방화벽
프로젝트

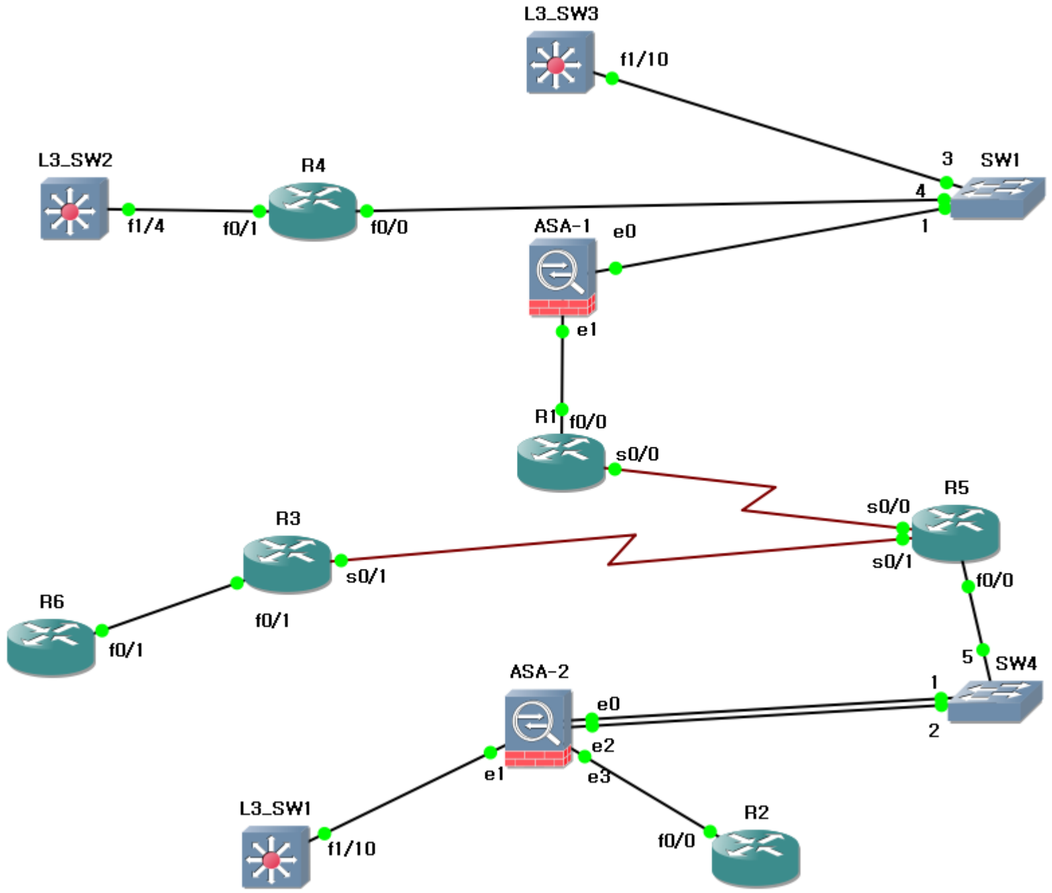
Rest | 강승환 고동우 유세종 최성민 한시완

목차

01. 구성도

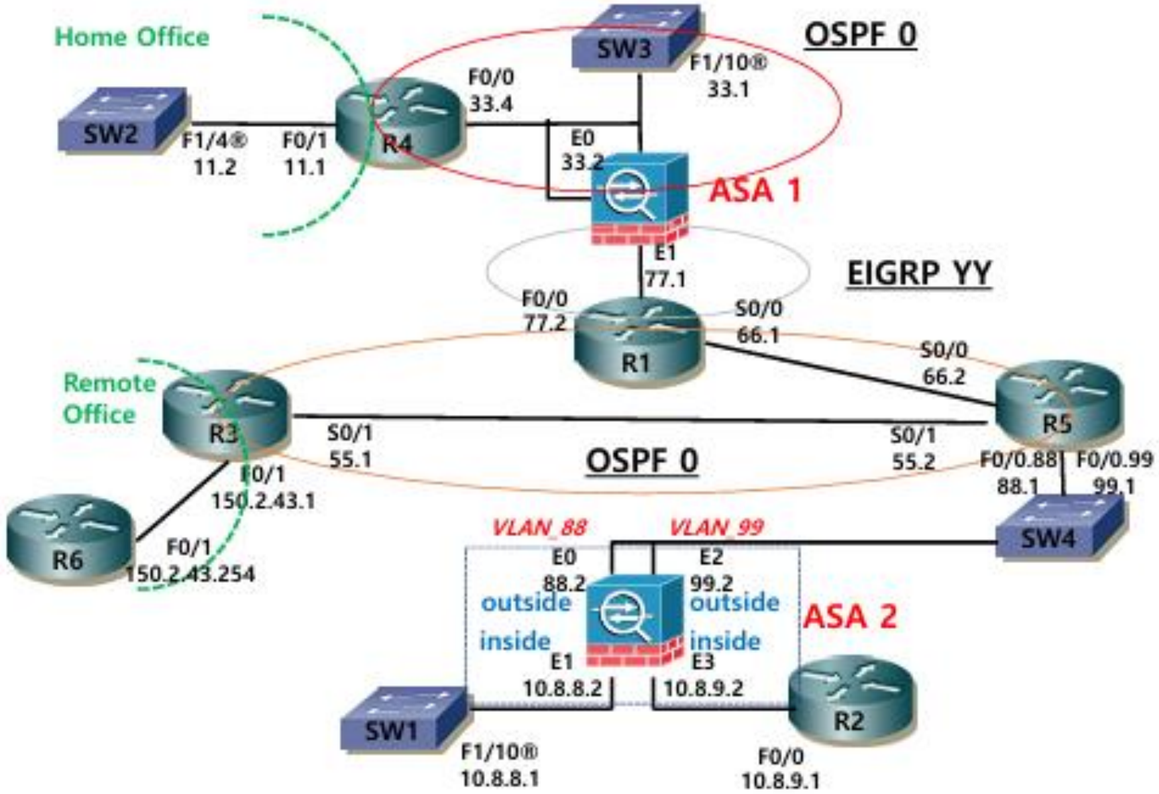
01 구성도

물리적 구성도



01 구성도

논리적 구성도



02. 스위치 설정

02 스위치 설정

2-1. SW1

```
L3_SW1(config)#int f1/10
L3_SW1(config-if)#no sw
L3_SW1(config-if)#ip add 10.8.8.1 255.255.255.0
L3_SW1(config-if)#ip route 0.0.0.0 0.0.0.0 10.8.8.2
```

→

```
L3_SW1#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 10.8.8.2 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 1 subnets
C       10.8.8.0 is directly connected, FastEthernet1/10
S*   0.0.0.0/0 [1/0] via 10.8.8.2
```

02 스위치 설정

2-2. SW2

```
L3_SW2(config)#int f1/4
L3_SW2(config-if)#no sw
L3_SW2(config-if)#ip add 43.43.11.2 255.255.255.0
L3_SW2(config-if)#ip route 0.0.0.0 0.0.0.0 43.43.11.1
```

→

```
L3_SW2#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 43.43.11.1 to network 0.0.0.0

     43.0.0.0/24 is subnetted, 1 subnets
C       43.43.11.0 is directly connected, FastEthernet1/4
S*   0.0.0.0/0 [1/0] via 43.43.11.1
```

02 스위치 설정

2-3. SW3

```
L3_SW3(config)#int f1/10
L3_SW3(config-if)#no sw
L3_SW3(config-if)#ip add 43.43.33.1 255.255.255.0
```

