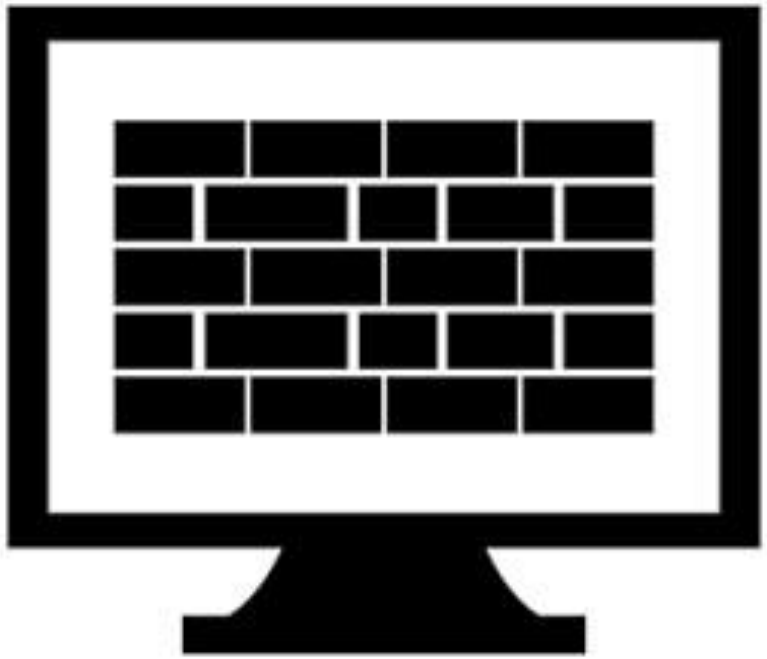
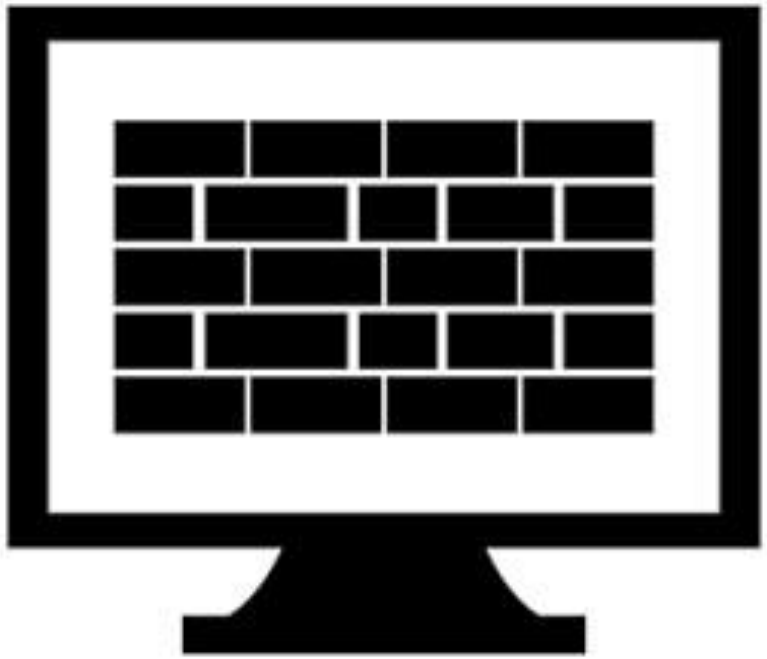
Firewall Project

