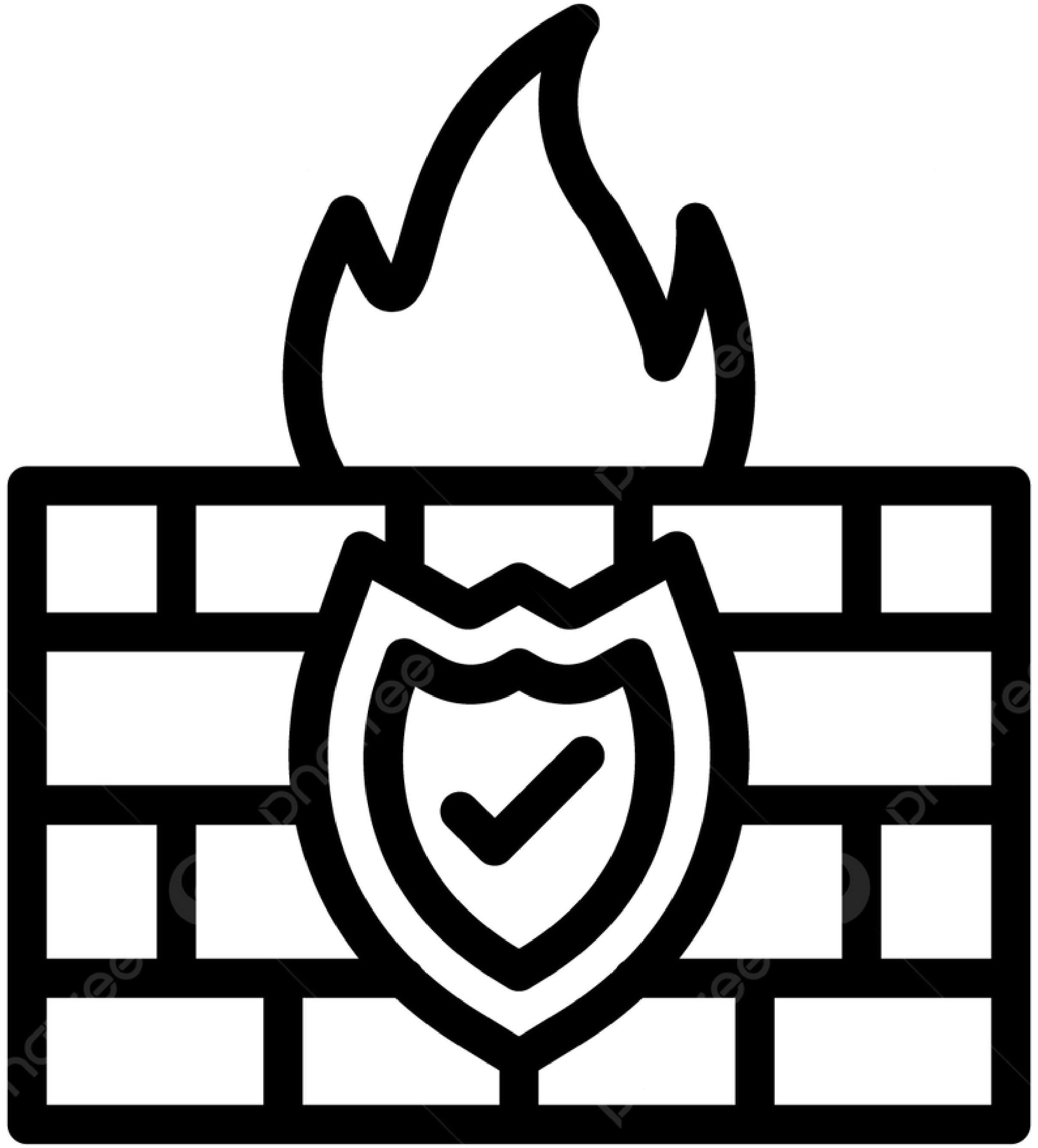
조환일,이서진,서재천,박상희

목 차

1. 물리적/논리적 구성도

2. 라우터/스위치 구성 및 라우팅

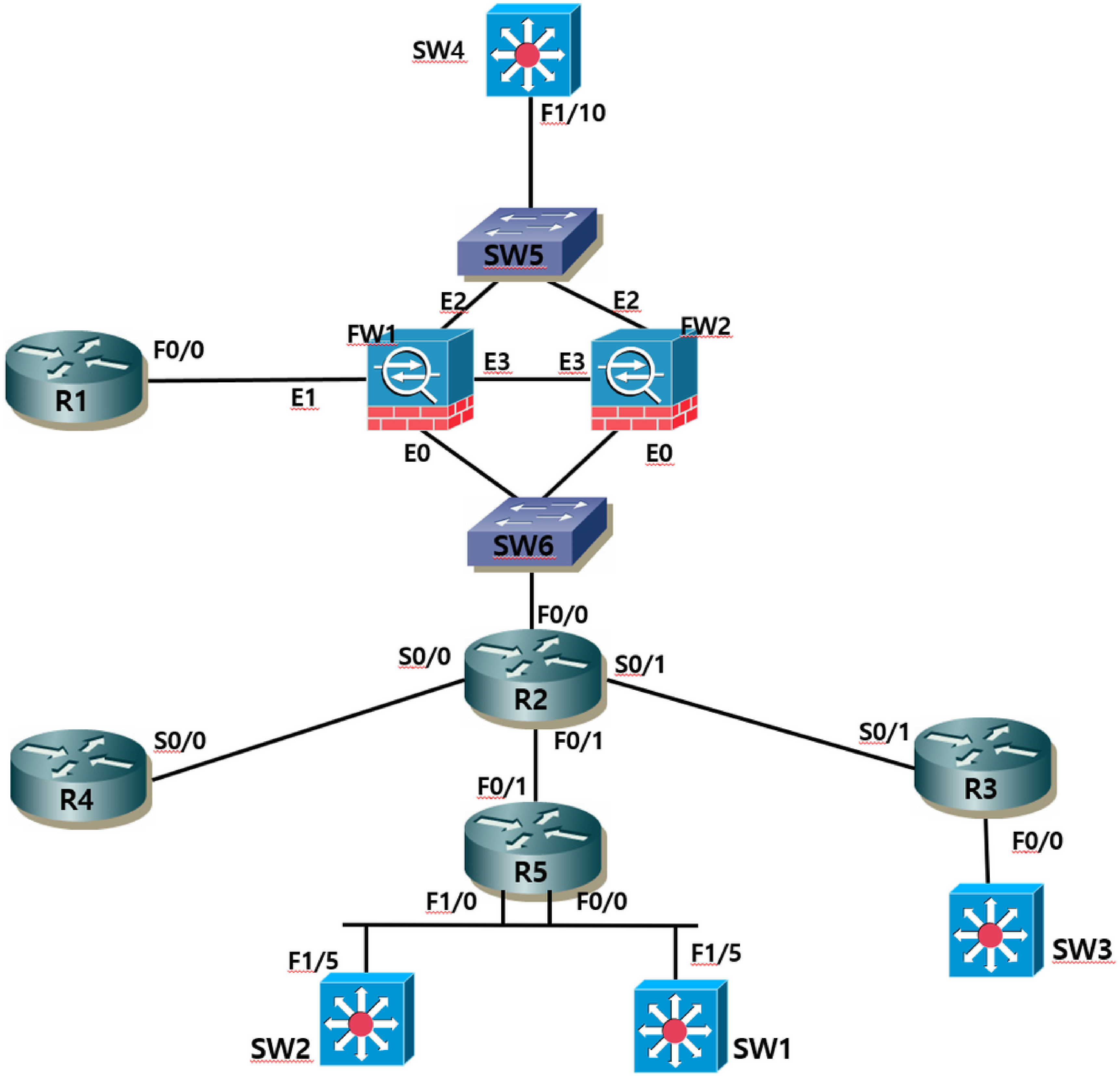
3. 방화벽 구성 및 이중화



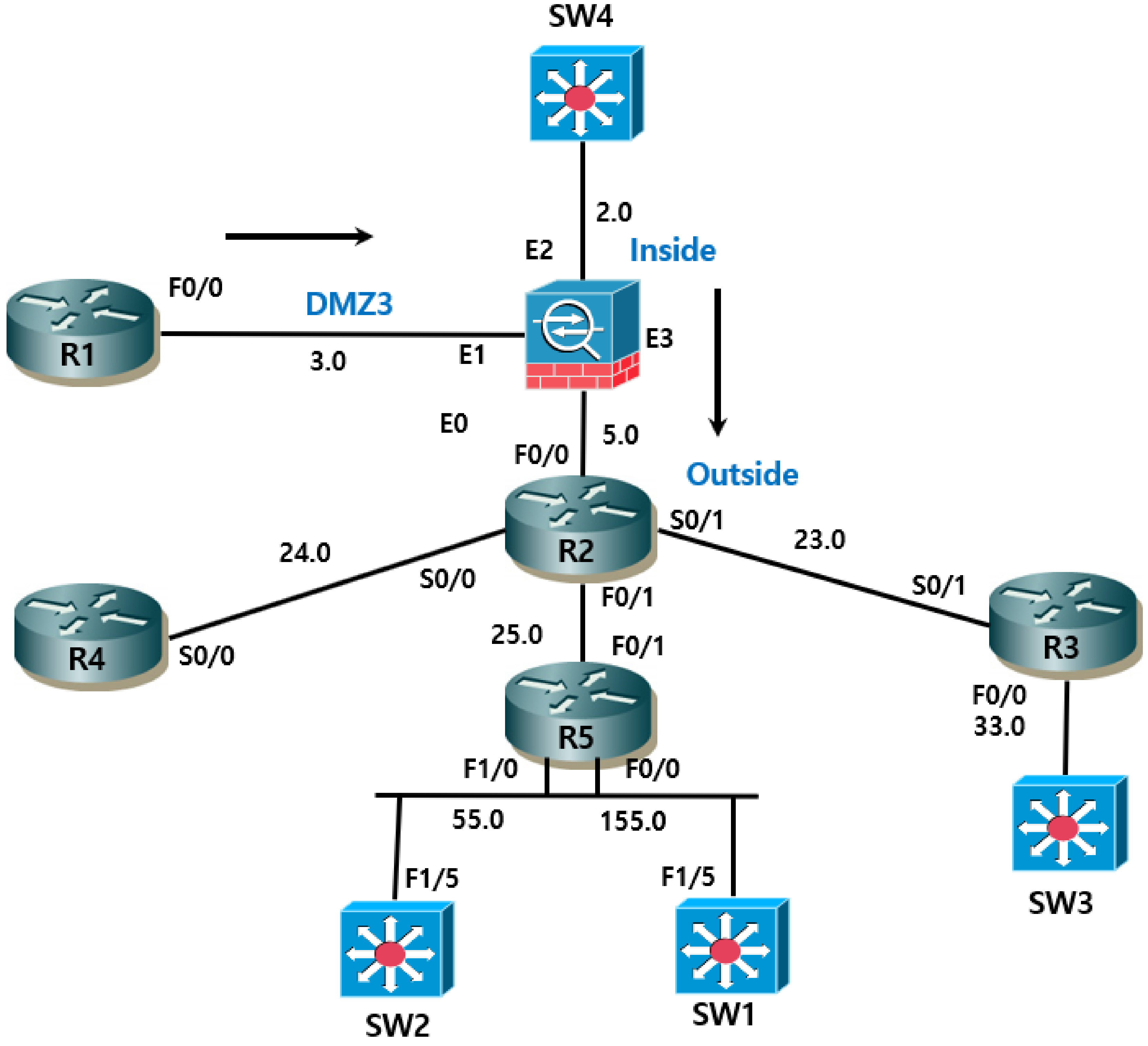
1

물리적/논리적 구성도

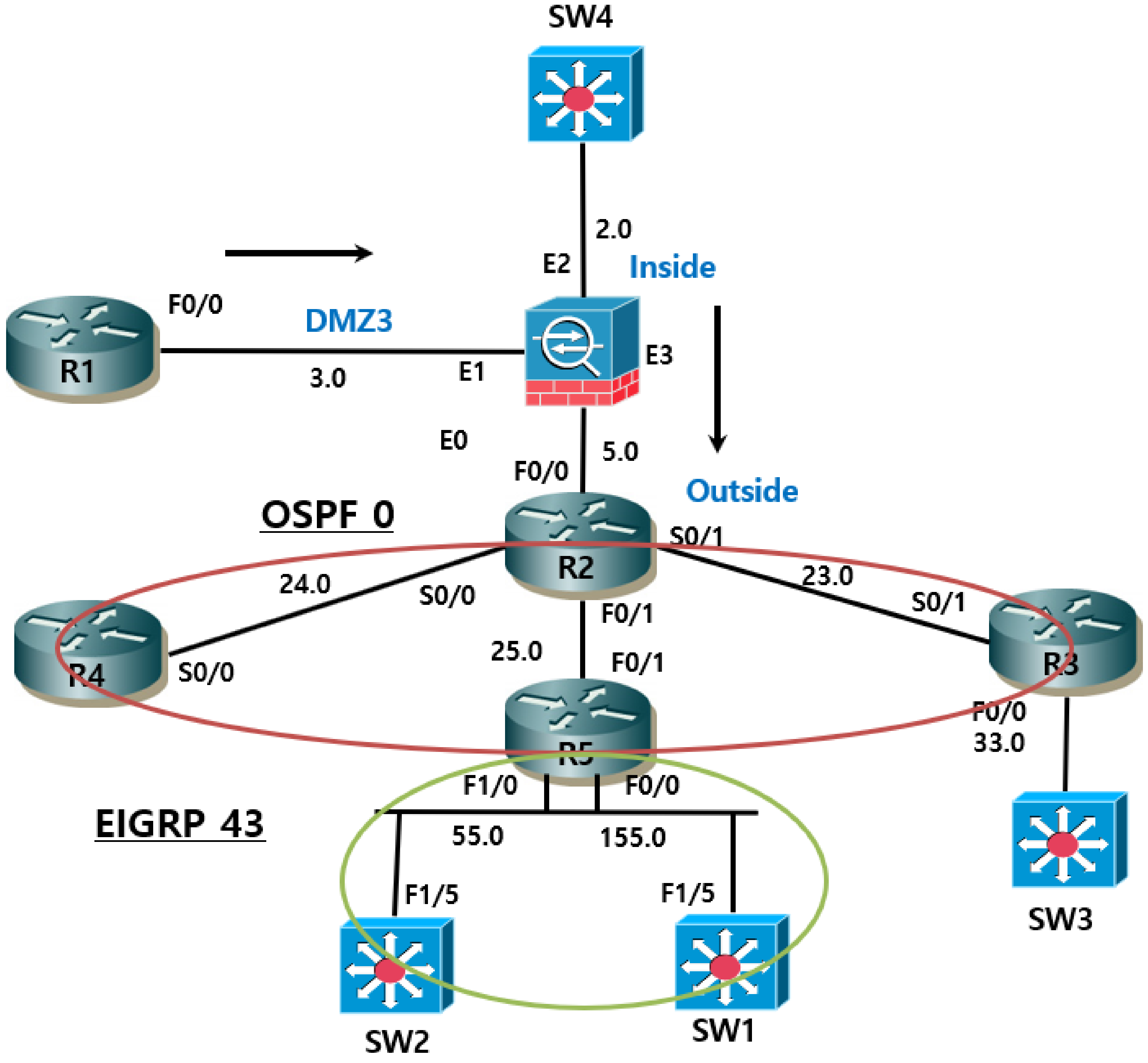
물리적 구성도


SW4
F1/10
SW5
E2
E2
FW1
FW2
F0/0
R1
E1
E3
E3
E0
E0
SW6
F0/0
S0/0
S0/1
R2
S0/0
R4
F0/1
S0/1
R3
F0/1
R5
F0/0
F1/0
F0/0
F1/5
F1/5
SW3
SW2
SW1

논리적 구성도


SW4
2.0
E2
Inside
F0/0
DMZ3
R1
3.0
E1
E3
E0
5.0
F0/0
Outside
R2
S0/1
23.0
24.0
S0/0
S0/1
R3
R4
S0/0
F0/1
25.0
F0/1
F0/0
33.0
R5
F1/0
F0/0
55.0
155.0
F1/5
F1/5
SW3
SW2
SW1

논리적 구성도 (영역)


SW4
2.0
E2
Inside
F0/0
DMZ3
R1
3.0
E1
E3
E0
5.0
F0/0
Outside
OSPF 0
R2
S0/1
24.0
S0/0
23.0
S0/1
F0/1
25.0
F0/1
R4
S0/0
R3
F0/0
33.0
R5
F1/0
F0/0
EIGRP 43
55.0
155.0
F1/5
F1/5
SW3
SW2
SW1

2

라우터/스위치 구성 및 라우팅

라우터 설정

R1 , R2 주소 입력 및 라우팅 설정

R1

```
int lo0
ip add 43.43.0.1
255.255.255.255
no sh

int lo100
ip add 111.111.111.111
255.255.255.0
no sh

int f0/0
no sh
