M02-05 · GIBALJA VISUAL MANUAL

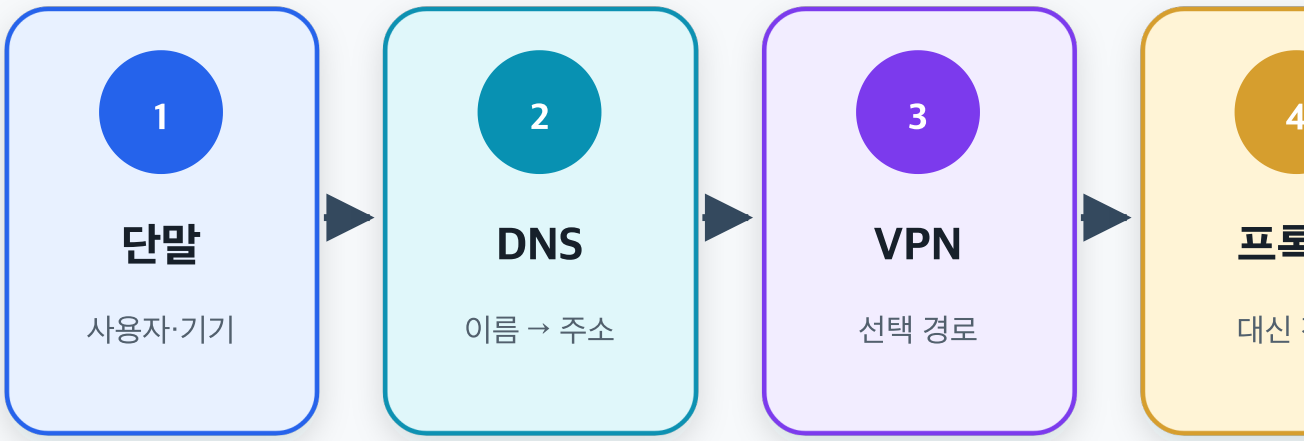
방화벽·VPN·프록시·망 분리 이해하기

한 문장 목표: 접속 문제를 출발 위치·목적지·DNS·VPN·프록시·방화벽·서버·권한의 흐름으로 그리고, 첫 실패 지점과 필요한 허용 조건을 증거로 설명합니다.

난이도	개념	실습	셀프 테스트	최종 산출물
Level 1	55분	50분	15분	접속 경로도, 연계 조건 점검표, 네트워크 문의 증거 묶음

"사내에서는 되는데 집에서는 안 돼요"를 장애 설명으로 끝내지 않습니다. 같은 주소가 어느 경계를 지나며, 어디까지 성공했고, 어떤 정책 조건에서 달라졌는지를 한 장의 경로로 바꿉니다.

그림 1. 접속 성공은 단말부터 업무 권한까지 여러 경계를 모두 통과한 결과입니다.



첫 실패 지점을 찾는 질문

이름을 찾았는가 → 경로가 있는가 → 중간 정책을 통과했는가 → 서버가

응답했는가 → 사용자가 허용됐는가

1. 이 PDF를 공부하는 방법

1회차 · 경로만 말하기 · 15분

그림 1을 보며 `단말 → DNS → VPN → 프록시 → 방화벽 → 서버 → 권한`을 소리 내어 읽습니다. 모든 접속이 일곱 단계를 그대로 거치는 것은 아니지만, 빠진 단계가 무엇인지 설명할 수 있어야 합니다.

2회차 · 역할 구분하기 · 25분

DNS·라우터·NAT·VPN·프록시·방화벽이 각각 대답하는 질문을 한 문장으로 적습니다. 한 장비가 여러 역할을 수행해도 개념은 나누어 봅니다.

3회차 · 시뮬레이터로 첫 실패 찾기 · 30분

VPN 없음, 프록시 인증 실패, 방화벽 차단, 애플리케이션 403 시나리오를 실행하고 첫 실패 지점을 기록합니다.

4회차 · 실제 접속 증거 만들기 · 35분

공개 시험 주소의 200·403·DNS 실패를 관찰하고, 현재 출발 망·VPN·프록시 조건과 정확한 오류 문구를 비교표에 적습니다.

5회차 · 셀프 테스트 · 15분

정답을 가리고 10문제를 풉니다. 틀린 문제는 관련 경로 그림에 오류 문구를 직접 올려 봅니다.

학습 완료 기준

“접속 안 됨”을 그대로 전달하지 않고, 출발 망·목적지 FQDN·프로토콜·포트·VPN·프록시·첫 실패 문구·비교 결과를 한 문장과 표로 만들 수 있습니다.

2. 같은 주소가 환경마다 다른 이유

웹 주소가 같아도 요청이 출발하는 위치와 중간 경계가 다르면 결과가 달라집니다.

그림 2. 집·VPN·사무실·핫스팟의 비교 결과는 서비스 자체보다 접속 경로와 정책을 먼저 보게 합니다.

집·VPN 없음

실패

api.intra.example:443

사내 경로 없음

시각·IP·오류 문구 기록

집·VPN 연결

성공

api.intra.example:443

터널·정책 통과

시각·IP·오류 문구 기록

비교 결론

VPN 연결 여부와 출발 망에 따라 결과가 달라졌으므로, 서비스 장애ㄴ

사무실 업무망

성공

api.intra.example:443

내부 경로

시각·IP·오류 문구 기록

모바일 핫스팟

실패

api.intra.example:443

외부망 조건

시각·IP·오류 문구 기록

ㄹ다 접속 경로·정책을 먼저 확인한다.

달라지는 조건	예시	결과에 미치는 영향
출발 망	사내 업무망·집·모바일 핫스팟	사용할 DNS·라우팅·보안 정책이 달라짐
단말	관리 PC·개인 PC·모바일	인증서·보안 에이전트·접속 허용 여부가 달라짐
사용자	직원·협력사·관리자	애플리케이션·VPN·프록시 권한이 달라짐
VPN	미연결·전체 터널·분할 터널	사내 사설 주소로 가는 경로가 달라짐
프록시	자동 설정·수동 설정·인증 실패	외부 웹 요청의 중계와 차단 정책이 달라짐
방화벽	출발·목적지·포트·방향 정책	같은 서버라도 특정 흐름만 허용
서비스	정상·점검·포트 미수신	연결 거부·시간 초과·5xx가 달라짐
업무 권한	역할·조직·자원 정책	네트워크 성공 뒤에도 401·403 가능

비교가 강한 증거인 이유

한 번의 실패에는 여러 원인이 섞입니다. 한 조건만 바꾸면 원인 후보가 줄어듭니다.

- 같은 단말, VPN만 끔·켬
- 같은 VPN, 공개 API와 사내 API 비교
- 같은 주소, 본인과 동료의 결과 비교
- 같은 사용자, 사무실과 외부망 비교

BIG IDEA 01

접속 문제는 장비 목록이 아니라 “어떤 조건을 바꾸었더니 결과가 달라졌는가”로 좁힙니다.

30초 확인

사무실에서는 사내 API가 열리고 집에서는 안 열리지만, 집에서 VPN을 연결하면 열립니다. 가장 먼저 어느 범주를 확인해야 할까요?

정답 보기

서비스 전체 장애보다 외부망에서 사내망으로 들어오는 VPN 경로·라우팅·접속 정책을 먼저 확인합니다. VPN 연결만으로 원인을 확정하지는 않고 할당 IP와 목적지 경로도 기록합니다.

3. 접속 경로의 여섯 역할을 구분합니다

그림 3. 각 역할은 접속 과정에서 서로 다른 질문에 답합니다.

NAME

DNS

이 이름은 어느 주소인가?

ROUTE

라우터

다음 홉은 어느 길인가?

TUNNEL

VPN

보호된 원격 경로를 만들까?

FORWARD

프록시

누구를 대신해 전달할까?

TRANSLATE

NAT

주소·포트를 무엇으로 바꿀까?

POLICY

방화벽

이 흐름을 허용할까?

