Firewall Project

대우능력개발원

방화벽
프레젠테이션

BS_FAN I 김태경 박종승 윤재영 김효은

목차

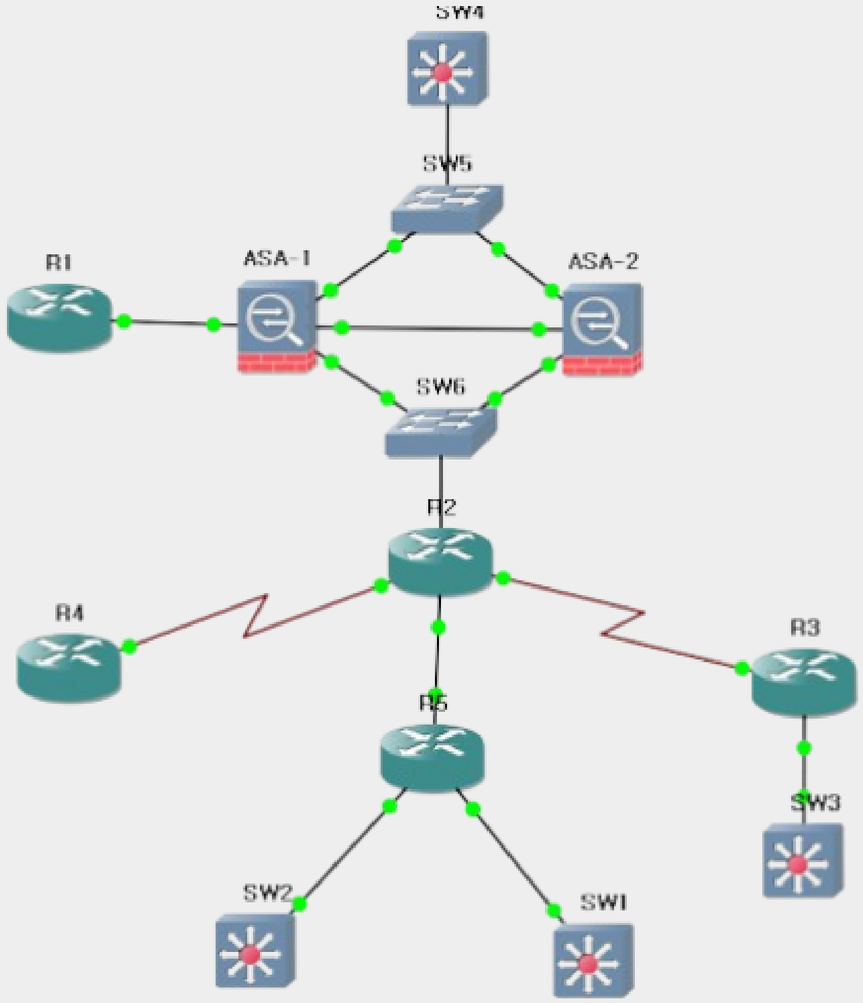
Firewall Project

방화벽

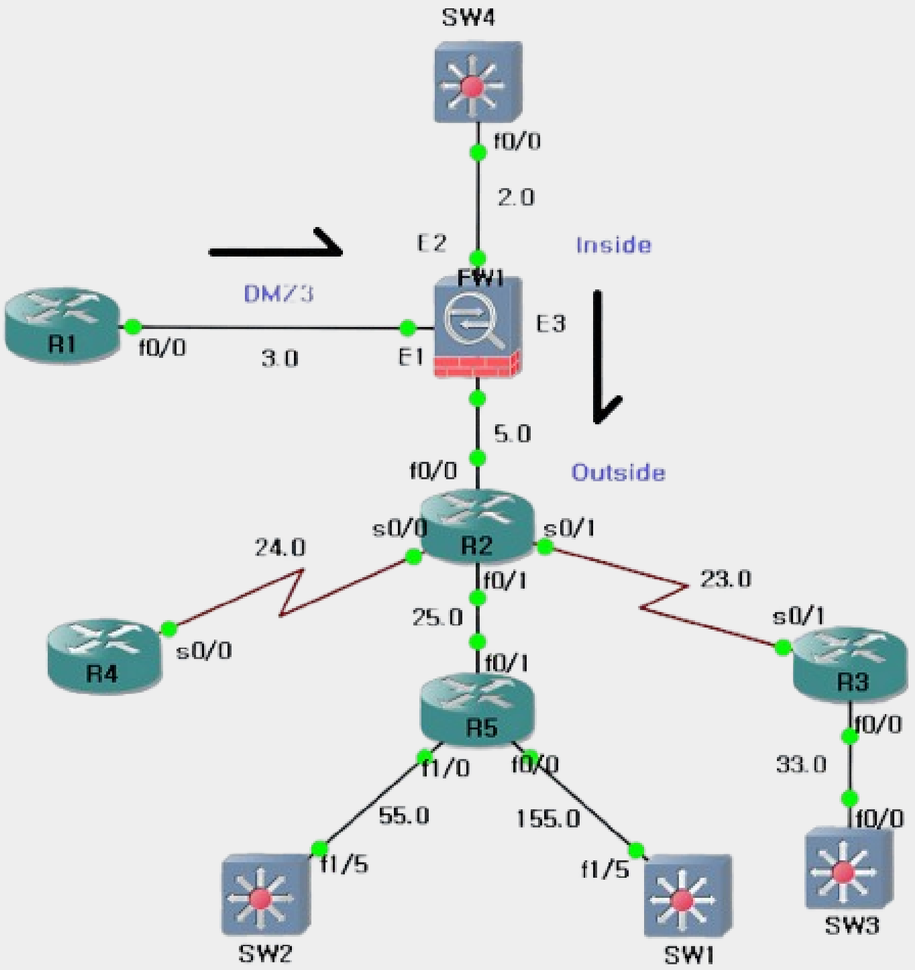
라우터, 스위치

물리적/논리적 구성도

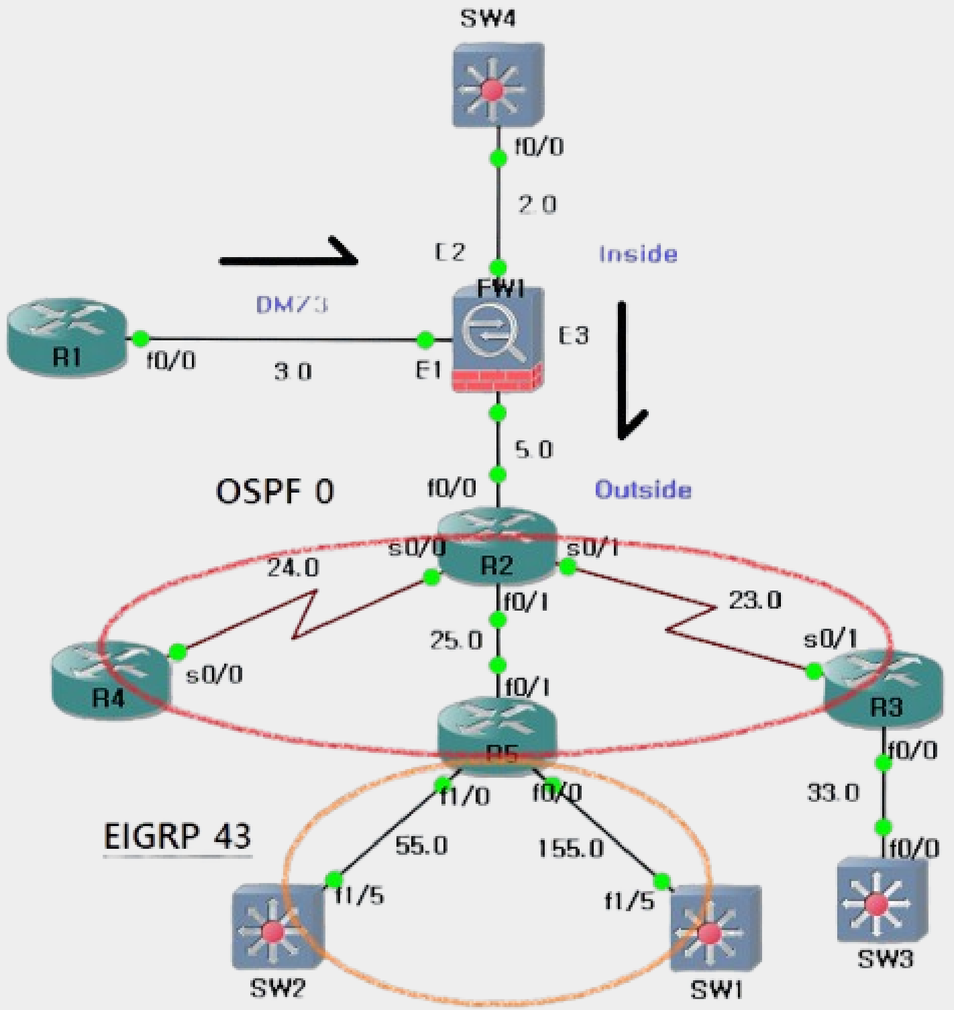
물리적 구성도



논리적 구성도


SW4
f0/0
2.0
E2
Inside
FW1
DMZ3
E3
R1
f0/0
3.0
E1
5.0
f0/0
Outside
s0/0
R2
s0/1
24.0
f0/1
23.0
25.0
s0/1
s0/0
R4
f0/1
R3
R5
f0/0
f1/0
f0/0
33.0
55.0
155.0
f0/0
f1/5
f1/5
SW2
SW1
SW3

논리적 구성도(영역)


SW4
f0/0
2 0
E2
Inside
FW1
DMZ
E3
R1
f0/0
3 0
E1
5 0
OSPF 0
f0/0
Outside
s0/0
R2
s0/1
24.0
23.0
f0/1
25.0
s0/1
s0/0
R4
f0/1
R3
R5
f0/0
f1/0
f0/0
33.0
EIGRP 43
55.0
155.0
f0/0
f1/5
f1/5
SW2
SW1
SW3

Firewall Project

방화벽

라우터, 스위치

라우터/스위치 구성 및 주소 설정

라우터/스위치 구성 및 주소 설정

R1

```
int lo0
ip address 43.43.0.1
255.255.255.255

int lo100
ip address 111.111.111.111
255.255.255.0
int f0/0

no shutdown
ip add 43.43.3.1
255.255.255.0
```

R2

```
int lo0
ip add 43.43.0.2
255.255.255.255

int lo100
ip address 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
ip ospf network broadcast

int s0/1
no sh
ip add 43.43.23.2
255.255.255.0
ip ospf network broadcast
```

라우터/스위치 구성 및 주소 설정

R3

```
int lo0
ip add 43.43.0.3
255.255.255.255

int f0/0
no shutdown
ip add 43.43.33.3
255.255.255.0

int s0/1
no shutdown
ip add 43.43.23.3
255.255.255.0
ip ospf network broadcast
ip ospf priority 0
```

R4

```
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
ip ospf network broadcast
ip ospf priority 0
```

라우터/스위치 구성 및 주소 설정

R5

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

SW1

int f1/5
no shutdown
no switchport
ip address 43.43.155.250
255.255.255.0

라우터/스위치 구성 및 주소 설정

SW2

int f1/5
no shutdown
no switchport
ip address 43.43.55.250
255.255.255.0

SW3

int f1/5
no shutdown
no switchport
