PRESENTATION

2024/12/20

KDT 클라우드 보안
방화벽 팀 프로젝트

설예림
김민지
진승우
현룡관

TEAM : STEAM

CONTENTS

목차

COOPERATION PROJECT
WORK REPORT

01 1. 구성도

1-1. 물리적 구성도
1-2. 논리적 구성도

02 2. 주소 설정 및 라우팅

2-1. 라우터 설정
2-2. 스위치 설정
2-3. 설정 확인

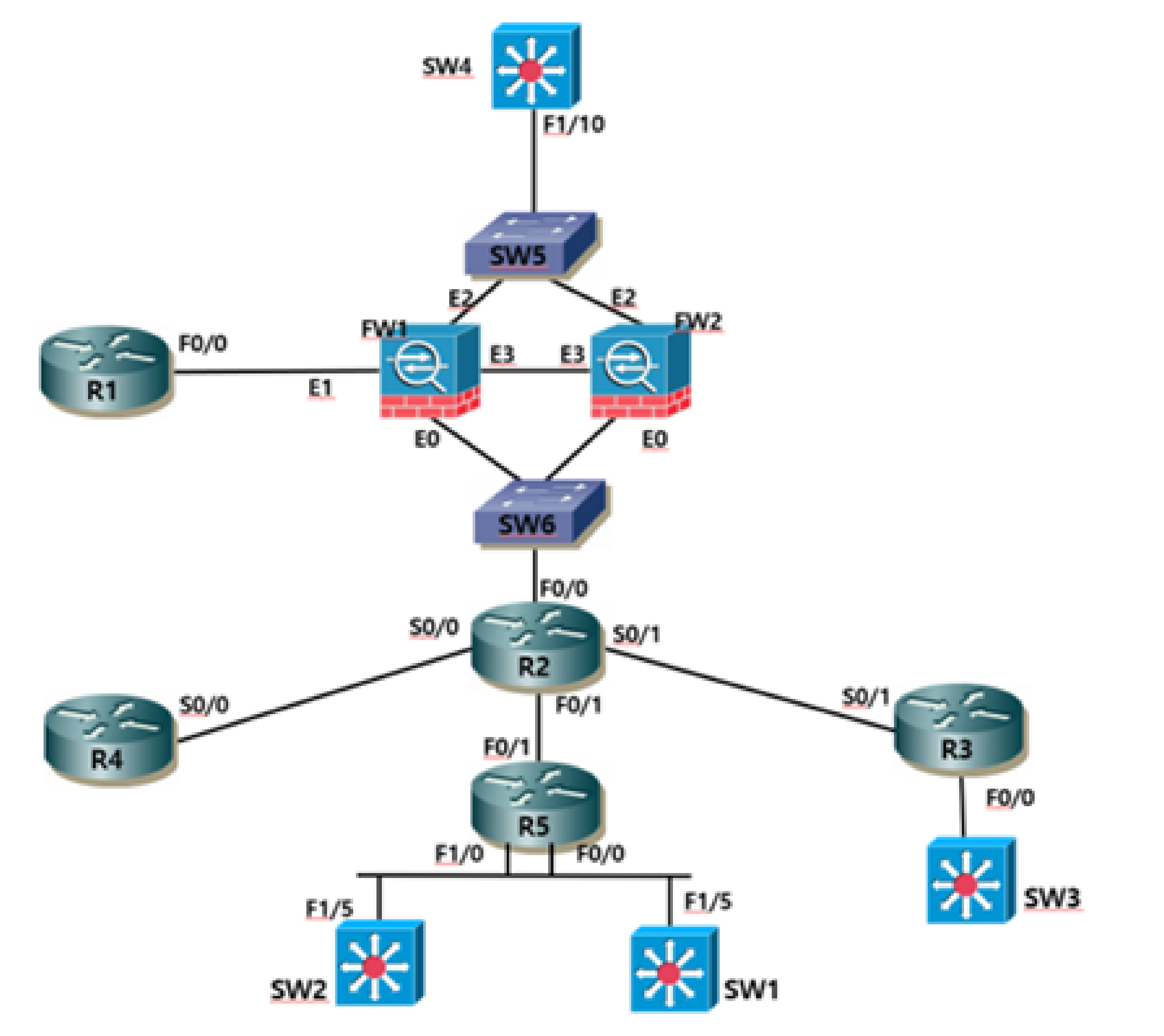
03 3. 방화벽 이중화(failover) 설정

3-1. 방화벽 기본 설정
3-2. 기본 설정 확인
3-3. 컨텍스트 생성 및 할당
3-4. Access List 설정
3-5. 방화벽 이중화 Active-Active 모드
3-6. Active-Active 모드 설정 확인