역할	한 문장 질문	하지 않는 일
DNS	이 이름은 어느 IP 주소인가	목적지까지 경로와 권한을 보장하지 않음
라우터	이 목적지로 가려면 다음에 어디로 보낼까	업무 사용자를 인증하지 않음
NAT	내부 주소·포트를 외부 주소·포트로 어떻게 바꿀까	NAT 자체가 곧 방화벽 정책은 아님
VPN	외부 단말과 조직 자원 사이에 보호된 원격 경로를 만들까	모든 자원 권한을 자동 부여하지 않음
프록시	클라이언트나 서버를 대신해 요청을 어디로 전달할까	모든 네트워크 흐름을 반드시 중계하지 않음
방화벽	이 출발·목적지·프로토콜·포트 흐름을 허용할까	서버 애플리케이션의 업무 권한까지 판단하지 않음

한 장비, 여러 역할

가정용 공유기는 라우팅·NAT·DNS 전달·기본 방화벽을 함께 수행할 수 있습니다. 기업 보안 장비는 방화벽·VPN 게이트웨이·프록시 기능을 함께 제공할 수 있습니다.

따라서 “어느 박스인가”보다 다음을 기록합니다.

1. 이 단계에서 입력으로 보는 정보
2. 허용·변환·전달 중 어떤 판단을 하는지
3. 성공했을 때 다음 홉이 어디인지
4. 실패했을 때 어떤 로그와 문구가 남는지

장비와 서비스 구분

방화벽·프록시·VPN은 물리 장비일 수도 있고 소프트웨어·클라우드 서비스일 수도 있습니다. 그림의 상자는 물리적 개수보다 **논리적 역할**을 뜻합니다.

4. DNS·사설 IP·라우팅을 먼저 봅니다

4.1. DNS 성공은 접속 성공이 아닙니다

DNS가 이름을 IP로 바꾸어도 그 주소까지 갈 경로가 없거나 포트가 막힐 수 있습니다.

```
api.intra.example → 10.20.30.40
```

이름 해석은 성공했지만 `10.20.30.40`은 사설 주소이므로 인터넷에서 직접 도달할 수 없습니다. 사내망이나 승인된 VPN·전용 경로가 필요할 수 있습니다.

4.2. 사설 IPv4 주소

RFC 1918은 다음 범위를 사설 인터넷용으로 정합니다.

범위	CIDR 표기	흔한 사용
`10.0.0.0` ~ `10.255.255.255`	`10.0.0.0/8`	큰 조직·클라우드 내부망
`172.16.0.0` ~ `172.31.255.255`	`172.16.0.0/12`	조직·컨테이너·클라우드 내부망
`192.168.0.0` ~ `192.168.255.255`	`192.168.0.0/16`	가정·소규모 네트워크

사설 주소는 보안 등급을 뜻하지 않습니다. 전 세계 여러 조직이 같은 주소를 재사용할 수 있고, VPN을 연결할 때 집과 회사 주소 대역이 겹치면 경로 충돌이 생길 수 있습니다.

4.3. 라우팅과 다음 홉

라우팅 표는 목적지 주소 범위마다 다음에 보낼 인터페이스와 게이트웨이를 정합니다.

```
목적지 10.20.0.0/16 → VPN 인터페이스
그 밖의 목적지      → 기본 인터넷 게이트웨이
```

VPN 아이콘이 연결 상태여도 사내 목적지 대역이 라우팅 표에 없으면 도달하지 못할 수 있습니다.

4.4. NAT는 주소 변환입니다

NAT(Network Address Translation)는 한 주소 영역의 IP를 다른 영역의 IP로 바꿉니다. NAPT는 IP와 TCP·UDP 포트를 함께 바꾸어 여러 내부 단말이 하나의 외부 주소를 공유하도록 할 수 있습니다.

NAT가 있다는 사실만으로 인바운드·아웃바운드 허용 여부를 확정하지 않습니다. 변환 규칙과 방화벽 정책을 따로 확인합니다.

읽는 순서: 이름이 풀리는가 → 받은 IP가 어느 주소 영역인가 → 목적지 대역의 경로가 있는가 → 다음 경계가 무엇인가.

5. VPN은 보호된 원격 경로를 만듭니다

가상 사설망(Virtual Private Network, VPN)은 외부 네트워크를 지나 조직 자원에 원격 접속할 수 있도록 보호된 통신 경로를 구성합니다. 실제 허용 범위는 VPN 제품·프로필·사용자·단말·조직 정책에 따라 달라집니다.