Front Team
정세환 김선혁
임영철 박채령

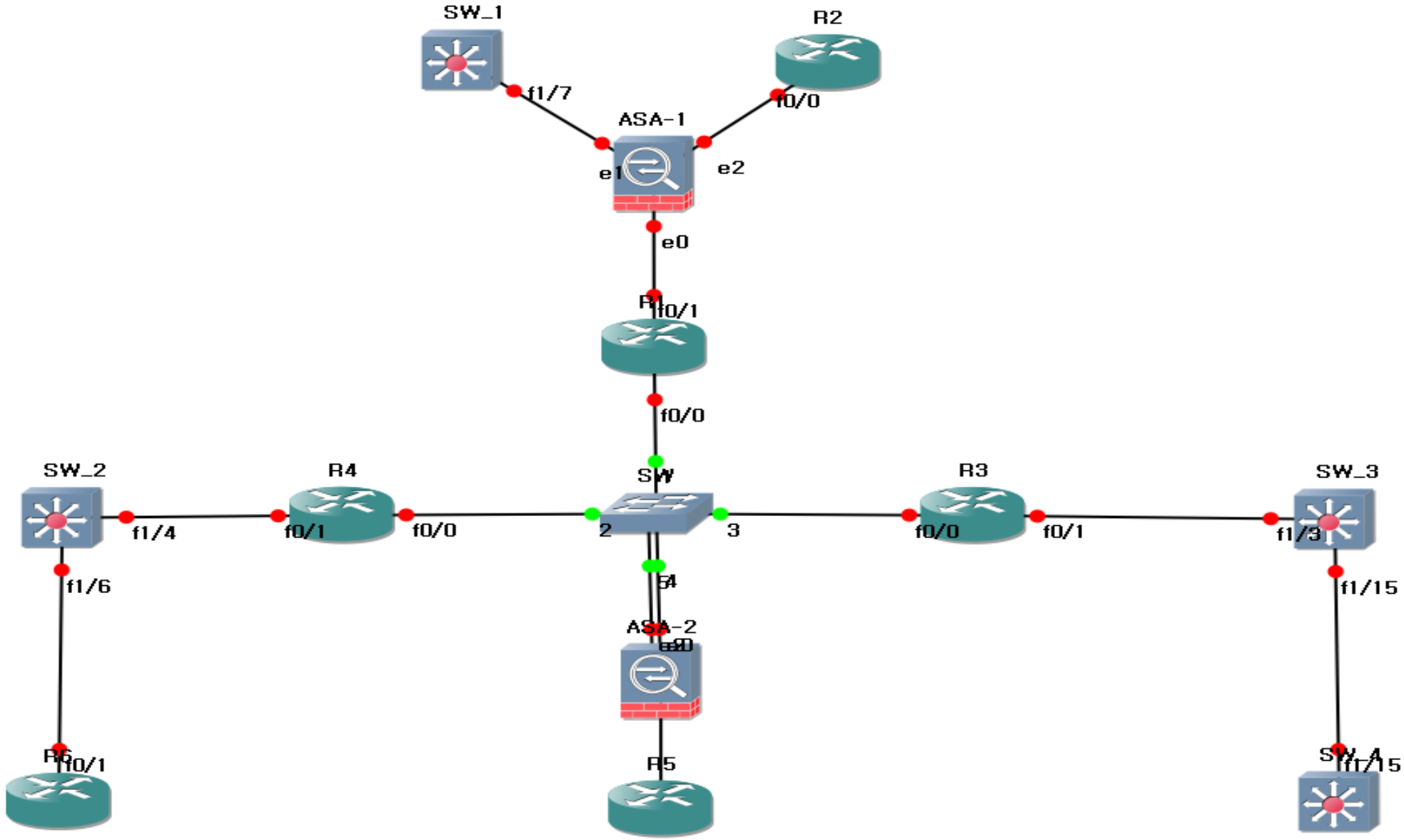
INDEX



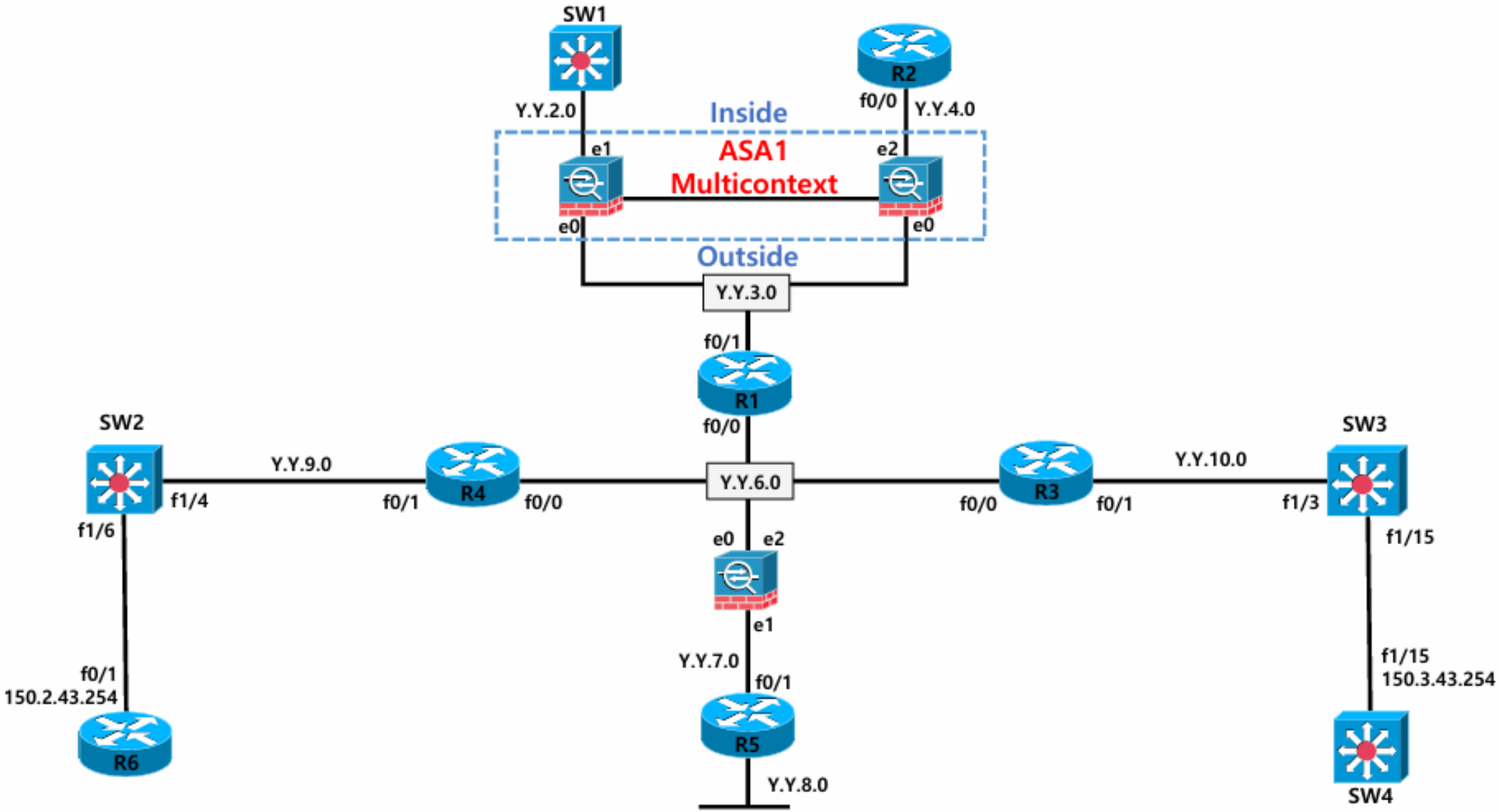


1. 방화벽 구성도

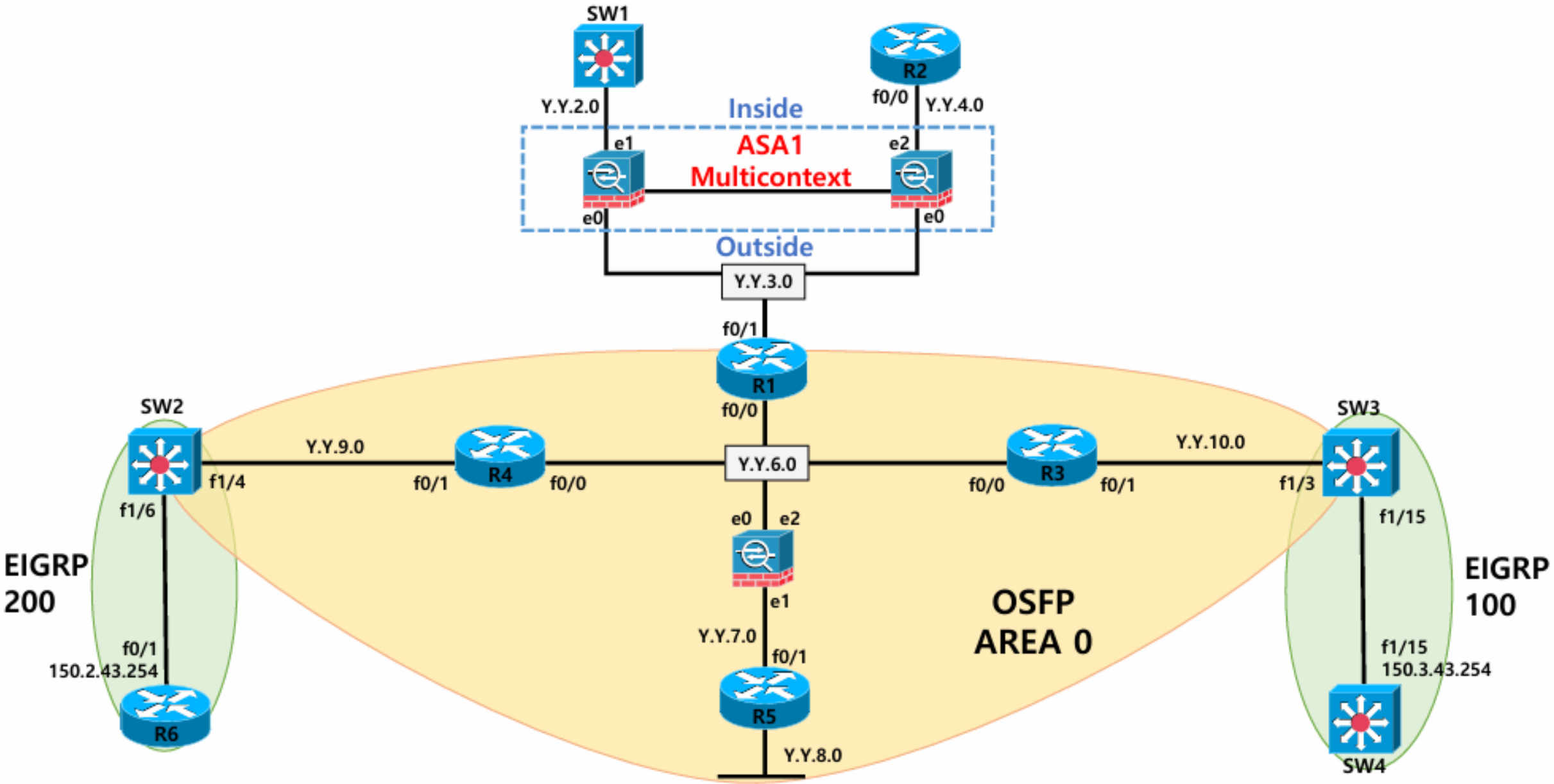
1-1. 물리적 구성


SW_1
R2
f1/7
f0/0
ASA-1
e1
e2
e0
R1
f0/1
f0/0
SW_2
R4
SW
R3
SW_3
f1/4
f0/1
f0/0
2
3
f0/0
f0/1
f1/3
f1/6
f1/15
ASA-2
R6
f0/1
R5
SW_4
f1/15