ip add 43.43.3.1 255.255.255.0

ip route 0.0.0.0 0.0.0.0
43.43.3.253
```

R2

```
int lo0
ip add 43.43.0.2 255.255.255.255
no sh

int lo100
ip add 222.222.222.222
255.255.255.255
no sh

int f0/0
ip add 43.43.5.2 255.255.255.0
no sh

int f0/1
ip add 43.43.25.2 255.255.255.0
no sh
```

```
int s0/0
ip add 43.43.24.2 255.255.255.0
ip os net broad
no sh

int s0/1
ip add 43.43.23.2 255.255.255.0
ip os net broad
no sh

router os 1
router-id 43.43.0.2
net 43.43.24.2 0.0.0.0 a 0
net 43.43.23.2 0.0.0.0 a 0
net 43.43.25.2 0.0.0.0 a 0
ip route 0.0.0.0 0.0.0.0 43.43.5.253
ip route 43.43.3.0 255.255.255.0 43.43.5.253

default-infor ori
```

라우터 설정

R3 , R4 주소 입력 및 라우팅 설정

R3

```
int lo0
ip add 43.43.0.3
255.255.255.255

int f0/0
ip add 43.43.33.3 255.255.255.0

int s0/1
ip add 43.43.23.3 255.255.255.0
ip os net broad
ip os pri 0
no sh

router os 1
router-id 43.43.0.3
net 43.43.23.3 0.0.0.0 a 0
```

R4

```
int lo0
ip add 43.43.0.4
255.255.255.255

int s0/0
ip add 43.43.24.4 255.255.255.0
