L4~L7 Device Deployment 시 발생할 수 있는 Asymmetric Traffic Flow Issue

이창주, changjoo@cisco.com

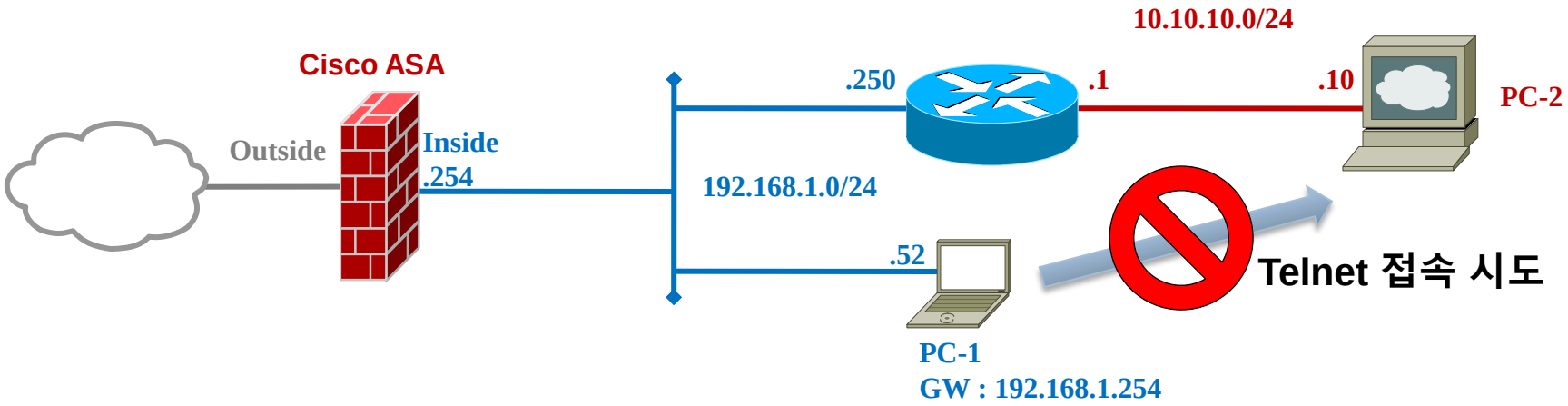
Product Marketing

Cisco Korea, Channels

Initial publication: Aug. 2008

※문서 내의 오타나 내용 상의 문의는 좌측의 E-mail로 연락 주십시오

Issue가 발생하는 Network Topology

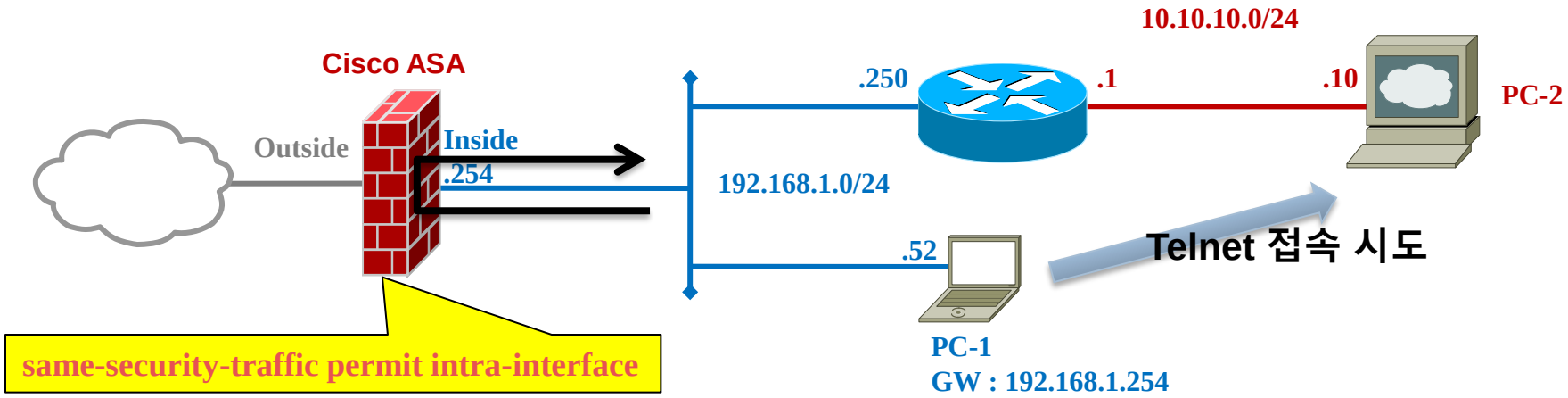


기본적인 네트워크 구성은 위와 같습니다. 이제 PC-1에서 PC-2로 Telnet을 합니다.
문제는 이게 안된 다는 것이죠?

참.. 여기서 왼쪽에 있는 방화벽은 일단 Cisco ASA라고 해 두죠.

하지만 뒷 부분에서(24페이지) 이 위치에 어떤 L4~L7 장비를 놓더라도 마찬가지 장애가 발생한다는 것도
따로 설명을 드리겠습니다.

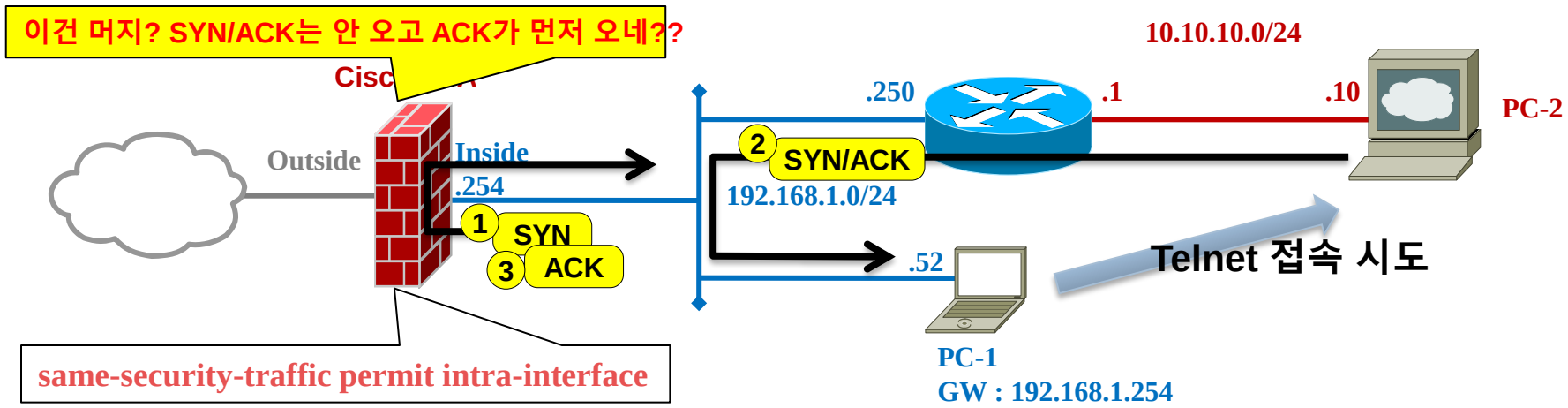
우선 답부터 알아 볼까요? (1)



일단 문제의 답을 먼저 알아 봅시다.

우선, 일단 트래픽이 Inside로 들어왔다가 Inside로 나가야 하므로 "**same-security-traffic permit intra-interface**" 명령어는 필수로 들어가야 합니다.

우선 답부터 알아 볼까요? (2)