→

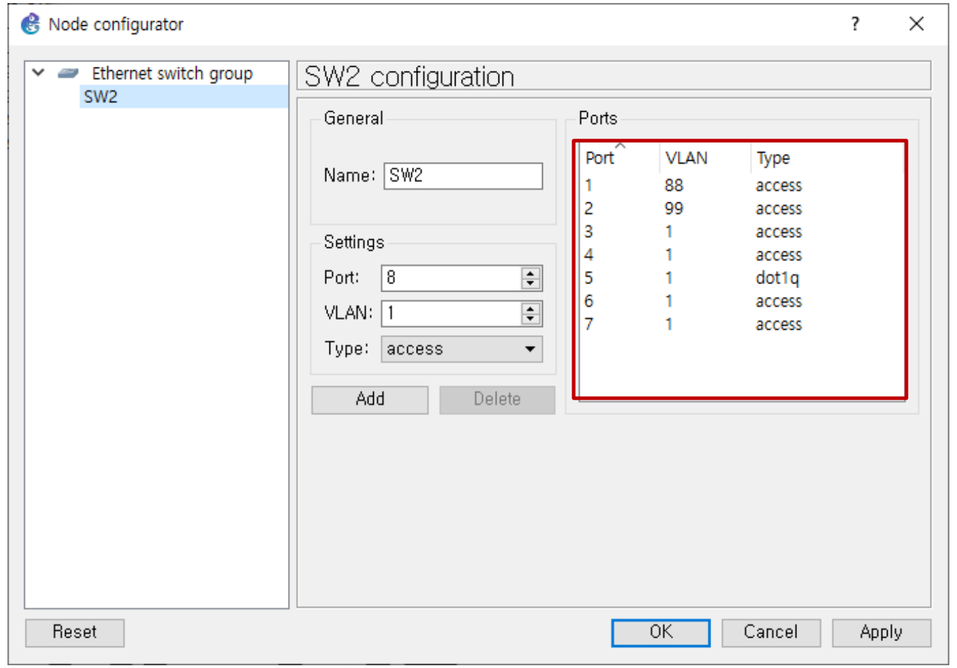
```
L3_SW3#sh ip ro
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, 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 not set

     43.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O       43.43.4.4/32 [110/2] via 43.43.33.4, 01:43:01, FastEthernet1/10
O E2    43.43.3.3/32 [110/20] via 43.43.33.2, 01:41:09, FastEthernet1/10
O E2    43.43.1.0/24 [110/20] via 43.43.33.2, 01:41:09, FastEthernet1/10
O       43.43.11.0/24 [110/11] via 43.43.33.4, 01:43:01, FastEthernet1/10
C       43.43.33.0/24 is directly connected, FastEthernet1/10
O E2    43.43.55.0/24 [110/20] via 43.43.33.2, 01:41:09, FastEthernet1/10
O E2    43.43.66.0/24 [110/20] via 43.43.33.2, 01:41:11, FastEthernet1/10
O E2    43.43.77.0/24 [110/20] via 43.43.33.2, 01:41:11, FastEthernet1/10
     10.0.0.0/24 is subnetted, 2 subnets
O E2    10.8.8.0 [110/20] via 43.43.33.2, 01:41:11, FastEthernet1/10
O E2    10.8.9.0 [110/20] via 43.43.33.2, 01:41:11, FastEthernet1/10
     150.2.0.0/24 is subnetted, 1 subnets
O E2    150.2.43.0 [110/20] via 43.43.33.2, 01:41:12, FastEthernet1/10
```

02 스위치 설정

2-4. SW4

```
vlan 88
vlan 99
!
5번 포트
switchport trunk encapsulation dot1q
switchport mode trunk
!
1번 포트
switchport mode access
switchport access vlan 88
!
2번 포트
switchport mode access
switchport access vlan 99
```

→



03. 라우터 설정

03 라우터 설정

3-1. R1

```
R1(config)#int lo0
R1(config-if)#ip add 43.43.1.1 255.255.255.0

R1(config-if)#int f0/0
R1(config-if)#no sh
R1(config-if)#ip add 43.43.77.2 255.255.255.0

R1(config-if)#int s0/0
R1(config-if)#no sh
R1(config-if)#ip add 43.43.66.1 255.255.255.0

R1(config-if)#router ei 43
R1(config-router)#no auto
R1(config-router)#net 43.43.1.1 0.0.0.0
R1(config-router)#net 43.43.77.2 0.0.0.0
R1(config-router)#redi os 1 met 1 1 1 1 1

R1(config-router)#router os 1
R1(config-router)#net 43.43.66.1 0.0.0.0 a 0
R1(config-router)#default-inf ori al
R1(config-router)#redi ei 43 sub
```