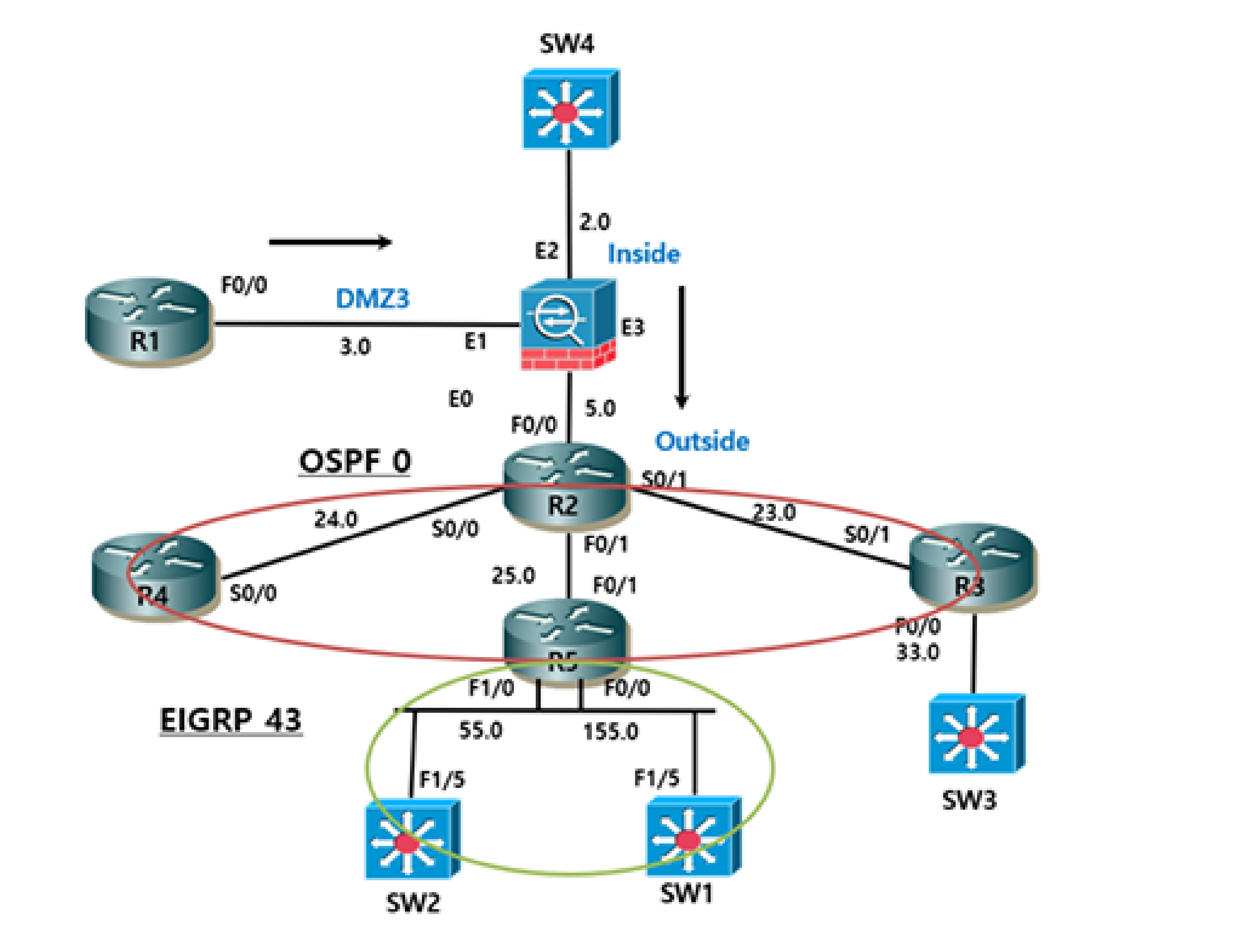
1. 구성도

1-1. 물리적 구성도

1-2. 논리적 구성도



▲ 물리적 구성도



▲ 논리적 구성도

2. 주소 설정 및 라우팅

2-1. 라우터 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
```

2. 주소 설정 및 라우팅

2-1. 라우터 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
no sh

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
```

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
ip add 43.43.155.5 255.255.255.0
no sh

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
```

2. 주소 설정 및 라우팅

2-2. 스위치 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
```

