APEX

APEX

방화벽 프로젝트

이정일 임재근 서재권 김민호

목차

APEX

01 **물리적/논리적 구성도**
- 1 - 1. 물리적 구성도
- 1 - 2. 논리적 구성도
- 1 - 3. 논리적 구성도(영역)

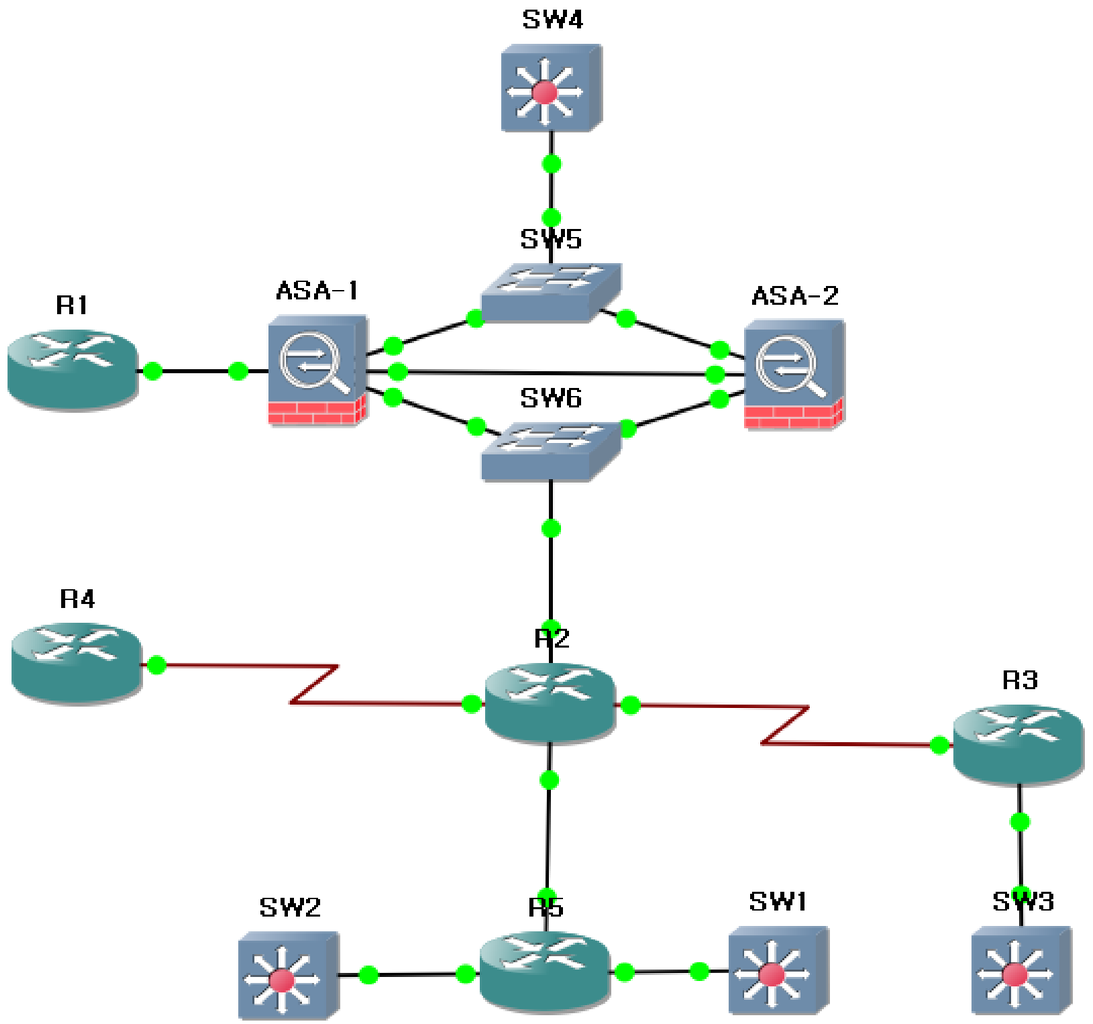
02 **라우터/스위치 설정**
- 2 - 1. 라우터 설정
- 2 - 2. 스위치 설정
- 2 - 3. 설정 확인