ip address 43.43.155.250
255.255.255.0

SW4

int lo 0
ip add 150.1.43.10
255.255.255.0

int f1/10
no shutdown
no switchport
ip address 43.43.2.250
255.255.255.0

라우터/스위치 구성 및 주소 설정 - 라우터 확인

```
R1(config-if)#do sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            43.43.3.1       YES manual up                    up
Serial0/0                  unassigned      YES unset  administratively down down
FastEthernet0/1            unassigned      YES unset  administratively down down
Serial0/1                  unassigned      YES unset  administratively down down
Serial0/2                  unassigned      YES unset  administratively down down
FastEthernet1/0            unassigned      YES unset  administratively down down
Loopback0                  43.43.0.1       YES manual up                    up
Loopback100                111.111.111.111 YES manual up                    up
```

```
R2(config-if)#do sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            43.43.5.2       YES manual up                    up
Serial0/0                  43.43.24.2      YES manual up                    up
FastEthernet0/1            43.43.25.2      YES manual up                    up
Serial0/1                  43.43.23.2      YES manual up                    up
Serial0/2                  unassigned      YES unset  administratively down down
FastEthernet1/0            unassigned      YES unset  administratively down down
oback0                     43.43.0.2       YES manual up                    up
oback100                   222.222.222.222 YES manual up                    up
```

```
R3(config-if)#do sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            43.43.33.3      YES manual up                    up
