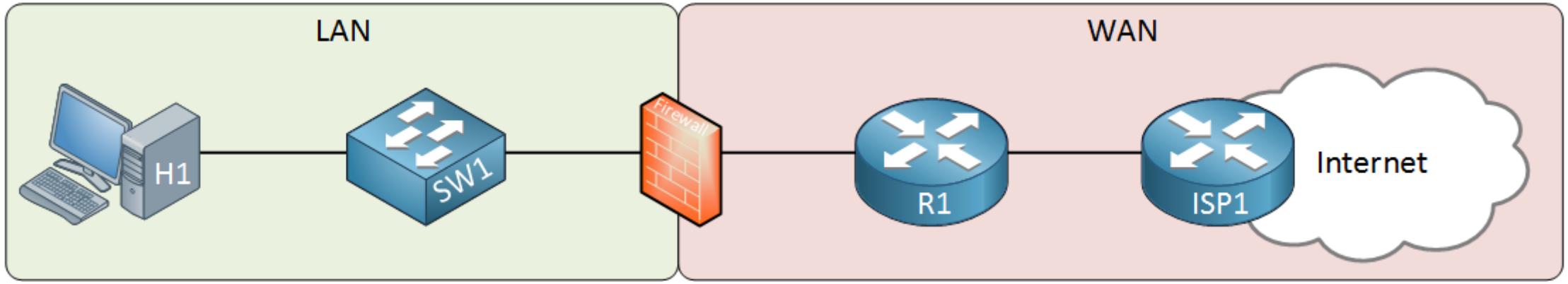
방화벽

- 신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 사이의 장벽
- LAN 과 WAN 사이에 사용
  - 즉. 데이터 전달 경로에 배치되어 패킷을 드롭 / 허용



Stateless Filtering

- 라우터는 ACL을 사용해 Source / Destination / Port number 확인
  - 패킷을 수신하면 ALC 매치 후 Permit 또는 Deny
  - 단일 패킷 또는 수천 개의 패킷을 수신해도 각 패킷을 개별적으로 처리
  - 이전에 본적이 있거나, 본적이 없는 패킷은 추적하지 않음

기록X

Stateful Filtering

- 방화벽은 모든 들어오는 또는 나가는 Connection 추적
  1) LAN 환경의 컴퓨터를 이용해 메일서버 연결
  2) TCP 3-Way handshake 진행 과정을 방화벽은 모니터링
  3) 방화벽은 이 연결을 기억하고 메일서버에 대한 응답을 자동으로 컴퓨터에게 들어오는 것을 허용

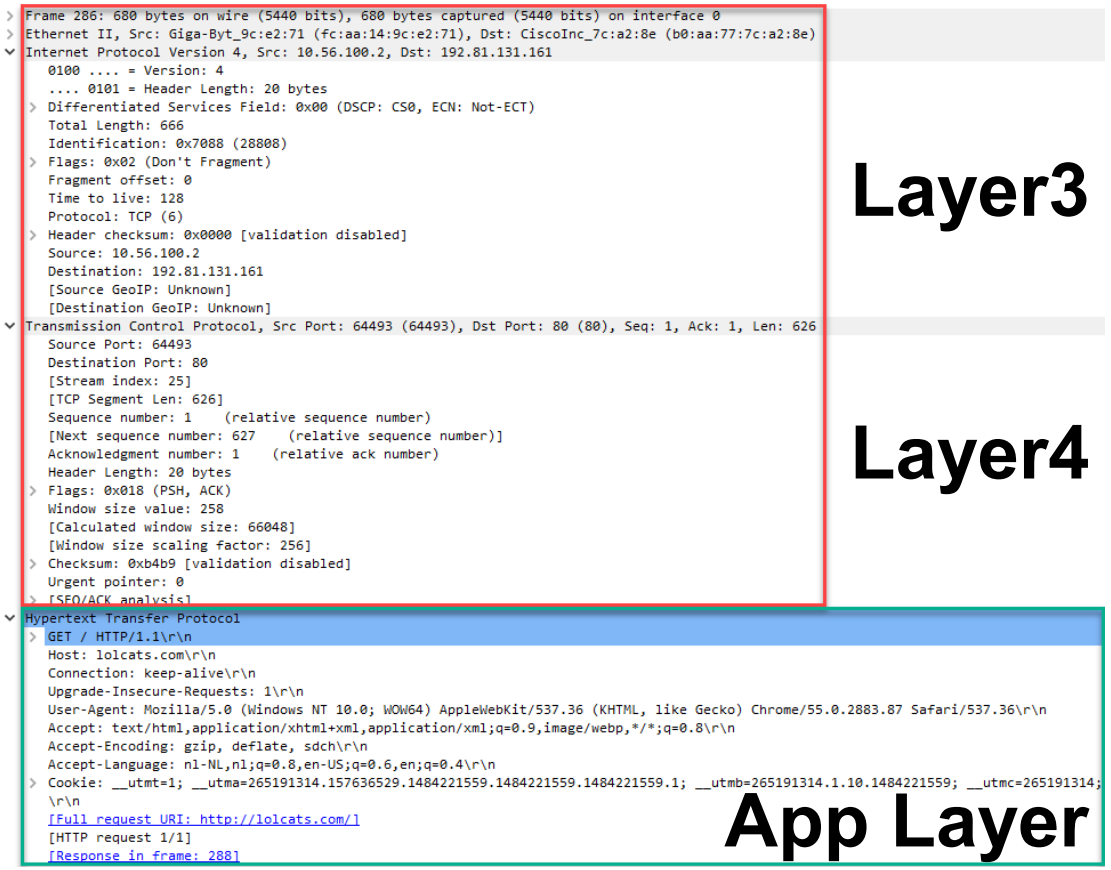
기록O

Packet Inspection

- 대부분의 방화벽은 어떤 형태로든 Deep Packet inspection 지원
  - ACL은 단순히 IP 와 Port number 확인
- Inspection은 OSI model의 Layer7 까지 확인 가능
  - 애플리케이션 헤더 및 실제 데이터 까지 확인

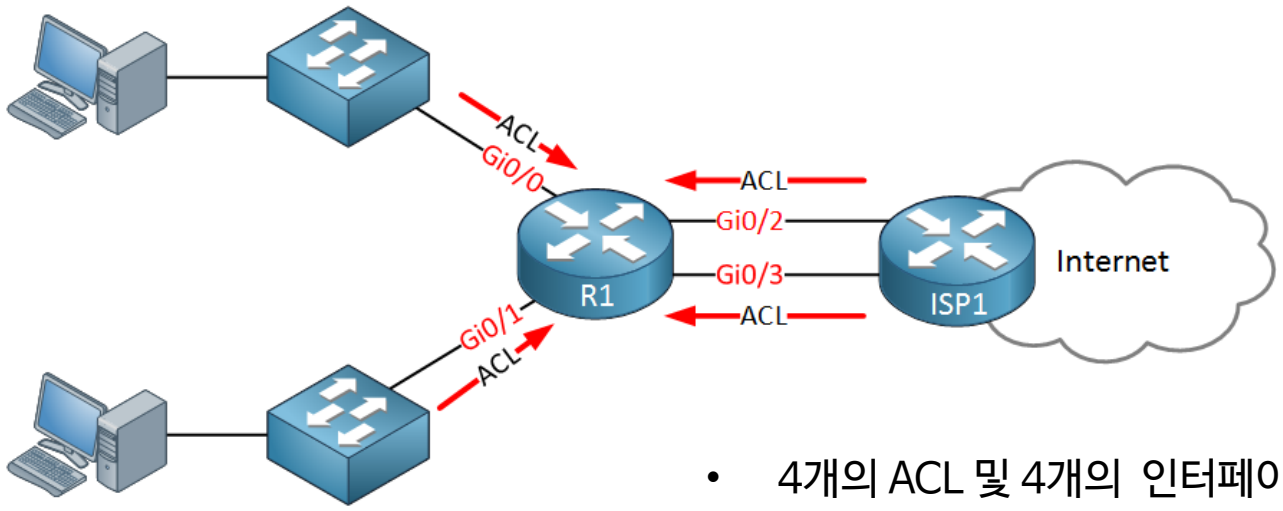
- IP 차단 대신 URL 차단 가능
- 페이로드를 확인해 바이러스 및 웜 패킷 차단

응용프로그램이 만들
어 주는 최초 데이터



Security Zone

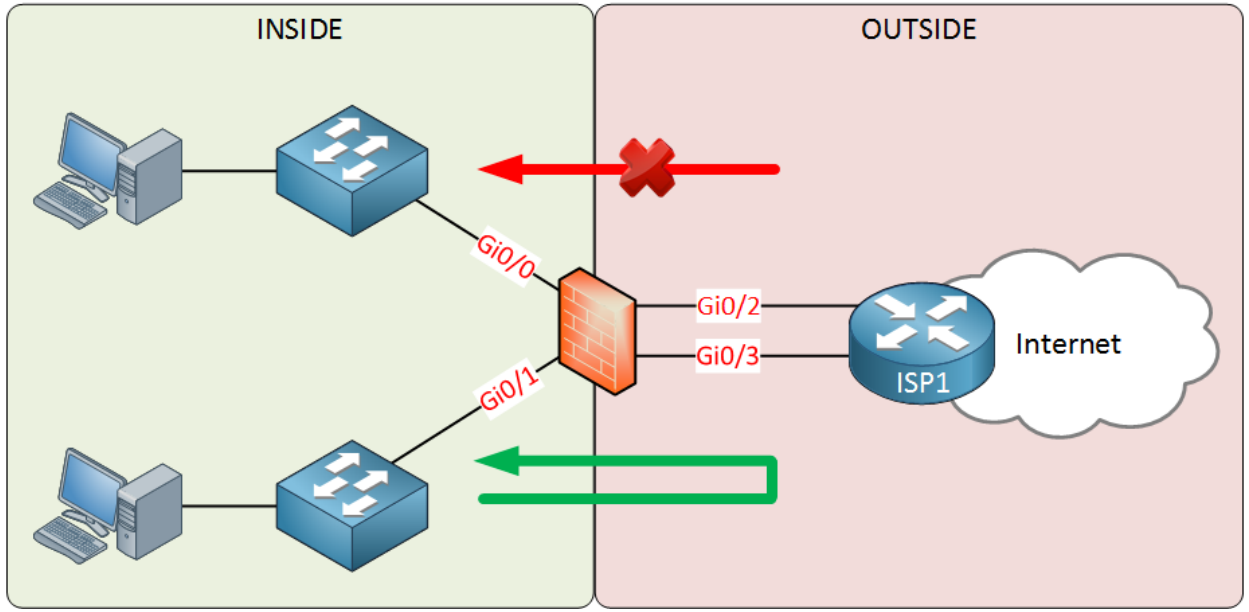
- 라우터는 기본적으로 라우팅 테이블을 기반으로 데이터를 허용/처리
  - 이를 제한하기 위해서는 ACL 필요
  - 많은 ACL과 많은 인터페이스는 관리의 어려움이 발생