03 **방화벽 설정**
- 3 - 1. 방화벽 이중화 기본 설정
- 3 - 2. 방화벽 Security Context 설정
- 3 – 3. 방화벽 ACL 설정
- 3 – 4. Active – Active Failover 설정

01 - 1

물리적 구성도

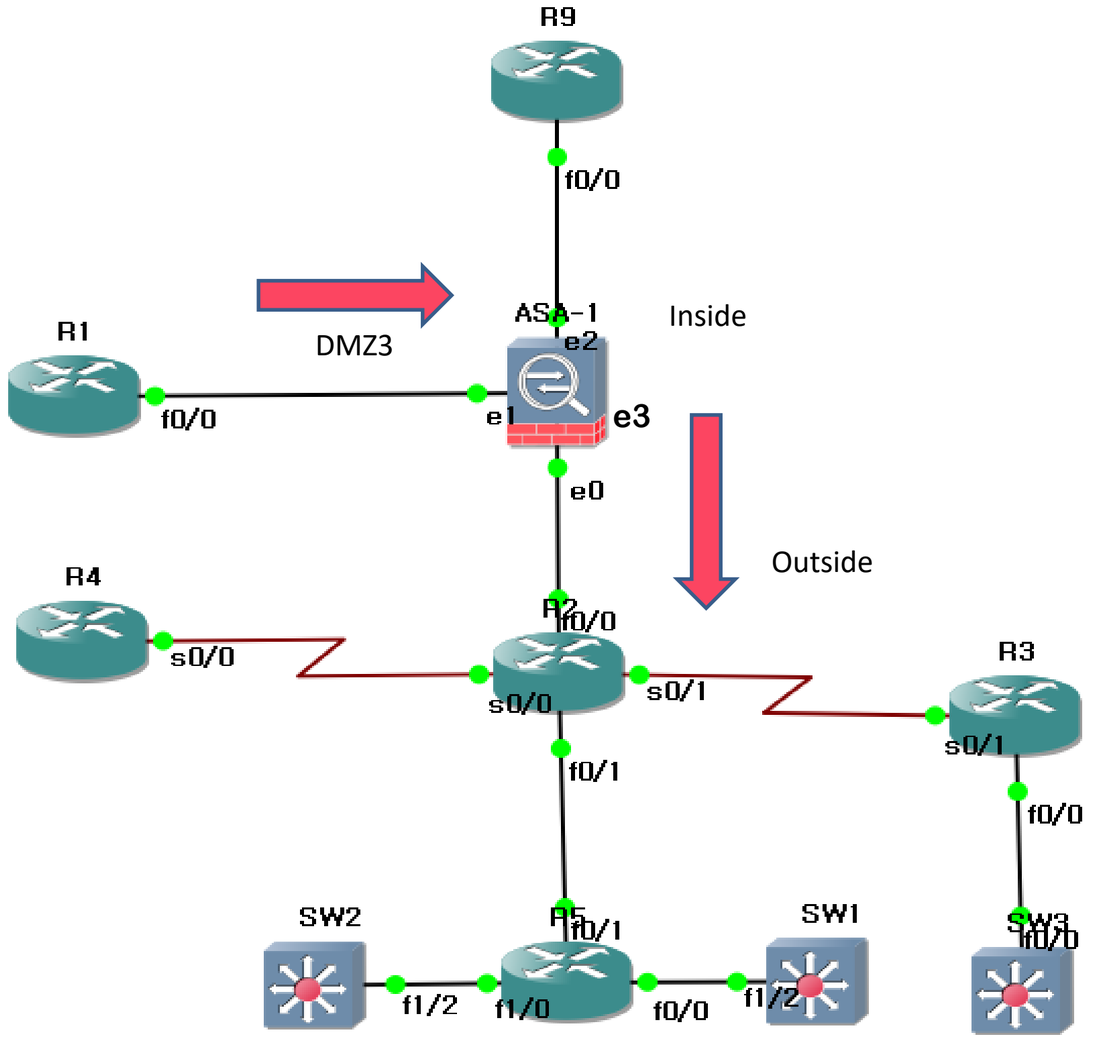
APEX



01 - 2

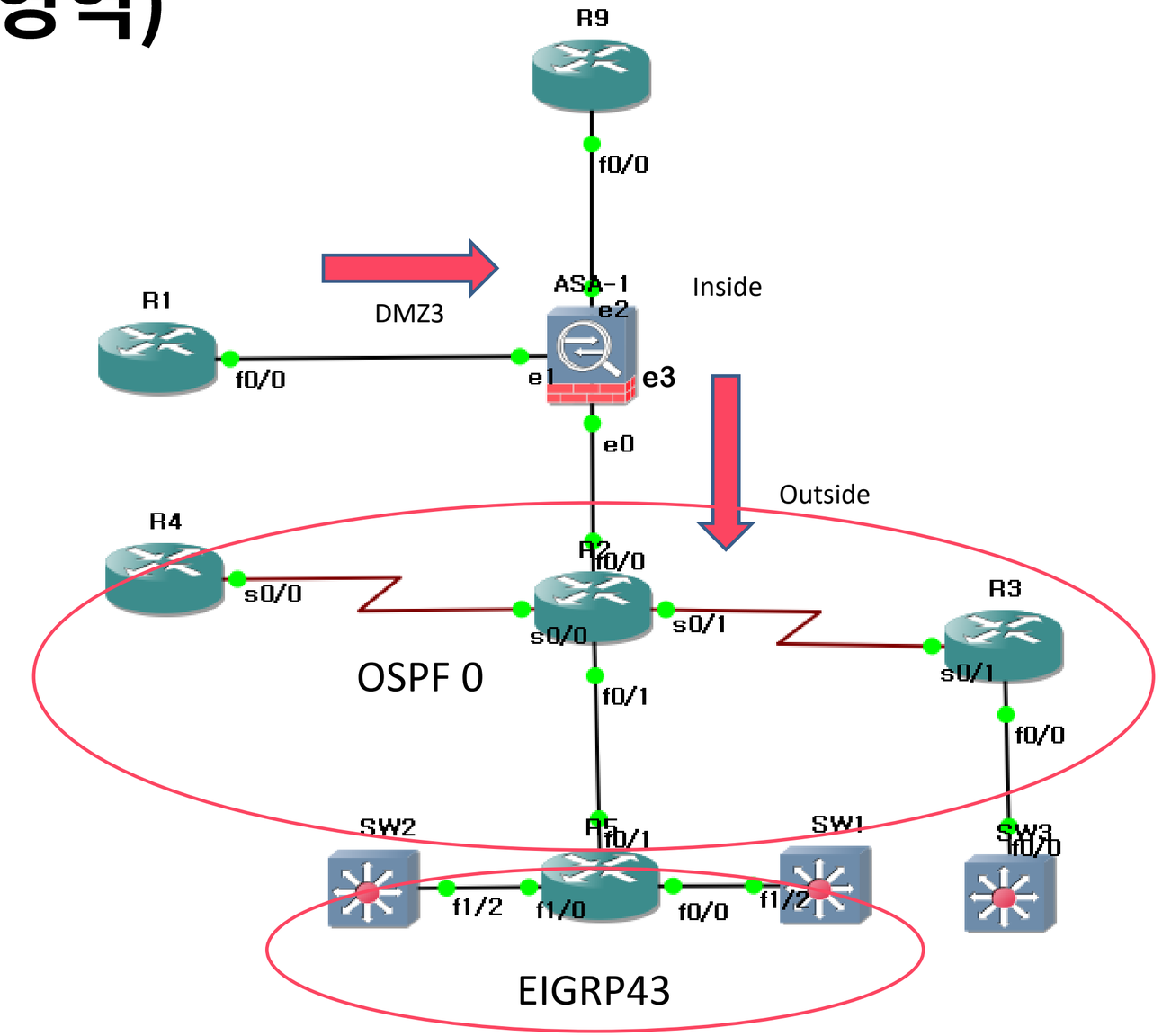
논리적 구성도

APEX



논리적 구성도(영역)

APEX



02 – 1

라우터 설정

APEX

R1

```
en
conf t
int lo0
ip address 43.43.0.1
255.255.255.0
int lo100
ip address 111.111.111.111
255.255.255.0
int f0/0
no shutdown
ip address 43.43.3.1
255.255.255.0
ip route 0.0.0.0 0.0.0.0
43.43.3.253
```