SW3

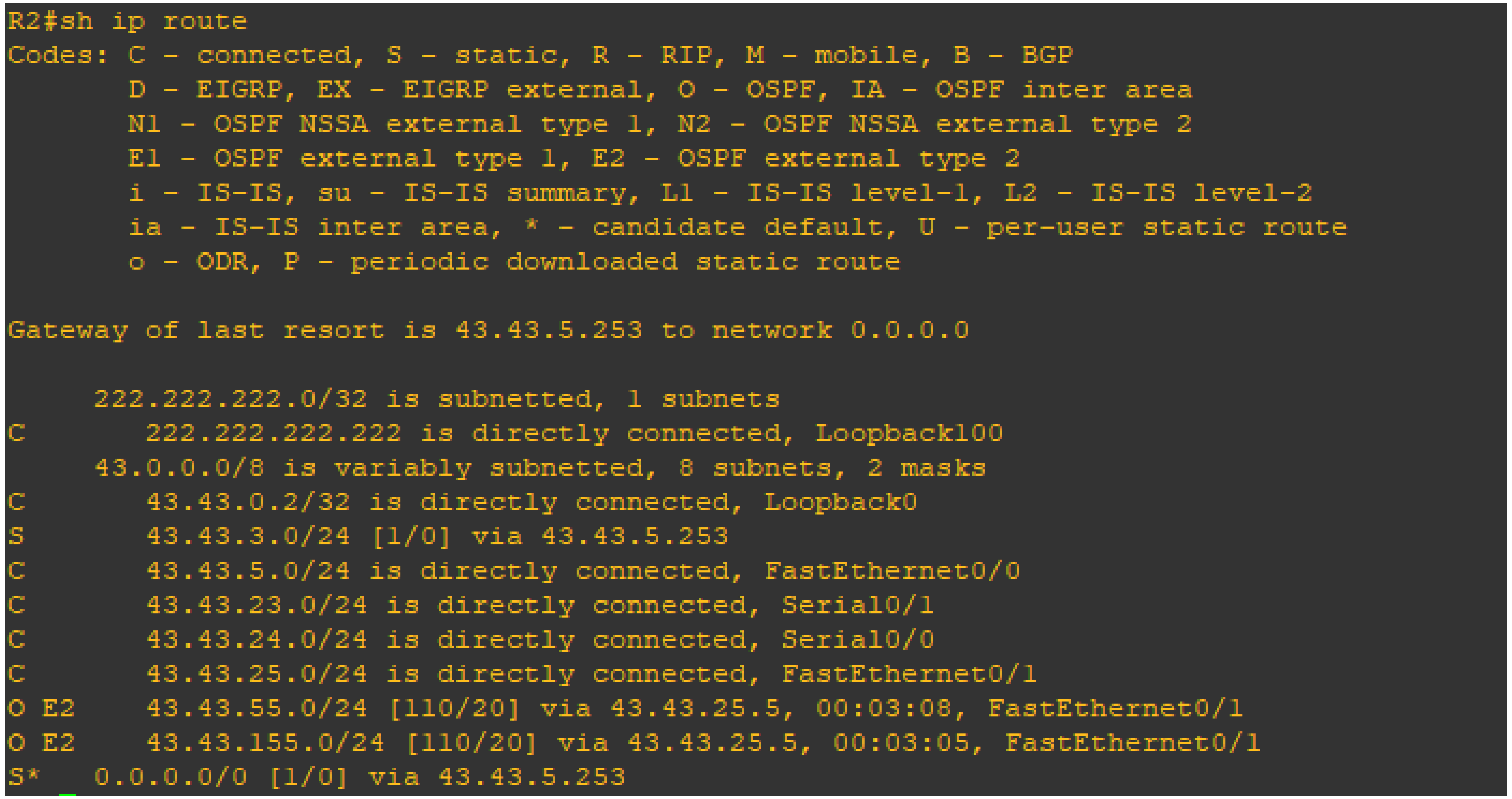
```
int f1/3
no sw
ip add 43.43.33.250
255.255.255.0
no sh
```

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
```

2. 주소 설정 및 라우팅

2-3. 설정 확인



```
R2#sh 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, 00:03:08, FastEthernet0/1
O E2    43.43.155.0/24 [110/20] via 43.43.25.5, 00:03:05, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 43.43.5.253
```

3. 방화벽 이중화(failover) 설정

3-1. 방화벽 기본 설정

FW1