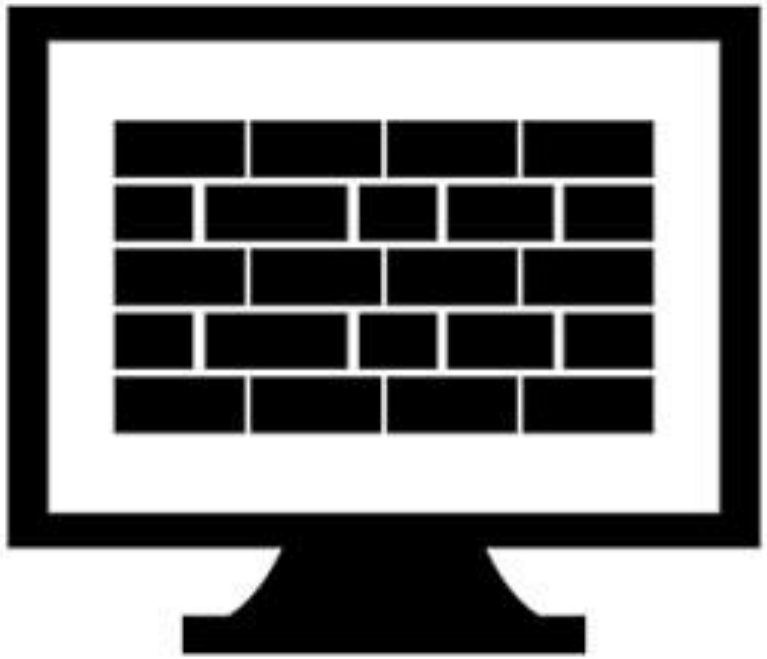
1-2. 논리적 구성


SW1
R2
Y.Y.2.0
Inside
f0/0
Y.Y.4.0
e1
ASA1
e2
Multicontext
e0
e0
Outside
Y.Y.3.0
f0/1
R1
f0/0
SW2
SW3
Y.Y.9.0
Y.Y.10.0
f1/4
f0/1
R4
f0/0
Y.Y.6.0
f0/0
R3
f0/1
f1/3
f1/6
e0
e2
f1/15
e1
f0/1
150.2.43.254
Y.Y.7.0
f0/1
f1/15
150.3.43.254
R6
R5
Y.Y.8.0
SW4

1-3. IGP 구성


SW1
R2
Y.Y.2.0
Inside
f0/0
Y.Y.4.0
e1
ASA1
e2
Multicontext
e0
e0
Outside
Y.Y.3.0
f0/1
R1
f0/0
SW2
SW3
Y.Y.9.0
R4
Y.Y.6.0
R3
Y.Y.10.0
f1/4
f0/1
f0/0
f0/0
f0/1
f1/3
f1/6
f1/15
e0
e2
EIGRP
200
e1
OSFP
AREA 0
EIGRP
100
Y.Y.7.0
f0/1
f1/15
f0/1
150.2.43.254
150.3.43.254
R5
R6
Y.Y.8.0
SW4

2. 장비 설정



2-1. Router Setting

Interface Setting

R1

```
int lo0
ip add 192.168.1.1 255.255.255.255

int lo2
ip add 43.43.51.1 255.255.255.255

int f0/0
no sh
ip add 43.43.6.1 255.255.255.0

int f0/1
no sh
ip add 43.43.3.1 255.255.255.0
```

R2

```
int lo0
ip add 192.168.2.2 255.255.255.255

int lo1
ip add 192.168.22.22 255.255.255.255

int f0/0
no sh
ip add 43.43.4.2 255.255.255.0
```

Interface Setting

R3

```
int lo0
ip add 192.168.3.3 255.255.255.255

int lo1
ip add 192.168.33.3 255.255.255.255

int f0/0
no sh
ip add 43.43.6.3 255.255.255.0

int f0/1
no sh
ip add 43.43.10.3 255.255.255.0
```

R4

```
int lo0
ip add 192.168.4.4 255.255.255.255

int f0/0
no sh
ip add 43.43.6.4 255.255.255.0

int f0/1
no sh
ip add 43.43.9.4 255.255.255.0
```

Interface Setting

R5

```
int lo0
ip add 192.168.5.5 255.255.255.255

int lo2
ip add 43.43.52.5 255.255.255.255

int f0/1
no sh
ip add 43.43.7.5 255.255.255.0

int f0/0
no sh
ip add 43.43.8.5 255.255.255.0
```

R6

```
int lo0
ip add 192.168.6.6 255.255.255.255

int f0/1
no sh
ip add 150.2.43.254 255.255.255.0
```

Routing

R1 Routing

```
ip route 0.0.0.0 0.0.0.0 43.43.3.10
ip route 43.43.4.0 255.255.255.0 43.43.3.12

router os 1
router-id 1.1.1.1
net 43.43.51.1 0.0.0.0 a 0
net 43.43.6.1 0.0.0.0 a 0
default-inf ori alway
```