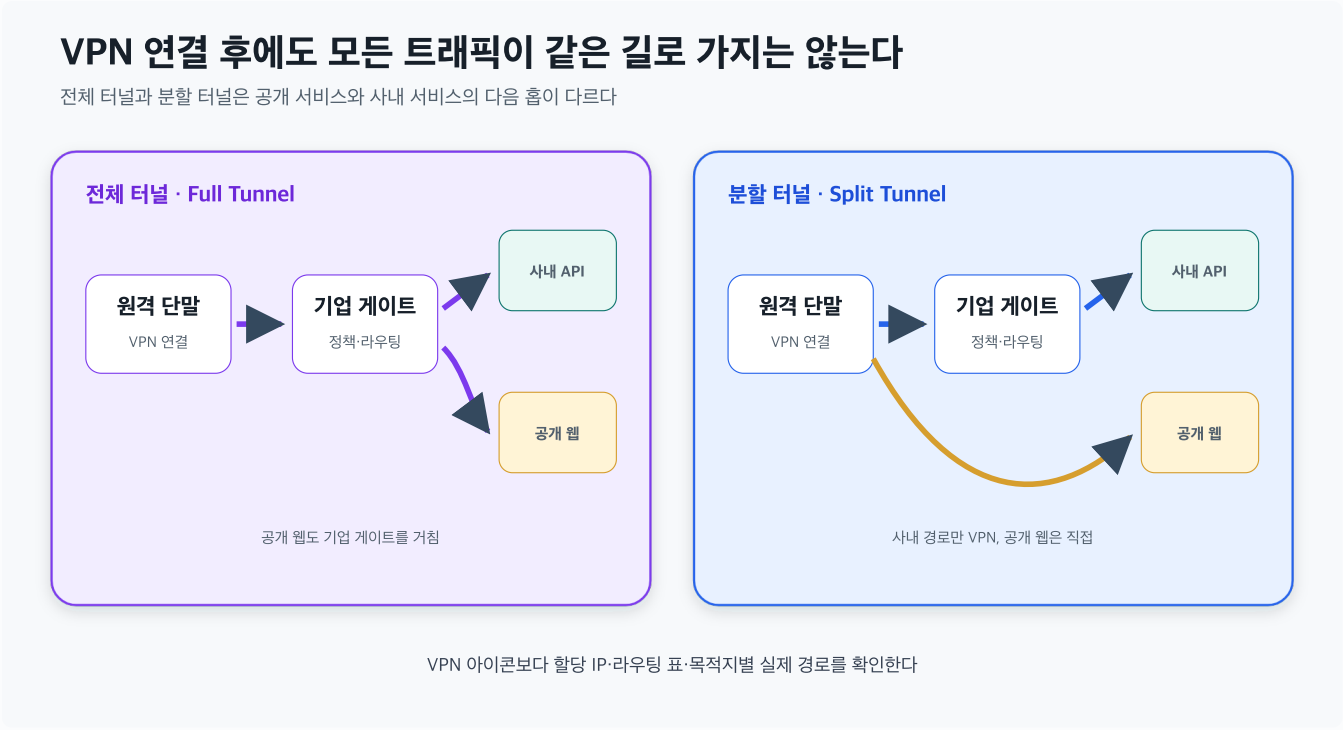
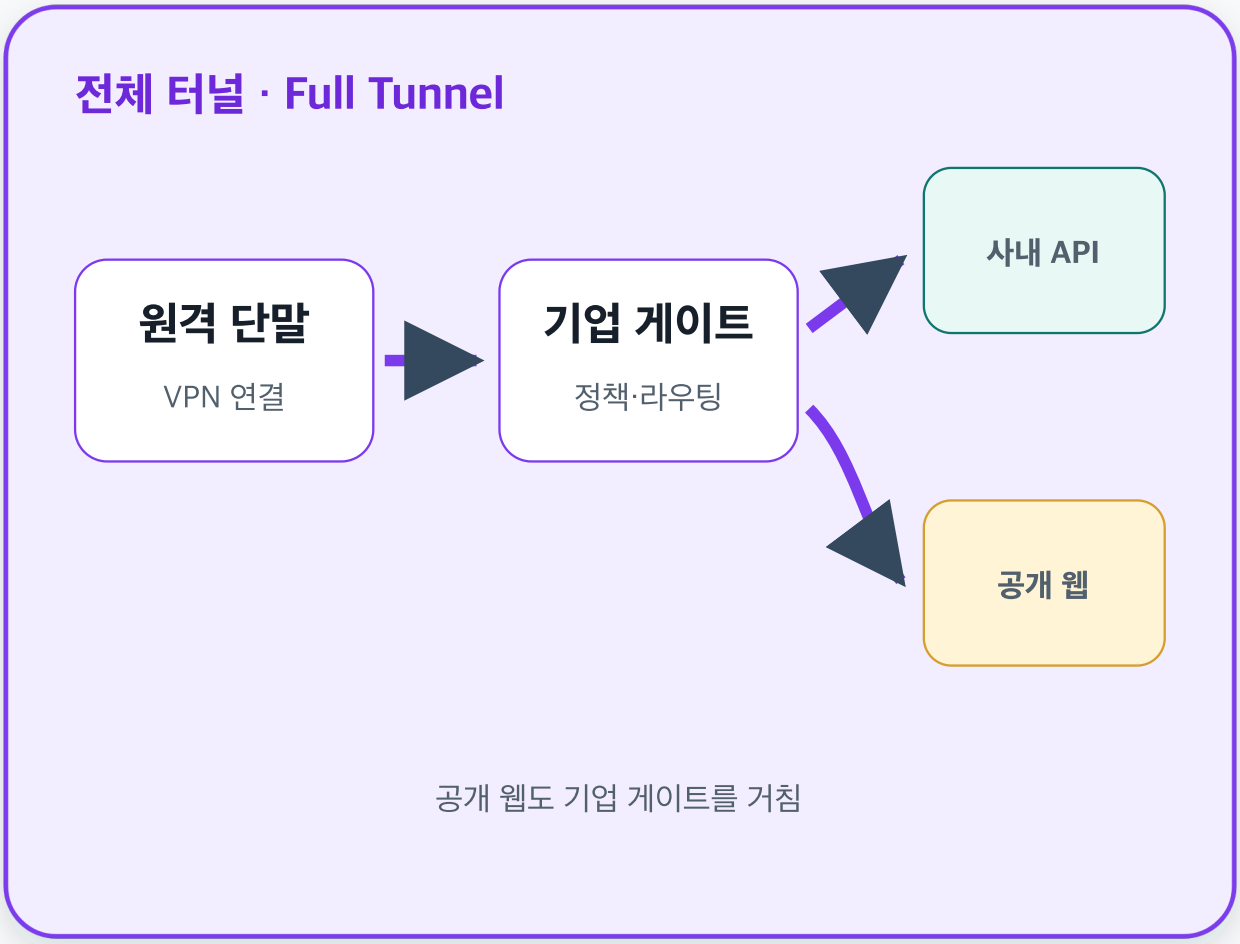
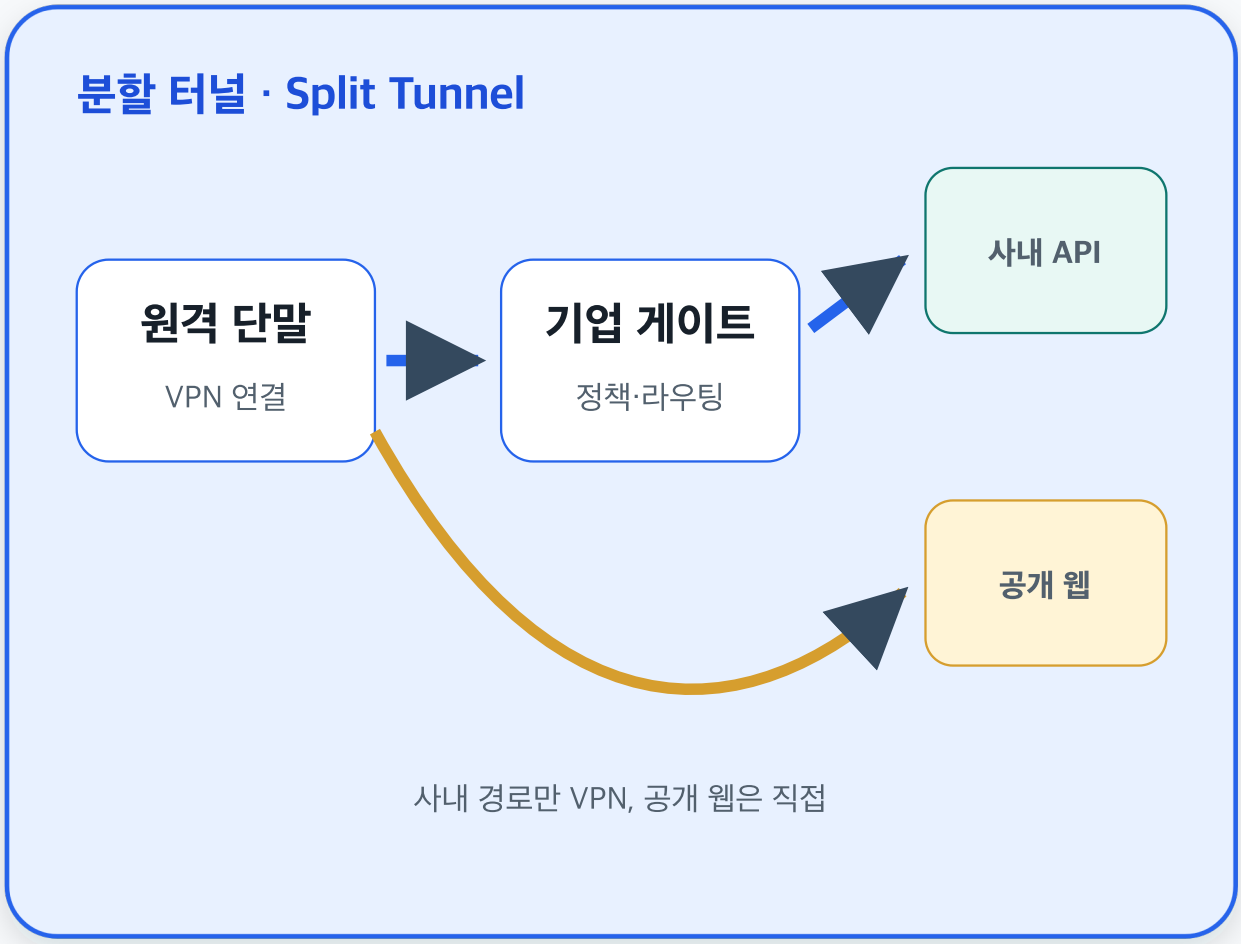


그림 4. 전체 터널은 공개 트래픽도 기업 게이트를 거치고, 분할 터널은 지정 목적지만 VPN으로 보냅니다.