- 4개의 ACL 및 4개의 인터페이스 관리 필요
  - 외부로 나가는 트래픽 중 일부를 차단하기 위해 두 개의 inbound ACL 생성/적용
  - 외부에서 들오는 트래픽 중 일부를 차단하기 위해 두 개의 inbound ACL 생성/적용

Security Zone

- 방화벽은 Zone 기반으로 데이터를 허용/처리



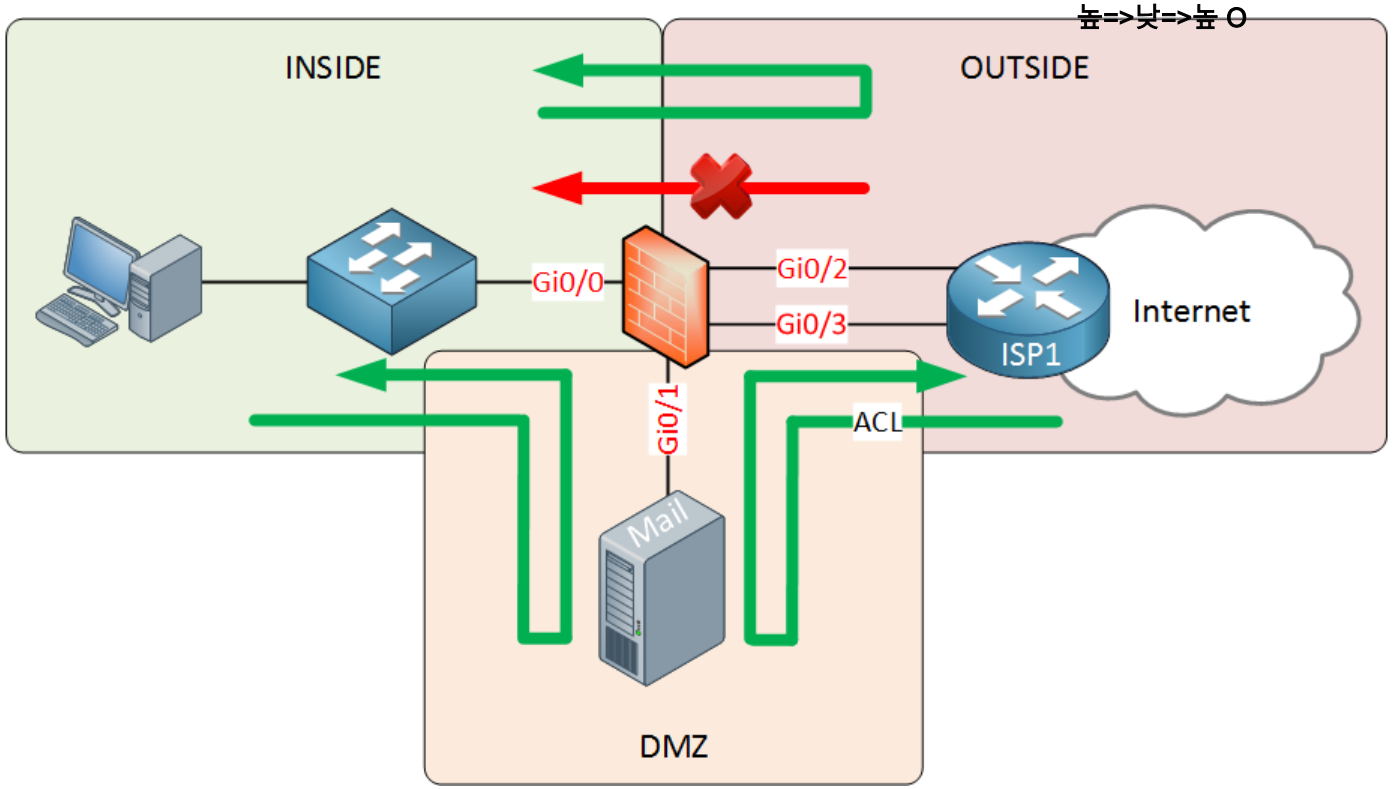
- INSIDE : 내부 LAN 구간 (High Security Level)
- OUTSIDE : 외부 WAN 구간 (Low Security Level)
- High Security Level ➔ Low Security Level : 허용
- Low Security Level ➔ High Security Level : 거부
  - 외부에서 시작해 내부로 접근하는 트래픽에 대해 ACL을 이용해 예외 적용
- 방화벽은 Stateful 동작으로 나가는 Connection 추적해 되돌아 오는 트래픽 허용

Security Zone

Cisco방화벽 기준

- DMZ를 운영하는 경우 INSIDE 와 OUTSIDE 사이의 Security Level 사용

높=>낮 O
낮=>높 X
높=>낮=>높 O



- INSIDE ➔ Outside 허용
- INSIDE ➔ DMZ 허용
- DMZ ➔ OUTSIDE 허용
- DMZ ➔ INSIDE 거부
- Outside ➔ DMZ 거부 (ACL 예외 필요)
- Outside ➔ INSIDE 거부

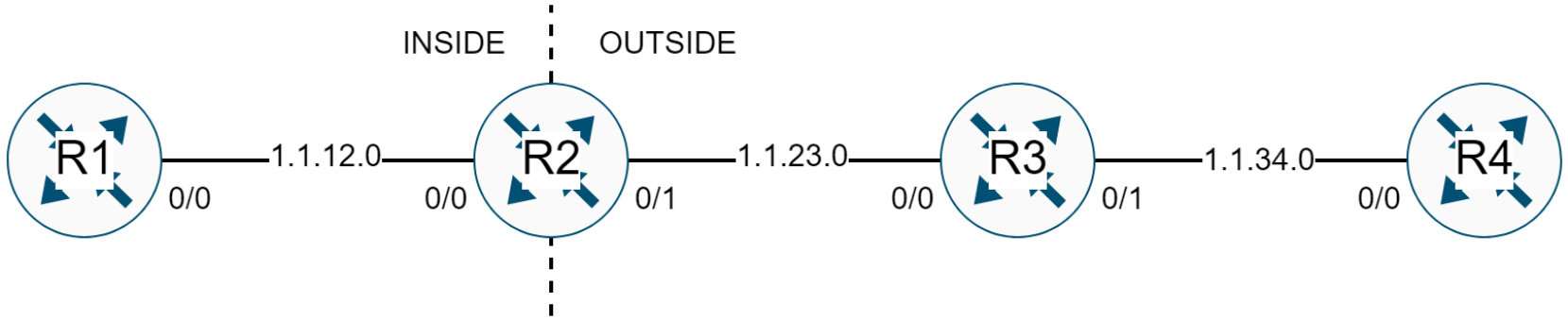
Summary

- 방화벽은 상태 정보 필터링을 사용해 모든 IN/OUT 연결 추적
- OSI 7계층 까지 검사 가능
- Zone 과 Security Laver 기반 동작으로 손쉽게 운영 가능

CBAC (Context-Based Access Control)

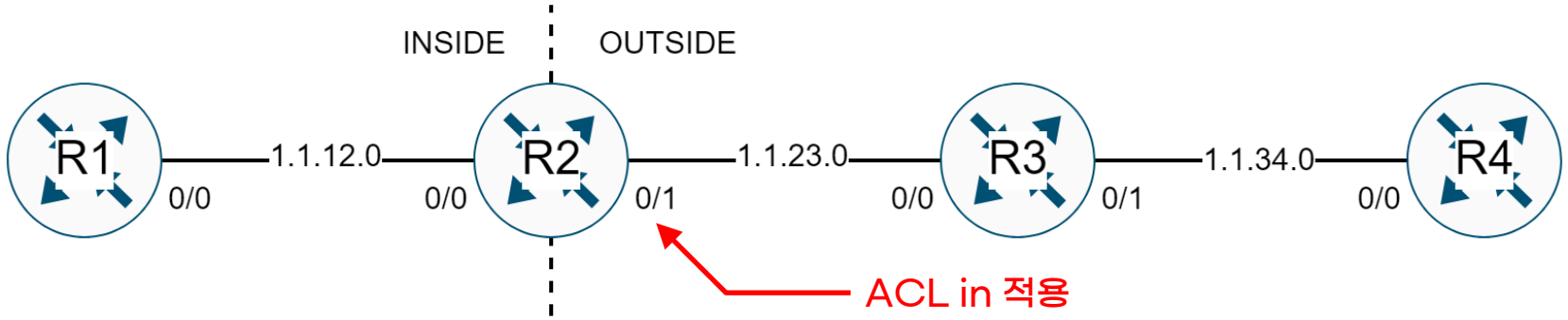
- L3 / L4 계층의 트래픽 뿐만 아니라 응용계층 트래픽 까지 제어 가능
- Stateful 방화벽 기능 지원
- CBAC 동작
  1) 돌아오는 패킷을 허용하는 임시 ACL 생성
  2) ACL이 이미 있다면 해당 ACL 우선 적용
  3) 패킷 처리 후 임시 ACL 삭제