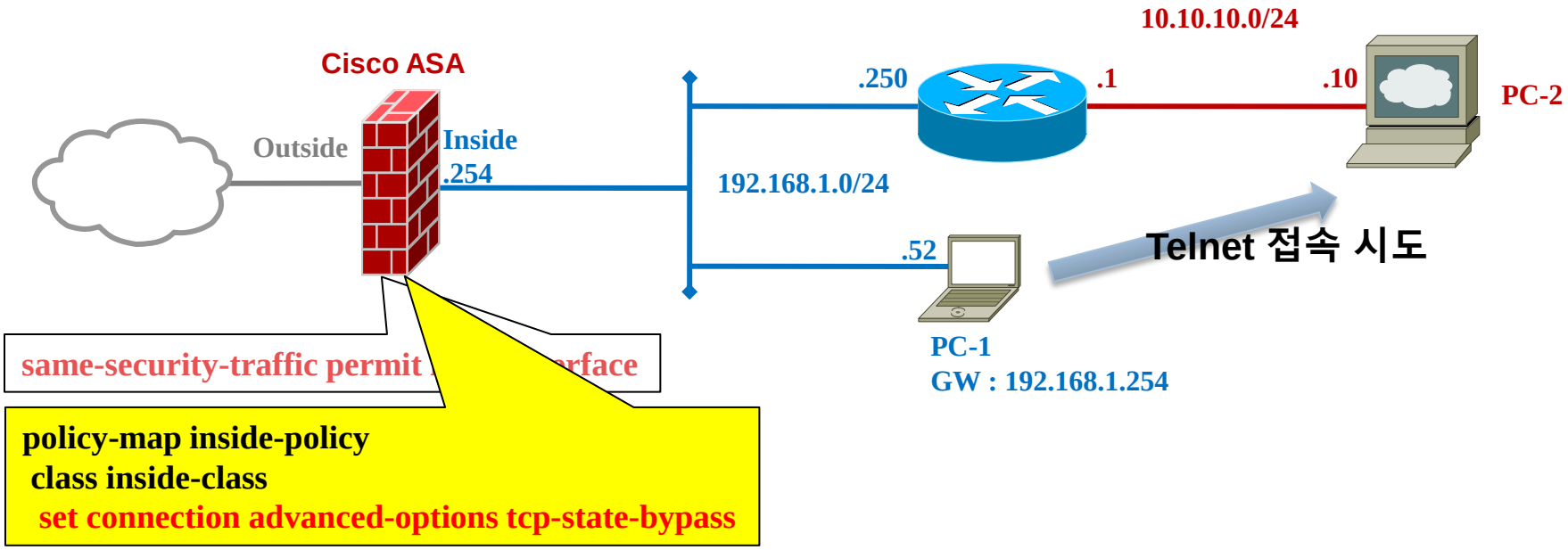


두번째로 고려할 점은, ①PC-1이 보내는 SYN은 ASA를 통하지만 ②PC-2에서 오는 SYN/ACK은 라우터에서 바로 PC-1으로 보내지기 때문에* 이 상태에서 ③PC-1이 ACK를 보내면, ASA는 "SYN-ACK는 안 오고, ACK가 먼저 왔네?"하며 이 Connection을 제대로 만들지 못해 통신이 안됩니다.**

그래서 추가로 적용하는 기능이 "**TCP-State Bypass**" 입니다.

* 라우터의 .250과 PC-1의 .254가 같은 네트워크에 있으니 Default Gateway의 도움 없이 ARP로 바로 가죠?
** 사실은 통신은 둘째 치고 3-way Handshake의 마지막 ACK 조차도 보내지 않기 때문에 위의 설명은 엄밀히 말하면 잘못 되었지요. (궁금하시면 나중에 12페이지를 잘 읽어보세요.)

우선 답부터 알아 볼까요? (3)

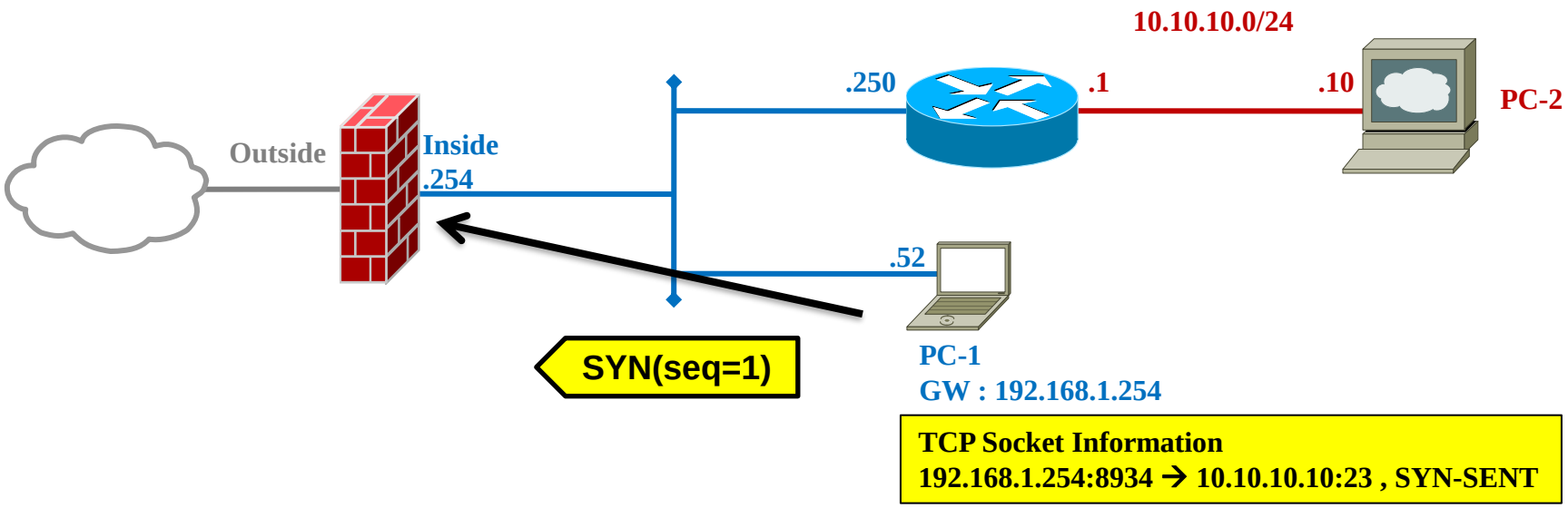


이 TCP-State bypass 기능을 이용하면 ASA는 현재의 Connection state와 관계 없이 ACL에 정의된 “IP/Port 번호”만 맞으면 트래픽을 허용하게 됩니다. 즉 위와 같은 Asymmetric 환경에서도 트래픽이
통할 수 있도록 해 준다는 거죠.

자. 그럼 이제 문제를 다 해결 했는데, 왜 뒤에 20장 가량의 추가 슬라이드가 있을까요?

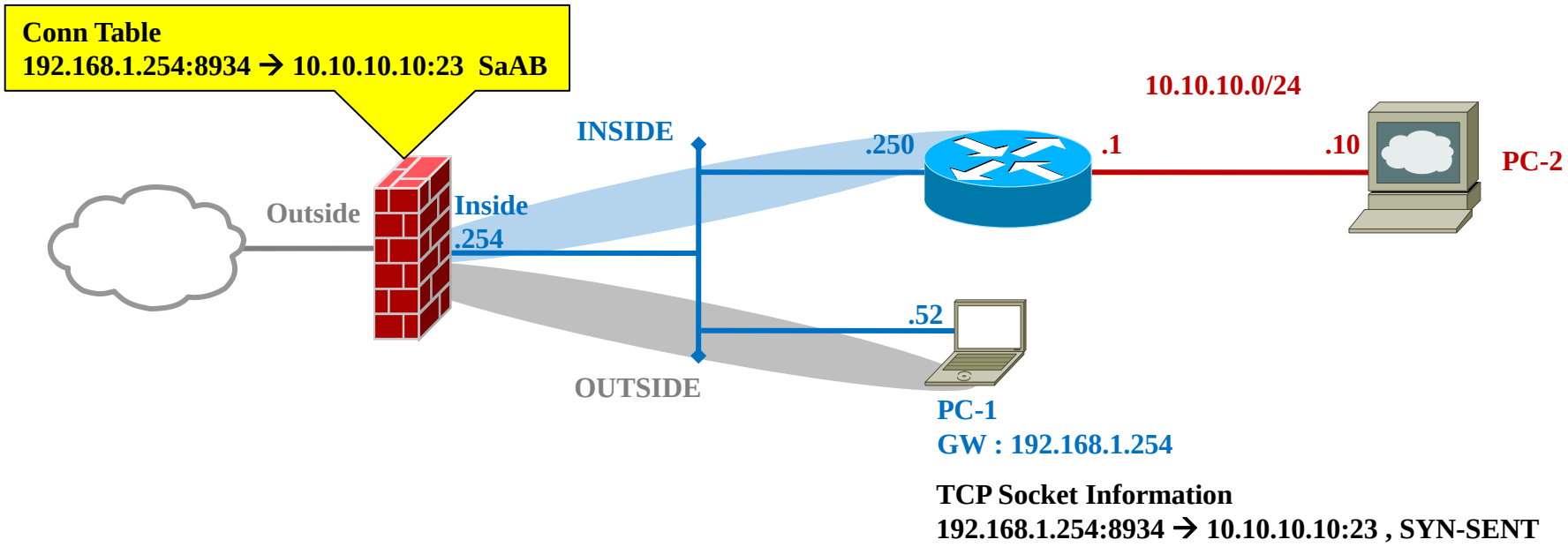
그건, 이렇게 제시해 드린 답변은 현상만을 보고 적용한 답변이어서, 문제의 본질을 살펴 보면 약간 다른 관점을 가질 수 있기 때문입니다. 그러니 지금 부터 나오는 내용도 꼭! 읽어보세요 ☺

PC-1에서 SYN을 보냄



자, 이제 PC-1이 3-way Handshake를 하기 위해 PC-2(10.10.10.10)으로 SYN 패킷을 보냅니다. 당연히 자기와 같은 IP 네트워크가 아니므로 Default gateway로 패킷을 보내겠죠?