R2 Routing

```
ip route 0.0.0.0 0.0.0.0 43.43.4.12
```

R3 Routing

```
router os 1
router-id 3.3.3.3
net 43.43.6.3 0.0.0.0 a 0
net 43.43.10.3 0.0.0.0 a 0
```

R4 Routing

```
router os 1
router-id 4.4.4.4
net 43.43.9.4 0.0.0.0 a 0
net 43.43.6.4 0.0.0.0 a 0
```

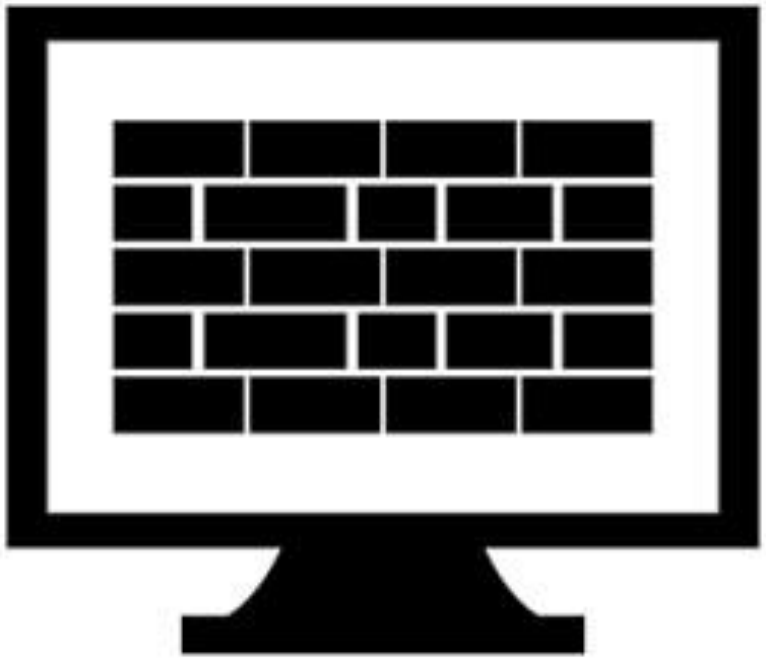
Routing

R5 Routing

```
router os 1
router-id 5.5.5.5
net 43.43.7.5 0.0.0.0 a 0
net 43.43.8.5 0.0.0.0 a 0
net 43.43.52.5 0.0.0.0 a 0
```

R6 Routing

```
router ei 200
no au
net 150.2.43.254 0.0.0.0
```



2-2. Switch Setting

Switch

SW1

```
int lo150
ip add 150.1.43.1 255.255.255.0

int f1/7
no sw
ip add 43.43.2.1 255.255.255.0

ip route 43.43.0.0 255.255.0.0 43.43.2.10
```

SW2

```
int f1/4
no sw
ip add 43.43.9.1 255.255.255.0

int f1/6
no sw
ip add 150.2.43.1 255.255.255.0

router os 1
net 43.43.9.1 0.0.0.0 ar 0
redi ei 200 sub

router ei 200
no au
net 150.2.43.1 0.0.0.0
redi os 1 met 1 1 1 1 1
```

Switch

SW3

```
int f1/3
no sw
ip add 43.43.10.1 255.255.255.0

int f1/15
no sw
ip add 150.3.43.1 255.255.255.0

router os 1
net 43.43.10.1 0.0.0.0 ar 0
redi ei 100 sub

router ei 100
no au
net 150.3.43.1 0.0.0.0
redi os 1 met 1 1 1 1 1
```

SW4

```
int f1/15
no sw
ip add 150.3.43.254 255.255.255.0

router ei 100
no au
net 150.3.43.254 0.0.0.0
```

2-3. Firewall Setting

ASA1

```
int g0
no sh

int g1
no sh

int g2
no sh

admin-context admin
context admon
config-u admin.cfg
```

Context 생성

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

context c2
config-u c2.cfg

allocate-int g0
allocate-int g2

mac-address auto
```

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

ASA1 (Context)

ASA1(Context c1)

nameif inside
ip add 43.43.2.10 255.255.255.0

int g0
nameif outside
ip add 43.43.3.10 255.255.255.0

route outside 0 0 43.43.3.1
route inside 150.1.0.0 255.255.0.0 43.43.2.1

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

```
FW1/c1# 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
```

ASA1(Context c2)

int g2
nameif inside
ip add 43.43.4.12 255.255.255.0

int g0
nameif outside
ip add 43.43.3.12 255.255.255.0

route outside 0 0 43.43.3.1
route inside 192.168.2.0 255.255.255.0
43.43.4.2
access-l acl_oi per icmp a a
access-g acl_oi in int outside

```
FW1/c2(config)# sh access-li
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
```

ASA2

int g0
no sh

int g1
no sh

int g2
no sh

ICMP 허용
access-l acl_oi per icmp a a
access-g acl_oi in int outside

라우팅
router os 1
net 43.43.6.0 255.255.255.0 a 0
net 43.43.7.0 255.255.255.0 a 0

ASA2 Redundant 기술

int re1
member-int g0
member-int g2
nameif outside
ip add 43.43.6.10 255.255.255.0

int g1
nameif inside
ip add 43.43.7.10 255.255.255.0

redundant-int re1 active-mem g0