ip os net broad
ip os pri 0
no sh

router os 1
router-id 43.43.0.4
net 43.43.24.4 0.0.0.0 a 0
```

라우터 설정

R5 주소 입력 및 라우팅 설정

R5

```
int lo0
ip add 43.43.0.5
255.255.255.255

int lo100
ip add 155.155.155.155
255.255.255.255

int f0/0
no sh
ip add 43.43.155.5
255.255.255.0

int f0/1
ip add 43.43.25.5 255.255.255.0
no sh
```

```
int f1/0
ip add 43.43.55.5 255.255.255.0
no sh

router os 1
router-id 43.43.0.5
net 43.43.25.5 0.0.0.0 a 0
redi ei 43 subnets

router e 43
no auto
net 43.43.55.5 0.0.0.0
net 43.43.155.5 0.0.0.0
redi os 1 metric 1544 2000 255
1 1500
```

스위치 설정

SW1 , SW2 주소 입력 및 라우팅 설정

SW1

```
int f1/5
no sw
ip add 43.43.155.250
255.255.255.0
no sh

router ei 43
no auto
net 43.43.155.250 0.0.0.0
```

SW2

```
int f1/5
no sw
ip add 43.43.55.250
255.255.255.0
no sh

router ei 43
no auto
net 43.43.55.250 0.0.0.0
```

스위치 설정

SW3, SW4 주소 입력 및 라우팅 설정

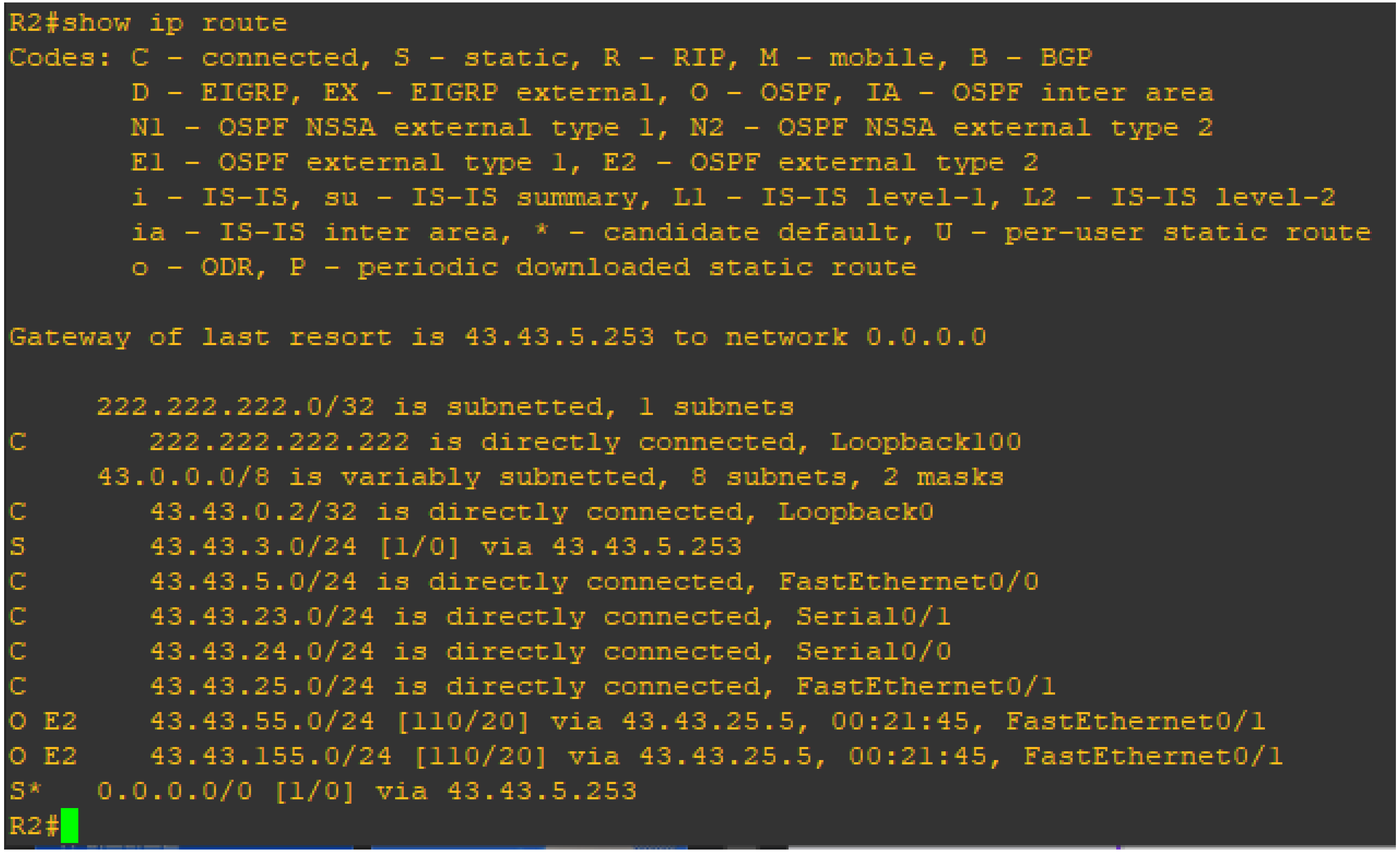
SW3

```
int f1/3
no sw
ip add 43.43.33.250
255.255.255.0
no sh
```