→

```
R1#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 not set

     43.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
D EX    43.43.4.4/32
           [170/2560025856] via 43.43.77.1, 01:42:07, FastEthernet0/0
O       43.43.3.3/32 [110/129] via 43.43.66.2, 01:43:26, Serial0/0
C       43.43.1.0/24 is directly connected, Loopback0
D EX    43.43.11.0/24
           [170/2560025856] via 43.43.77.1, 01:42:07, FastEthernet0/0
D EX    43.43.33.0/24
           [170/2560025856] via 43.43.77.1, 01:42:18, FastEthernet0/0
O       43.43.55.0/24 [110/128] via 43.43.66.2, 01:43:27, Serial0/0
C       43.43.66.0/24 is directly connected, Serial0/0
C       43.43.77.0/24 is directly connected, FastEthernet0/0
     10.0.0.0/24 is subnetted, 2 subnets
O E2    10.8.8.0 [110/20] via 43.43.66.2, 01:43:28, Serial0/0
O E2    10.8.9.0 [110/20] via 43.43.66.2, 01:43:28, Serial0/0
     150.2.0.0/24 is subnetted, 1 subnets
O E2    150.2.43.0 [110/20] via 43.43.66.2, 01:43:28, Serial0/0
```

03 라우터 설정

3-2. R2

```
R2(config)#int lo0
R2(config-if)#ip add 10.8.2.2 255.255.255.0


R2(config-if)#int f0/0
R2(config-if)#no sh
R2(config-if)#ip add 10.8.9.1 255.255.255.0


R2(config-if)#ip route 0.0.0.0 0.0.0.0 10.8.9.2
```

→

```
R2#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 10.8.9.2 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 2 subnets
C       10.8.2.0 is directly connected, Loopback0
C       10.8.9.0 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.8.9.2
```

03 라우터 설정

3-3. R3

```
R3(config)#int lo0
R3(config-if)#ip add 43.43.3.3 255.255.255.0

R3(config-if)#int s0/1
R3(config-if)#no sh
R3(config-if)#ip add 43.43.55.1 255.255.255.0

R3(config-if)#int f0/1
R3(config-if)#no sh
R3(config-if)#ip add 150.2.43.1 255.255.255.0

R3(config-if)#router os 1
R3(config-router)#net 43.43.3.3 0.0.0.0 a 0
R3(config-router)#net 43.43.55.1 0.0.0.0 a 0
R3(config-router)#redi ei 254 sub

R3(config-router)#router ei 254
R3(config-router)#no auto
R3(config-router)#net 150.2.43.1 0.0.0.0
R3(config-router)#redi os 1 met 1 1 1 1 1
```

→

```
R3#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 43.43.55.2 to network 0.0.0.0

     43.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O E2    43.43.4.4/32 [110/20] via 43.43.55.2, 01:44:49, Serial0/1
O E2    43.43.1.0/24 [110/20] via 43.43.55.2, 01:46:07, Serial0/1
C       43.43.3.0/24 is directly connected, Loopback0
O E2    43.43.11.0/24 [110/20] via 43.43.55.2, 01:44:49, Serial0/1
O E2    43.43.33.0/24 [110/20] via 43.43.55.2, 01:44:51, Serial0/1
C       43.43.55.0/24 is directly connected, Serial0/1
O       43.43.66.0/24 [110/128] via 43.43.55.2, 01:46:19, Serial0/1
O E2    43.43.77.0/24 [110/20] via 43.43.55.2, 01:46:09, Serial0/1
     10.0.0.0/24 is subnetted, 2 subnets
O E2    10.8.8.0 [110/20] via 43.43.55.2, 01:46:19, Serial0/1
O E2    10.8.9.0 [110/20] via 43.43.55.2, 01:46:19, Serial0/1
     150.2.0.0/24 is subnetted, 1 subnets
C       150.2.43.0 is directly connected, FastEthernet0/1
O*E2 0.0.0.0/0 [110/1] via 43.43.55.2, 01:46:11, Serial0/1
```

03 라우터 설정

3-4. R4

```
R4(config)#int lo0
R4(config-if)#ip add 43.43.4.4 255.255.255.0


R4(config-if)#int f0/0
R4(config-if)#no sh
R4(config-if)#ip add 43.43.33.4 255.255.255.0


R4(config-if)#int f0/1
R4(config-if)#no sh
R4(config-if)#ip add 43.43.11.1 255.255.255.0


R4(config-if)#router os 1
R4(config-router)#net 43.43.4.4 0.0.0.0 a 0
R4(config-router)#net 43.43.33.4 0.0.0.0 a 0
R4(config-router)#net 43.43.11.1 0.0.0.0 a 0
```