Basic CBAC (Context-Based Access Control)



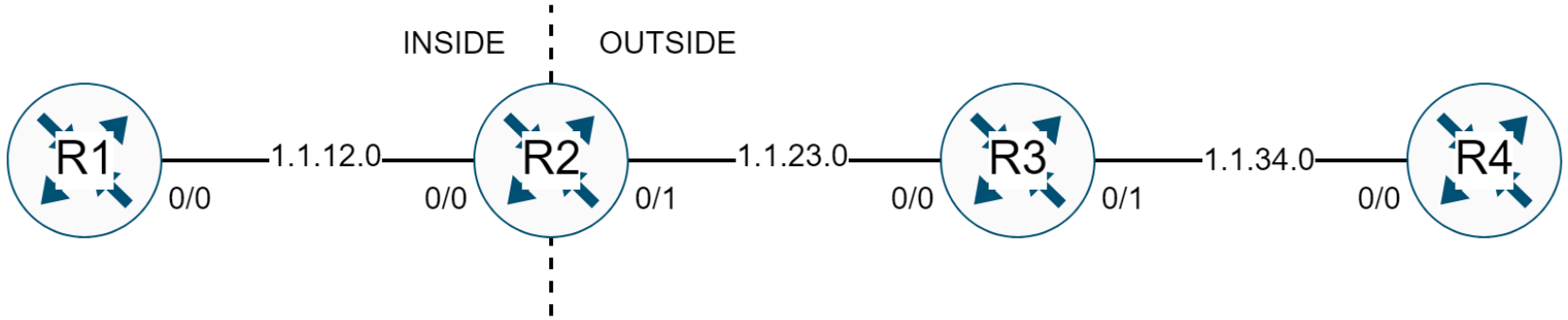
- 정책 결정
  - 외부에서 내부로 접근하는 모든 트래픽 차단
  - TCP , UDP 및 ICMP 패킷만 되돌아 올 수 있도록 허용

Basic CBAC (Context-Based Access Control)



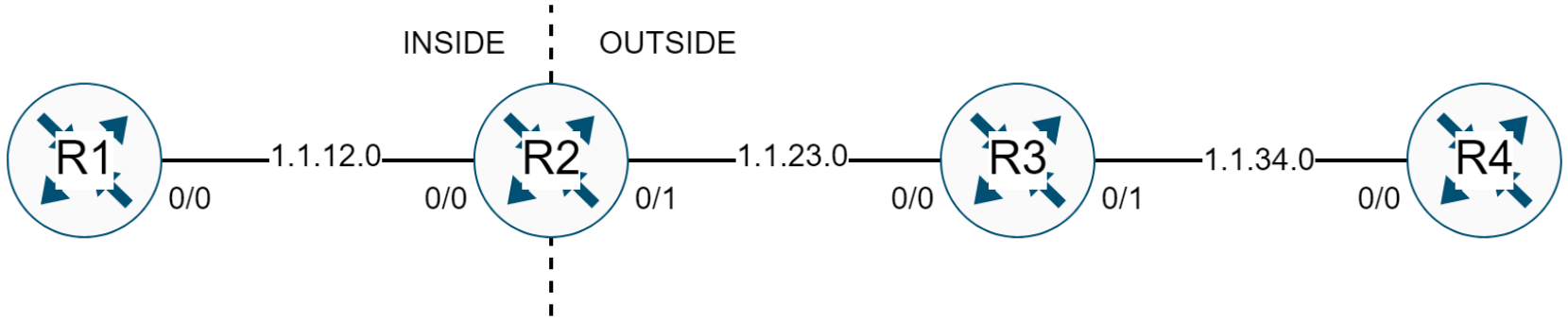

```
R2(config)# ip access-list extended outside-acl-in
R2(config-ext-nacl)# deny ip any any
R2(config-ext-nacl)# exit

R2(config)# int f0/1
R2(config-if)# ip access-group outside-acl-in in
```

Basic CBAC (Context-Based Access Control)



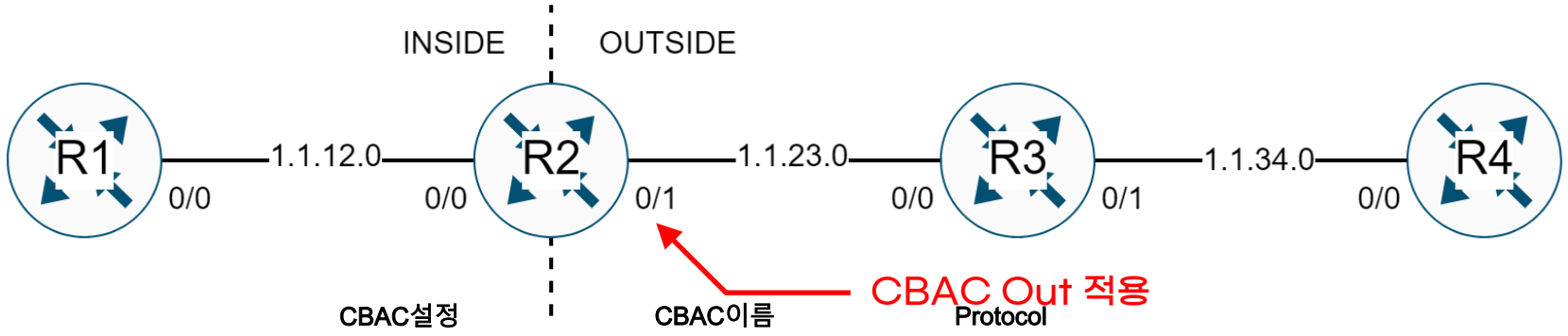

```
R4# ping 1.1.12.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.12.1, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)

R4# telnet 1.1.12.1
Trying 1.1.12.1 ...
% Destination unreachable; gateway or host down
```

Basic CBAC (Context-Based Access Control)




```
R1# ping 1.1.34.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1 .34.4, timeout is 2 seconds:
.....
```

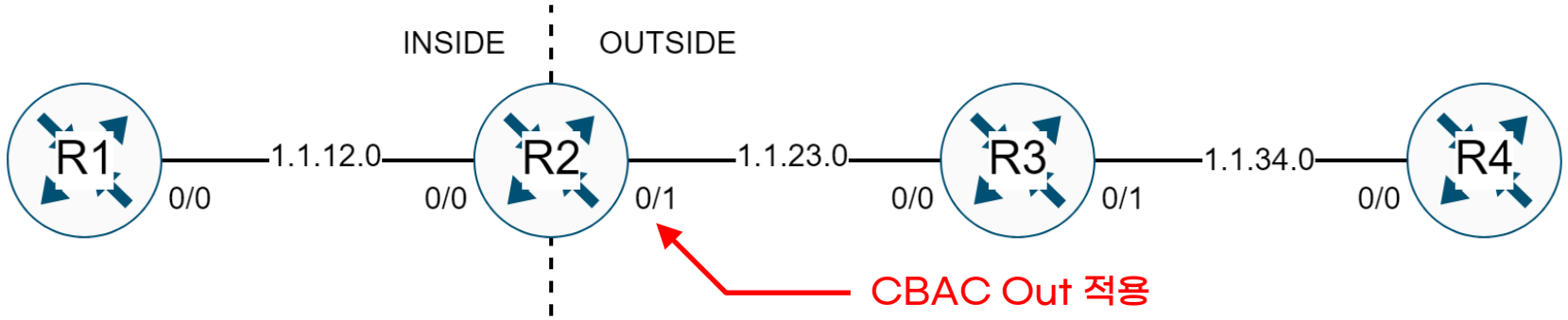
Basic CBAC (Context-Based Access Control)




```
R2(config)# ip inspect name Outside-outbound tcp
R2(config)# ip inspect name Outside-outbound udp
R2(config)# ip inspect name Outside-outbound icmp

R2(config)# int f0/1
R2(config-ip)# ip inspect Outside-outbound out
```

- TCP , UDP , ICMP를 모두 검사하고 돌아올 때 허용할 임시 ACL을 만들어 기존 ACL 상단에 추가
- E0/1 인터페이스에서 패킷이 외부로 빠져나가는 시점에 임시 ACL 생성

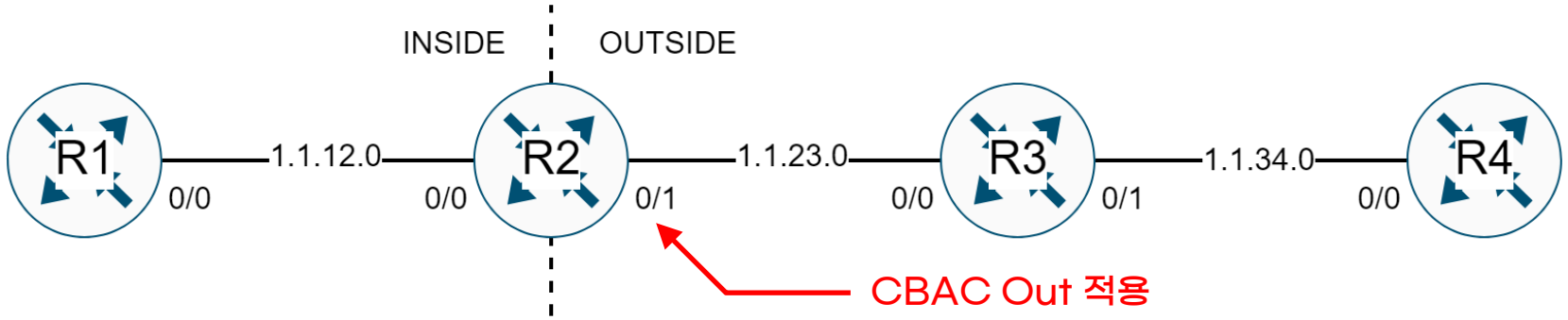
Basic CBAC (Context-Based Access Control)