Serial0/0                  unassigned      YES unset  administratively down down
FastEthernet0/1            unassigned      YES unset  administratively down down
Serial0/1                  43.43.23.3      YES manual up                    up
Serial0/2                  unassigned      YES unset  administratively down down
FastEthernet1/0            unassigned      YES unset  administratively down down
Loopback0                  43.43.0.3       YES manual up                    up
```

```
R4(config-if)#do sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES unset  administratively down down
Serial0/0                  43.43.24.4      YES manual up                    up
FastEthernet0/1            unassigned      YES unset  administratively down down
Serial0/1                  unassigned      YES unset  administratively down down
al0/2                      unassigned      YES unset  administratively down down
Ethernet1/0                unassigned      YES unset  administratively down down
back0                      43.43.0.4       YES manual up                    up
```

```
R5(config-if)#do sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            43.43.155.5     YES manual up                    up
Serial0/0                  unassigned      YES unset  administratively down down
FastEthernet0/1            43.43.25.5      YES manual up                    up
Serial0/1                  unassigned      YES unset  administratively down down
Serial0/2                  unassigned      YES unset  administratively down down
FastEthernet1/0            43.43.55.5      YES manual up                    up
Loopback0                  43.43.0.5       YES manual up                    up
Loopback100                155.155.155.155 YES manual up                    up
```