```
FW2(config)# sh int ip b
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0           unassigned      YES unset  up                    up
GigabitEthernet1           43.43.7.10      YES manual up                    up
GigabitEthernet2           unassigned      YES unset  up                    up
GigabitEthernet3           unassigned      YES unset  administratively down up
Redundant1                 43.43.6.10      YES manual up                    up
```

2-4. Firewall (NAT)

Firewall(NAT)

정적 PAT 설정

```
! 43.43.51.1 → 43.43.52.5로 TCP 포트 23을 매핑
access-l acl_oi per tcp ho 43.43.51.1 ho 43.43.52.5 eq 23
! 43.43.6.1 → 43.43.52.5로 TCP 포트 23을 매핑
access-l acl_oi per tcp ho 43.43.6.1 ho 43.43.52.5 eq 23
```

정적 NAT 설정

```
! 43.43.51.1 → 43.43.7.30으로 1:1 정적 NAT 변환
access-l acl_nat1 per ip ho 43.43.51.1 ho 43.43.52.5
! 43.43.6.1 → 43.43.7.31으로 1:1 정적 NAT 변환
access-l acl_nat2 per ip ho 43.43.6.1 ho 43.43.52.5
```

정적 NAT 매핑명령

```
! 내부 네트워크의 43.43.51.1 → 외부 네트워크의 43.43.7.30
static (outside,inside) 43.43.7.30 access-l acl_nat1
! 내부 네트워크의 43.43.6.1 → 외부 네트워크의 43.43.7.31
static (outside,inside) 43.43.7.31 access-l acl_nat2
```

정적 PAT와 NAT 테스트를 위한 패킷 트레이서

```
! 43.43.51.1에서 TCP 포트 1024 → 43.43.52.5의 포트 23로 테스트
packet-tracer input outside tcp 43.43.51.1 1024 43.43.52.5 23
! 43.43.6.1에서 TCP 포트 1024 → 43.43.52.5의 포트 23로 테스트
packet-tracer input outside tcp 43.43.6.1 1024 43.43.52.5 23
```

동적 PAT를 위한 ACL 설정

```
! 43.43.8.0/24와 64.102.51.0/24 간의 트래픽에 대해 NAT 허용
access-l acl_st per 43.43.8.0 255.255.255.0 64.102.51.0 255.255.255.0
```

동적 PAT 설정

```
! 43.43.8.0/24의 내부 IP를 외부 IP 43.43.6.30으로 변환
nat (inside) 1 access acl_st
global (outside) 1 43.43.6.30
```

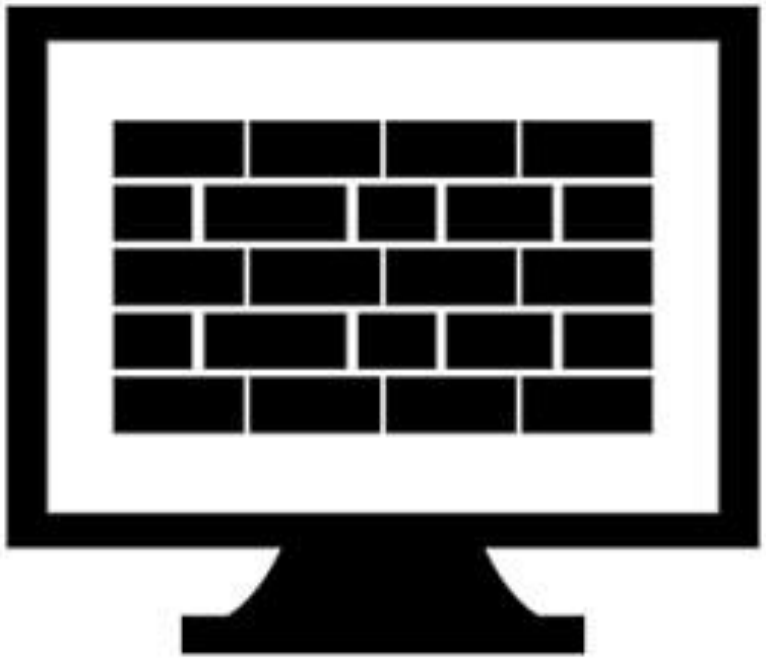
추가적인 동적 PAT 설정

! 내부 네트워크 43.43.8.0/24 → 외부 IP 43.43.6.31로 동적 PAT 매핑
nat (inside) 2 43.43.8.0 255.255.255.0
global (outside) 2 43.43.6.31

동적 PAT 테스트를 위한 패킷 트레이서

! 43.43.8.1에서 ICMP 요청 (Echo Request) → 64.102.51.1로 테스트
packet-tracer input inside icmp 43.43.8.1 8 0 64.102.51.1
! 43.43.8.1에서 ICMP 요청 (Echo Request) → 43.43.4.2로 테스트
packet-tracer input inside icmp 43.43.8.1 8 0 43.43.4.2