SW4

```
int lo 0
ip add 150.1.43.10
255.255.255.0
no sh

int f1/10
no sw
ip add 43.43.2.250
255.255.255.0
no sh

ip route 0.0.0.0 0.0.0.0
43.43.2.253
```

라우터 & 스위치 설정 확인



```
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 43.43.5.253 to network 0.0.0.0

     222.222.222.0/32 is subnetted, 1 subnets
C       222.222.222.222 is directly connected, Loopback100
     43.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C       43.43.0.2/32 is directly connected, Loopback0
S       43.43.3.0/24 [1/0] via 43.43.5.253
C       43.43.5.0/24 is directly connected, FastEthernet0/0
C       43.43.23.0/24 is directly connected, Serial0/1
C       43.43.24.0/24 is directly connected, Serial0/0
C       43.43.25.0/24 is directly connected, FastEthernet0/1
O E2    43.43.55.0/24 [110/20] via 43.43.25.5, 00:21:45, FastEthernet0/1
O E2    43.43.155.0/24 [110/20] via 43.43.25.5, 00:21:45, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 43.43.5.253
R2#
```

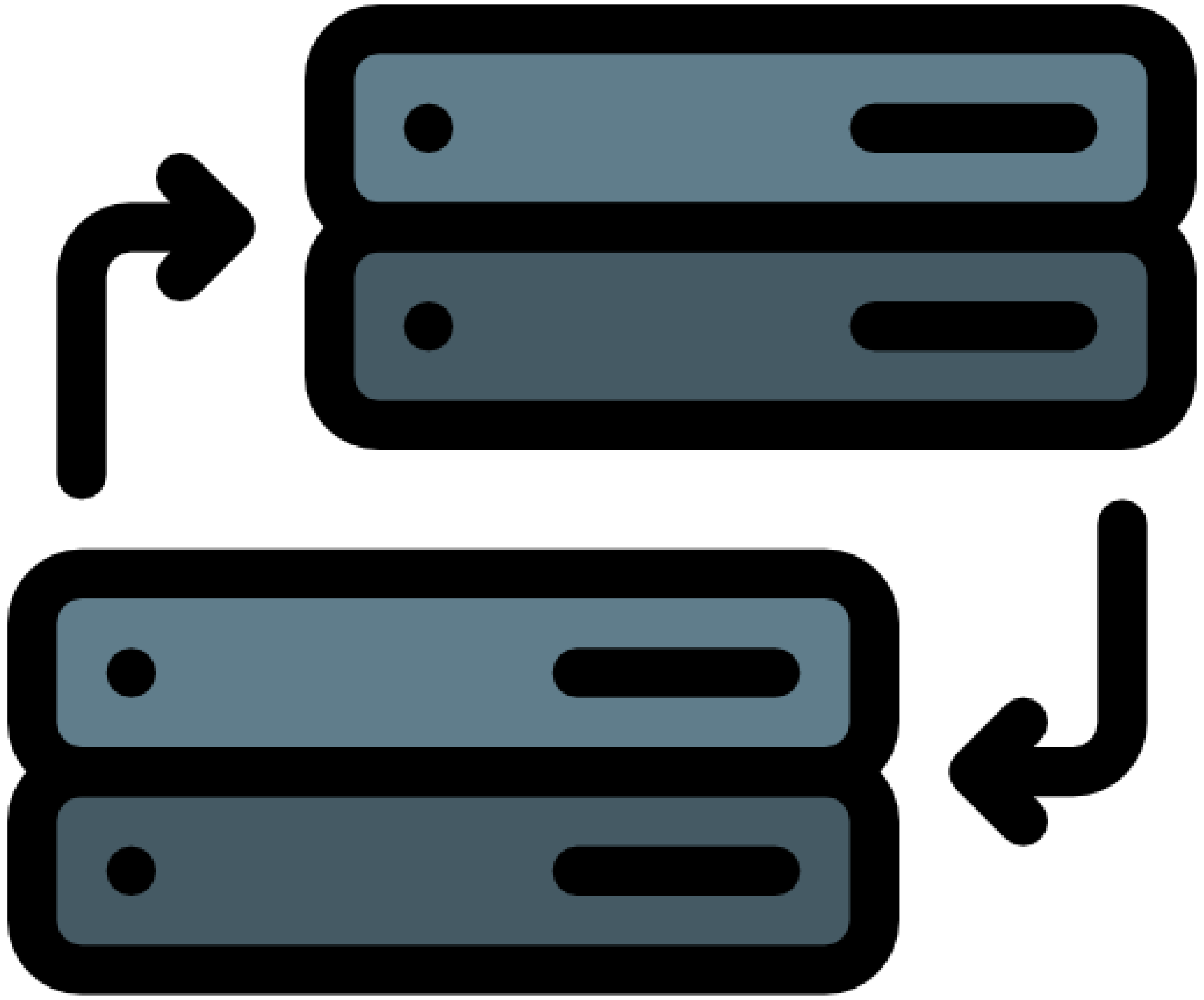
R2의 라우팅 테이블

3

방화벽 구성 및 이중화

이중화란?

장애에 대비하기 위해 두개의 동일한 장비를 사용하는 것으로 이중화가 구성된 방화벽은 대상 인터페이스들의 상태를 모니터링하다가 장애가 발생하면 failover(역할 교대)가 동작한다.



A-S , A-A 이중화 종류

Active-Standby 이중화

한 장비에서만 트래픽을 처리하며 단일,다중 컨텍스트를 모두 설정할 수 있다.

Active-Active 이중화

두 장비 모두 트래픽을 처리하는 부하 분산이 가능하며 다중 컨텍스트만 설정할 수 있다.