```
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
```

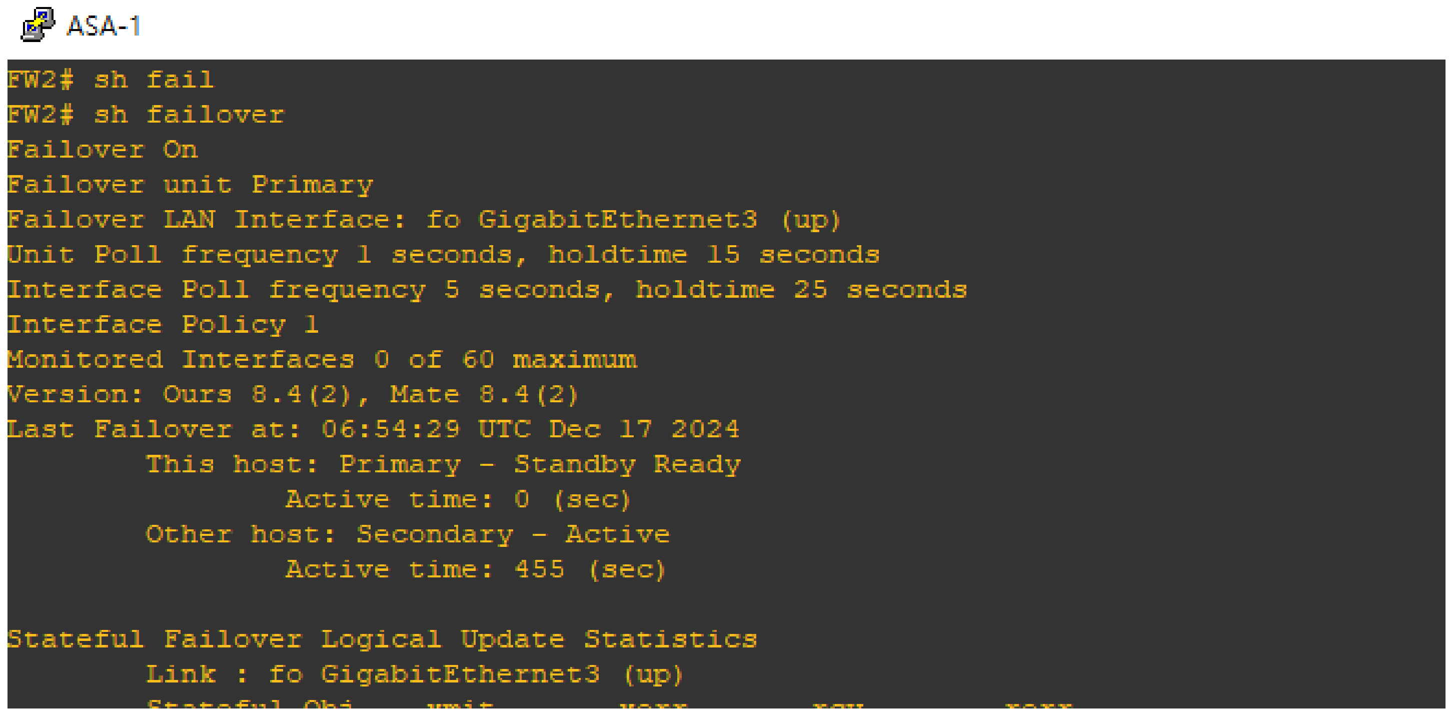
FW2