R1 to R4 Telnet

```
R1# telnet 1.1.34.4
Trying 1.1.34.4 … Open
User Access Verification
Password:

R4>
```

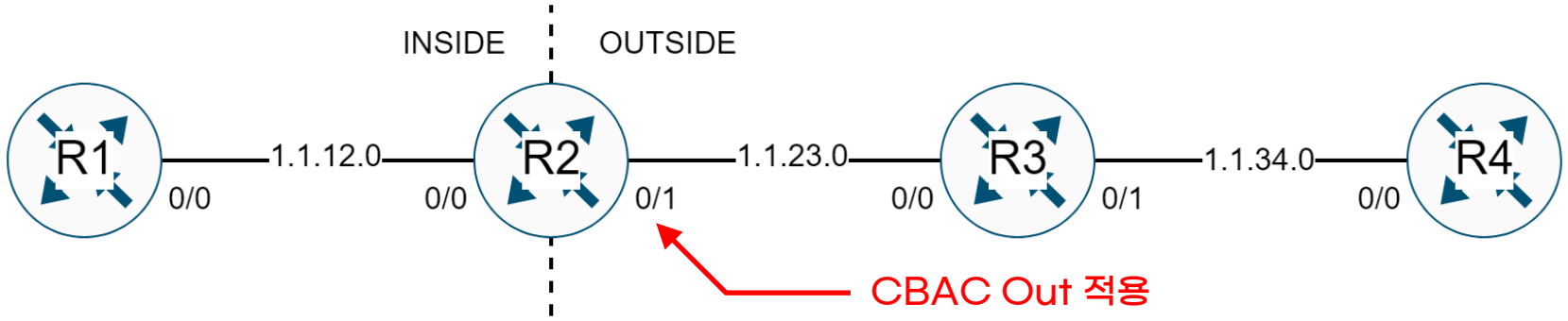
Basic CBAC (Context-Based Access Control)




```
R2# show ip inspect sessions detail
Established Sessions
 Session F2DD72F8 (1.1.12.1:41259)=>(1.1.34.4:23) tcp SIS_OPEN
  Created 00:00:17, Last heard 00:00:14
  Bytes sent (initiator:responder) [49:87]
  In SID 1.1.34.4[23:23]=>1.1.1.12.[41259:41259] on ACL outside-acl-in (21 matches)
```

- 내부 1.1.12.1 에서 외부 1.1.34.4으로 전송된 텔넷 패킷이 돌아올 때 허용 하는 임시 ACL 생성
- 이 ACL에 의해 돌아오는 텔넷 패킷 허용

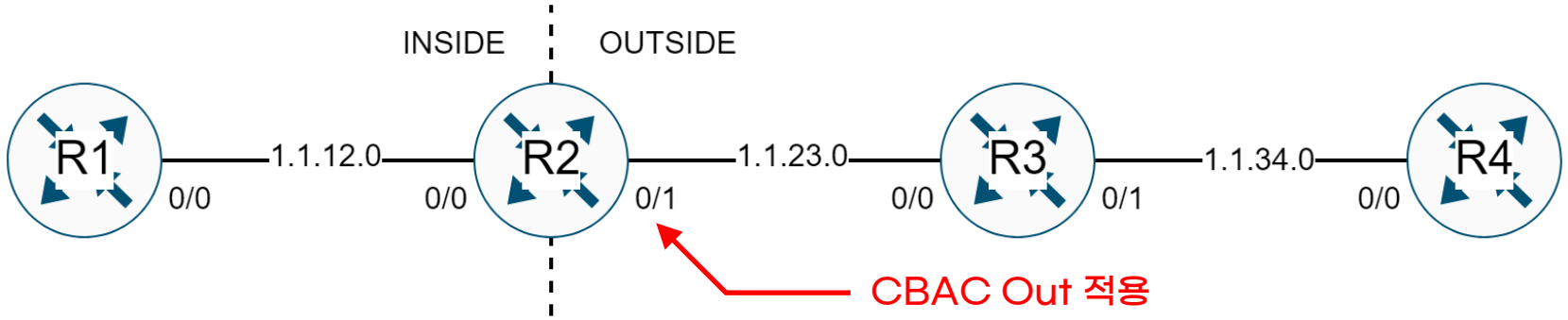
Basic CBAC (Context-Based Access Control)



R1 to R4 ICMP

```
R1# ping 1.1.34.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.34.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

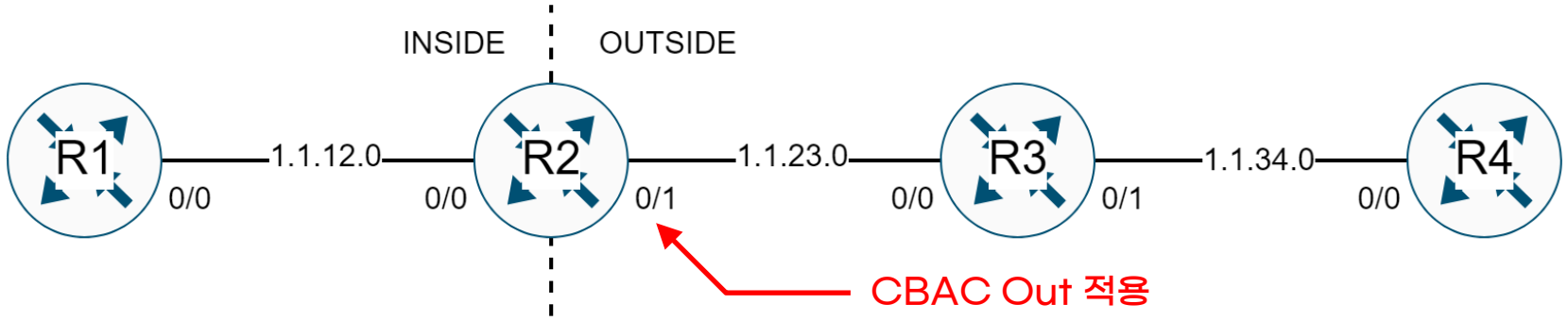
Basic CBAC (Context-Based Access Control)




```
R2# show ip inspect sessions detail
Established Sessions
 Session F2DD70D8 (1.1.12.1:8)=>(1.1.34.4:0) icmp SIS_OPEN
  Created 00:00:00, Last heard 00:00:00
   ECHO request
  Bytes sent (initiator:responder) [360:360]
  In SID 1.1.34.4[0:0]=>1.1.12.[0:0] on ACL outside-acl-in (5 matches)
```

- 내부 1.1.12.1 에서 외부 1.1.34.4으로 전송된 ICMP 패킷이 돌아올 때 허용 하는 임시 ACL 생성
- 이 ACL에 의해 돌아오는 ICMP 패킷 허용

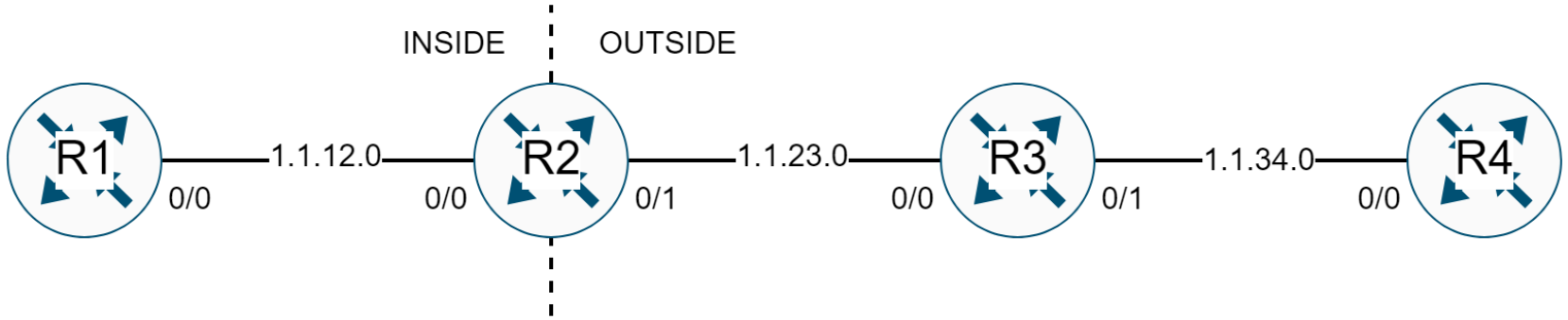
Basic CBAC (Context-Based Access Control)




```
R4# ping 1.1.12.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.12.1, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)