방화벽 설정

FW1 이중화 기본 설정

FW 1

```
mode multiple

int g0
no sh

int g1
no sh

int g2
no sh

int g3
no sh
```

```
no failover

failover lan unit pri
failover lan int fover g3
failover link fover g3
failover int ip fover
43.43.100.100 255.255.255.0
stand 43.43.100.101

failover
```

방화벽 설정

FW2 이중화 기본 설정

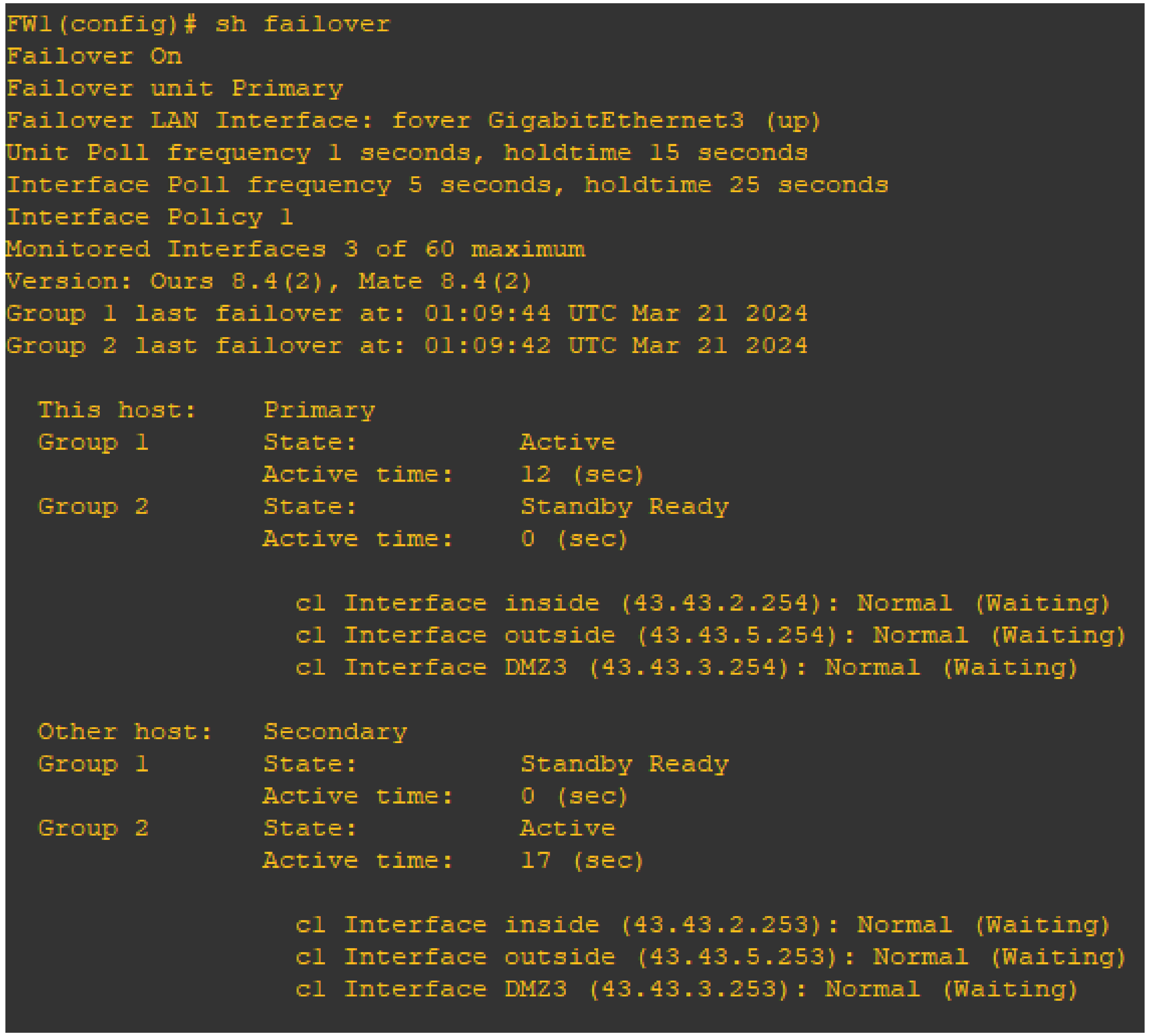
FW 2

```
mode multiple

int g0
no sh

int g1
no sh

int g2
no sh

int g3
no sh
```

```
no failover

failover lan unit sec
failover lan int fover g3
failover link fover g3
failover int ip fover
43.43.100.100 255.255.255.0
stand 43.43.100.101

failover
```