→

```
R4#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 not set

     43.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O E2    43.43.3.3/32 [110/20] via 43.43.33.2, 01:45:45, FastEthernet0/0
O E2    43.43.1.0/24 [110/20] via 43.43.33.2, 01:45:45, FastEthernet0/0
C       43.43.4.0/24 is directly connected, Loopback0
C       43.43.11.0/24 is directly connected, FastEthernet0/1
C       43.43.33.0/24 is directly connected, FastEthernet0/0
O E2    43.43.55.0/24 [110/20] via 43.43.33.2, 01:45:45, FastEthernet0/0
O E2    43.43.66.0/24 [110/20] via 43.43.33.2, 01:45:45, FastEthernet0/0
O E2    43.43.77.0/24 [110/20] via 43.43.33.2, 01:45:47, FastEthernet0/0
     10.0.0.0/24 is subnetted, 2 subnets
O E2    10.8.8.0 [110/20] via 43.43.33.2, 01:45:47, FastEthernet0/0
O E2    10.8.9.0 [110/20] via 43.43.33.2, 01:45:47, FastEthernet0/0
     150.2.0.0/24 is subnetted, 1 subnets
O E2    150.2.43.0 [110/20] via 43.43.33.2, 01:45:48, FastEthernet0/0
```

03 라우터 설정

3-5. R5

```
R5(config)#int lo0
R5(config-if)#ip add 43.43.5.5 255.255.255.0

R5(config-if)#int f0/0
R5(config-if)#no  sh

R5(config-if)#int f0/0.99
R5(config-subif)#en dot 99
R5(config-subif)#ip add 43.43.99.1 255.255.255.0

R5(config-subif)#int f0/0.88
R5(config-subif)#en dot 88
R5(config-subif)#ip add 43.43.88.1 255.255.255.0

R5(config-subif)#int s0/0
R5(config-if)#no sh
R5(config-if)#ip add 43.43.66.2 255.255.255.0

R5(config-if)#int s0/1
R5(config-if)#no sh
R5(config-if)#ip add 43.43.55.2 255.255.255.0

R5(config-if)#router os 1
R5(config-router)#net 43.43.55.2 0.0.0.0 a 0
R5(config-router)#net 43.43.66.2 0.0.0.0 a 0

R5(config)#ip route 10.8.8.0 255.255.255.0 43.43.88.2
R5(config)#ip route 10.8.9.0 255.255.255.0 43.43.99.2
```

→

```
R5#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 43.43.66.1 to network 0.0.0.0

     43.0.0.0/8 is variably subnetted, 11 subnets, 2 masks
O E2    43.43.4.4/32 [110/20] via 43.43.66.1, 01:46:50, Serial0/0
O       43.43.3.3/32 [110/65] via 43.43.55.1, 01:48:15, Serial0/1
O E2    43.43.1.0/24 [110/20] via 43.43.66.1, 01:48:05, Serial0/0
C       43.43.5.0/24 is directly connected, Loopback0
O E2    43.43.11.0/24 [110/20] via 43.43.66.1, 01:46:50, Serial0/0
O E2    43.43.33.0/24 [110/20] via 43.43.66.1, 01:46:51, Serial0/0
C       43.43.55.0/24 is directly connected, Serial0/1
C       43.43.66.0/24 is directly connected, Serial0/0
O E2    43.43.77.0/24 [110/20] via 43.43.66.1, 01:48:07, Serial0/0
C       43.43.88.0/24 is directly connected, FastEthernet0/0.88
C       43.43.99.0/24 is directly connected, FastEthernet0/0.99
     10.0.0.0/24 is subnetted, 2 subnets
S       10.8.8.0 [1/0] via 43.43.88.2
S       10.8.9.0 [1/0] via 43.43.99.2
     150.2.0.0/24 is subnetted, 1 subnets
O E2    150.2.43.0 [110/20] via 43.43.55.1, 01:48:17, Serial0/1
O*E2 0.0.0.0/0 [110/1] via 43.43.66.1, 01:48:07, Serial0/0
```