ASA가 SYN을 받음

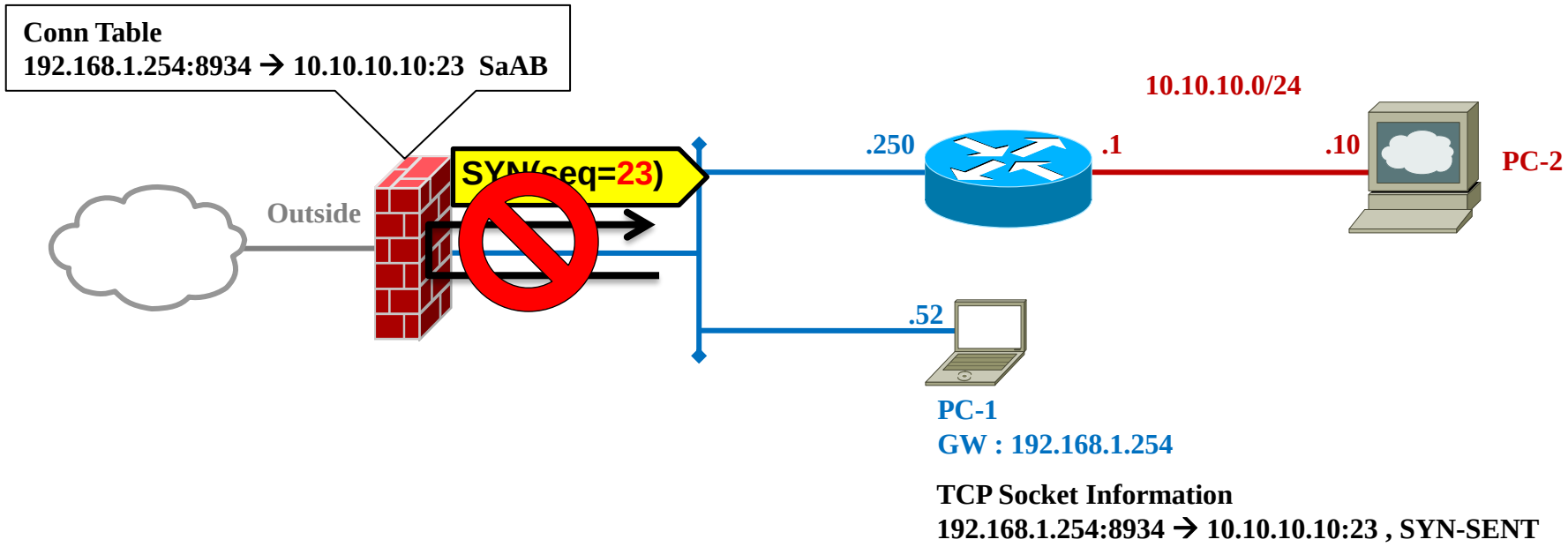


ASA는 받은 SYN 패킷을 근거로 Connection 테이블을 만들고 flag을 “SaAB”로 표기합니다.
벌써 어려울 지도 모르겠지만, 쉽게 설명 드리면 아래와 같은 내용이니까 찬찬히 살펴 보세요.

S : Inside에서 SYN이 오길 기다리고 있습니다 / a : Outside에서 ACK이 오길 기다리고 있습니다.
A : Inside에서 ACK이 오길 기다리고 있습니다 / B : 이 세션은 Outside에서 시작된 세션입니다.

자, 여기에서 “이 세션은 Outside하고는 전혀 관계가 없는데요?”라는 질문이 나올 수 있습니다.
ASA에서 Inside → Inside로 트래픽이 갈 때는 들어오는 방향이 논리적으로 Outside가 됩니다.
그림에서 회색으로 나타난 것 처럼 말이죠. ☺

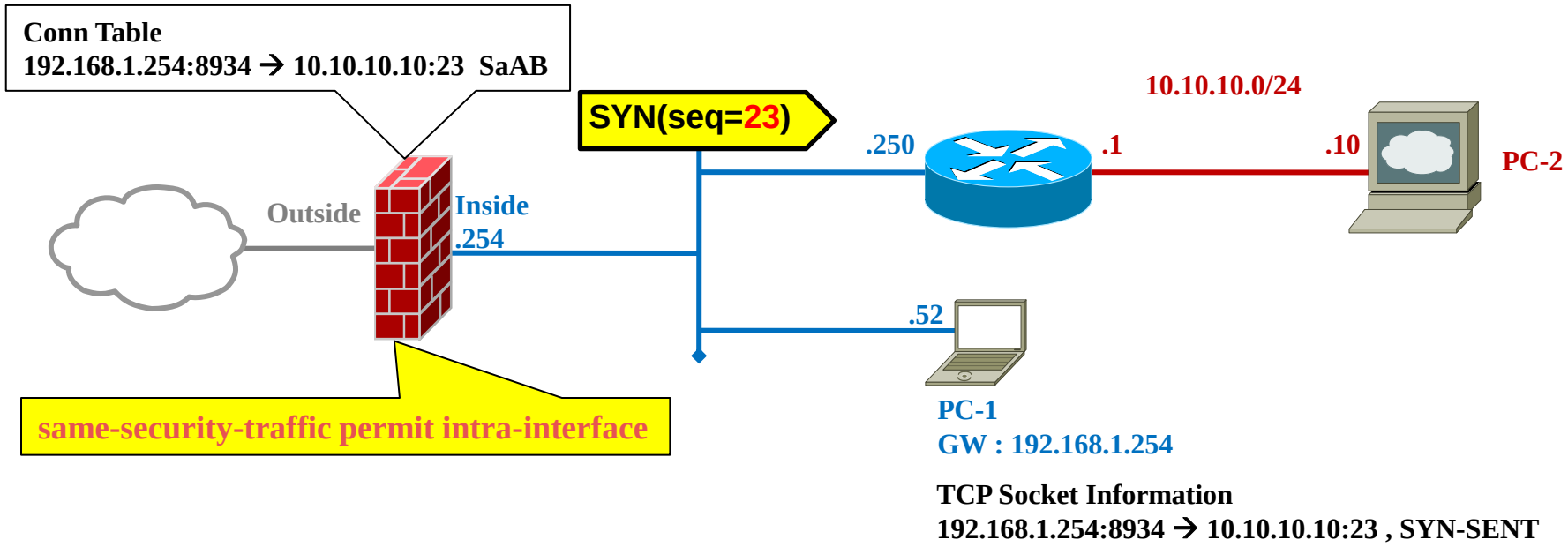
여기서 이 명령어가 필요합니다.
same-security-traffic permit intra-interface



앞 페이지 처럼 ASA에서 Connection Table은 만들어지지만, Default Configuraiton 만으로는 이런 Flow의 Packet이 통과 되지 않습니다.

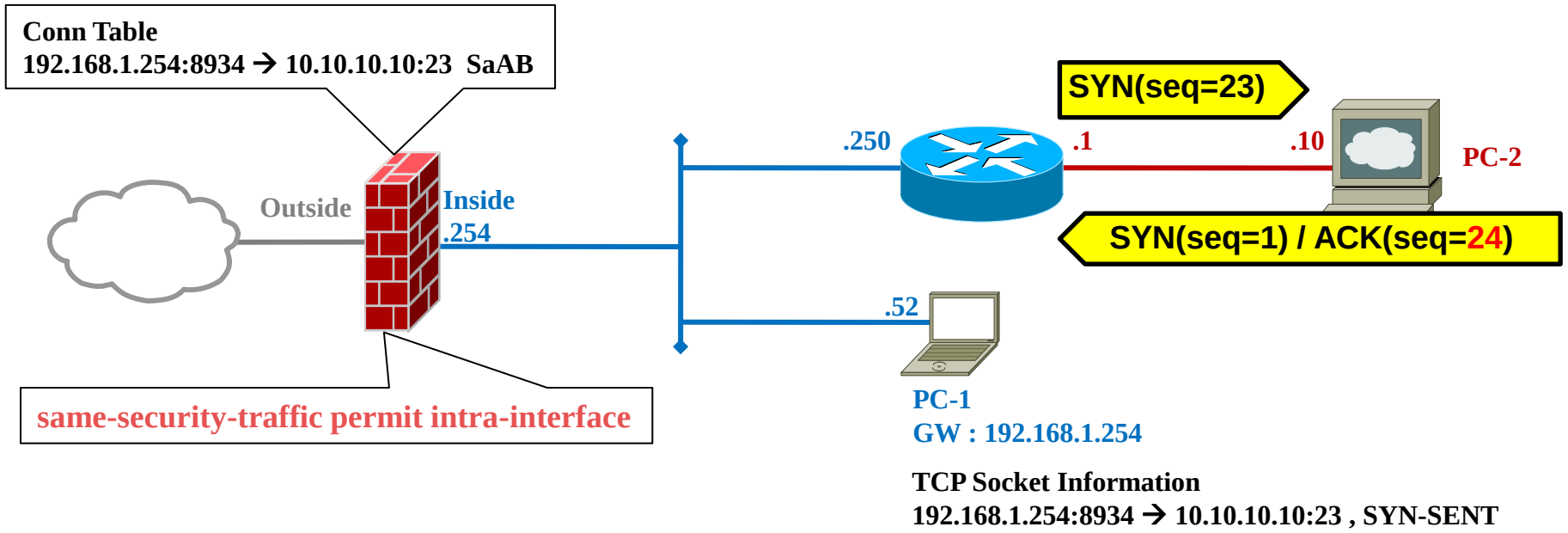
그래서 7.1 버전 부터는 IPSec 트래픽에 대해서만, 7.2 버전 부터는 모든 트래픽에대해 이런 Flow의 트래픽을 허용는 **`same-security-traffic permit intra-interface`** 명령어가 추가 되었습니다.