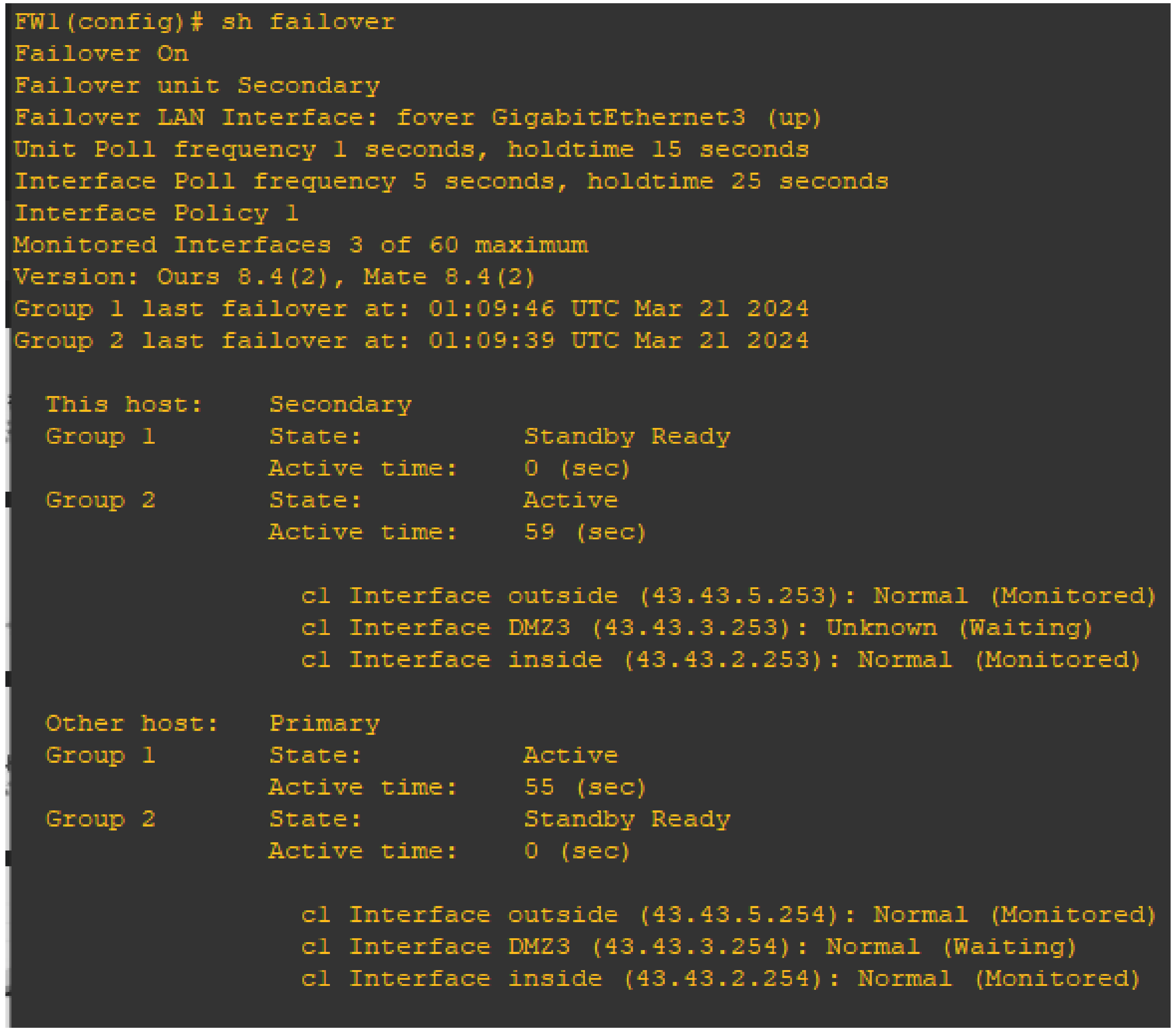
방화벽 설정

FW1,FW2 이중화 기본 설정 후 확인



```
FW1(config)# sh failover
Failover On
Failover unit Primary
Failover LAN Interface: fover GigabitEthernet3 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 60 maximum
Version: Ours 8.4(2), Mate 8.4(2)
Group 1 last failover at: 01:09:44 UTC Mar 21 2024
Group 2 last failover at: 01:09:42 UTC Mar 21 2024

  This host:    Primary
  Group 1       State:          Active
                Active time:    12 (sec)
  Group 2       State:          Standby Ready
                Active time:    0 (sec)

                  c1 Interface inside (43.43.2.254): Normal (Waiting)
                  c1 Interface outside (43.43.5.254): Normal (Waiting)
                  c1 Interface DMZ3 (43.43.3.254): Normal (Waiting)

  Other host:   Secondary
  Group 1       State:          Standby Ready
                Active time:    0 (sec)
  Group 2       State:          Active
                Active time:    17 (sec)

                  c1 Interface inside (43.43.2.253): Normal (Waiting)
                  c1 Interface outside (43.43.5.253): Normal (Waiting)
                  c1 Interface DMZ3 (43.43.3.253): Normal (Waiting)
```

FW1 failover 확인



```
FW1(config)# sh failover
Failover On
Failover unit Secondary
Failover LAN Interface: fover GigabitEthernet3 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 60 maximum
Version: Ours 8.4(2), Mate 8.4(2)
Group 1 last failover at: 01:09:46 UTC Mar 21 2024
Group 2 last failover at: 01:09:39 UTC Mar 21 2024

  This host:    Secondary
  Group 1       State:          Standby Ready
                Active time:    0 (sec)
  Group 2       State:          Active
                Active time:    59 (sec)

                  c1 Interface outside (43.43.5.253): Normal (Monitored)
                  c1 Interface DMZ3 (43.43.3.253): Unknown (Waiting)
                  c1 Interface inside (43.43.2.253): Normal (Monitored)

  Other host:   Primary
  Group 1       State:          Active
                Active time:    55 (sec)
  Group 2       State:          Standby Ready
                Active time:    0 (sec)

                  c1 Interface outside (43.43.5.254): Normal (Monitored)
                  c1 Interface DMZ3 (43.43.3.254): Normal (Waiting)
                  c1 Interface inside (43.43.2.254): Normal (Monitored)
```

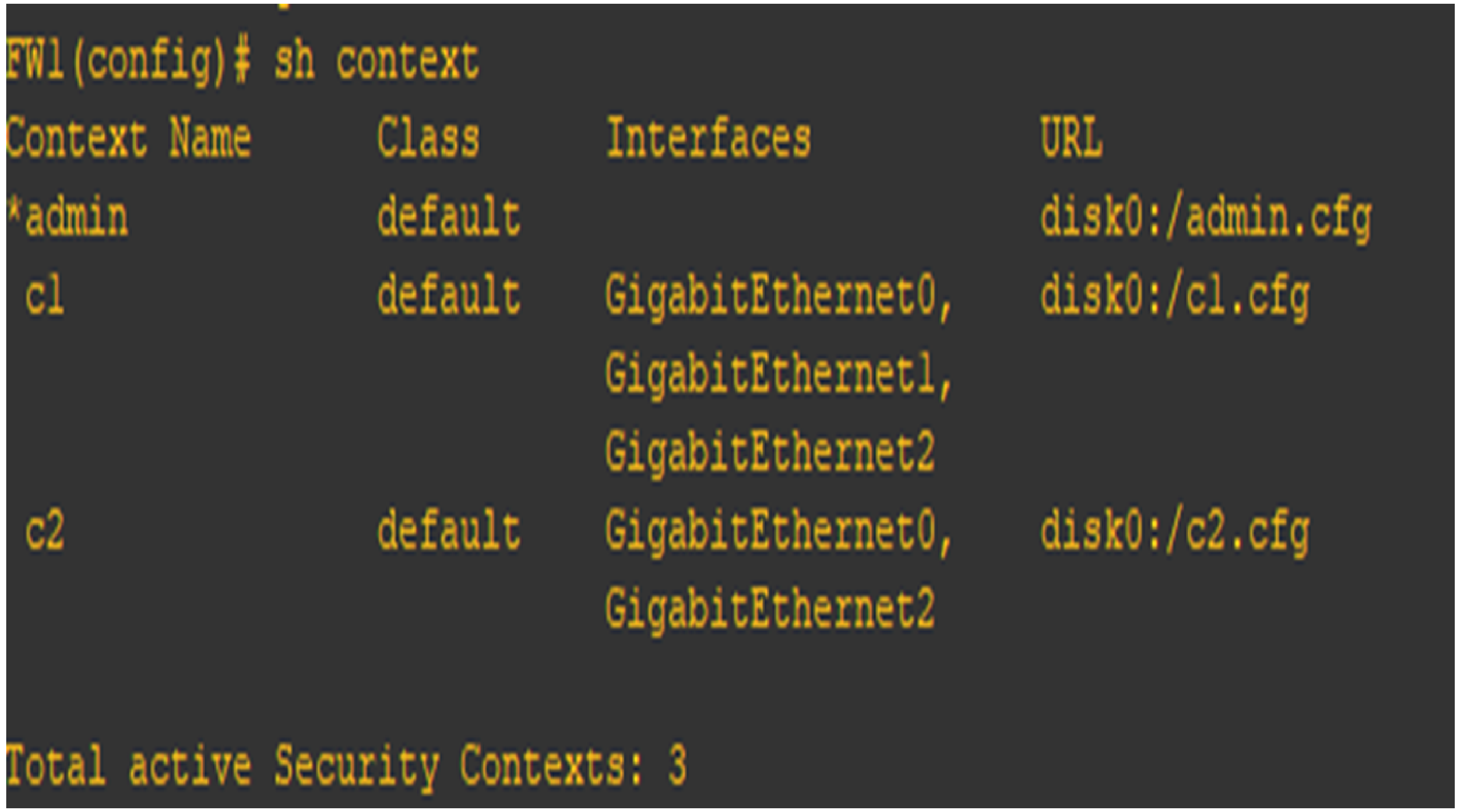
FW2 failover 확인

방화벽 설정

FW1 컨텍스트 생성 및 URL,인터페이스 할당

FW 1

```
context c1
config-u c1.cfg
allocate-int g2
allocate-int g0
allocate-int g1

context c2
config-u c2.cfg
allocate-int g2
allocate-int g0
```



```
FW1(config)# sh context
Context Name      Class      Interfaces            URL
*admin            default                          disk0:/admin.cfg
 c1               default    GigabitEthernet0,     disk0:/c1.cfg
                             GigabitEthernet1,
                             GigabitEthernet2
 c2               default    GigabitEthernet0,     disk0:/c2.cfg
                             GigabitEthernet2

Total active Security Contexts: 3
```