R4# telnet 1.1.12.1
Trying 1.1.12.1 ...
% Destination unreachable; gateway or host down
```

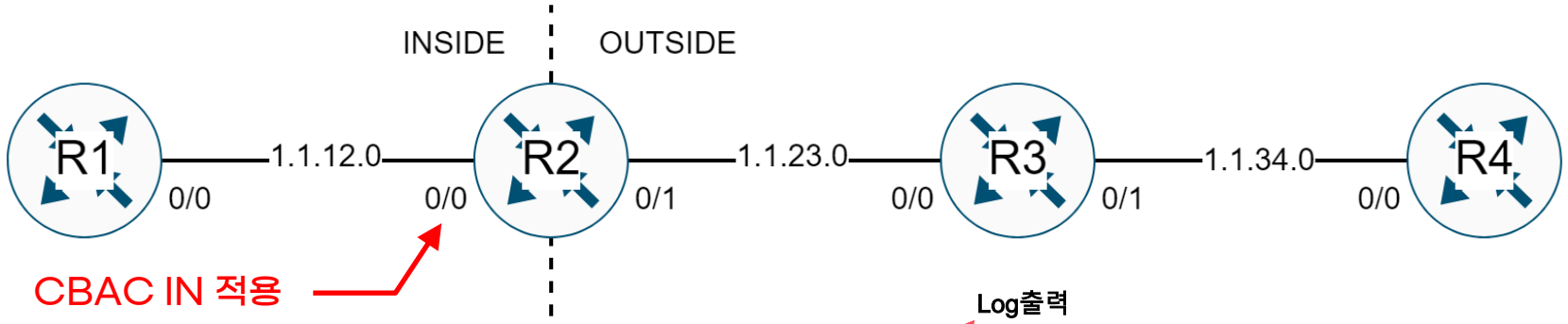
- 여전히 외부에서 시작해 내부로 들어오는 패킷은 모두 차단됨

Application CBAC (Context-Based Access Control)



- 정책 결정
  - 외부에서 내부로 접근하는 모든 트래픽 차단
  - 내부로 돌아오는 TCP 패킷 중 HTTP만 허용

Application CBAC (Context-Based Access Control)



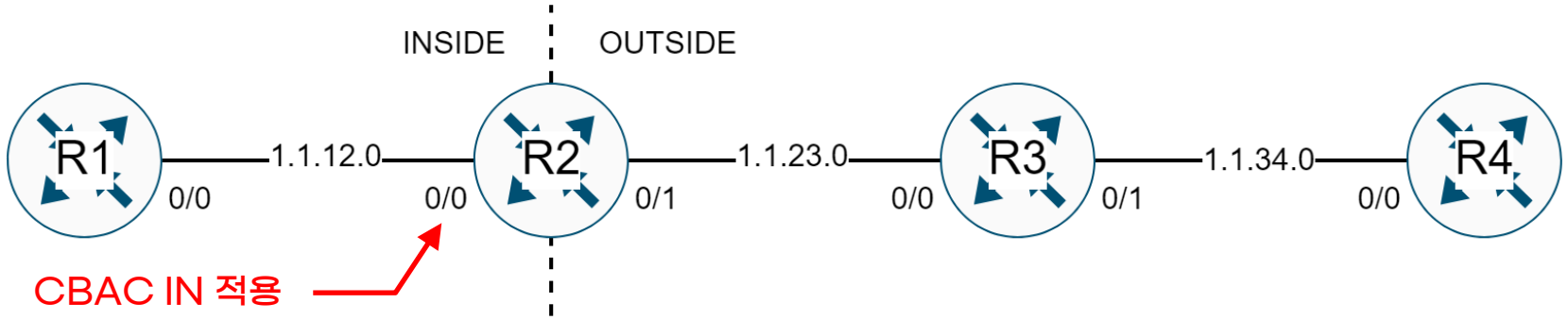
Log출력

```
R2(config)# ip inspect name mycbac http audit-trail on

R2(config)# int f0/0
R2(config-ip)# ip inspect mycbac in
```

서비스 이름

- audit-trail on : 해당 패킷의 log 출력
- R2의 Inside 방향에 있는 e0/0 인터페이스에 CBACA in 적용 (e0/1 out 과 결과는 동일)

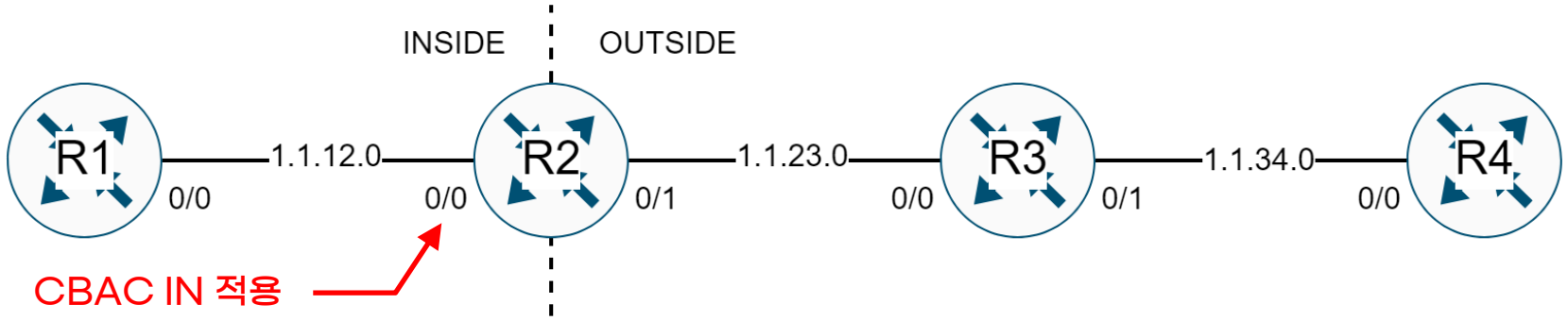
Application CBAC (Context-Based Access Control)



R1 to R3 Telnet

```
R1# telnet 1.1.23.3
Trying 1.1.23.3 ...
% Connection timed out; remote host not responding
```

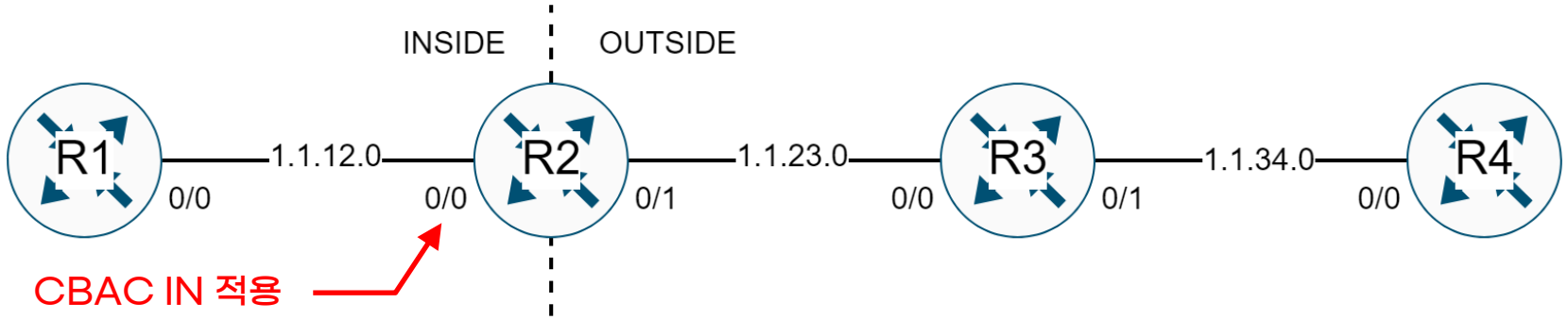
Application CBAC (Context-Based Access Control)



R1 to R3 Telnet

```
R1# telnet 1.1.23.3 80
Trying 1.1.23.3, 80 ... Open
```

Application CBAC (Context-Based Access Control)




```
R2#
%FW-6-SESS_AUDIT_TRAIL_START: Start http session: initiator (1.1.12.1:17643) -- responder (1.1.23.3:80)
```