```
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
```

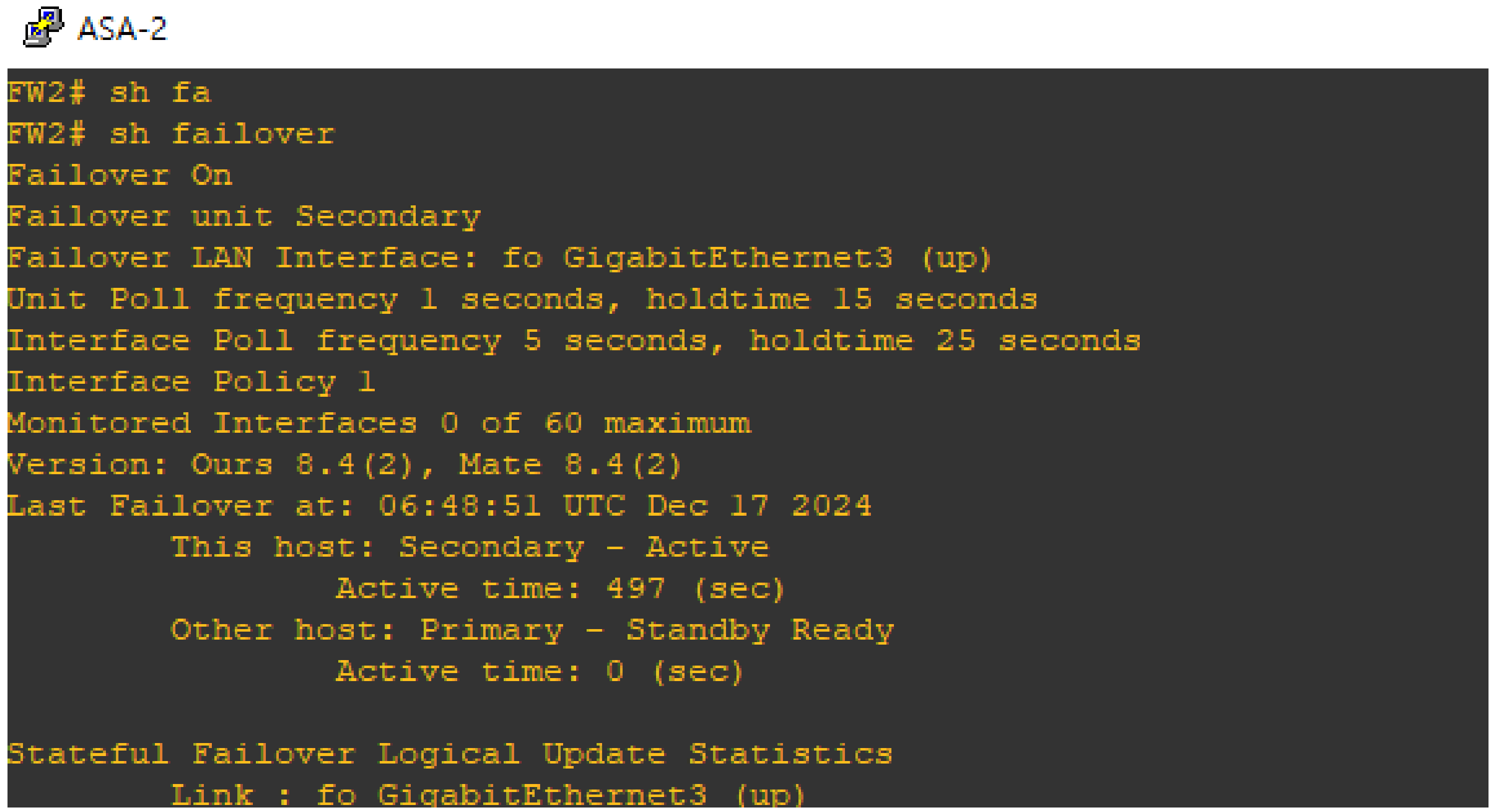
3. 방화벽 이중화(failover) 설정

3-2. 기본 설정 확인


ASA-1

```
FW2# sh fail
FW2# sh failover
Failover On
Failover unit Primary
Failover LAN Interface: fo GigabitEthernet3 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 0 of 60 maximum
Version: Ours 8.4(2), Mate 8.4(2)
Last Failover at: 06:54:29 UTC Dec 17 2024
        This host: Primary - Standby Ready
                Active time: 0 (sec)
        Other host: Secondary - Active
                Active time: 455 (sec)

Stateful Failover Logical Update Statistics
        Link : fo GigabitEthernet3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
```

▲ FW1


ASA-2

```
FW2# sh fa
FW2# sh failover
Failover On
Failover unit Secondary
Failover LAN Interface: fo GigabitEthernet3 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 0 of 60 maximum
Version: Ours 8.4(2), Mate 8.4(2)
Last Failover at: 06:48:51 UTC Dec 17 2024
        This host: Secondary - Active
                Active time: 497 (sec)
        Other host: Primary - Standby Ready
                Active time: 0 (sec)