R2

```
en
conf t
int lo0
ip add 43.43.0.2
255.255.255.255
int lo 100
ip add 222.222.222.222
255.255.255.255
int f0/0
no sh
ip add 43.43.5.2 255.255.255.0
int f0/1
no sh
ip add 43.43.25.2 255.255.255.0
int s0/0
no sh
ip add 43.43.24.2 255.255.255.0
int s0/1
no sh
ip add 43.43.23.2 255.255.255.0
```

```
router ospf 1
router-id 43.43.0.2
network 43.43.23.2 0.0.0.0 area 0
network 43.43.24.2 0.0.0.0 area 0
network 43.43.25.2 0.0.0.0 area 0
default-information originate
ip route 43.43.3.0 255.255.255.0 43.43.5.253
ip route 0.0.0.0 0.0.0.0 43.43.5.253
```

02 – 1

라우터 설정

APEX

R3

```
en
conf t
int lo0
ip address 43.43.0.3
255.255.255.255
int s0/1
no shutdown
ip address 43.43.23.3
255.255.255.0
int f0/0
no sh
ip add 43.43.33.3 255.255.255.0
router ospf 1
router-id 43.43.0.3
network 43.43.23.3 0.0.0.0 area 0
```

R4

```
en
conf t
int lo0
ip address 43.43.0.4
255.255.255.255
int s0/0
no shutdown
ip address 43.43.24.4
255.255.255.0
router ospf 1
router-id 43.43.0.4
network 43.43.24.4 0.0.0.0 area 0
```

02 – 1

라우터 설정

APEX

R5

```
en
conf t
int lo0
ip address 43.43.0.5
255.255.255.255
int lo100
ip address 155.155.155.155
255.255.255.255
int f0/0
no shutdown
ip address 43.43.155.5
255.255.255.0
int f0/1
no shutdown
ip address 43.43.25.5
255.255.255.0
int f1/0
no shutdown
ip address 43.43.55.5
255.255.255.0
```

```
router ospf 1
router-id 43.43.0.5
network 43.43.25.5 0.0.0.0 area 0
redistribute eigrp 43 subnets
router eigrp 43
no auto-summary
network 43.43.55.5 0.0.0.0
network 43.43.155.5 0.0.0.0
redistribute ospf 1 metric 1544 2000 255 1 1500
```

02 – 2

스위치 설정

APEX

SW1

```
en
conf t
int f1/2
no swi
no sh
ip add 43.43.155.250
255.255.255.0
router eigrp 43
no auto-summary
network 43.43.155.250 0.0.0.0
```

SW2

```
en
conf t
int f1/2
no swi
no sh
ip add 43.43.55.250 255.255.255.0
router eigrp 43
no auto-summary
network 43.43.55.250 0.0.0.0
```

스위치 설정

APEX

SW3

```
en
conf t
int f1/5
no shutdown
no switchport
ip address 43.43.33.250
255.255.255.0
```

SW4

```
en
conf t
int lo0
ip add 150.1.43.10 255.255.255.0
no sh
int f1/10
no shutdown
no switchport
ip address 43.43.2.250
255.255.255.0
ip route 0.0.0.0 0.0.0.0
43.43.2.253
```

02 – 3

설정 확인

R2

```
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, 00:27:10, FastEthernet0/1
O E2    43.43.155.0/24 [110/20] via 43.43.25.5, 00:27:10, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 43.43.5.253
R2#
```

R2 라우팅 테이블 확인

APEX

03 – 1

방화벽 이중화 기본 설정

APEX

FW1

```
mode multiple

int g0
no sh

int g1
no sh

int g2
no sh

int g3
no sh
```

```
no failover

failover lan unit primary
failover lan interface FO g3
failover link FO
failover int ip FO
43.43.100.100 255.255.255.0
standby 43.43.100.101
```

FW2

```
mode multiple

int g0
no sh

int g1
no sh

int g2
no sh

int g3
no sh
```

```
no failover

failover lan unit secondary
failover lan interface FO g3
failover link FO
failover int ip FO
43.43.100.100 255.255.255.0
standby 43.43.100.101
```