```
R2# show ip inspect sessions detail
Established Sessions
 Session F2DD6858 (1.1.12.1:17643)=>(1.1.23.3:80) http SIS_OPEN
  Created 00:00:54, Last heard 00:00:54
  Bytes sent (initiator:responder) [0:0]
  In SID 1.1.23.3[80:80]=>1.1.12.1 [17643:17643] on ACL outside-acl-in (2 matches)
```

ZFW (Zone-Based Policy Firewall)

- CBAC 단점
  - 인터페이스 기반 트래픽 검사로 정책 설정 및 관리 어려움
  - 다수 개의 인터페이스 구성 시 설정이 복잡

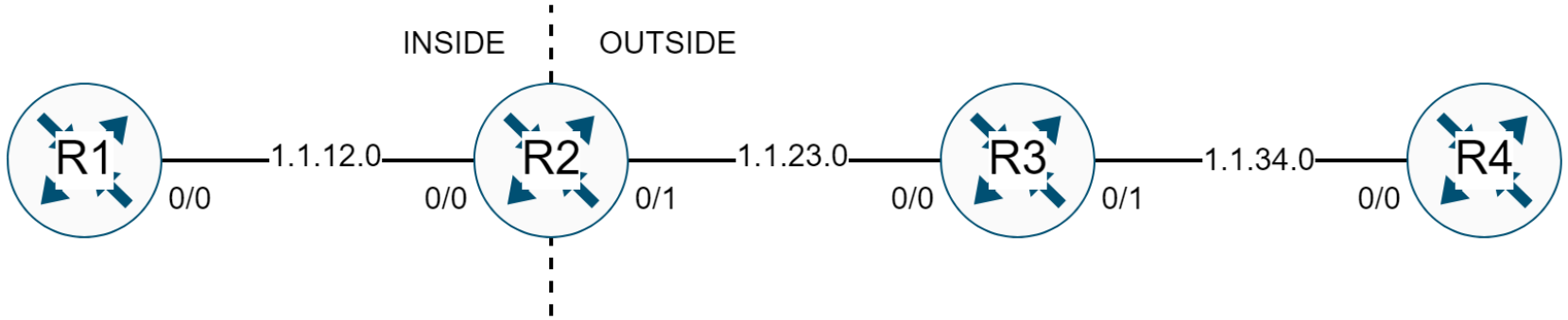
- 라우터의 각 인터페이스를 특정 Zone에 할당하고, Zone 사이에 보안 정책 적용
  - 전용 방화벽 ASA와 유사

Cisco 방화벽 제품

ZFW (Zone-Based Policy Firewall)

- Zone / Security Zone (or)
  - 보안 정책이 적용되는 인터페이스 그룹
- Zone member
  - Zone에 속한 인터페이스
- Self-Zone
  - 시스템에서 정의한 Default Zone
  - 라우터의 모든 인터페이스는 Zone 소속 여부와 관계 없이 Self-Zone에 포함
  - 라우터가 출발지 또는 목적지인 패킷을 제어할 때 사용
- Zone Pair
  - 출발지 Zone 과 목적지 Zone의 묶음
  - Zone Pair를 설정하기 전까지는 Zone간 통신 불가 (Self Zone 예외)

ZFW (Zone-Based Policy Firewall)

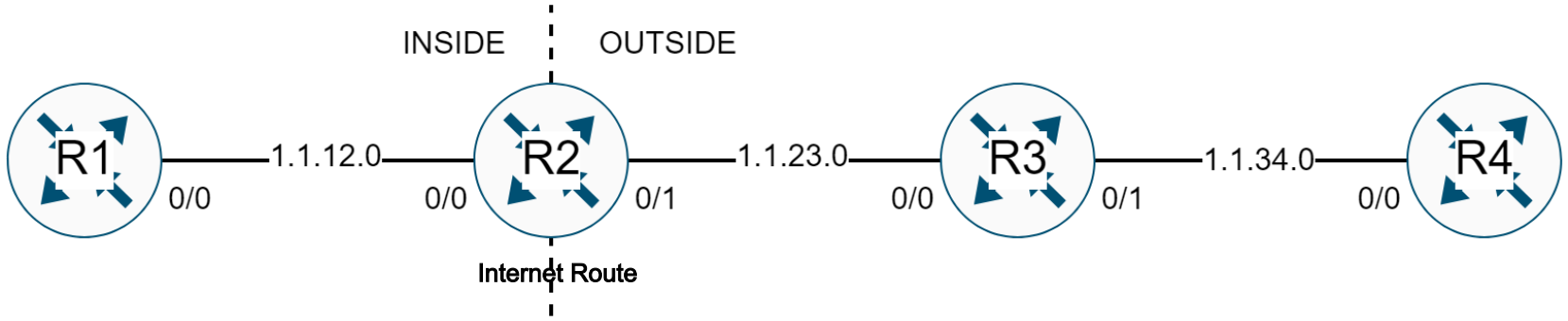


- 설정 순서
  1) Zone 생성 및 인터페이스 할당
  2) Zone Pair 생성
  3) 보안정책 정의
  4) Zone Pair에 보안정책 적용

ZFW (Zone-Based Policy Firewall)

- Zone 규칙
  - 인터페이스는 오직 하나의 Zone에만 소속
  - 동일 Zone에 소속된 인터페이스간 트래픽 기본 허용
  - 서로 다른 Zone에 소속된 인터페이스간 허용되지 않은 트래픽은 기본 차단 (허용 정책 필요)
  - Self Zone은 Zone과 반대로 기본 허용 (차단 정책 필요)
  - Zone에 소속되지 않은 인터페이스는 Zone 소속 인터페이스와 통신 불가
  - 인터페이스간 통신이 이루어지기 위해서는 모든 인터페이스가 반드시 Zone에 소속돼야 함 (정책 통신)
  - 서로 다른 Zone 통신에는 ACL 적용 불가 (오직 Zone Pair & 정책)
  - Zone 멤버에 속한 인터페이스는 ACL 적용 불가
  - Zone 멤버에 속한 인터페이스는 CBAC 설정 불가 (ZFW & CBAC 동시 적용 불가)

ZFW (Zone-Based Policy Firewall) - Zone 생성 및 Interface 할당




```
R2(config)# zone security inside
R2(config-sec-zone)# exit
R2(config)# zone security outside
R2(config-sec-zone)# exit
```

zone 만드는 명령어

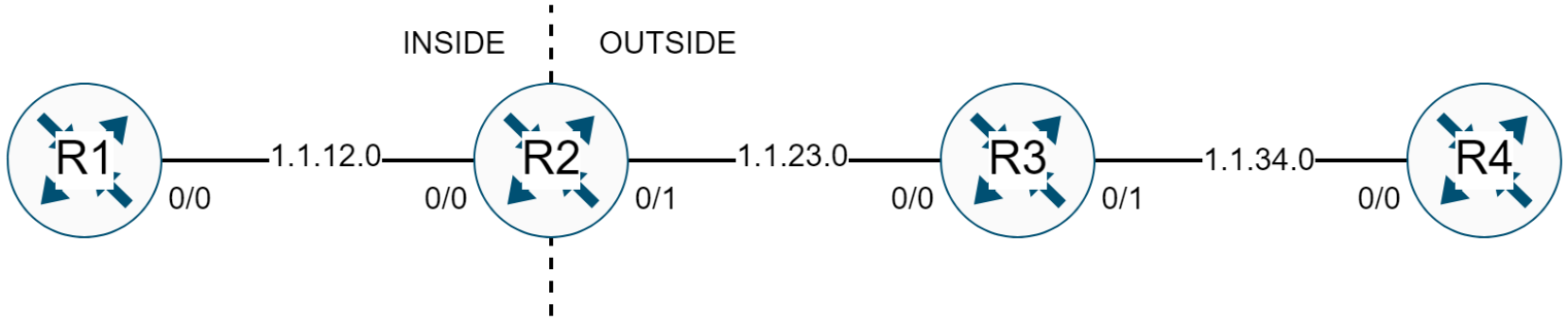
zone 이름

```
R2(config)# int f0/0
R2(config-if)# zone-member security inside
```

inside 이름을 가진 zone의 member로 사용하겠다는 의미

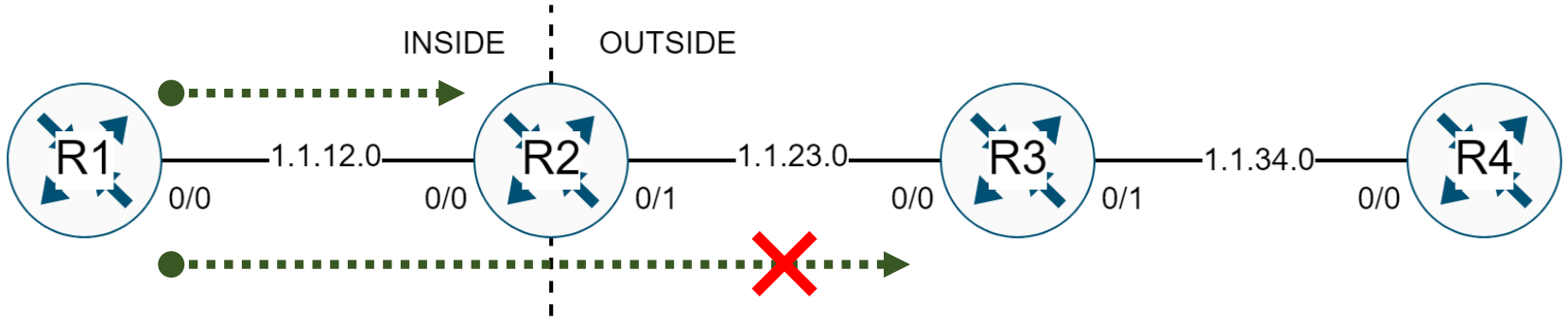
```
R2(config)# int f0/1
R2(config-if)# zone-member security outside
```

ZFW (Zone-Based Policy Firewall) - Zone 및 Interface 확인




```
R2#show zone security 어떤 zone에 어떤 interface가 있는지 확인
zone self
  Description: System defined zone

zone inside
  Member Interfaces:
    FastEthernet0/0

zone outside
  Member Interfaces:
    FastEthernet0/1
```

ZFW (Zone-Based Policy Firewall) - 통신 확인



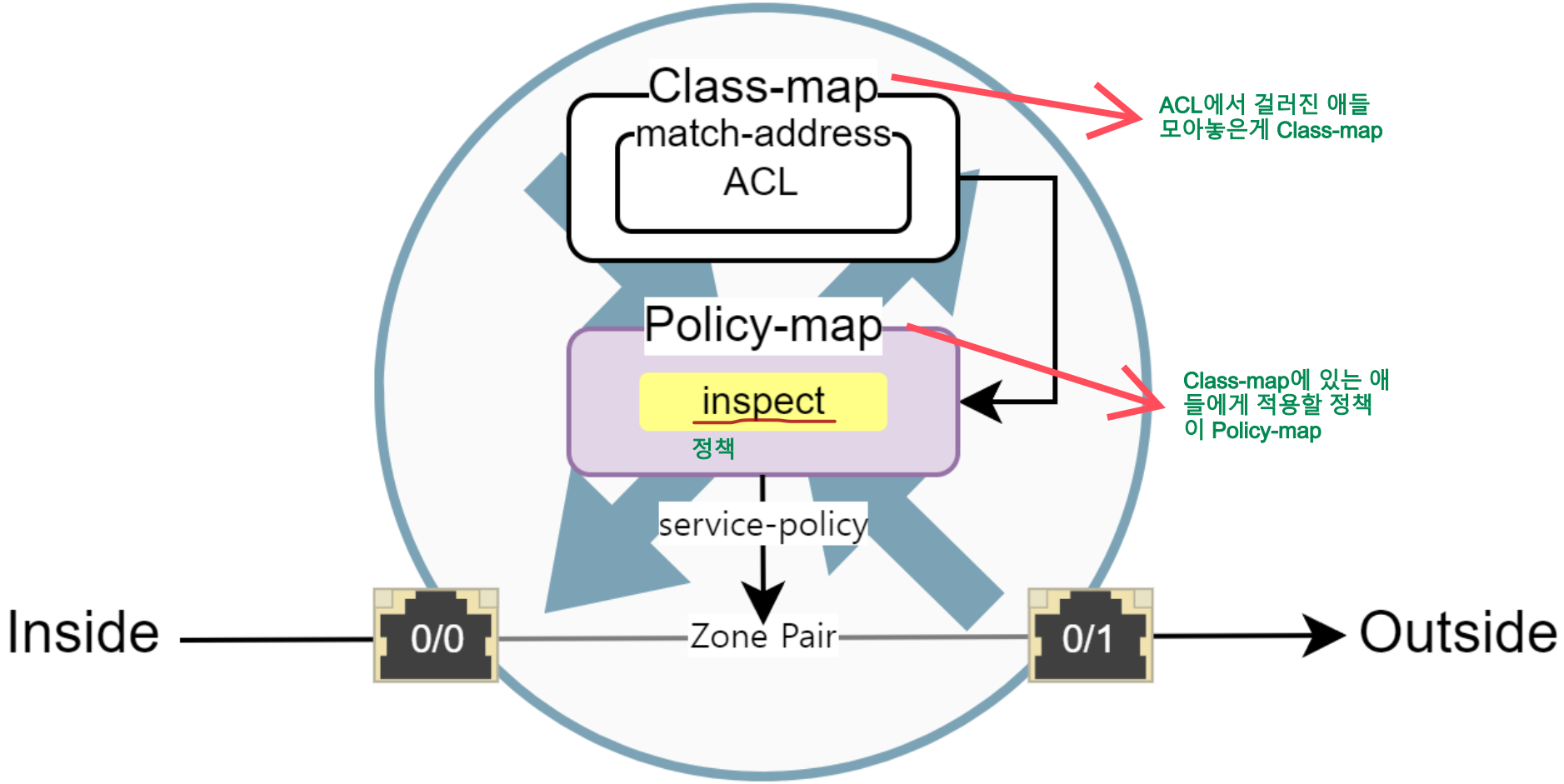