ASA가 SYN을 내보냄



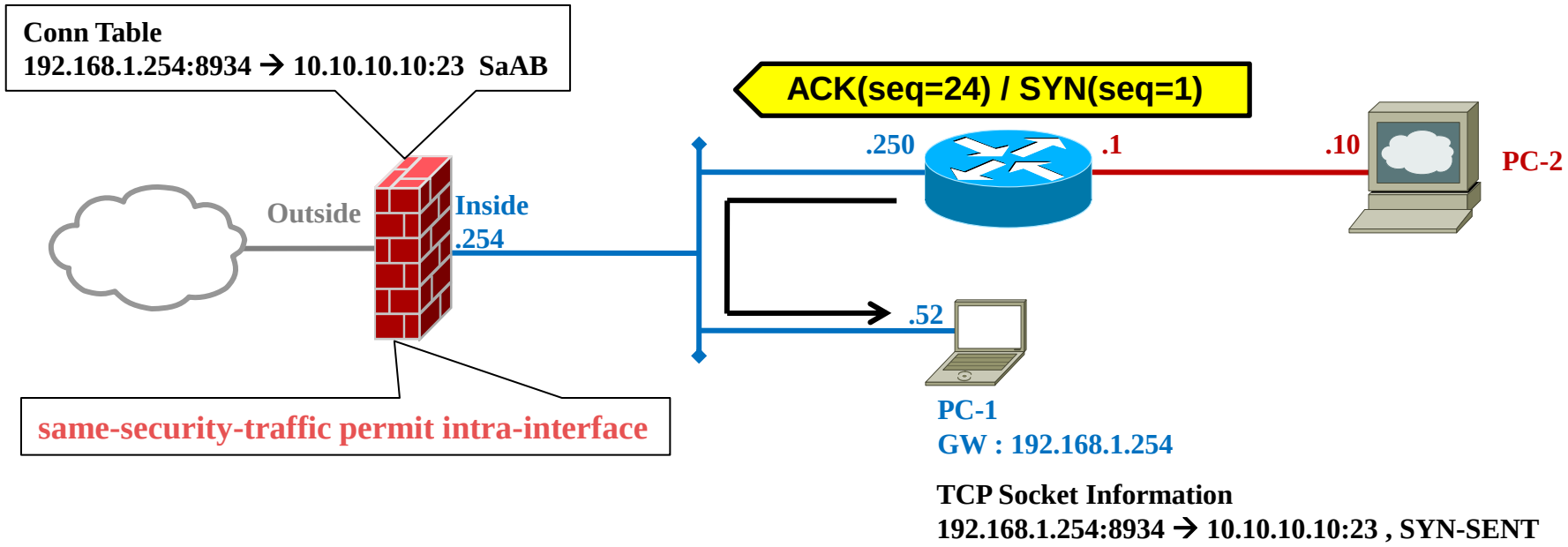
자 이제 ASA는 자체 Security Algorithm에 따라 Sequence number를 randomize한 후에 목적지 쪽으로 SYN을 보냅니다.

PC-2가 SYN을 받고 SYN/ACK를 보냄



이 SYN을 받은 PC-2는 SYN-ACK를 PC-1으로 보내게 됩니다.
이 때 사용하는 ACK의 Sequence 번호는 받은 “SYN+1”, 즉 24가 되지요.

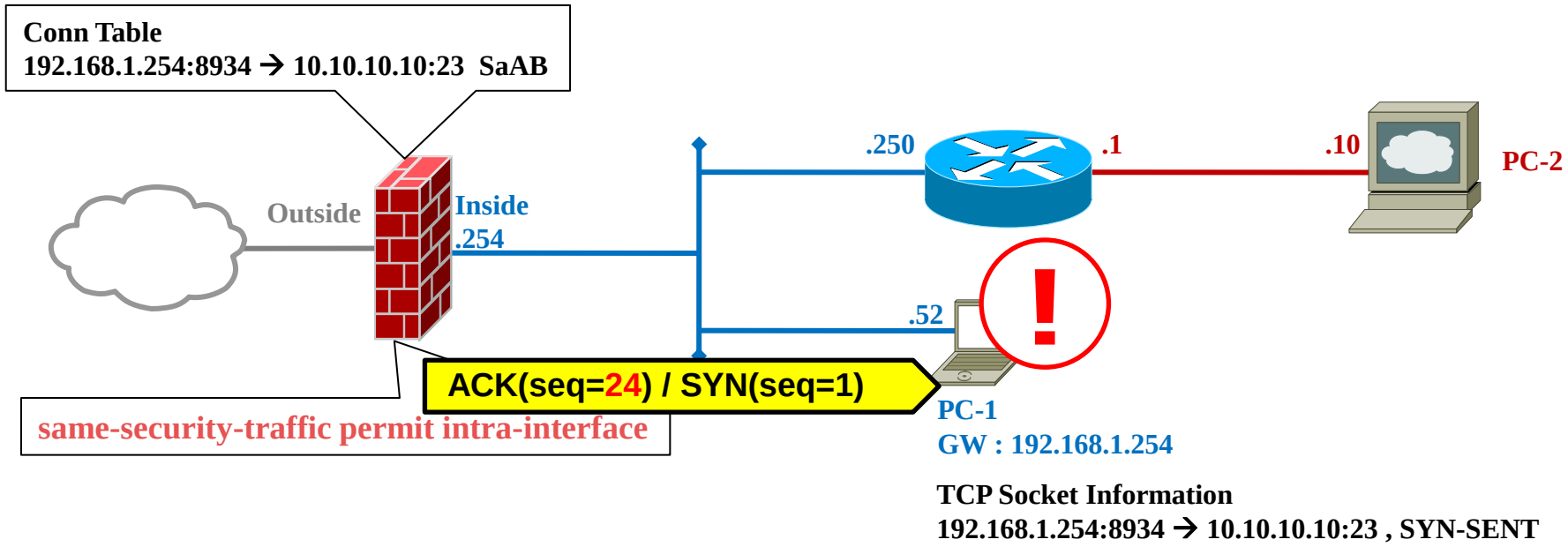
라우터는 이 패킷을 어디로 보낼까?



자, 여기서 가장 큰 문제가 발생을 합니다.

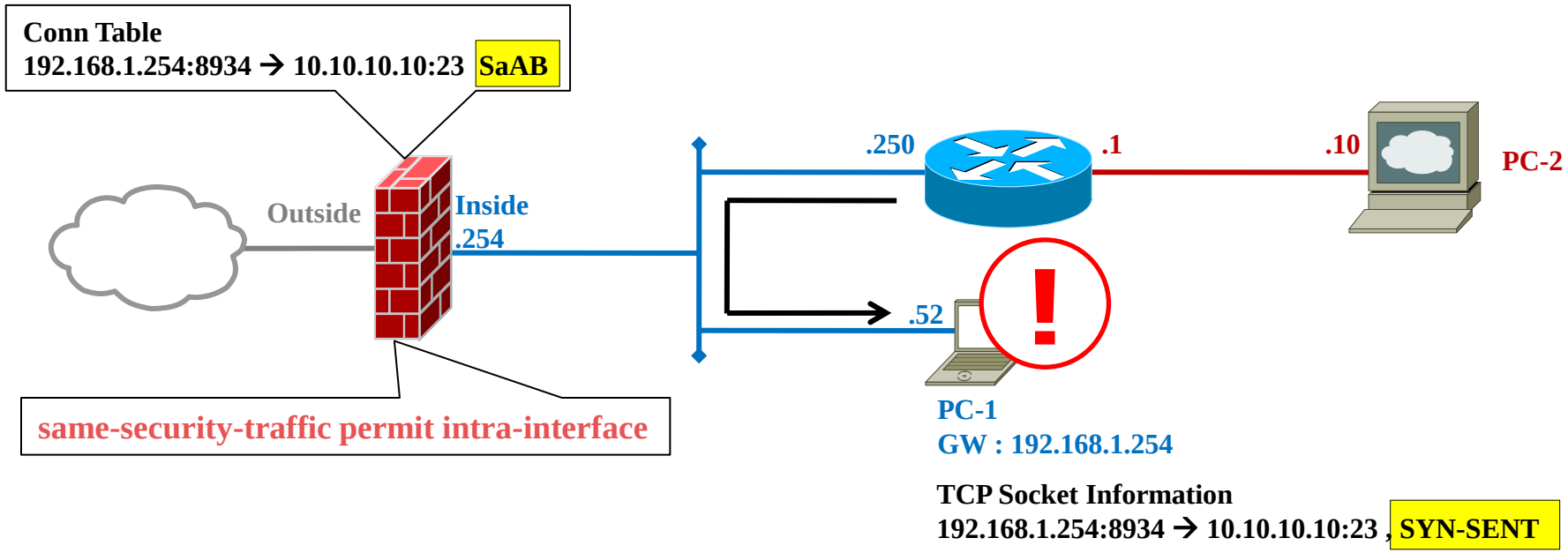
라우터의 .250 인터페이스는 PC-1과 같은 네트워크에 있기 때문에, 이 SYN/ACK 패킷을 ASA로 보내는 것이 아니라, 자기의 ARP Table을 참조하여 PC-1으로 바로 보내게 됩니다.