03 라우터 설정

3-6. R6

```
R6(config)#int f0/1
R6(config-if)#no sh
R6(config-if)#ip add 150.2.43.254 255.255.255.0

R6(config-if)#router ei 254
R6(config-router)#no auto
R6(config-router)#net 150.2.43.254 0.0.0.0
```

→

```
R6#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 150.2.43.1 to network 0.0.0.0

     43.0.0.0/24 is subnetted, 5 subnets
D EX    43.43.1.0 [170/2560025856] via 150.2.43.1, 00:12:44, FastEthernet0/1
D EX    43.43.3.0 [170/2560025856] via 150.2.43.1, 00:12:48, FastEthernet0/1
D EX    43.43.55.0 [170/2560025856] via 150.2.43.1, 00:12:48, FastEthernet0/1
D EX    43.43.66.0 [170/2560025856] via 150.2.43.1, 00:12:48, FastEthernet0/1
D EX    43.43.77.0 [170/2560025856] via 150.2.43.1, 00:12:44, FastEthernet0/1
     10.0.0.0/24 is sub
*Mar  1 00:27:00.887: %SYS-5-CONFIG_I: Configured from console by consolenetted, 2 subnets
D EX    10.8.8.0 [170/2560025856] via 150.2.43.1, 00:12:50, FastEthernet0/1
D EX    10.8.9.0 [170/2560025856] via 150.2.43.1, 00:12:50, FastEthernet0/1
     150.2.0.0/24 is subnetted, 1 subnets
C       150.2.43.0 is directly connected, FastEthernet0/1
D*EX 0.0.0.0/0 [170/2560025856] via 150.2.43.1, 00:12:46, FastEthernet0/1
```

04. 방화벽 1 설정

04 방화벽 1 설정

4-1. Redundant 설정 → ASA Redundant 구성은 두 개 이상의 ASA 장비를 Active/Standby 또는 Active/Active 형태로 연결하여, 하나의 장비에 장애가 발생했을 때, 자동으로 다른 장비가 역할을 이어받는 구조

```
FW1(config-if)# int redundant 1
FW1(config-if)# member-int g0
FW1(config-if)# member-int g2
FW1(config-if)# nameif inside
FW1(config-if)# ip add 43.43.33.2 255.255.255.0
```

→

```
FW1(config)# show int re 1
Interface Redundant1 "inside", is up, line protocol is up
  Hardware is Linux Ethernet Dev, BW 100 Mbps, DLY 100 usec
        (Full-duplex), (100 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0000.ab1a.df00, MTU 1500
        IP address 43.43.33.2, subnet mask 255.255.255.0
        1090 packets input, 145039 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        481 packets output, 43286 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "inside":
        1090 packets input, 128571 bytes
        481 packets output, 36552 bytes
        165 packets dropped
      1 minute input rate 0 pkts/sec,  37 bytes/sec
      1 minute output rate 0 pkts/sec,  12 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  30 bytes/sec
      5 minute output rate 0 pkts/sec,  7 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Redundancy Information:
        Member GigabitEthernet0(Active), GigabitEthernet2
        Last switchover at 03:36:26 UTC Jul 16 2025
```

04 방화벽 1 설정

4-2. 인터페이스 설정

```
FW1(config)# int g0
FW1(config-if)# no sh

FW1(config-if)# int g1
FW1(config-if)# no sh

FW1(config-if)# int g2
FW1(config-if)# no sh

 FW1(config-if)# int g1
 FW1(config-if)# nameif outside
 FW1(config-if)# ip add 43.43.77.1 255.255.255.0
```

→

```
FW1(config)# show int ip br
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0           unassigned      YES unset  up                    up
GigabitEthernet1           43.43.77.1      YES manual up                    up
GigabitEthernet2           unassigned      YES unset  up                    up
Redundant1                 43.43.33.2      YES manual up                    up
```

04 방화벽 1 설정

4-3. 라우팅

```
FW1(config-if)# router os 1
FW1(config-router)# net 43.43.33.2 255.255.255.255 a 0
FW1(config-router)# redi ei 43 sub

FW1(config-router)# router ei 43
FW1(config-router)# no auto
FW1(config-router)# net 43.43.77.1 255.255.255.255
FW1(config-router)# redi os 1 met 1 1 1 1 1
```