전체 터널 · Full Tunnel
원격 단말
VPN 연결
기업 게이트
정책·라우팅
사내 API
공개 웹
공개 웹도 기업 게이트를 거침


분할 터널 · Split Tunnel
원격 단말
VPN 연결
기업 게이트
정책·라우팅
사내 API
공개 웹
사내 경로만 VPN, 공개 웹은 직접

전체 터널

- 기본 인터넷 트래픽까지 VPN 게이트웨이로 보냄
- 조직이 보안 통제와 기록을 한 경로에 모으기 쉬움
- 지연·대역폭·외부 서비스 위치 인식이 달라질 수 있음

분할 터널

- 사내 주소·지정 목적지만 VPN으로 보냄
- 공개 인터넷은 현재 로컬 네트워크로 직접 나갈 수 있음
- 목적지별 경로와 DNS 정책이 복잡해질 수 있음

VPN 연결 뒤 확인할 것

항목	기록 예시
VPN 프로필	`corp-standard`
연결 시각	2026-07-15 15:30 KST
할당 IP	`10.99.8.24`
사내 목적지 경로	VPN 인터페이스
공개 목적지 경로	VPN 또는 로컬 게이트웨이
DNS 서버·검색 도메인	조직 DNS· `intra.example`
사용자·단말 인증	성공·실패·추가 인증 요구

VPN 연결 = 모든 권한이 아닙니다

VPN은 경로와 접속 정책의 한 단계입니다. 그 뒤 방화벽이 목적지·포트를 거부하거나 애플리케이션이 사용자 역할을 거부할 수 있습니다.

실습 주의: 조직 정책이 요구하는 VPN을 임의로 끄거나 보안 에이전트를 중지하지 않습니다. 승인된 시험 자원과 절차에서만 비교합니다.

30초 확인

VPN은 연결됐고 사내 DNS도 이름을 풀지만 TCP 443 연결이 시간 초과됩니다. “VPN 문제 없음”이라고 결론 내릴 수 있을까요?

정답 보기

아닙니다. VPN 터널은 연결됐지만 목적지 대역 라우팅, VPN 이후 방화벽, 서버 포트, 응답 경로를 더 확인해야 합니다.

6. 프록시는 한쪽을 대신해 요청을 전달합니다

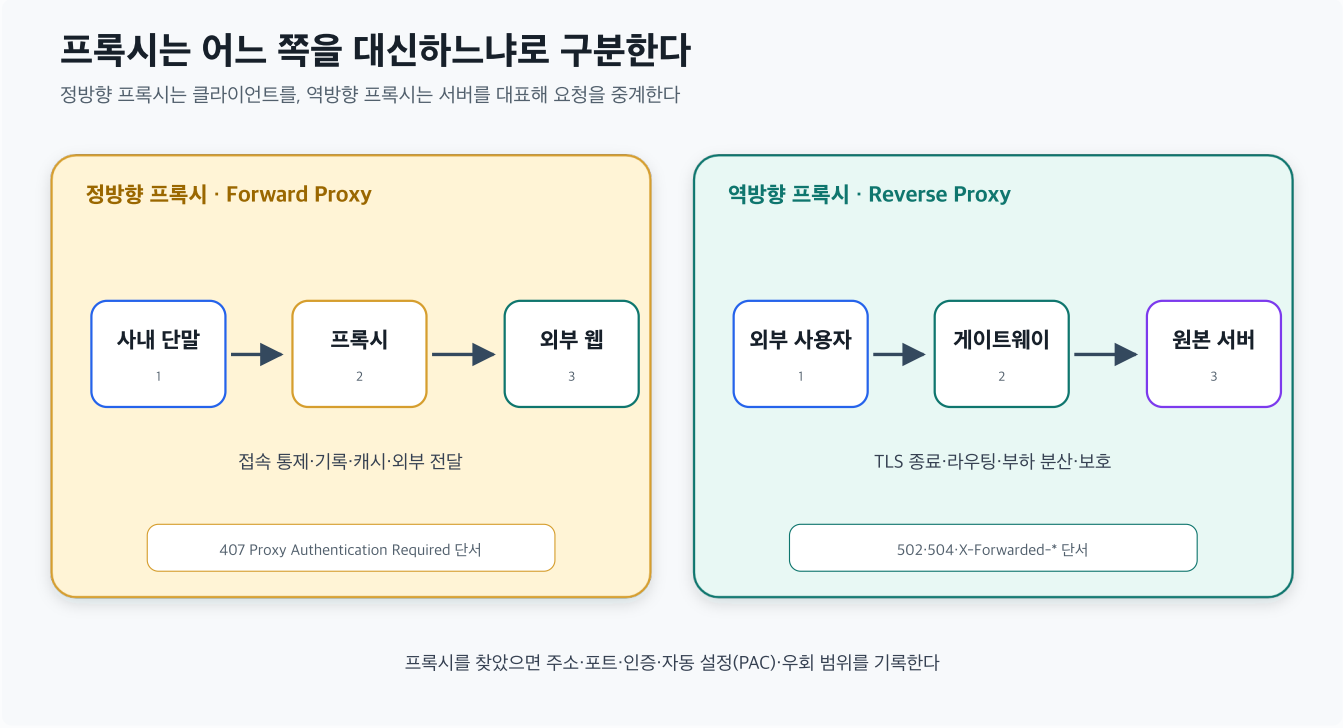
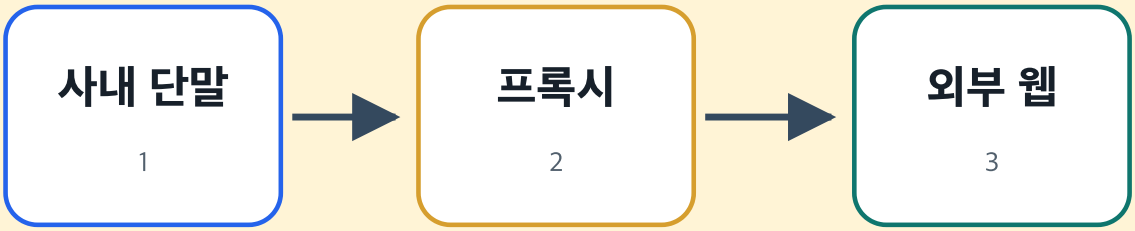


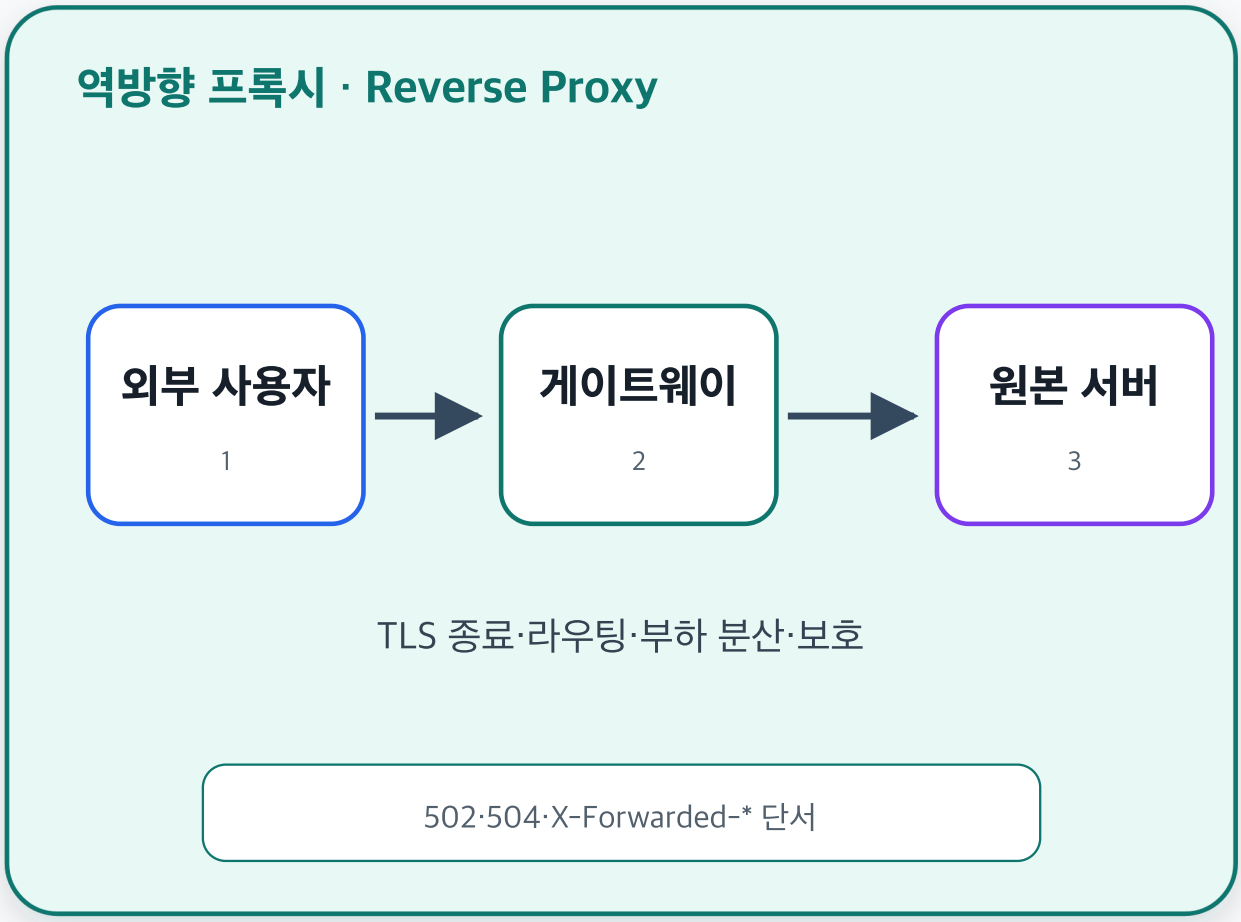
그림 5. 정방향 프록시와 역방향 프록시는 누구를 대신하느냐가 다릅니다.