PC-1 曰 “Sequence 번호가 왜 이러지?”



PC-1이 SYN/ACK를 받기는 했지만, 받은 ACK의 Sequence 번호가 기다리던 값(=2)이 아니기 때문에 이 SYN-ACK를 무시하게 되는 것입니다. 그러니 PC-1이 마지막 ACK를 보낼 리도 없지요?

PC-1 曰 “Sequence 번호가 왜 이러지?”

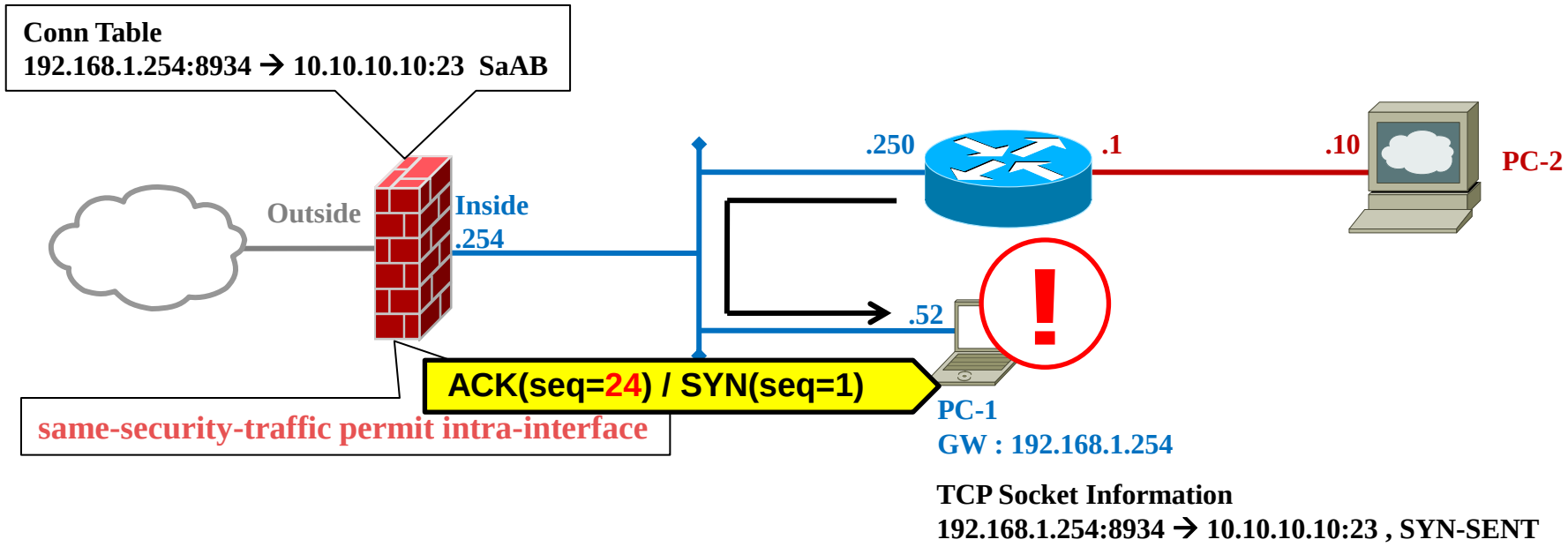


“그걸 어떻게 알 수 있나요?”라고 질문을 하신다면..? 무려 두 군데서나 확인할 수 있습니다.

일단 ASA에서 “show conn”을 쳐 보면 여전히 SaAB로 남아 있는 걸 알 수 있습니다.
만약 PC-1이 ACK를 보냈다면 Flag이 SaAB가 아니라 SAB 이어야 할 겁니다.(7페이지의 Flag 설명 참고)

그리고 PC-1에서 netstat로 보면 이 TCP Socket 의 state가 SYN-SENT로 남아 있습니다.
만약 ACK를 보냈다면 Established로 되어 있어야 하죠?

PC-1 曰 “Sequence 번호가 왜 이러지?”



결국 ASA에서 TCP-State Bypass를 적용하더라도 PC-1이 Sequence 번호가 다른 SYN/ACK를 무시하고 ACK 자체를 안 보내 버리면 결국 아무런 데이터도 보내지지 않을 것이고,
사용자 입장에서는 통신이 안 되는 것 처럼 보이겠죠.

그런데 TCP-State Bypass를 적용하면 이 문제를 해결할 수 있다는 4페이지의 설명은 뭘까요?

그것은 TCP-State Bypass가 하는 일이 단순히 TCP-State를 무시하고 트래픽을 전달하는 것 이외에
중요한 몇가지 기능이 더 있기 때문입니다. 다음 페이지를 볼까요?

TCP-State Bypass가 하는 일

ASA 8.2 Command Reference

http://www.cisco.com/en/US/docs/security/asa/asa82/command/reference/s1.html#wp1420119

Unsupported Features

The following features are not supported when you use TCP state bypass:

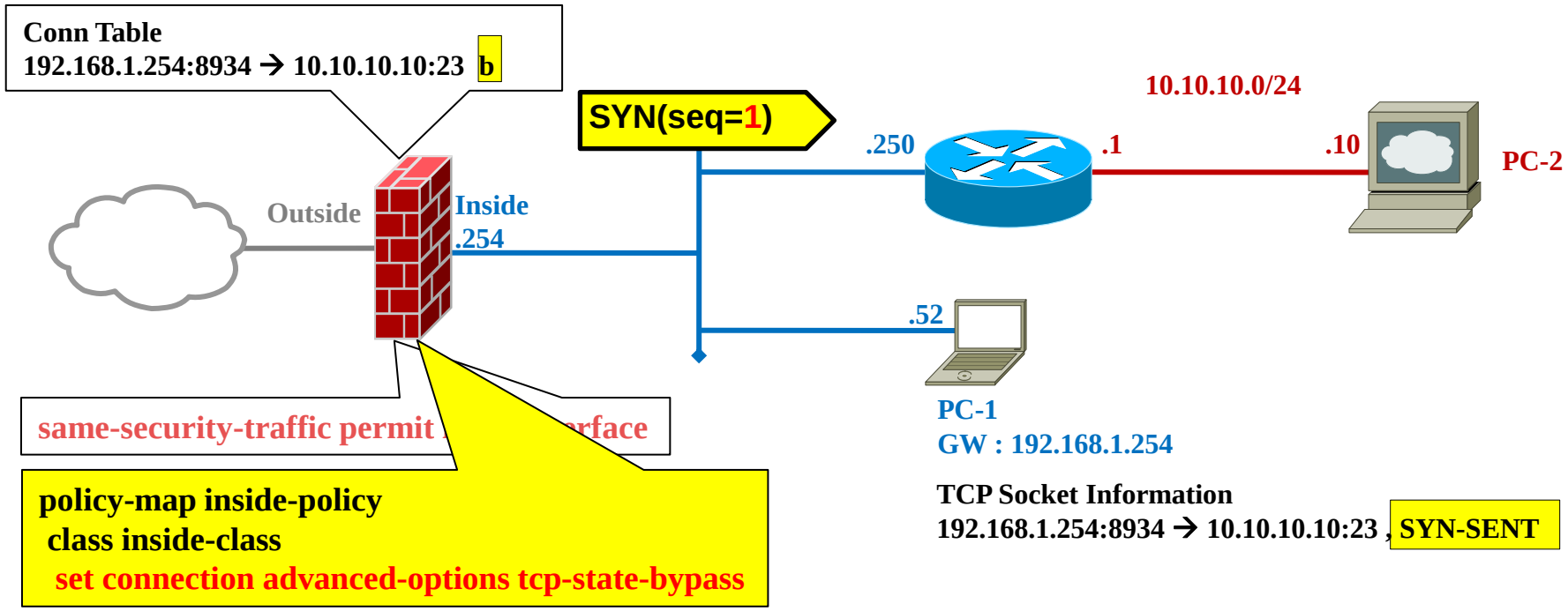
- Application inspection—Application inspection requires both inbound and outbound traffic to go through the same adaptive security appliance, so application inspection is not supported with TCP state bypass.
- AAA authenticated sessions—When a user authenticates with one adaptive security appliance, traffic returning via the other adaptive security appliance will be denied because the user did not authenticate with that adaptive security appliance.
- TCP Intercept, maximum embryonic connection limit, TCP sequence number randomization—The adaptive security appliance does not keep track of the state of the connection, so these features are not applied.
- TCP normalization—The TCP normalizer is disabled.
- SSM functionality—You cannot use TCP state bypass and any application running on an SSM, such as IPS or CSC.

위의 Command Reference를 자세히 들여다 보면, TCP-State Bypass를 적용할 때 지원하지 않는 기
몇 가지가 있는데, 그 중에 “TCP sequence number randomization”이 있습니다.

즉 9페이지에서 SYN의 Sequence number가 23으로 바뀌지 않고 그대로 1로 간다는 것이죠.