03 – 1

방화벽 이중화 기본 설정

APEX

FW1

```
FW1(config)# show 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: 06:10:50 UTC Jul 16 2025
        This host: Primary - Active
                Active time: 69 (sec)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)

Stateful Failover Logical Update Statistics
        Link : FO GigabitEthernet3 (up)
        Stateful Obj     xmit       xerr       rcv        rerr
        General          8          0          7          0
        sys cmd          7          0          7          0
        up time          0          0          0          0
        RPC services     0          0          0          0
        TCP conn         0          0          0          0
        UDP conn         0          0          0          0
        ARP tbl          0          0          0          0
        Xlate_Timeout    0          0          0          0
        IPv6 ND tbl      0          0          0          0
        SIP Session      0          0          0          0
        Route Session    0          0          0          0
        User-Identity    1          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       7
        Xmit Q:         0       1       8
```

방화벽 이중화 기본설정 확인

FW2

```
FW1(config)# show 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: 06:06:20 UTC Jul 16 2025
        This host: Secondary - Standby Ready
                Active time: 0 (sec)
        Other host: Primary - Active
                Active time: 113 (sec)

Stateful Failover Logical Update Statistics
        Link : FO GigabitEthernet3 (up)
        Stateful Obj     xmit       xerr       rcv        rerr
        General          13         0          14         0
        sys cmd          13         0          13         0
        up time          0          0          0          0
        RPC services     0          0          0          0
        TCP conn         0          0          0          0
        UDP conn         0          0          0          0
        ARP tbl          0          0          0          0
        Xlate_Timeout    0          0          0          0
        IPv6 ND tbl      0          0          0          0
        SIP Session      0          0          0          0
        Route Session    0          0          0          0
        User-Identity    0          0          1          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       14
        Xmit Q:         0       1       13
```

방화벽 이중화 기본설정 확인

03 – 2

방화벽 Security Context 설정

APEX

FW1

```
admin-context admin
context admin
allocate-interface g0
allocate-interface g2
config-url admin.cfg

context R1
allocate-interface g0
allocate-interface g1
allocate-interface g2
config-url r1.cfg

changeto context admin
int g2
nameif inside
ip add 43.43.2.253 255.255.255.0 standby 43.43.2.254
int g0
nameif outside
ip add 43.43.5.253 255.255.25.0 standby 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

ch con R1

int g2
nameif inside
ip add 43.43.2.251 255.255.255.0 standby 43.43.2.252

int g1
nameif DMZ3
ip add 43.43.3.253 255.255.255.0 standby 43.43.3.254
security-level 100
ip add 43.43.3.253 255.255.255.0 standby 43.43.3.254

int g0
nameif outside
ip add 43.43.5.251 255.255.255.0 standby 43.43.3.250
route outside 0 0 43.43.5.2
route inside 150.1.43.0 255.255.255.0 43.43.2.250
route DMZ3 43.43.0.1 255.255.255.255 43.43.3.1
```

FW2

```
admin-context admin
context admin
allocate-interface g0
allocate-interface g2
config-url admin.cfg

context R1
allocate-interface g0
allocate-interface g1
allocate-interface g2
config-url r1.cfg
```

방화벽 Security Context 설정

APEX

FW1

```
FW1# show context
Context Name       Class       Interfaces              URL
*admin             default     GigabitEthernet0,       disk0:/admin.cfg
                               GigabitEthernet2
 R1                default     GigabitEthernet0,       disk0:/r1.cfg
                               GigabitEthernet1,
                               GigabitEthernet2

Total active Security Contexts: 2
FW1#
```

Context 생성 확인

방화벽 ACL 설정

APEX

FW1

ch con admin
access-list acl_oi per icmp any any
access-group acl_oi in int outside

ch con R1
access-list acl_inside per icmp a a
access-g acl_inside in int outside
same-security-traffic per inter-interface

```
FW1/admin# 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=4) 0x865e8c90
FW1/admin#
```

방화벽 ACL 설정 확인 admin

```
FW1/R1# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list acl_inside; 1 elements; name hash: 0x9619630d
access-list acl_inside line 1 extended permit icmp any any (hitcnt=0) 0x2a153715
FW1/R1#
```

방화벽 ACL 설정 확인 R1

03 – 3

방화벽 ACL 설정

APEX

```
R2#ping 43.43.2.250

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 43.43.2.250, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/62/72 ms
R2#
```

R2 -> Sw4 연결 확인

```
SW4#ping 43.43.5.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 43.43.5.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/58/64 ms
SW4#
```