정방향 프록시 · Forward Proxy



접속 통제·기록·캐시·외부 전달

407 Proxy Authentication Required 단서


역방향 프록시 · Reverse Proxy
외부 사용자
1
게이트웨이
2
원본 서버
3
TLS 종료·라우팅·부하 분산·보호
502·504·X-Forwarded-* 단서

6.1. 정방향 프록시

클라이언트를 대신해 외부 서버로 요청을 보냅니다.

- 외부 사이트 접속 통제
- 사용자·단말 인증
- 요청 기록과 정책 검사
- 캐시·콘텐츠 검사
- 조직의 외부 출발 IP 통합

브라우저·운영체제는 프록시 주소를 직접 설정하거나 PAC(Proxy Auto-Configuration) 파일로 목적지별 프록시 사용 여부를 정할 수 있습니다.

6.2. HTTPS 터널과 CONNECT

HTTP 프록시는 `CONNECT host:port` 요청으로 대상 서버까지 터널을 만들 수 있습니다. 성공한 뒤 클라이언트와 서버 사이의 TLS 통신이 터널을 통과합니다. 조직 정책에 따라 TLS 검사 구조가 추가될 수 있습니다.

6.3. 역방향 프록시

외부 사용자에게 원본 서버를 대신합니다.

- TLS 종료
- 원본 서버 선택과 부하 분산
- 공개 주소와 내부 서버 분리
- 웹 애플리케이션 방화벽·속도 제한
- 캐시와 압축

프록시 오류 단서

관찰	가능한 단계	다음 확인
`407 Proxy Authentication Required`	정방향 프록시 인증	프록시 주소·계정·PAC·인증 방식
조직 차단 안내 HTML	프록시·보안 게이트웨이 정책	응답 본문·정책 분류·요청 목적
`502 Bad Gateway`	역방향 프록시가 뒷단 응답을 받지 못함	게이트웨이·원본 서버 연결
`504 Gateway Timeout`	역방향 프록시가 뒷단을 기다리다 시간 초과	원본 처리 시간·연결·시간 제한
인증서 발급자가 조직 CA	TLS 검사 경로 가능성	승인된 인증서 설치와 보안 정책

HTTP 403도 프록시나 원본 애플리케이션 어느 쪽에서든 만들어질 수 있습니다. Response 본문·응답 헤더·인증서·요청 ID를 함께 봅니다.

BIG IDEA 02

프록시 오류는 최종 서버가 아니라 중간 전달자가 만든 응답일 수 있습니다.

7. 방화벽은 흐름을 정책으로 판정합니다

NIST는 방화벽을 서로 다른 보안 상태의 네트워크나 호스트 사이에서 트래픽 흐름을 통제하는 장치 또는 프로그램으로 설명합니다.

7.1. 기본 판단 재료

- 출발 IP·출발 구역
- 목적지 IP·목적지 구역
- IP 프로토콜: TCP·UDP·ICMP 등
- 출발 포트·목적지 포트
- 연결 상태
- 사용자·애플리케이션·단말 정보가 추가될 수 있음

출발 IP, 출발 포트, 목적지 IP, 목적지 포트, 프로토콜을 묶어 5-튜플이라고 부릅니다.

7.2. 인바운드와 아웃바운드

방향은 기준 경계에 따라 달라집니다.

```
인터넷 → 조직 DMZ      : 조직 경계 기준 인바운드
업무망 → 외부 API      : 조직 경계 기준 아웃바운드
업무망 → 데이터망      : 내부 구역 경계의 동서 트래픽
```

“인바운드 열어 주세요”만으로는 출발·목적지·포트를 알 수 없습니다. 어느 경계를 기준으로 하는지도 적습니다.

7.3. 기본 거부와 최소 허용

NIST SP 800-41 Rev. 1은 방화벽 정책이 명시적으로 허용하지 않은 불필요한 인바운드·아웃바운드 트래픽을 기본 거부하는 접근을 권고합니다. 실제 정책은 조직의 위험 평가와 업무 요구에 따라 설계합니다.

8. 방화벽 허용 요청을 한 장으로 씁니다

그림 6. “사이트가 안 열림”을 최소 허용 흐름이 명확한 정책 요청으로 바꿉니다.

출발

업무망 · 10.10.20.0/24

프로토콜

TCP

방향

Outbound

기간

2026-07-20 ~ 2026-10-31

필요한 흐름만 명시하고, 나머지는

목적지

api.partner.example · 203.0.113.40

목적지 포트

443

업무 목적

주문 상태 조회

담당·승인

서비스 A · 보안 검토

는 조직 정책에 따라 기본 거부한다

필드	좋은 기록	부족한 기록
출발	업무망 `10.10.20.0/24`	사내
목적지	`api.partner.example`, 확인 IP	파트너 사이트
프로토콜	TCP	인터넷
목적지 포트	443	HTTPS쯤
방향	업무망 → 외부, 아웃바운드	열어 주세요
업무 목적	주문 상태 조회 API	업무용
기간	시험 7일·운영 상시·종료일	계속
담당·승인	서비스 담당·보안 검토·티켓	홍길동이 말함

FQDN과 IP를 함께 다루는 이유

클라우드·콘텐츠 전송 네트워크·SaaS는 IP가 여러 개이거나 바뀔 수 있습니다. 방화벽이 FQDN 정책을 지원하는지, 공급자가 공식 IP 대역을 제공하는지, DNS 결과 변화와 갱신 절차가 무엇인지 확인합니다.

출발 포트는 보통 고정 요청 항목이 아닙니다

클라이언트는 연결할 때 임시 출발 포트를 사용하는 경우가 많습니다. 업무팀이 주로 요청하는 것은 목적지 서비스의 TCP 443 같은 **목적지 포트**입니다. 서버가 역방향으로 새 연결을 시작하는 구조라면 별도의 흐름으로 적습니다.