→

```
FW1(config)# show route

Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, 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 not set

O    43.43.4.4 255.255.255.255 [110/11] via 43.43.33.4, 1:09:46, inside
D EX 43.43.3.3 255.255.255.255
           [170/2560002816] via 43.43.77.2, 1:09:57, outside
D    43.43.1.0 255.255.255.0 [90/156160] via 43.43.77.2, 1:09:57, outside
O    43.43.11.0 255.255.255.0 [110/20] via 43.43.33.4, 1:09:46, inside
C    43.43.33.0 255.255.255.0 is directly connected, inside
D EX 43.43.55.0 255.255.255.0
           [170/2560002816] via 43.43.77.2, 1:09:57, outside
D EX 43.43.66.0 255.255.255.0
           [170/2560002816] via 43.43.77.2, 1:09:57, outside
C    43.43.77.0 255.255.255.0 is directly connected, outside
D EX 10.8.8.0 255.255.255.0 [170/2560002816] via 43.43.77.2, 1:09:57, outside
D EX 10.8.9.0 255.255.255.0 [170/2560002816] via 43.43.77.2, 1:09:57, outside
D EX 150.2.43.0 255.255.255.0
           [170/2560002816] via 43.43.77.2, 1:09:57, outside
```

04 방화벽 1 설정

4-4. MPF

```
FW1(config-pmap-c)# class-map inspection_default
FW1(config-cmap)# match default-inspection-traffic
```

→ 클래스 맵 설정 (트래픽 분류)

```
FW1(config-cmap)# policy-map global_policy
FW1(config-pmap)# class inspection_default
```

→ 폴리시 맵 설정 (보안 정책 설정)

```
FW1(config-pmap-c)# service-policy global_policy global
```

→ 폴리시 맵 적용

```
FW1(config)# policy-map global_policy
FW1(config-pmap)# class inspection_default
FW1(config-pmap-c)# inspect icmp
```

→

```
FW1(config)# sh run policy-map
!
policy-map global_policy
 class inspection_default
  inspect icmp
!
```

```
FW1(config)# show service-policy

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: icmp, packet 0, drop 0, reset-drop 0
```

05. 방화벽 2 설정

05 방화벽 2 설정

5-1. Active Key 설정 → 방화벽 이중화 구성에서 어떤 장비가 Active(주 장비) 역할을 수행할지 결정하는 식별자나 인증 키

```
FW2(config)# show mode
Security context mode: single

FW2(config)# activation-key 0x4a3ec071 0x0d86fbf6 0x7cb1bc48 0x8b48b8b0 0xf317$
```

Active Key 입력 후, reload (재부팅)

```
FW2(config)# mode multiple


FW2(config)# show mode
Security context mode: multiple
```

05 방화벽 2 설정

5-2. 인터페이스 및 Context 생성

```
FW2(config)# int g0
FW2(config-if)# no sh

FW2(config-if)# int g1
FW2(config-if)# no sh

FW2(config-if)# int g2
FW2(config-if)# no sh

FW2(config-if)# int g3
FW2(config-if)# no sh
```

```
FW2(config)# admin-context admin
FW2(config)# context admin
FW2(config-ctx)# config-url admin.cfg

FW2(config-ctx)# context C1
Creating context 'C1'... Done. (2)
FW2(config-ctx)# config-url C1.cfg

FW2(config-ctx)# allocate-int g0 outside
FW2(config-ctx)# allocate-int g1 inside
FW2(config-ctx)# context C2
Creating context 'C2'... Done. (3)
FW2(config-ctx)# config-url C2.cfg

FW2(config-ctx)# allocate-int g2 outside
FW2(config-ctx)# allocate-int g3 inside
```

→

```
FW2(config)# sh context
Context Name       Class        Interfaces              URL
*admin             default                              disk0:/admin.cfg
 C1                default      GigabitEthernet0,       disk0:/C1.cfg
                                GigabitEthernet1
 C2                default      GigabitEthernet2,       disk0:/C2.cfg
                                GigabitEthernet3

Total active Security Contexts: 3
```

05 방화벽 2 설정

5-3. Context 설정

```
FW2(config-ctx)# changeto context C1
FW2/C1(config)# int outside
FW2/C1(config-if)# nameif outside
FW2/C1(config-if)# ip add 43.43.88.2 255.255.255.0
```

```
FW2/C1(config-if)# int inside
FW2/C1(config-if)# nameif inside
FW2/C1(config-if)# ip add 10.8.8.2 255.255.255.0
```