```
FW2(config)# sh run access-list
access-list acl_oi extended permit icmp any any
access-list acl_oi extended permit tcp host 43.43.51.1 host 43.43.52.5 eq telnet
access-list acl_oi extended permit tcp host 43.43.6.1 host 43.43.52.5 eq telnet
access-list acl_nat1 extended permit ip host 43.43.51.1 host 43.43.52.5
access-list acl_nat2 extended permit ip host 43.43.6.1 host 43.43.52.5
access-list acl_st extended permit ip 43.43.8.0 255.255.255.0 64.102.51.0 255.255.255.0
```



2-5. Routing Table

Multi Context – Routing Table

FW1_c1

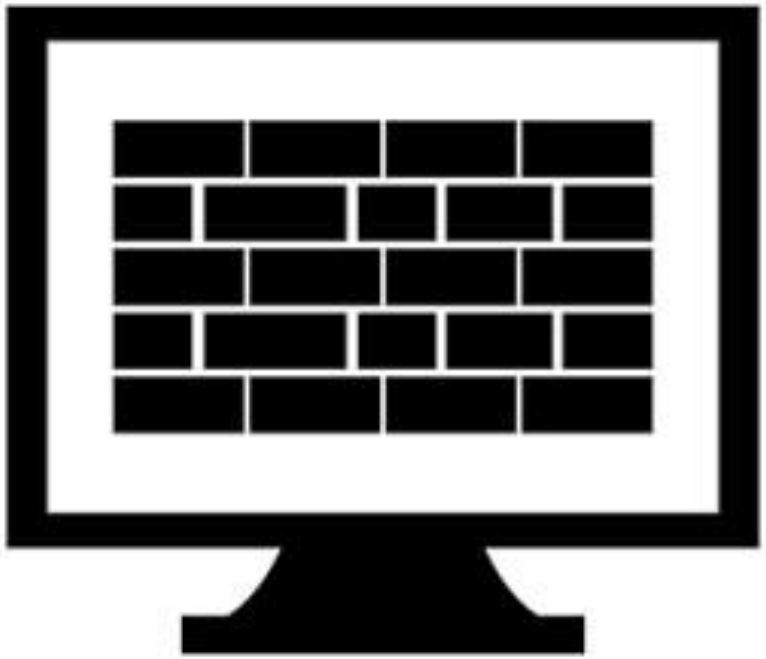
```
FW1/c1(config)# show route

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 43.43.3.1 to network 0.0.0.0

C    43.43.2.0 255.255.255.0 is directly connected, inside
C    43.43.3.0 255.255.255.0 is directly connected, outside
S    150.1.0.0 255.255.0.0 [1/0] via 43.43.2.1, inside
S*   0.0.0.0 0.0.0.0 [1/0] via 43.43.3.1, outside
```

FW1_c2

```
FW1/c2(config)# sh 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 int
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 43.43.3.1 to network 0.0.0.0

C    43.43.3.0 255.255.255.0 is directly connected, outside
C    43.43.4.0 255.255.255.0 is directly connected, inside
S    192.168.2.0 255.255.255.0 [1/0] via 43.43.4.2, inside
S*   0.0.0.0 0.0.0.0 [1/0] via 43.43.3.1, outside
```

FW2 Routing Table

```
SW2#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 not set

     43.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
O       43.43.6.0/24 [110/11] via 43.43.9.4, 00:02:20, FastEthernet1/4
O       43.43.7.0/24 [110/21] via 43.43.9.4, 00:02:20, FastEthernet1/4
O       43.43.8.0/24 [110/31] via 43.43.9.4, 00:02:20, FastEthernet1/4
C       43.43.9.0/24 is directly connected, FastEthernet1/4
O       43.43.10.0/24 [110/21] via 43.43.9.4, 00:02:20, FastEthernet1/4
O       43.43.52.5/32 [110/22] via 43.43.9.4, 00:02:20, FastEthernet1/4
O       43.43.51.1/32 [110/12] via 43.43.9.4, 00:02:22, FastEthernet1/4
     150.2.0.0/24 is subnetted, 1 subnets
C       150.2.43.0 is directly connected, FastEthernet1/6
```



2-6. Ping Test

인접 (FW)

FW1_c1 <-> SW1

```
FW1/c1(config)# pi 43.43.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 43.43.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/26/30 ms
```

FW1_c2 <-> R1

```
FW1/c2(config)# pi 43.43.4.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 43.43.4.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/48/80 ms
```

FW2 <-> R5

```
FW2(config)# pi 43.43.8.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 43.43.8.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/34/70 ms
```

FW2 <-> R1

```
FW2(config)# pi 43.43.6.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 43.43.6.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/38/70 ms
```

FW2 <-> R4

```
FW2(config)# pi 43.43.6.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 43.43.6.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 30/42/70 ms
```

FW2 <-> R3

```
FW2(config)# pi 43.43.6.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 43.43.6.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/30/70 ms
```

인접 (SW)

SW2 <-> R6

```
SW2(config)#do pi 150.2.43.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.2.43.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/29/32 ms
```

SW2 <-> R4

```
SW2(config)#do pi 43.43.6.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 43.43.6.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/35/52 ms
```

SW3 <-> SW4

```
SW3(config)#do pi 150.3.43.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.3.43.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/28/44 ms
```

SW3 <-> R3

```
SW3(config)#do pi 43.43.6.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 43.43.6.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/28/32 ms
```

인접 (Router)

R1 <-> R3,4