SW4 -> R2 연결 확인

Active – Active failover 설정

APEX

FW1

```
ch sys
failover group 1
primary
preempt
failover group 2
secondary
preempt
context admin
join-failover-group 1
context R1
join-failover-group 2
failover
```

FW2

```
failover group 1
secondary
preempt
failover group 2
primary
preempt
context R1
allocate-interface g0
allocate-interface g1
allocate-interface g2
config-url r1.cfg
con admin
join-failover-group 1
con R1
join-failover-group 2
failover
```

Active – Active failover 설정

APEX

FW1

```
FW1(config)# show 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 5 of 60 maximum
Version: Ours 8.4(2), Mate 8.4(2)
Group 1 last failover at: 06:00:53 UTC Jul 16 2025
Group 2 last failover at: 06:00:51 UTC Jul 16 2025

  This host:    Primary
  Group 1       State:          Active
                Active time:    29 (sec)
  Group 2       State:          Standby Ready
                Active time:    0 (sec)

                  admin Interface inside (43.43.2.253): Normal (Monitored)
                  admin Interface outside (0.0.0.0): Normal (Waiting)
                  R1 Interface inside (43.43.2.252): Normal (Monitored)
                  R1 Interface DMZ3 (43.43.3.254): Normal (Waiting)
                  R1 Interface outside (0.0.0.0): Normal (Waiting)

  Other host:   Secondary
  Group 1       State:          Standby Ready
                Active time:    0 (sec)
  Group 2       State:          Active
                Active time:    34 (sec)

                  admin Interface inside (43.43.2.254): Normal (Monitored)
                  admin Interface outside (0.0.0.0): Normal (Waiting)
                  R1 Interface inside (43.43.2.251): Normal (Monitored)
                  R1 Interface DMZ3 (43.43.3.253): Unknown (Waiting)
                  R1 Interface outside (0.0.0.0): Normal (Waiting)

Stateful Failover Logical Update Statistics
        Link : FO GigabitEthernet3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         6          0          6          0
        sys cmd         5          0          5          0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        Xlate_Timeout   0          0          0          0
        IPv6 ND tbl     0          0          0          0
        SIP Session     0          0          0          0
        Route Session   0          0          0          0
        User-Identity   1          0          1          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       7
        Xmit Q:         0       1       7
FW1(config)#
```

Show failover

FW2

```
FW1(config)# show 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 5 of 60 maximum
Version: Ours 8.4(2), Mate 8.4(2)
Group 1 last failover at: 06:00:55 UTC Jul 16 2025
Group 2 last failover at: 06:00:49 UTC Jul 16 2025

  This host:    Secondary
  Group 1       State:          Standby Ready
                Active time:    0 (sec)
  Group 2       State:          Active
                Active time:    106 (sec)

                  admin Interface outside (0.0.0.0): Normal (Waiting)
                  admin Interface inside (43.43.2.254): Normal (Monitored)
                  R1 Interface outside (0.0.0.0): Normal (Waiting)
                  R1 Interface DMZ3 (43.43.3.253): Unknown (Waiting)
                  R1 Interface inside (43.43.2.251): Normal (Monitored)

  Other host:   Primary
  Group 1       State:          Active
                Active time:    102 (sec)
  Group 2       State:          Standby Ready
                Active time:    0 (sec)

                  admin Interface outside (0.0.0.0): Normal (Waiting)
                  admin Interface inside (43.43.2.253): Normal (Monitored)
                  R1 Interface outside (0.0.0.0): Normal (Waiting)
                  R1 Interface DMZ3 (43.43.3.254): Normal (Waiting)
                  R1 Interface inside (43.43.2.252): Normal (Monitored)

Stateful Failover Logical Update Statistics
        Link : FO GigabitEthernet3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         15         0          15         0
        sys cmd         14         0          14         0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        Xlate_Timeout   0          0          0          0
        IPv6 ND tbl     0          0          0          0
        SIP Session     0          0          0          0
        Route Session   0          0          0          0
        User-Identity   1          0          1          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       16
        Xmit Q:         0       1       16
FW1(config)#
```

Show failover

이상으로 프로젝트를 마칩니다.
감사합니다.

#APEX #FireWall #NetWork #Router #Switch