방화벽 설정

FW1의 Context c1 인터페이스 설정

FW 1

```
ch con c1

int g2
nameif inside
ip add 43.43.2.253
255.255.255.0 stand 43.43.2.254

int g1
nameif DMZ3
secu 100
ip add 43.43.3.253
255.255.255.0 stand 43.43.3.254
```

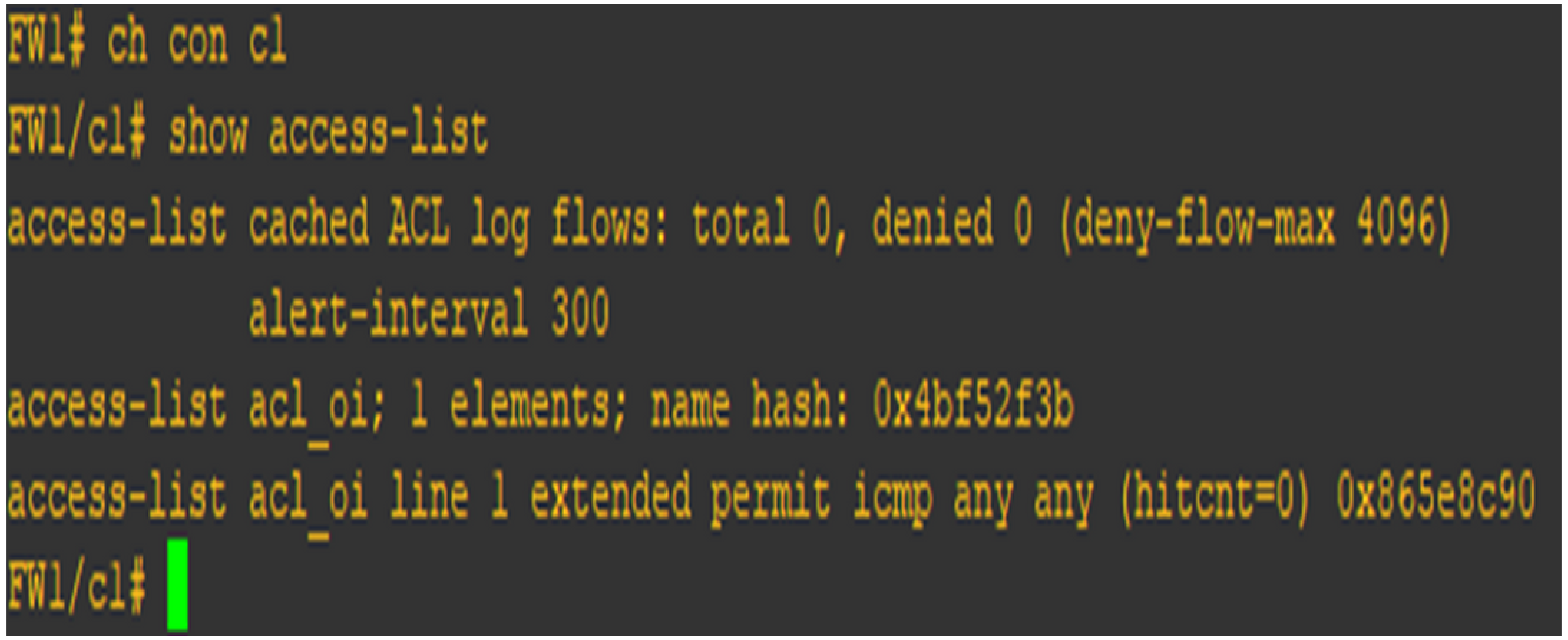
```
int g0
nameif outside
secu 0
ip add 43.43.5.253
255.255.255.0 stand 43.43.5.254

route outside 0 0 43.43.5.2
route inside 150.1.43.0
255.255.255.0 43.43.2.250
route DMZ 43.43.0.1
255.255.255.255 43.43.3.1
```

방화벽 설정

FW1 Access-list 생성 및 적용

FW 1

```
access-l acl_oi per icmp a a
access-g acl_oi in int outside

same-security-traffic per inter-interface
```



```
FW1# ch con cl
FW1/cl# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list acl_oi; 1 elements; name hash: 0x4bf52f3b
access-list acl_oi line 1 extended permit icmp any any (hitcnt=0) 0x865e8c90
FW1/cl#
```