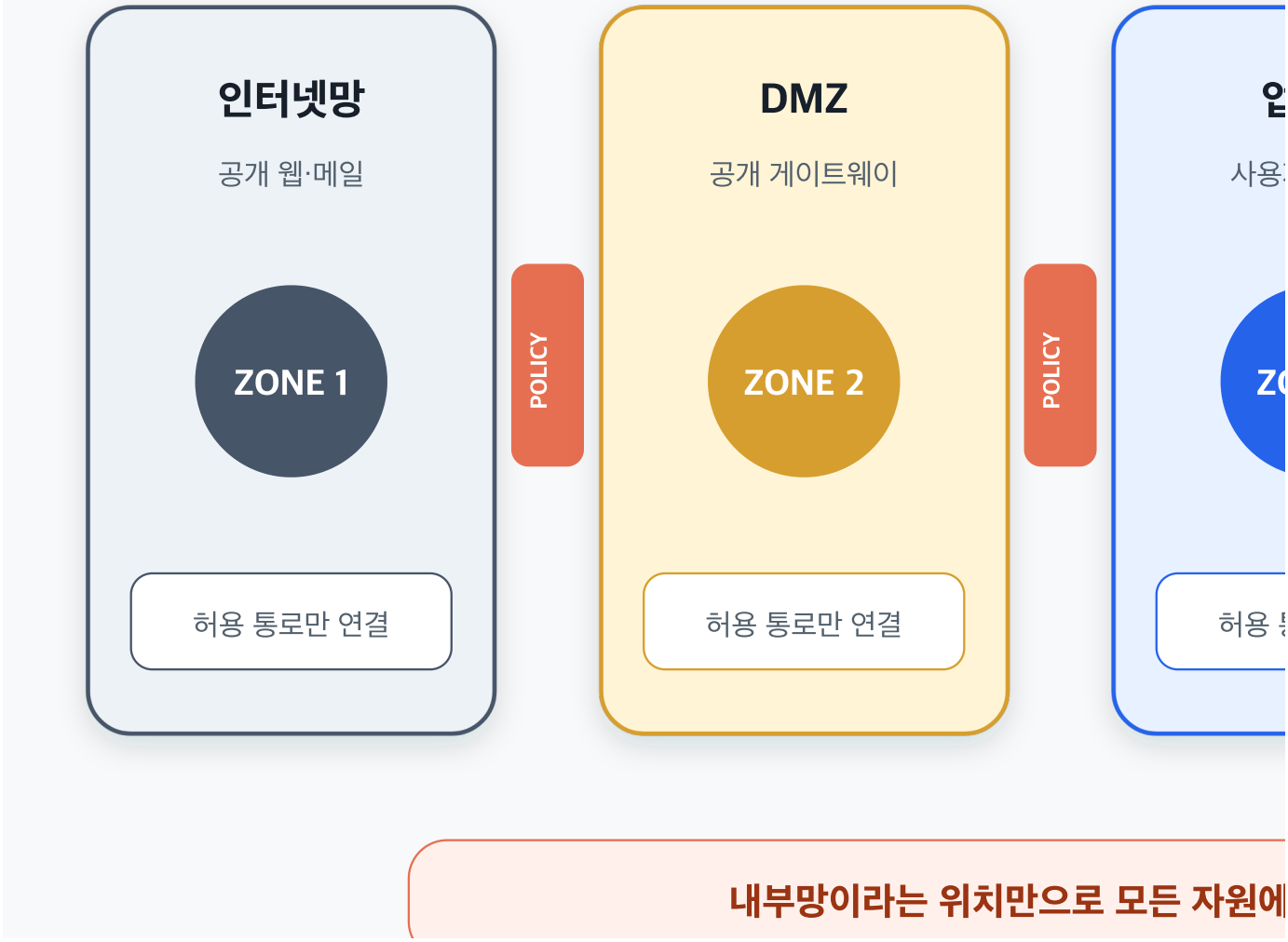
양방향이라는 표현을 피합니다

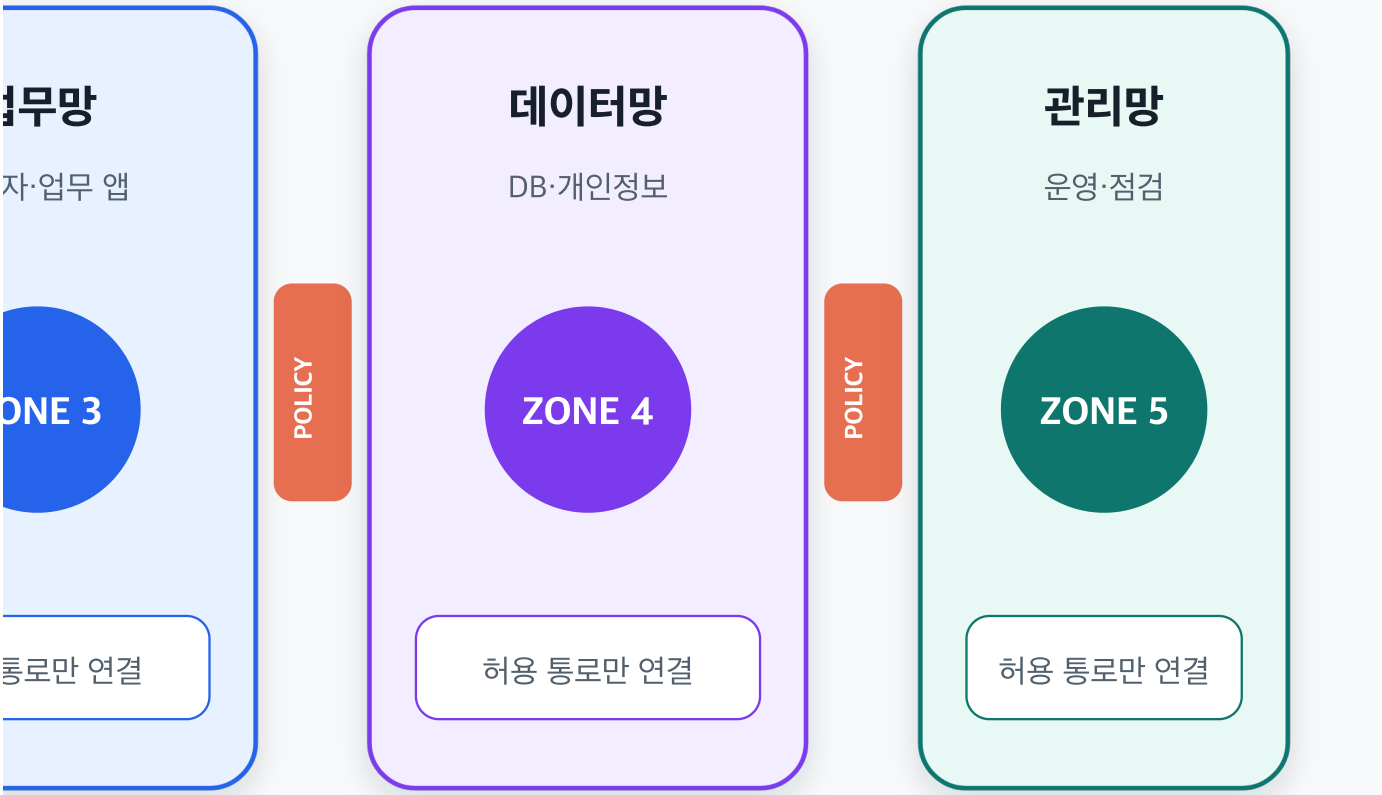
상태 추적 방화벽은 허용된 연결의 응답 트래픽을 상태에 따라 허용할 수 있습니다. “양방향 전체 허용” 대신 누가 연결을 시작하는지와 필요한 별도 역방향 연결이 있는지 구분합니다.

> **좋은 허용 요청:** 누가 어디에서 어느 목적지의 어떤 서비스로 왜, 언제까지 연결을 시작하는지가 보입니다.

9. 망 분리는 신뢰 수준이 다른 구역을 나눕니다

그림 7. 망 분리는 구역을 나누는 데서 끝나지 않고 필요한 데이터 흐름을 제한된 통로로 연결합니다.


인터넷망
공개 웹·메일
ZONE 1
허용 통로만 연결
POLICY
DMZ
공개 게이트웨이
ZONE 2
허용 통로만 연결
POLICY
내부망이라는 위치만으로 모든 자원에



| 대한 신뢰와 권한이 생기지는 않는다

9.1. 구역의 예

구역	대표 자원	주된 질문
인터넷망	공개 웹·외부 메일·SaaS	외부와 어떤 데이터를 주고받는가
DMZ	공개 게이트웨이·역방향 프록시	외부에 노출할 최소 접점은 무엇인가
업무망	사용자 PC·업무 애플리케이션	어떤 사용자와 단말이 접근하는가
데이터망	DB·개인정보 처리 시스템	어느 앱이 어떤 포트로 접근하는가
관리망	운영 단말·모니터링·관리 인터페이스	누가 어떤 승인으로 관리하는가

구역 이름과 범위는 조직마다 다릅니다. 클라우드의 VPC·서브넷·보안 그룹, 컨테이너 네트워크, 서비스 메시도 논리적 경계를 만들 수 있습니다.