→

```
FW2/C1(config)# sh run int inside
!
interface inside
 nameif inside
 security-level 100
 ip address 10.8.8.2 255.255.255.0
```

```
FW2/C1(config)# sh run int outside
!
interface outside
 nameif outside
 security-level 0
 ip address 43.43.88.2 255.255.255.0
```

05 방화벽 2 설정

5-4. Context 설정

```
FW2(config)# changeto context C2
FW2/C2(config)# int outside
FW2/C2(config-if)# nameif outside
FW2/C2(config-if)# ip add 43.43.99.2 255.255.255.0
```

```
FW2/C2(config-if)# int inside
FW2/C2(config-if)# nameif inside
FW2/C2(config-if)# ip add 10.8.9.2 255.255.255.0
```

→

```
FW2/C2(config-if)# sh run int inside
!
interface inside
 nameif inside
 security-level 100
 ip address 10.8.9.2 255.255.255.0
```

```
FW2/C2(config-if)# sh run int outside
!
interface outside
 nameif outside
 security-level 0
 ip address 43.43.99.2 255.255.255.0
```

05 방화벽 2 설정

5-5. ACL ⟶ Context C1, C2 외부에서 내부로 ICMP 패킷 허용

```
FW2/C1(config)# access-l acl_oi per icmp a a
FW2/C1(config)# access-g acl_oi in int outside
```

⟶

```
FW2/C1(config)# show run access-list
access-list acl_oi extended permit icmp any any
```

```
FW2/C2(config)# access-l acl_oi per icmp a a
FW2/C2(config)# access-g acl_oi in int outside
```

⟶

```
FW2/C2(config)# show run access-list
access-list acl_oi extended permit icmp any any
```

05 방화벽 2 설정

5-6. 라우팅

```
FW2/C1(config)# route outside 0 0 43.43.88.1
FW2/C1(config)# route inside 10.8.7.0 255.255.255.0 10.8.8.1
```

↓

```
FW2/C1(config)# show route

Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, 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 43.43.88.1 to network 0.0.0.0

C    43.43.88.0 255.255.255.0 is directly connected, outside
S    10.8.7.0 255.255.255.0 [1/0] via 10.8.8.1, inside
C    10.8.8.0 255.255.255.0 is directly connected, inside
S*   0.0.0.0 0.0.0.0 [1/0] via 43.43.88.1, outside
```

```
FW2/C2(config)# route outside 0 0 43.43.99.1
FW2/C2(config)# route inside 10.8.2.0 255.255.255.0 10.8.9.1
```

↓

```
FW2/C2(config)# show route

Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, 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 43.43.99.1 to network 0.0.0.0

C    43.43.99.0 255.255.255.0 is directly connected, outside
S    10.8.2.0 255.255.255.0 [1/0] via 10.8.9.1, inside
C    10.8.9.0 255.255.255.0 is directly connected, inside
S*   0.0.0.0 0.0.0.0 [1/0] via 43.43.99.1, outside
```

05 방화벽 2 설정

5-7. Object NAT → Static Object NAT - 내부 사설 주소와 외부 공인 IP 주소를 1:1로 고정 매핑하는 방식
Dynamic Object NAT - 동적 주소 변환 방식으로, 내부 사설 IP 주소를 외부 공인 IP 주소로 자동 매핑하는 방식

```
FW2/C1(config)# object network inside_Server
FW2/C1(config-network-object)# host 10.8.8.1
FW2/C1(config-network-object)# nat (inside,outside) static 43.43.88.3
```

→

```
FW2/C1(config-network-object)# show nat

Auto NAT Policies (Section 2)
1 (inside) to (outside) source static inside_Server 43.43.88.3
    translate_hits = 0, untranslate_hits = 0
```

```
FW2/C2(config)# object network inside_NAT
FW2/C2(config-network-object)# subnet 10.8.0.0 255.255.0.0
FW2/C2(config-network-object)# nat (inside,outside) dynamic int
```

→

```
FW2/C2(config)# show nat

Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic inside_NAT interface
    translate_hits = 0, untranslate_hits = 0
```

감사합니다

Rest | 강승환 고동우 유세종 최성민 한시완