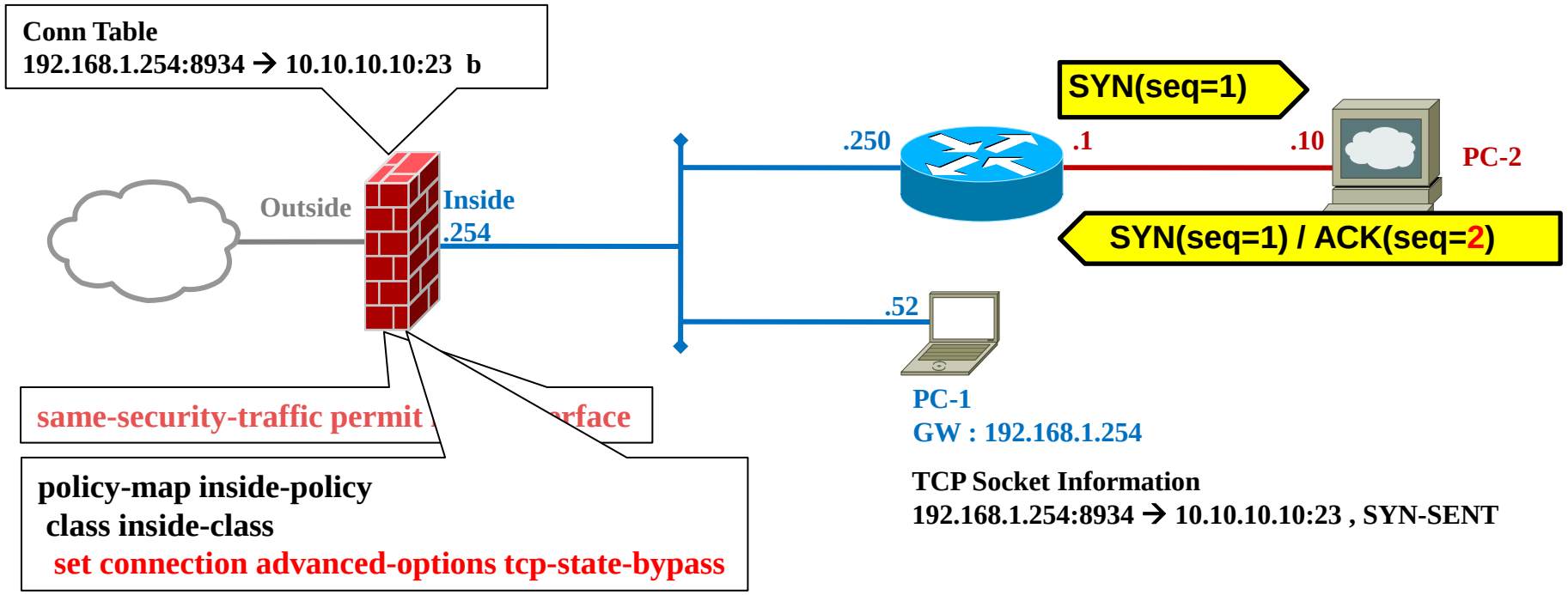
따라서 , 10페이지 SYN/ACK 패킷의 ACK Sequence 번호가 “2”로 되기 때문에
12페이지에서 PC-1이 이 SYN/ACK를 Asymmetric하게 받더라도 문제없이 ACK를 보낼 수 있게 됩니
그럼 이 TCP-State Bypass를 적용하면 정말로 어떻게 되는 지 한 번 볼까요?

ASA가 SYN을 내보냄



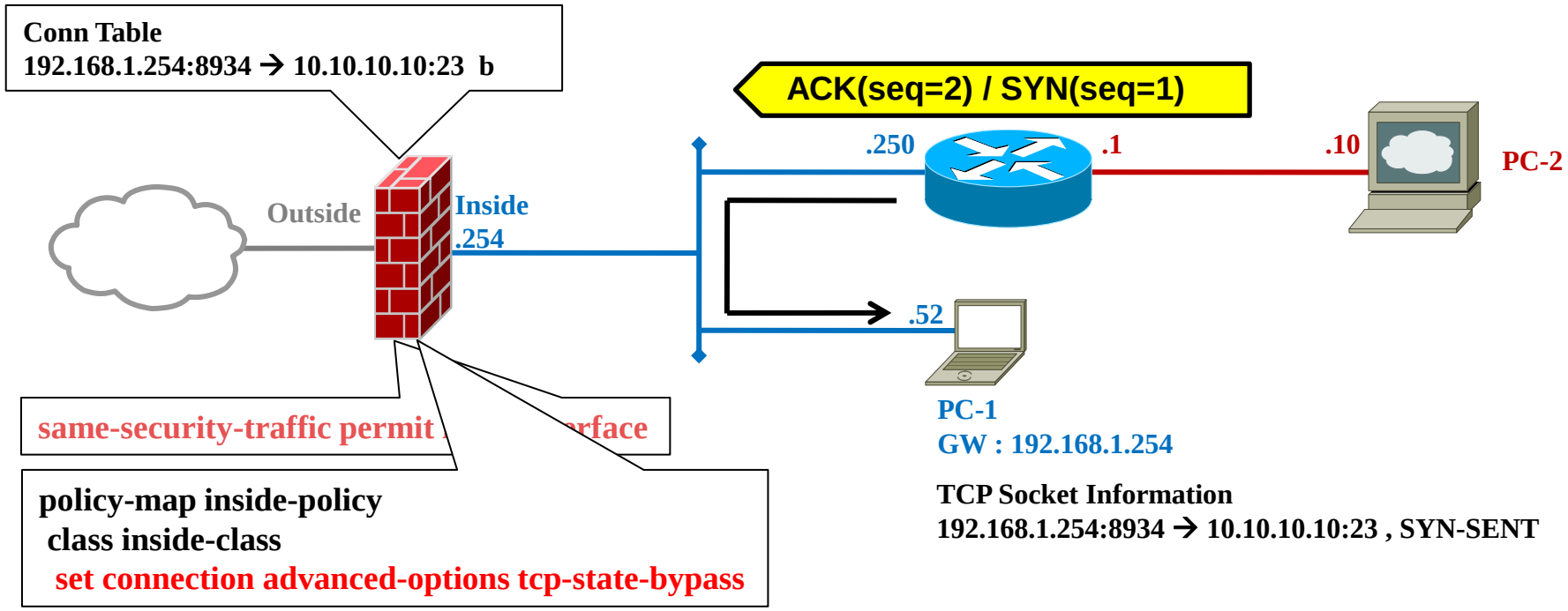
자, 이제 ASA는 Sequence number를 randomize하지 않은 원래의 번호(1)로 SYN을 보내줍니다. 그리고 이 Connection의 Flag는 “b”로 표기합니다.(8.2에서 추가된 Flag)

PC-2가 SYN을 받고 SYN/ACK를 보냄



이 SYN을 받은 PC-2는 마찬가지로 SYN-ACK를 PC-1으로 보내게 됩니다. 이 때 사용하는 ACK의 Sequence 번호는 “받은 SYN의 Sequence 번호+1” 즉 2가 되지요.

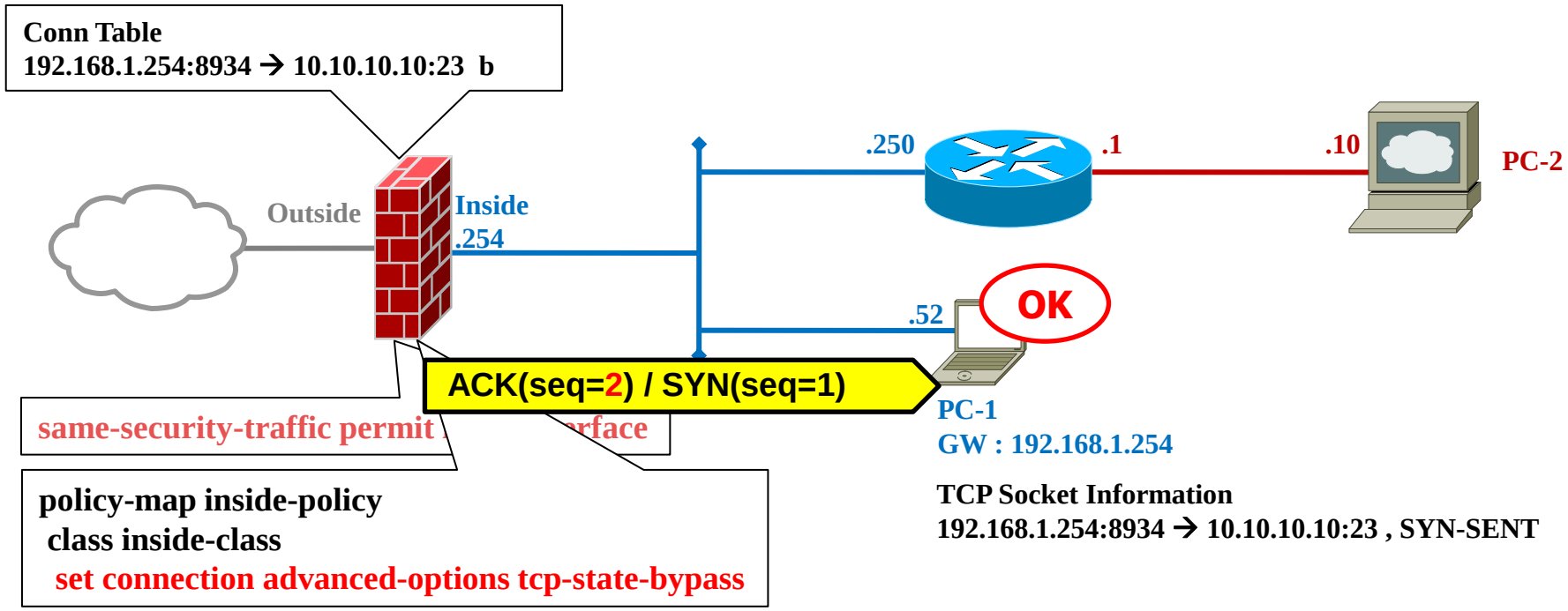
라우터는 이 패킷을 어디로 보낼까?