9.2. 물리적 분리와 논리적 분리

- 물리적 분리: 단말·스위치·케이블 등 물리 인프라를 별도로 구성
- 논리적 분리: VLAN·가상 네트워크·방화벽·접근 제어 등으로 흐름을 분리
- 가상화 기반 분리: 한 물리 자원 위에서 격리된 가상 환경을 운영

어느 방식이 적합한지는 정보의 민감도, 위협, 법·규제, 운영 가능성, 예외 절차를 함께 판단합니다.

9.3. 내부망은 자동 신뢰 구역이 아닙니다

NIST의 제로 트러스트 원칙은 물리적·네트워크 위치나 자산 소유만으로 사용자·자산에 암묵적 신뢰를 부여하지 않는다고 설명합니다. 내부망에 있다는 이유만으로 모든 데이터와 관리 기능을 허용해서는 안 됩니다.

9.4. 연결 통로를 문서화합니다

```
외부 사용자 → 역방향 프록시: TCP 443
역방향 프록시 → 업무 API: TCP 8443
업무 API → 데이터베이스: TCP 5432
관리 단말 → 서버 관리: 승인된 관리 프로토콜·시간대
```

각 화살표는 별도의 출발·목적지·포트·인증·기록 정책을 가질 수 있습니다.

10. 국내 망 분리 기준은 적용 영역과 최신 시점을 확인합니다

망 분리는 모든 조직에 같은 형태로 적용되는 하나의 기술 규칙이 아닙니다. 개인정보, 공공, 금융, 의료, 국방, 중요정보통신기반시설 등 적용 영역과 정보 유형에 따라 관련 법령·고시·감독규정·기관 지침이 다를 수 있습니다.

2026-07-15 기준 확인 예시

- 개인정보보호위원회는 「개인정보의 안전성 확보조치 기준」을 고시하며, 현재 페이지에는 개인정보보호위원회고시 제2025-9호가 2025-10-31 시행 기준으로 게시되어 있습니다.
- 금융위원회는 2024년 금융분야 망분리 개선 로드맵 이후 규제 개선을 단계적으로 추진했고, 2026-01-19에는 일정한 보안 통제를 전제로 업무망의 SaaS 활용 예외를 추진하는 자료를 게시했습니다.
- NIST의 최신 제로 트러스트 구현 가이드 SP 1800-35는 2025년 최종본으로, 온프레미스·멀티클라우드 자원과 하이브리드 인력에 대한 승인된 접근을 다룹니다.

이 예시는 “망 분리가 없어졌다”거나 “모든 SaaS가 허용된다”는 뜻이 아닙니다. 규정의 시행 상태, 적용 대상, 처리 정보, 보완 통제, 조직 내부 기준을 함께 확인해야 합니다.

기획자가 확인할 질문

1. 우리 조직은 어느 법·고시·감독규정·기관 지침의 적용을 받는가
2. 이 시스템이 처리하는 정보의 분류와 민감도는 무엇인가
3. 물리·논리·가상화·제로 트러스트 중 승인된 구조는 무엇인가
4. 예외 승인과 보완 통제는 무엇인가
5. 기준일과 개정 이력은 언제인가
6. 보안·개인정보·법무·감사 중 누가 최종 해석하는가

정책 주의: 이 매뉴얼은 기술 학습 자료이며 특정 조직의 법률·규제 준수 판정을 대신하지 않습니다. 실제 설계와 예외는 최신 원문과 담당 부서의 공식 해석을 확인합니다.

11. 오류 문구를 첫 실패 단계에 놓습니다

그림 8. 앞 단계부터 확인하면 같은 “접속 실패”를 서로 다른 담당 영역으로 좁힐 수 있습니다.

1	**DNS**	이름을 찾을 수 없음
2	**경로·VPN**	No route · 사설 IP 미도달
3	**프록시**	407 · 차단 페이지
4	**TCP·방화벽**	Timeout · Refused
5	**TLS**	인증서·협상 오류
6	**HTTP·앱**	403 · 404 · 5xx


DNS·도메인
네트워크·VPN
프록시·보안
네트워크·서버
인증서·플랫폼
서비스·권한

11.1. DNS 단계

문구 예시	직접 알 수 있는 것	다음 확인
`Could not resolve host`	이름에서 IP를 얻지 못함	도메인 철자·DNS 서버·VPN DNS·검색 도메인
`ERR_NAME_NOT_RESOLVED`	브라우저 이름 해석 실패	다른 이름·다른 망·DNS 결과 비교

11.2. 경로·VPN 단계

문구 예시	가능한 의미	다음 확인
`No route to host`	목적지로 보낼 경로를 찾지 못함	라우팅 표·VPN 대역·게이트웨이
사설 IP에 외부망에서 미도달	승인된 사내 경로 없음	VPN·전용선·접속 게이트웨이

11.3. 프록시 단계

문구 예시	가능한 의미	다음 확인
`407`	프록시 인증 필요	프록시 계정·PAC·인증 흐름
조직 차단 페이지	URL 분류·정책 차단	차단 사유·업무 목적·예외 절차

11.4. TCP·방화벽·서버 포트 단계

문구 예시	가능한 의미	주의
Connection timed out	경로 중 드롭·무응답·서버 지연	방화벽 차단으로 단정할 수 없음
Connection refused	목적지에 도달했으나 포트가 수신하지 않거나 거부	서버 서비스·리스닝 포트 확인
Connection reset	중간 장비나 서버가 연결 종료	TLS·정책·서버 로그 함께 확인

11.5. TLS 단계

인증서 이름·유효기간·신뢰 체인·TLS 협상 오류를 확인합니다. 인증서를 무시하는 옵션으로 운영 문제를 덮지 않습니다.

11.6. HTTP·애플리케이션 단계

상태 코드가 보이면 DNS·경로·TCP·TLS의 상당 부분을 지나 HTTP 응답을 받았다는 뜻입니다. 401·403은 인증·권한·중간 정책을, 404는 경로·자원·공개 정책을, 5xx는 서버·게이트웨이 처리 실패를 더 봅니다.

BIG IDEA 03

Timeout은 관찰값이지 “방화벽 차단”이라는 원인 확정이 아닙니다.

12. 네트워크 문의 증거 묶음을 만듭니다

그림 9. 재현에 필요한 여섯 사실과 비교 결과를 함께 보내면 담당자가 같은 흐름을 찾을 수 있습니다.

WHO

사용자·단말

계정·기기·관리 상태

WHERE

출발 망

사무실·집·VPN·핫스팟

TARGET

목적지

FQDN·IP·프로토콜·포트

POLICY

중간 조건

VPN·프록시·방화벽

비교 행렬

VPN 끔/켬 · 사무실/외부 · 동료 성공/본인 실패 · 공개 API/사내 API

WHEN

정확한 시각

KST·재현 횟수

ERROR

관찰 결과

원문·상태·요청 ID

여섯 묶음

묶음	기록할 값
Who	사용자 역할·단말 종류·관리 상태·동료 비교
Where	사무실·집·핫스팟·VPN 프로필·출발 IP
When	발생 시각·표준시간대·재현 횟수
Target	URL·FQDN·확인 IP·프로토콜·목적지 포트
Policy	VPN·프록시·방화벽·인증서·권한 조건
Error	정확한 원문·HTTP 상태·요청 ID·스크린샷

비교 행렬

조건	결과	첫 실패·문구
사무실·VPN 없음		
외부망·VPN 없음		
외부망·VPN 연결		
동료 단말·같은 망		
공개 시험 API		
실제 사내 API		

모든 비교를 실행할 필요는 없습니다. 정책상 허용되고 원인 구분에 도움이 되는 최소 비교만 합니다.