Stateful Failover Logical Update Statistics
        Link : fo GigabitEthernet3 (up)
```

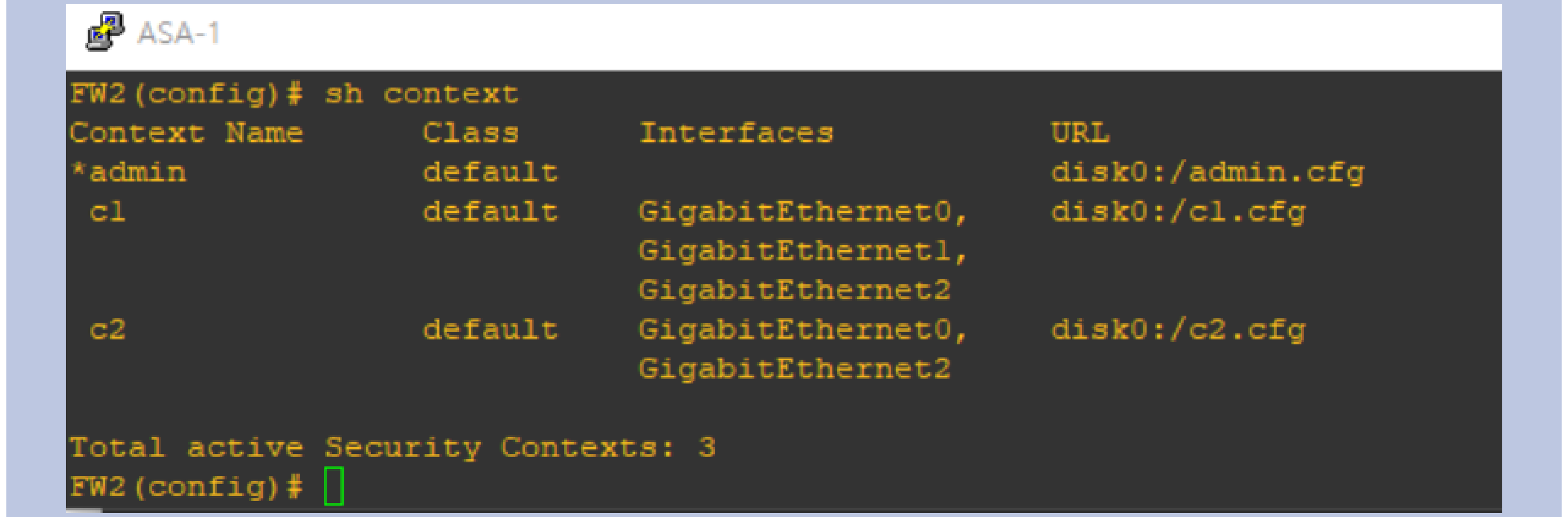
▲ FW2

3. 방화벽 이중화(failover) 설정

3-3. 컨텍스트 생성 및 할당

FW1

```
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
```



```
FW2(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
FW2(config)# 
```

3. 방화벽 이중화(failover) 설정

3-3. 컨텍스트 생성 및 할당

FW1

```
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
```

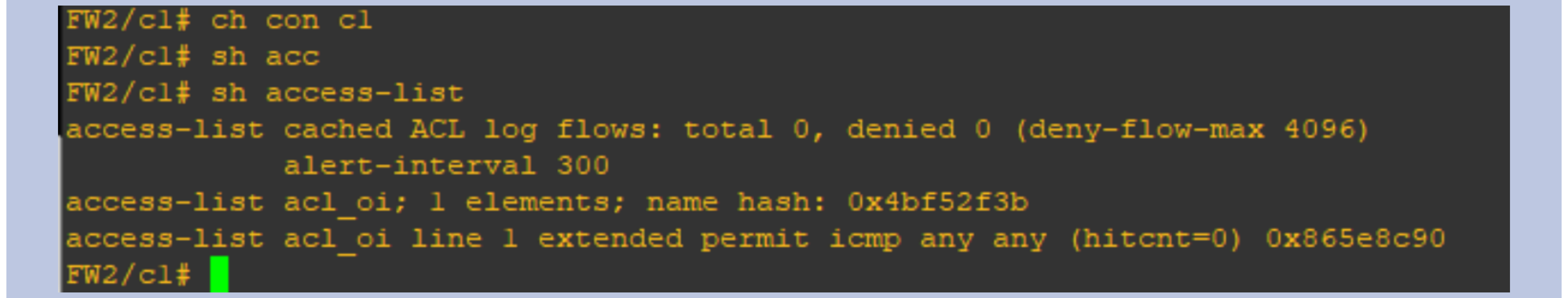
```
int g0
nameif outside
secu 0
ip add 43.43.5.253
255.255.255.0 stand 43.43.5.254

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
```

3. 방화벽 이중화(failover) 설정

3-4. Access List 설정

FW1

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

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