```
R1# ping 1.1.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.12.2, timeout is 2 seconds:
!!!!!
```

INSIDE to INSIDE

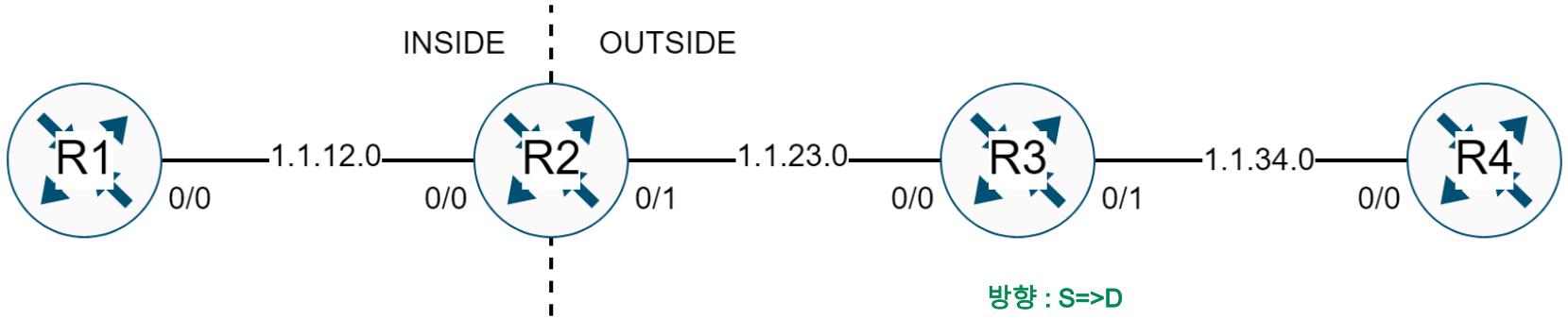
```
R1# ping 1.1.23.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.23.3, timeout is 2 seconds:
.....

R1 # telnet 1.1.23.3
Trying 1.1 .23.3 ...
% Connection timed out; remote host not responding
```

INSIDE to OUTSIDE

ZFW (Zone-Based Policy Firewall) - 보안정책 적용 및 확인



ZFW (Zone-Based Policy Firewall) - Zone Pair




```
R2(config)# zone-pair security Outbound source inside destination outside
```

zone pair 이름

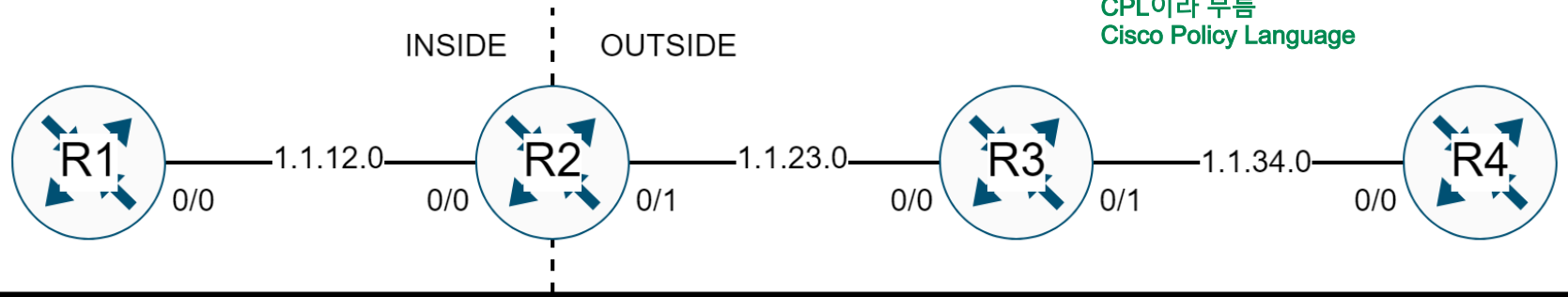
zone 이름

```
R2# show zone-pair security
Zone-pair name Outbound
    Source-Zone inside  Destination-Zone outside
    service-policy not configured
```

- Zone Pair를 사용해 두 개의 Zone 간에 단방향 방화벽 정책 정의
- 출발지 및 목적지 Zone을 지정해 트래픽 방향 설정
  - 리턴 트래픽은 자동으로 허용

ZFW (Zone-Based Policy Firewall) - 보안정책 정의

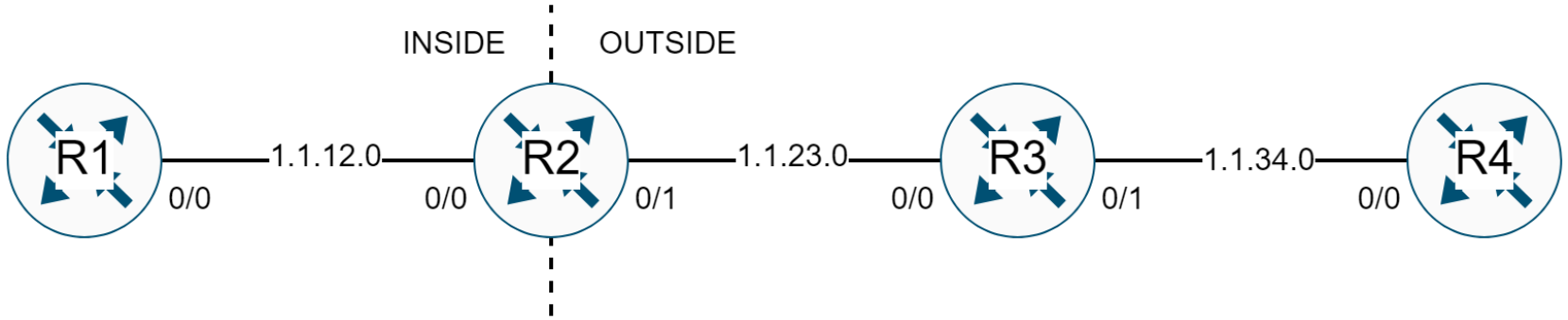
정책으로는
class-map
policy-map 사용
CPL이라 부름
Cisco Policy Language




```
R2(config)# ip access-list extended acl-outbound ACL을 먼저 만듬
R2(config-ext-nacl)# permit ip any any

R2(config)# class-map type inspect class-outbound class 이름
R2(config-cmap)# match access-group name acl-outbound
```

```
R2(config)# policy-map type inspect policy-outbound map 이름
R2(config-pmap)# class type inspect class-outbound
R2(config-pmap-c)# inspect
%No specific protocol configured in class class-outbound for inspection. All
protocols will be inspected
```

ZFW (Zone-Based Policy Firewall) - 보안정책 적용 및 확인



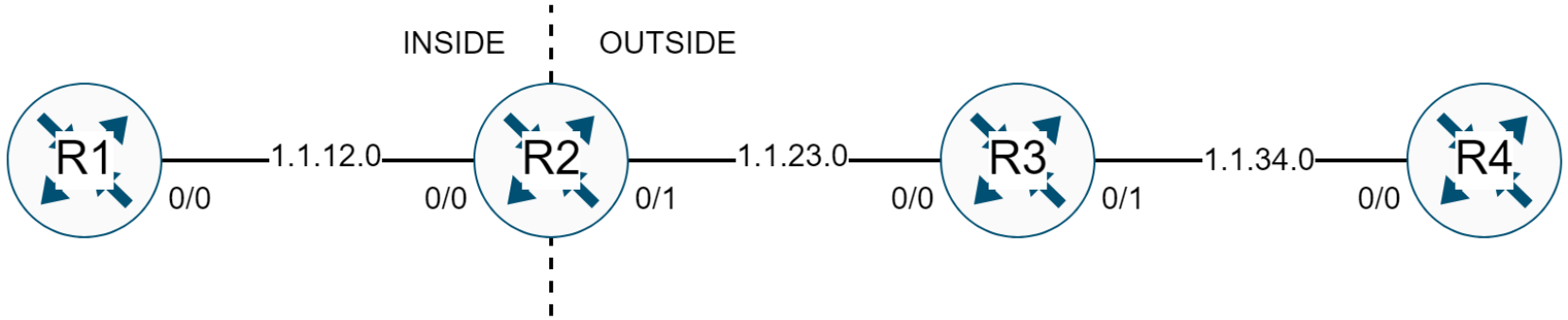

```
R2(config)# zone-pair security Outbound source inside destination outside
R2(config-sec-zone-pair)# service-policy type inspect policy-outbound
```

```
R1# ping 1.1.23.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.23.3, timeout is 2 seconds:
!!!!!