```
R1#pi 43.43.6.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 43.43.6.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/34/56 ms
R1#pi 43.43.6.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 43.43.6.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/33/40 ms
```

R3 <-> R1,4

```
R3#pi 43.43.6.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 43.43.6.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/34/48 ms
R3#pi 43.43.6.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 43.43.6.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/27/32 ms
```

R4 <-> R1,3

```
R4#pi 43.43.6.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 43.43.6.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/32/44 ms
R4#pi 43.43.6.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 43.43.6.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/36/56 ms
```

원격

SW1 <-> SW3

```
SW1#pi 43.43.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 43.43.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 148/171/232 ms
```

R2 <-> R6

```
R2#pi  150.2.43.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.2.43.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 124/154/192 ms
```

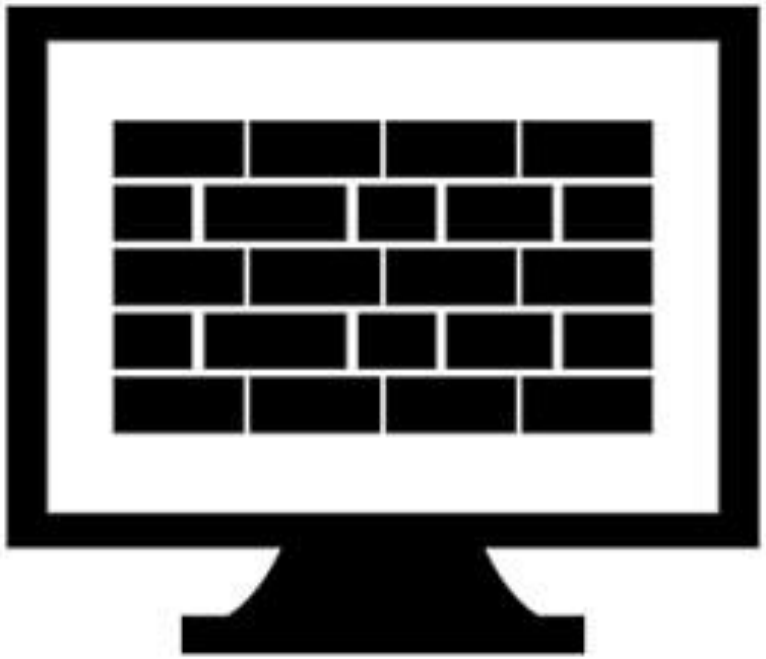
SW1 <-> R5

```
SW1#pi 43.43.52.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 43.43.52.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 188/204/220 ms
```

R2 <-> R5

```
R2#pi 43.43.52.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 43.43.52.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/125/208 ms
```

2. 장비 설정



3. ZBF

ZBF (Zone-Based-Firewall)

Zone 정의

```
zone security internal
zone security external
```

Zone 멤버 지정

```
Interface f0/0
zone-member security internal
Interface f0/1
zone-member security external
```

Class-map 정의

```
class-map type inspect cm_telnet
match protocol telnet

class-map type inspect cm_icmp
match protocol icmp

class-map type inspect cm_http
match protocol http
```

(in | out)bound 정책 정의

```
policy-map type inspect Inbound-policy class type
inspect cm_icmp
inspect
police rate 20000 burst 2000
class type inspect cm_telnet
inspect
class type inspect cm_http
inspect reset log header-length greater 4096

Policy-map type inspect Outbound-policy
Class class-default
inspect
```

Zone-Pair 설정

```
zone-pair security Outbound source internal destination external
service-policy type inspect Outbound-policy

zone-pair security Inbound source external destination internal
service-policy type inspect Inbound-policy
```

ZBF (Zone-Based-Firewall)

sh run class-map

```
R3#sh run class-map
Building configuration...

Current configuration : 200 bytes
!
class-map type inspect match-any cm_icmp
 match protocol icmp
class-map type inspect match-any cm_http
 match protocol http
class-map type inspect match-any cm_telnet
 match protocol telnet
!
end
```

sh run policy-map

```
R3#sh run policy-map
Building configuration...

Current configuration : 288 bytes
!
policy-map type inspect Outbound-policy
 class class-default
  inspect
policy-map type inspect Inbound-policy
 class type inspect cm_icmp
  inspect
  police rate 20000 burst 2000
 class type inspect cm_telnet
  inspect
 class type inspect cm_http
  inspect
 class class-default
!
end
```

ZBF (Zone-Based-Firewall)

sh run | include service-policy

```
R3#sh run | i service-policy
 service-policy type inspect Outbound-policy
 service-policy type inspect Inbound-policy
```

sh run | include member

```
R3#sh run | i member
  zone-member security internal
  zone-member security external
```

show zone security

```
R3#sh zone security
zone self
  Description: System defined zone


zone internal
  Member Interfaces:
    FastEthernet0/0


zone external
  Member Interfaces:
    FastEthernet0/1
```

show zone-pair security

```
R3#sh zone-pair security
Zone-pair name Outbound
    Source-Zone internal  Destination-Zone external
    service-policy Outbound-policy
Zone-pair name Inbound
    Source-Zone external  Destination-Zone internal
    service-policy Inbound-policy
```