자, 그래도 라우터가 이 SYN/ACK를 곧바로 PC-1으로 보내는 문제는 어떻게 해결을 할 수가 없습니

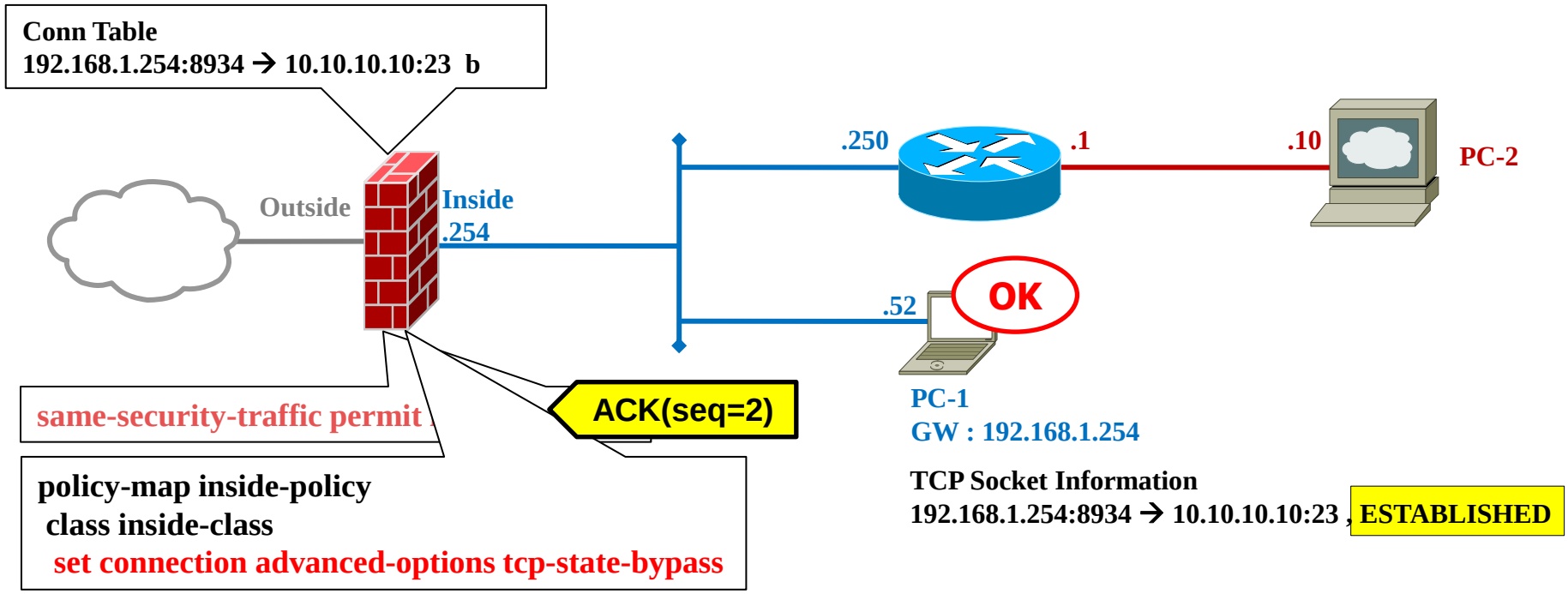
그럼 이 TCP-State Bypass가 이 문제를 어떻게 해결하는 지 계속 살펴 보겠습니다.

PC-1이 정상적인 SYN/ACK를 받음



PC-1이 SYN/ACK를 받고 보니 ACK의 Sequence 번호가 기다리던 “2”네요.

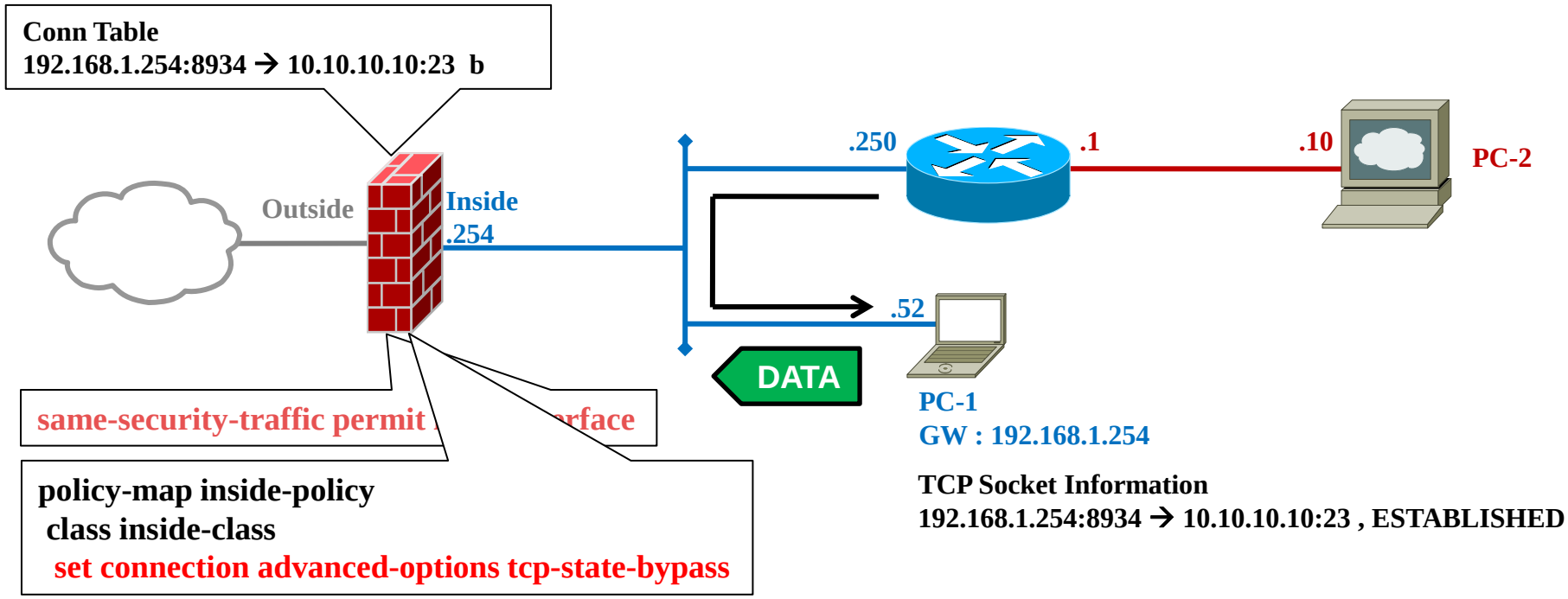
PC-1이 3-way Handshake를 완료함



이제 PC-1은 앞서 받은 SYN/ACK 중에 SYN의 Sequence 번호인 “1”에 1을 더해서 ACK를 보내게 됨
PC-1 입장에서는 3-way Handshake가 끝났기 때문에, Socket 정보가 Established로 바뀌었습니다.

ASA는 이 Connection에 TCP-State Bypass가 적용되어 있기 때문에(즉 TCP의 State는 보지 않고 IP:Port number만 보기 때문에) 이 ACK를 그대로 전달합니다.

PC-1이 데이터를 전송하기 시작함



이제 PC-1는 실제로 Data를 전송하게 됩니다. 이 Data 패킷을 받은 ASA는 이 Connection에 대해 TCP-State Bypass가 적용되어 있기 때문에(Flag “b”) 이제는 Connection의 상태에 관계 없이 ACL에만 허용이 되어 있다면 해당 트래픽을 통과를 시켜 줍니다.

이것이 ASA/FWSM 만의 Issue일까요?

지금까지의 내용을 잘 이해하셨다면 앞서 발생한 Asymmetric Traffic Flow에 의한 문제가 비단 Cisco ASA나 FWSM에만 국한 되는 것이 아닌 것을 알아 채셨을 것입니다.

그 자리에 TCP Connection 정보를 관리하는 장비, 즉 Firewall, L4 Switch 등 L4~7에 해당하는 장비가 있는데, 이 “TCP-State Bypass” 같은 기능이 구현되어 있지 않다면 모두 마찬가지이지요.