```
FW2/c1# ch con c1
FW2/c1# sh acc
FW2/c1# sh 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
FW2/c1#
```

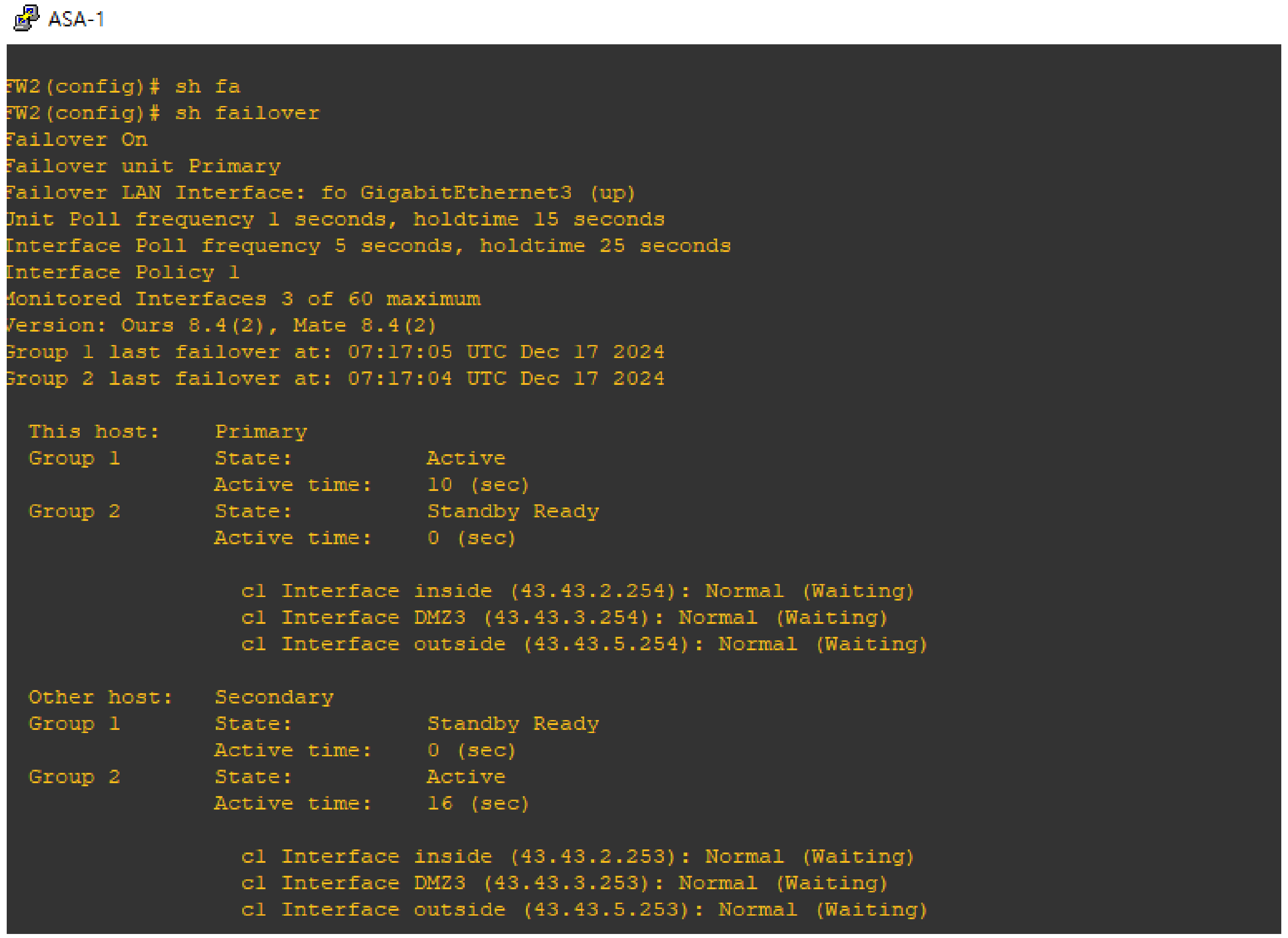
3. 방화벽 이중화(failover) 설정

3-5. 방화벽 이중화 Active-Active 모드