access-list 확인

방화벽 설정

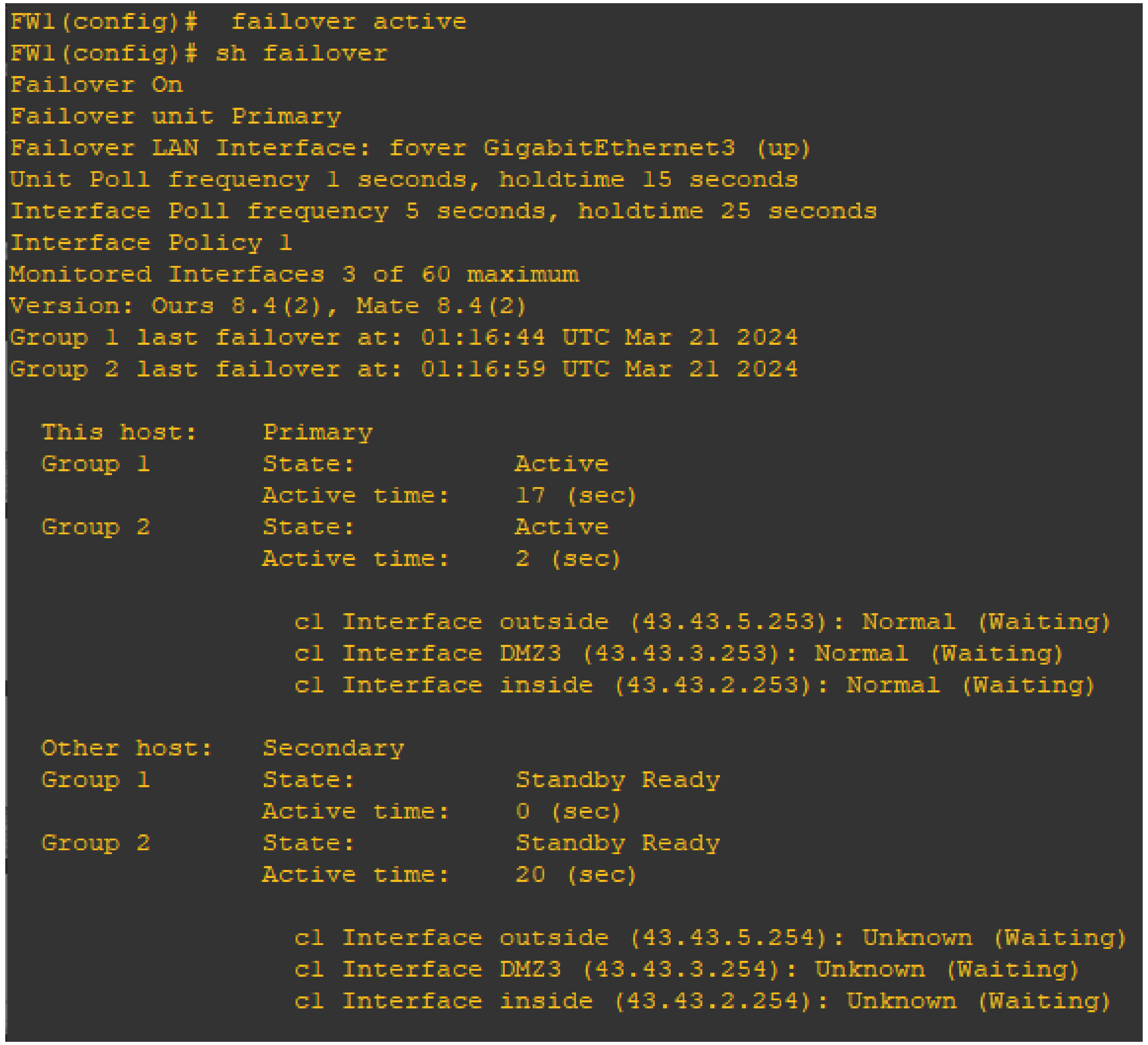
방화벽 이중화 Active - Active 모드

FW 1

```
ch sys

no fail

failover group 1
preempt
failover group 2
secondary
preempt


context c2
join-failover-group 1

context c1
join-failover-group 2

failover
failover active
```

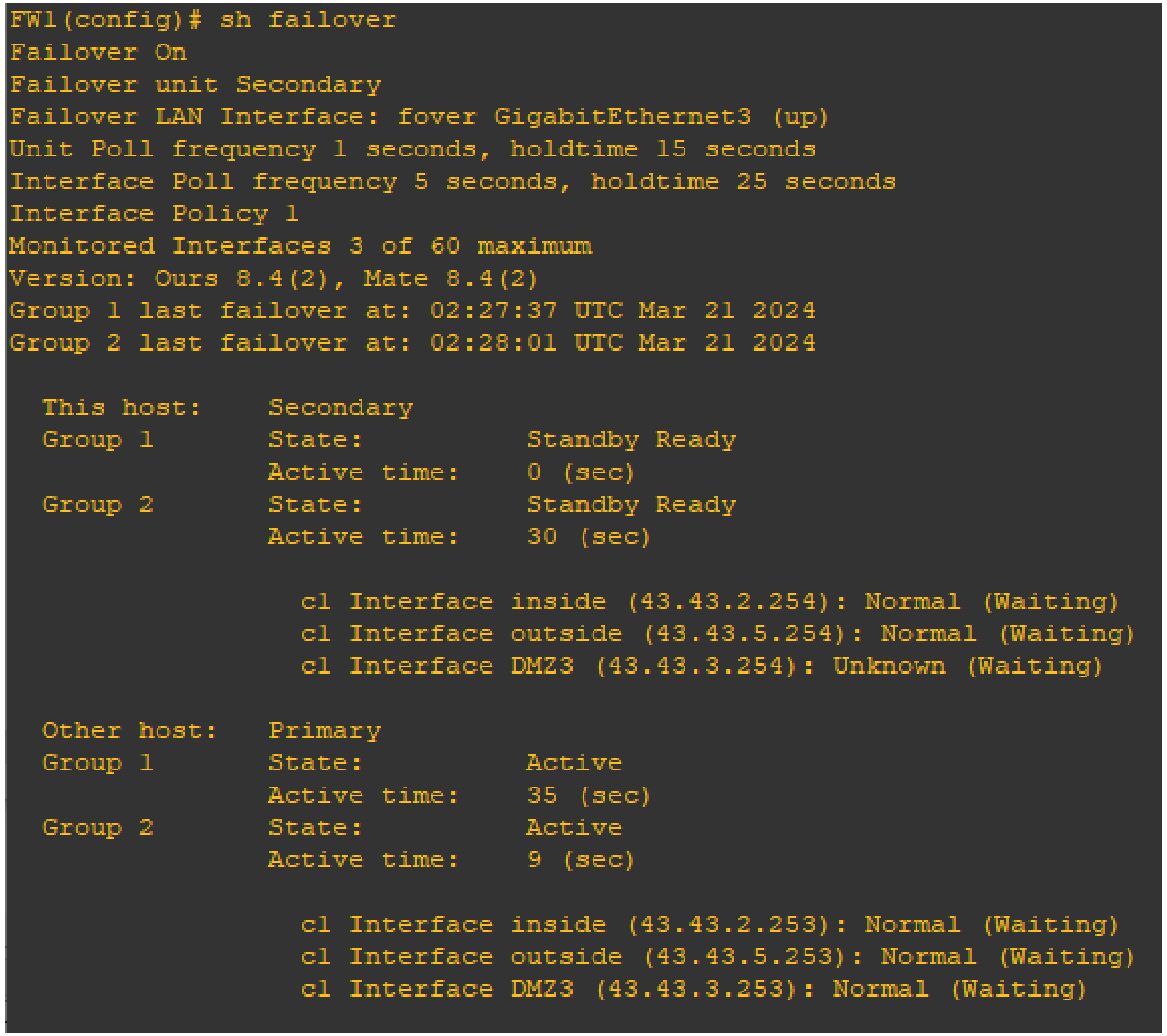
방화벽 설정

방화벽 이중화 Active - Active 모드 적용 후 확인



```
FW1(config)#  failover active
FW1(config)# sh failover
Failover On
Failover unit Primary
Failover LAN Interface: fover GigabitEthernet3 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 60 maximum
Version: Ours 8.4(2), Mate 8.4(2)
Group 1 last failover at: 01:16:44 UTC Mar 21 2024
Group 2 last failover at: 01:16:59 UTC Mar 21 2024

  This host:    Primary
  Group 1       State:          Active
                Active time:    17 (sec)
  Group 2       State:          Active
                Active time:    2 (sec)

                  c1 Interface outside (43.43.5.253): Normal (Waiting)
                  c1 Interface DMZ3 (43.43.3.253): Normal (Waiting)
                  c1 Interface inside (43.43.2.253): Normal (Waiting)

  Other host:   Secondary
  Group 1       State:          Standby Ready
                Active time:    0 (sec)
  Group 2       State:          Standby Ready
                Active time:    20 (sec)

                  c1 Interface outside (43.43.5.254): Unknown (Waiting)
                  c1 Interface DMZ3 (43.43.3.254): Unknown (Waiting)
                  c1 Interface inside (43.43.2.254): Unknown (Waiting)
```

FW 1



```
FW1(config)# sh failover
Failover On
Failover unit Secondary
Failover LAN Interface: fover GigabitEthernet3 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 60 maximum
Version: Ours 8.4(2), Mate 8.4(2)
Group 1 last failover at: 02:27:37 UTC Mar 21 2024
Group 2 last failover at: 02:28:01 UTC Mar 21 2024

  This host:    Secondary
  Group 1       State:          Standby Ready
                Active time:    0 (sec)
  Group 2       State:          Standby Ready
                Active time:    30 (sec)

                  c1 Interface inside (43.43.2.254): Normal (Waiting)
                  c1 Interface outside (43.43.5.254): Normal (Waiting)
                  c1 Interface DMZ3 (43.43.3.254): Unknown (Waiting)

  Other host:   Primary
  Group 1       State:          Active
                Active time:    35 (sec)
  Group 2       State:          Active
                Active time:    9 (sec)

                  c1 Interface inside (43.43.2.253): Normal (Waiting)
                  c1 Interface outside (43.43.5.253): Normal (Waiting)
                  c1 Interface DMZ3 (43.43.3.253): Normal (Waiting)
```

FW 2

감사합니다