라우터/스위치 구성 및 주소 설정 - 스위치 확인

SW1(config-if)#do sh ip int br

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	administratively down	down
Serial0/0	unassigned	YES	unset	administratively down	down
FastEthernet0/1	unassigned	YES	unset	administratively down	down
Serial0/1	unassigned	YES	unset	administratively down	down
Serial0/2	unassigned	YES	unset	administratively down	down
FastEthernet1/0	unassigned	YES	unset	up	down
FastEthernet1/1	unassigned	YES	unset	up	down
FastEthernet1/2	unassigned	YES	unset	up	down
FastEthernet1/3	unassigned	YES	unset	up	down
FastEthernet1/4	unassigned	YES	unset	up	down
FastEthernet1/5	43.43.155.250	YES	manual	up	up

SW2(config-if)#do sh ip int br

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	administratively down	down
Serial0/0	unassigned	YES	unset	administratively down	down
FastEthernet0/1	unassigned	YES	unset	administratively down	down
Serial0/1	unassigned	YES	unset	administratively down	down
Serial0/2	unassigned	YES	unset	administratively down	down
FastEthernet1/0	unassigned	YES	unset	up	down
FastEthernet1/1	unassigned	YES	unset	up	down
FastEthernet1/2	unassigned	YES	unset	up	down
FastEthernet1/3	unassigned	YES	unset	up	down
FastEthernet1/4	unassigned	YES	unset	up	down
FastEthernet1/5	43.43.55.250	YES	manual	up	up

SW3(config-if)#do sh ip int br

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	administratively down	down
Serial0/0	unassigned	YES	unset	administratively down	down
FastEthernet0/1	unassigned	YES	unset	administratively down	down
Serial0/1	unassigned	YES	unset	administratively down	down
Serial0/2	unassigned	YES	unset	administratively down	down
FastEthernet1/0	unassigned	YES	unset	up	down
FastEthernet1/1	unassigned	YES	unset	up	down
FastEthernet1/2	unassigned	YES	unset	up	down
FastEthernet1/3	43.43.33.250	YES	manual	up	up

SW4

FastEthernet1/10	43.43.2.250	YES	manual	up	up
FastEthernet1/11	unassigned	YES	unset	up	down
FastEthernet1/12	unassigned	YES	unset	up	down
FastEthernet1/13	unassigned	YES	unset	up	down
FastEthernet1/14	unassigned	YES	unset	up	down
FastEthernet1/15	unassigned	YES	unset	up	down

Firewall Project

방화벽

라우터, 스위치

라우터/스위치 라우팅 설정

라우터/스위치 라우팅 설정

R1

```
ip route 0.0.0.0 0.0.0.0 43.43.3.253
```

R2

```
router ospf 1
router-id 43.43.0.2
network 43.43.24.2 0.0.0.0 area 0
network 43.43.23.2 0.0.0.0 a 0
network 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-information originate
```