```
FW1

 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
```

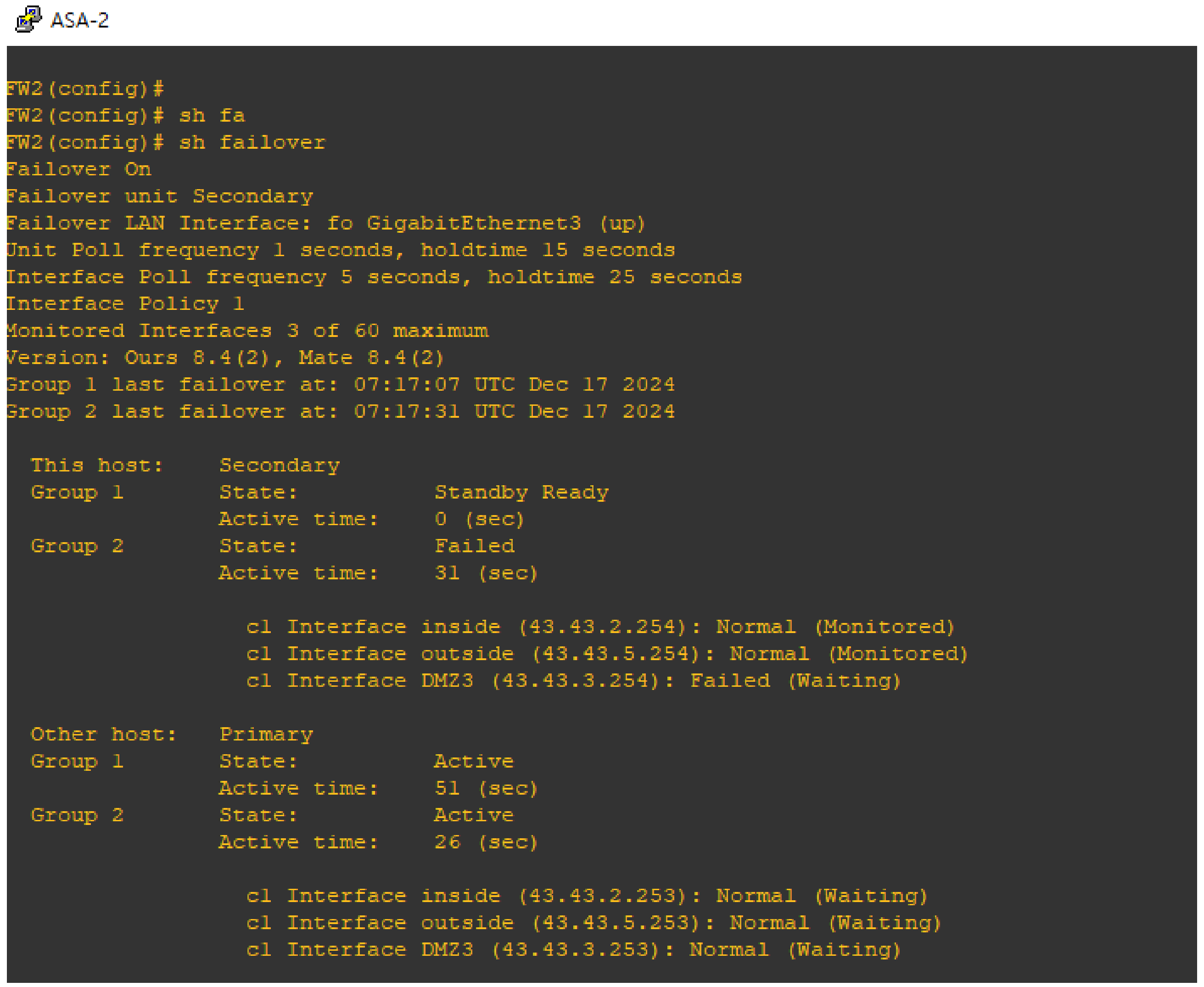
3. 방화벽 이중화(failover) 설정

3-6. Active-Active 모드 설정 확인



```
FW2(config)# sh fa
FW2(config)# sh failover
Failover On
Failover unit Primary
Failover LAN Interface: fo 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: 07:17:05 UTC Dec 17 2024
Group 2 last failover at: 07:17:04 UTC Dec 17 2024

  This host:    Primary
  Group 1       State:          Active
                Active time:    10 (sec)
  Group 2       State:          Standby Ready
                Active time:    0 (sec)

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

  Other host:   Secondary
  Group 1       State:          Standby Ready
                Active time:    0 (sec)
  Group 2       State:          Active
                Active time:    16 (sec)

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

▲ FW1



```
FW2(config)#
FW2(config)# sh fa
FW2(config)# sh failover
Failover On
Failover unit Secondary
Failover LAN Interface: fo 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: 07:17:07 UTC Dec 17 2024
Group 2 last failover at: 07:17:31 UTC Dec 17 2024

  This host:    Secondary
  Group 1       State:          Standby Ready
                Active time:    0 (sec)
  Group 2       State:          Failed
                Active time:    31 (sec)

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

  Other host:   Primary
  Group 1       State:          Active
                Active time:    51 (sec)
  Group 2       State:          Active
                Active time:    26 (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)
```

▲ FW2

감사합니다.