R1# telnet 1.1.23.3
Trying 1.1.23.3 ... Open
```

ZFW (Zone-Based Policy Firewall) - 보안정책 적용 및 확인

```
R2# show policy-map type inspect zone-pair sessions

policy exists on zp Outbound
 Zone-pair: Outbound

  Service-policy inspect : policy-outbound

    Class-map: class-outbound (match-all)
      Match: access-group name acl-outbound
      Inspect
        Number of Established Sessions = 1
        Established Sessions
         Session 3974673632 (1.1.12.1:1027)=>(1.1.23.3:80) tcp SIS_OPEN/TCP_ESTAB
          Created 00:00:32, Last heard  00:00:32
          Bytes sent (initiator:responder) [84:44]
    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
```

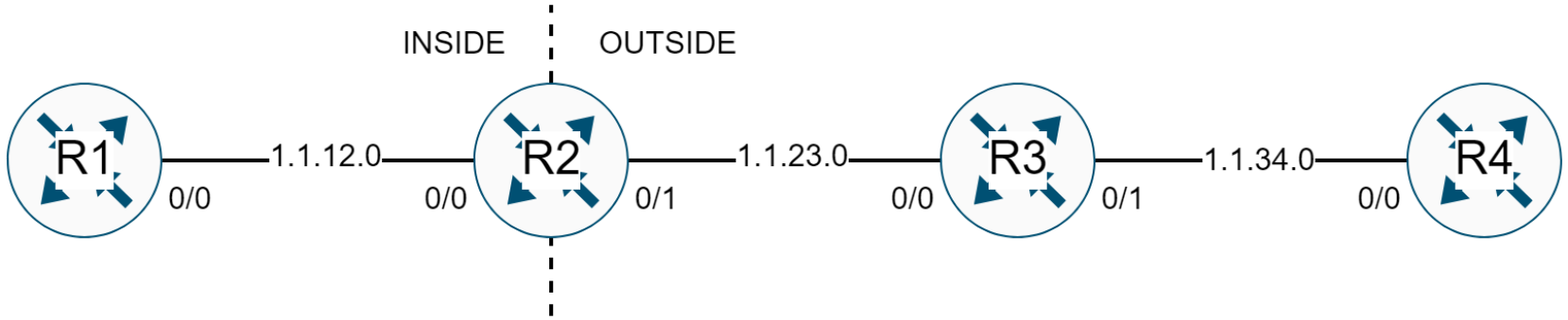
ZFW (Zone-Based Policy Firewall) - ACL 관계




```
R2(config)# ip access-list extended acl-inbound
R2(config-ext-nacl)# deny tcp host 1.1.34.4 host 1.1.12.1 eq 23
R2(config-ext-nacl)# permit ip any any

R2(config)# int f0/1
R2(config-if)# ip access-group acl-inbound in
```

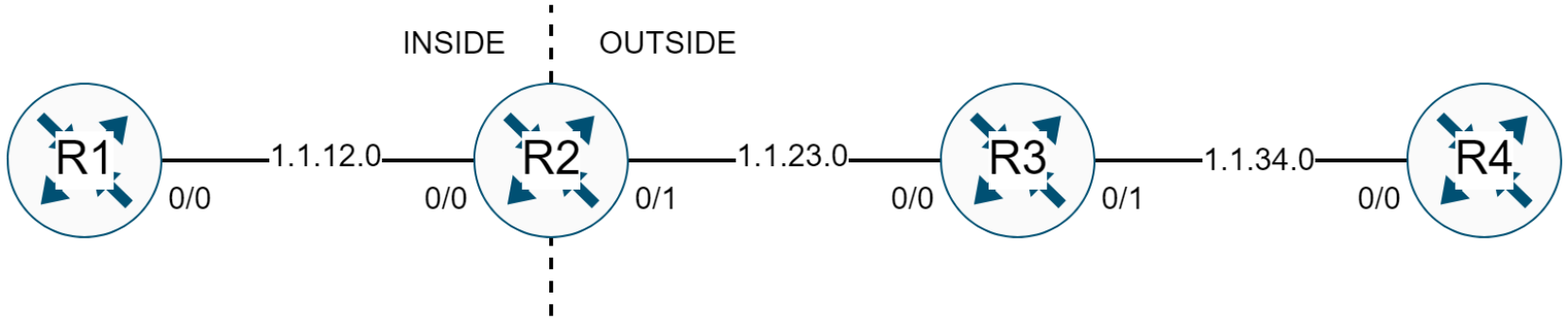
```
R4# telnet 1.1.12.1
Trying 1.1.12.1 ...
% Destination unreachable; gateway or host down
```

ZFW (Zone-Based Policy Firewall) - ACL 관계




```
R2(config)# ip access-list extended acl-inbound
R2(config-ext-nacl)# deny tcp host 1.1.34.4 host 1.1.12.1 eq 23
R2(config-ext-nacl)# permit ip any any

R2(config)# int f0/1
R2(config-if)# ip access-group acl-inbound in
```

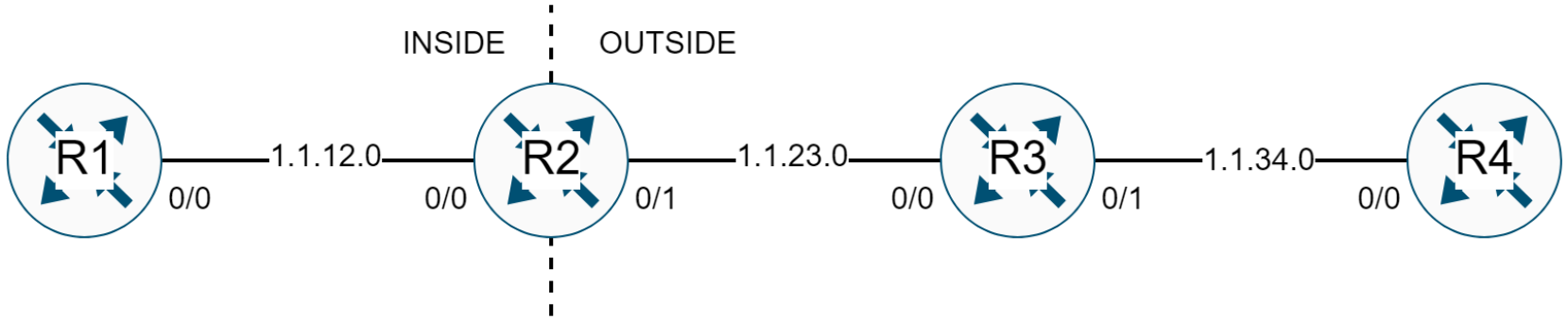
ZFW (Zone-Based Policy Firewall) - ACL 관계




```
R4# telnet 1.1.12.1
Trying 1.1.12.1 ...
% Destination unreachable; gateway or host down
```

```
R2# show ip access-lists acl-inbound

Extended IP access list acl-inbound
    10 deny tcp host 1.1.34.4 host 1.1.12.1 eq telnet (1 match)
    20 permit ip any any (6 matches)
```

ZFW (Zone-Based Policy Firewall) - ACL 관계

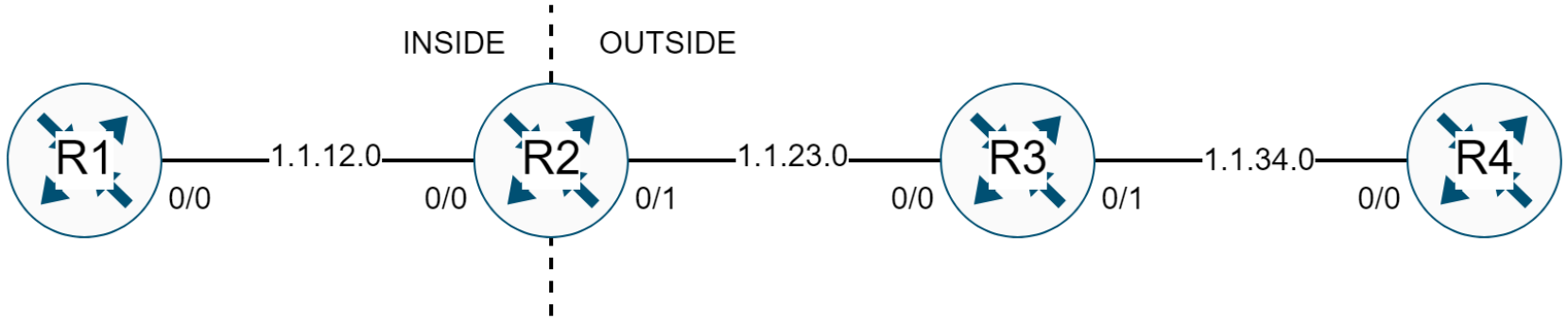



```
R4# ping 1.1.12.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.12.1 , timeout is 2 seconds:
.....
```

ZFW에 의해서 다른 zone간에 통신 차단

```
R2# show policy-map type inspect zone-pair Inbound
<...>
  Class-map: class-default (match-anv)
    Match: any
    Drop
      5 packets. 400 bytes
```

ZFW (Zone-Based Policy Firewall) - ACL 관계




```
R3# ping 1.1.12.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.12.1 , timeout is 2 seconds:
.....
```

```
R3# telnet 1.1.12.1
Trying 1.1.12.1 ... Open
User Access Verification

Password:
```