R3

```
router ospf 1
router-id 43.43.0.3
network 43.43.23.3 0.0.0.0 area 0
```

R4

```
router ospf 1
router-id 43.43.0.4
network 43.43.24.4 0.0.0.0 area 0
```

라우터/스위치 라우팅 설정

R5

```
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 1 1 1 1 1
```

SW1

```
router eigrp 43
no auto-summary
network 43.43.155.250 0.0.0.0
```

SW2

```
router eigrp 43
no auto-summary
network 43.43.55.250 0.0.0.0
```

SW4

```
ip route 0.0.0.0 0.0.0.0 43.43.2.253
```

라우팅 설정 확인(R2)

```
R2(config)#do sh ip ro
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, 00:02:04, FastEthernet0/1
O E2    43.43.155.0/24 [110/20] via 43.43.25.5, 00:01:58, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 43.43.5.253
```

Firewall Project

방화벽

라우터, 스위치

방화벽 설정 및 이중화

방화벽 설정 및 이중화 - 기본 설정

FW1

```
mode multiple

interface g0
no shutdown

interface g1
no shutdown

interface g2
no shutdown
```

```
no failover

failover lan unit primary
failover lan interface fover g3
failover link fover g3

failover interface ip fover 43.43.100.100
255.255.255.0 standby 43.43.100.101

failover
```

FW2

```
mode multiple

interface g0
no shutdown

interface g1
no shutdown

interface g2
no shutdown

interface g3
no shutdown
```

```
no failover

failover lan unit secondary
failover lan interface fover g3
failover link fover g3

failover interface ip fover 43.43.100.100
255.255.255.0 standby 43.43.100.101

failover
```

방화벽 설정 및 이중화 - 기본 설정 확인

```
FW1(config)# show 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 0 of 60 maximum
Version: Ours 8.4(2), Mate 8.4(2)
Last Failover at: 06:10:48 UTC Dec 13 2024
        This host: Primary - Active
                Active time: 51 (sec)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)

Stateful Failover Logical Update Statistics
        Link : fover GigabitEthernet3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         6          0          5          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          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       5
        Xmit Q:         0       1       6
```

```
FW1(config)# show 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 0 of 60 maximum
Version: Ours 8.4(2), Mate 8.4(2)
Last Failover at: 06:10:42 UTC Dec 13 2024
        This host: Secondary - Standby Ready
                Active time: 0 (sec)
        Other host: Primary - Active
                Active time: 44 (sec)

Stateful Failover Logical Update Statistics
        Link : fover GigabitEthernet3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         4          0          5          0
        sys cmd         4          0          4          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       6
        Xmit Q:         0       1       5
```

방화벽 설정 및 이중화 - 컨텍스트 생성 및 할당

FW1

context c1
config-url c1.cfg
allocate-interface g2
allocate-interface g0
allocate-interface g1

context c2
config-u c2.cfg
allocate-interface g2

```
FW1(config-ctx)# show 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 및 이중화 - 컨텍스트 주소 설정

FW1

changeto context c1

interface g2
nameif inside
ip address 43.43.2.253 255.255.255.0 standby 43.43.2.254

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

int g0
nameif outside
security-level 0
ip address 43.43.5.253 255.255.255.0 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
route DMZ 43.43.0.1 255.255.255.255 43.43.3.1

방화벽 설정 및 이중화 - Active&Active 모드

FW1

changeto sys
no failover

failover group 1
preempt

failover group 2
secondary

preempt

context c2
join-failover-group 1

context c1
join-failover-group 2

failover
failover active

FW 1

```
FW1(config)# show failo
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: 06:44:41 UTC Dec 13 2024
Group 2 last failover at: 06:45:07 UTC Dec 13 2024

  This host:    Primary
  Group 1       State:          Active
                Active time:    33 (sec)
  Group 2       State:          Active
                Active time:    7 (sec)

                  cl Interface inside (43.43.2.253): N
                  cl Interface DMZ3 (43.43.3.253): Nor
                  cl Interface outside (43.43.5.253):

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

                  cl Interface inside (43.43.2.254): N
                  cl Interface DMZ3 (43.43.3.254): Fai
                  cl Interface outside (43.43.5.254):
```

FW 2

```
FW1(config)# sh failo
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: 06:44:42 UTC Dec 13 2024
Group 2 last failover at: 06:45:07 UTC Dec 13 2024

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

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

  Other host:   Primary
  Group 1       State:          Active
                Active time:    64 (sec)
  Group 2       State:          Active
                Active time:    38 (sec)

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

Firewall Project

방화벽

라우터, 스위치

Thank you!

감사합니다.

이상으로 프레젠테이션을 마칩니다.