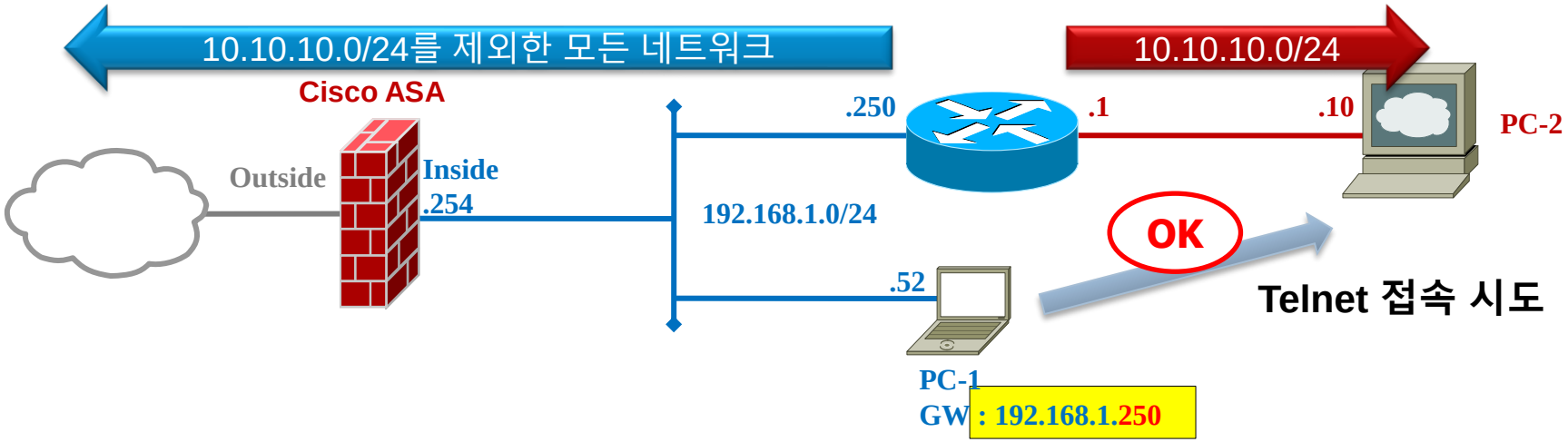
물론, ASA은 기본적으로 Sequence 번호를 Randomize하는 특성 때문에 이 “TCP-State Bypass”의 두가지 기능, 즉 “TCP Connection State와 관계 없이 트래픽을 통과 시키는 기능”과 “Sequence 번호 Randomize를 끄는 기능” 모두를 필요로 했지만,

다른 장비의 경우라도 최소한 “TCP Connection State와 관계 없이 트래픽을 시키는 기능”을 제공해야만 이 Asymmetric Traffic Flow Issue를 해결할 수 있습니다.

그럼 이런 문제는 근본적으로 어떻게 해결할 수 있을 까요?

두가지 방안을 생각해 볼 수 있는데, 뒤에서 각각 설명을 드리도록 하지요.

해결 방안 1.
PC-1의 Default Gateway를 라우터로 설정

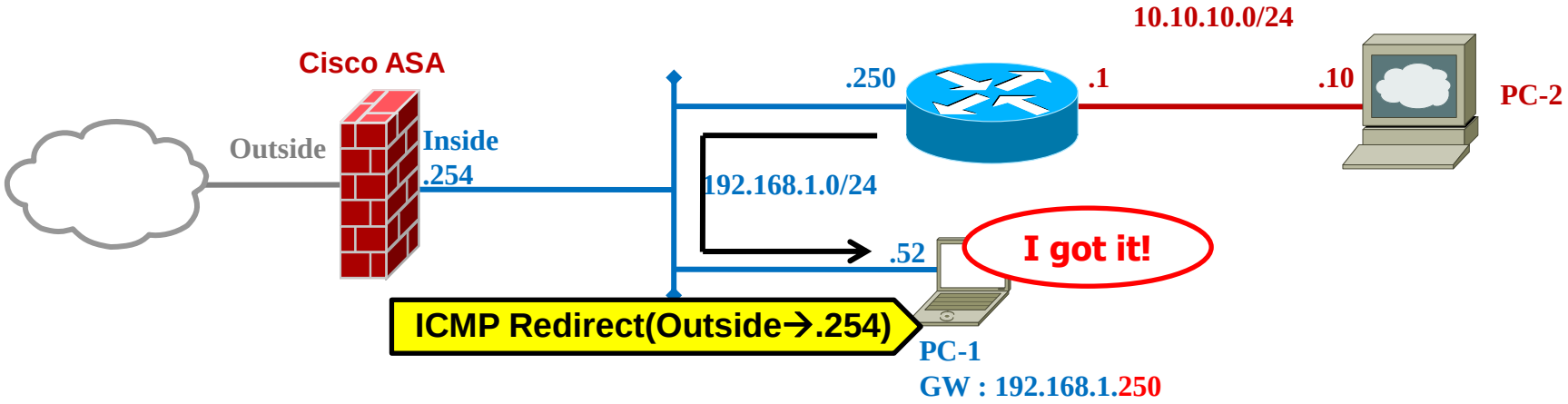


PC의 Default Gateway를 ASA가 아닌 Router로 잡아 주면 일단 모든 트래픽이 라우터로 향하게 되고
라우터가 Outside로 나갈 트래픽과 10.10.10.0/24로 가는 트래픽을 구분해서 보내주게 되니,

앞서 필요했던 same-security-traffic permit intra-interface 도 필요 없고,
TCP-State Bypass도 필요 없게 됩니다. 아주 간단하죠? ☺

그런데 여러분 중에 “그럼 Outside로 나가는 트래픽은 Hop을 두 번 거치게 되는 거 아닌가요” 하는 분이

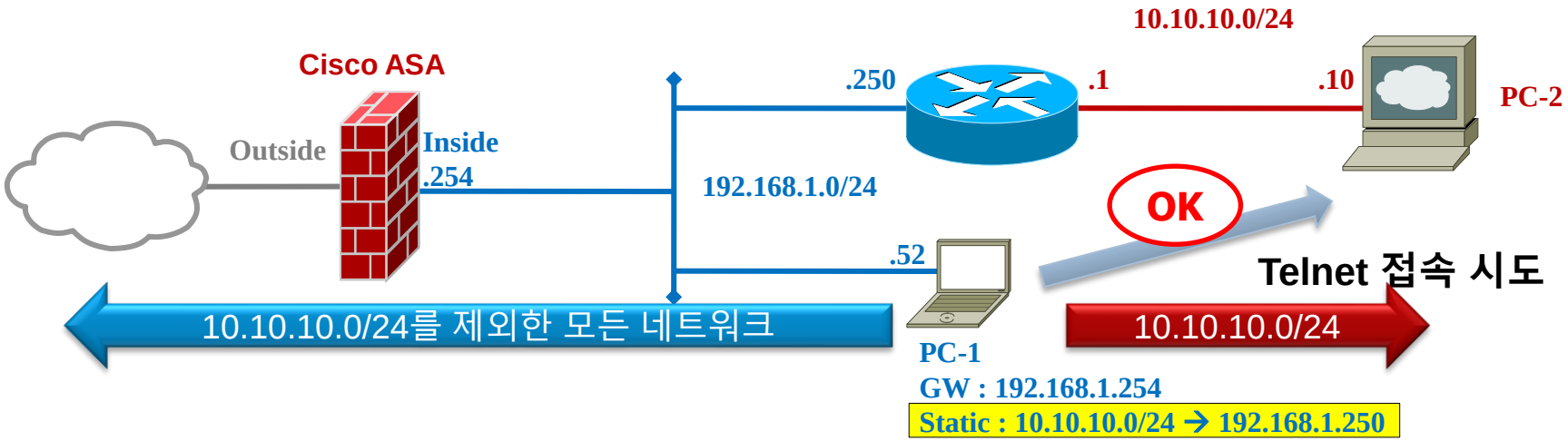
해결 방안 1.
PC-1의 Default Gateway를 라우터로 설정



PC-1이 Outside로 향하는 트래픽을 라우터로 보내면 친절한 라우터는(친절한 금자씨..?) ICMP 패킷에
Redirect 메시지를 넣어서 “헬로 Mr. PC-1, 앞으로 Outside로 트래픽을 보낼 때는 나한테 보내지 말고
192.168.1.254로 보내세요~”라고 전해 줍니다.

이 ICMP Redirect 메시지를 받은 PC-1은 앞으로 Outside로 트래픽을 보낼 때 .250으로 보내는 것이 아니라 .254, 즉 ASA로 보내게 됩니다.

해결 방안 2.
PC-1의 라우팅 테이블을 조정



그래도 좀 찜찜하다 하시는 분들은 아예 PC-1의 라우팅 테이블을 손 봐 주시면 됩니다.

Command 창에서 `route -p add 10.10.10.0 mask 255.255.255.0 192.168.1.250` 를 입력해 주시면 되죠? (-p 옵션은 PC-1을 껐다가 켜더라도 이 라우팅 정보가 남아 있게 하는 거구요)

이 방법도 PC-1에서 PC-2로 패킷을 보낼 때 ASA를 통하지 않도록 할 수 있지만, PC-1 같은 애들이 무쟈게 많다면… 음… 한 번 쯤 고려 해 봐야 하겠죠? ☺