전달용 한 문장

> 2026-07-15 15:30 KST 관리 PC를 집 인터넷에 연결한 상태에서 `api.intra.example:443` 접속은 시간 초과됐고, 승인된 VPN `corp-standard` 연결 뒤에는 200으로 성공했습니다. 같은 시각 공개 시험 API는 VPN 전후 모두 200이었으며, 사내 목적지의 VPN 경로·정책 확인을 요청합니다.

포함하지 않을 것

- VPN 비밀번호·일회용 코드
- 프록시 인증 헤더·Cookie·토큰
- 전체 라우팅 표의 불필요한 내부 정보
- 개인정보·업무 응답 본문 원문
- 승인되지 않은 포트 스캔 결과

13. 실습 · 경로를 바꾸어 첫 실패 찾기

연결 파일: L02-05 접속 경로 진단 실습

시뮬레이터: L02-05 접속 조건 시뮬레이터

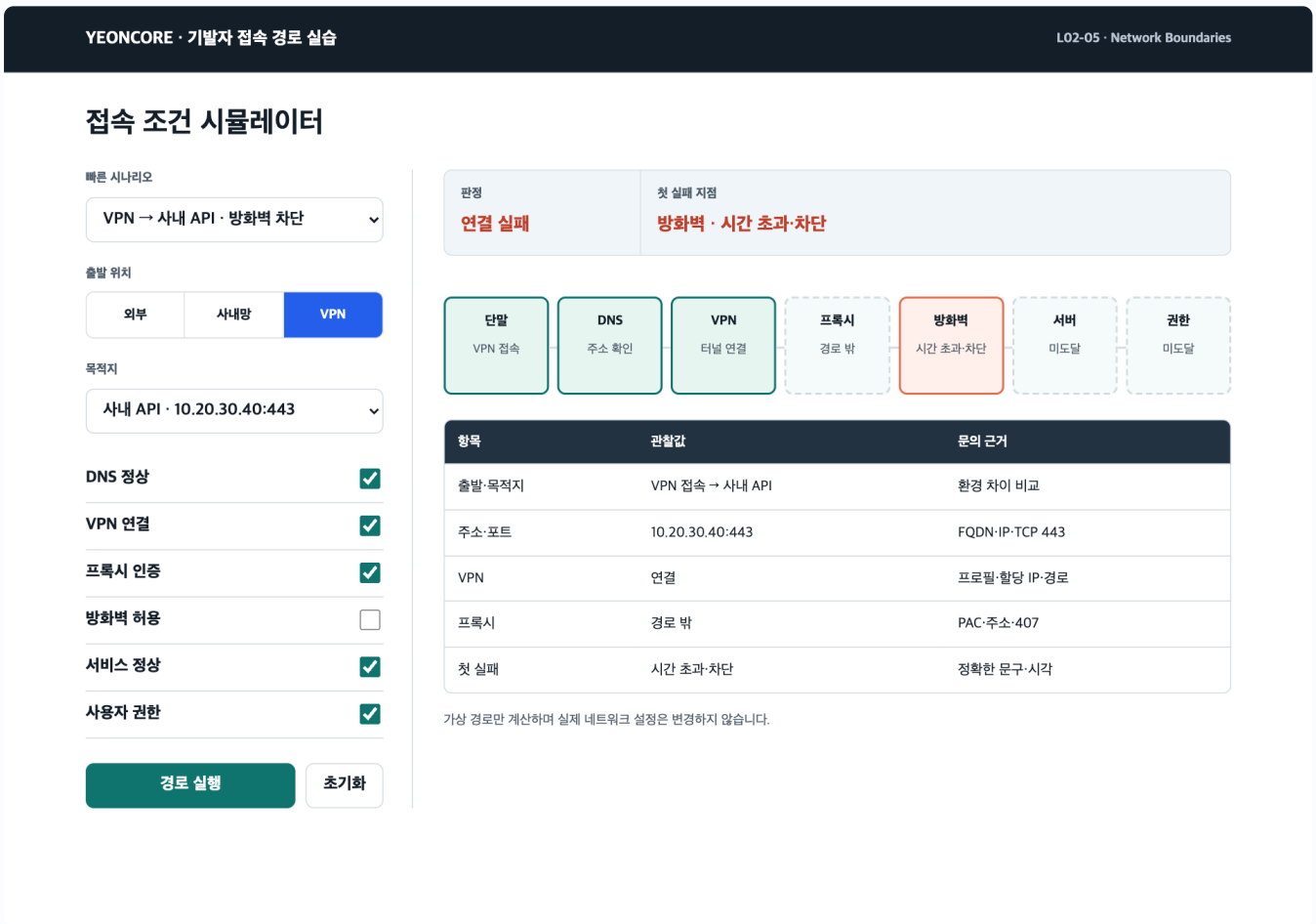


그림 10. 시뮬레이터는 실제 설정을 바꾸지 않고 첫 실패 지점과 문의 근거를 연습하게 합니다.

실습 A · 다섯 가상 시나리오

시나리오	예상 첫 실패
외부 인터넷 → 공개 API	없음·성공
외부 인터넷 → 사내 API·VPN 없음	VPN·사내 경로 없음
VPN → 사내 API·방화벽 차단	방화벽·시간 초과·차단
사내망 → 외부 API·프록시 인증 실패	프록시·407
사내망 → 사내 API·애플리케이션 403	권한·HTTP 403

각 시나리오에서 통과·실패·미도달 노드를 구분하고, 시간 초과가 방화벽 확정이 아니라는 점을 기록합니다.

실습 B · 공개 시험 주소 세 가지

```
curl -I --connect-timeout 5 --max-time 10 https://httpbingo.org/status/200
curl -I --connect-timeout 5 --max-time 10 https://httpbingo.org/status/403
curl -I --connect-timeout 5 --max-time 10 https://name-does-not-exist.invalid
```

`.invalid`는 시험·문서에서 확실히 유효하지 않은 이름을 만들도록 예약된 최상위 도메인입니다.

시험	예상 관찰	첫 실패 단계
status/200	HTTP 200	모든 경계 통과
status/403	HTTP 403	HTTP·정책·권한 단계
`.invalid`	이름 해석 오류	DNS 단계

프록시·보안 게이트웨이가 있는 환경에서는 다른 응답이 보일 수 있습니다. 그 차이 자체를 실습 기록에 남깁니다.

실습 C · 승인된 환경 비교

조직에서 허용한 시험 자원과 절차가 있을 때만 VPN 끔·켬 또는 사무실·외부망 비교를 수행합니다. 실제 개인정보 시스템이나 관리 포트를 시험하지 않습니다.

완료 산출물

- 접속 경로도 1개

- 가상 시나리오 비교표 5행
- 실제 200·403·DNS 실패 기록
- 방화벽 허용 요청 카드 1개
- 네트워크 문의 한 문장 1개

14. 인쇄용 접속 경로 학습지

A. 출발과 목적지

항목	기록
사용자·단말	
출발 위치·망	
VPN 프로필·상태	
프록시 주소·방식	
URL·FQDN	
확인 IP	
프로토콜·목적지 포트	
발생 시각·표준시간대	

B. 경계별 통과 여부

단계	관찰값	통과·실패·미확인	근거
단말·인증			
DNS			
라우팅·VPN			
프록시			
방화벽·TCP			
TLS			
HTTP·서비스			
업무 권한			

C. 첫 실패

```
첫 실패 단계: _____
정확한 오류 문구: _____
이 문구가 직접 말하는 사실: _____
아직 확정할 수 없는 원인: _____
다음 비교·확인: _____
```

D. 방화벽·연계 조건

출발	목적지	프로토콜	목적지 포트	방향	목적	기간·담당

E. 경로 직접 그리기

```
[사용자·단말] → [출발 망] → [DNS] → [VPN] → [프록시]
       → [방화벽] → [서버:포트] → [애플리케이션 권한]

통과: ○   실패: ×   경로 밖: –   미확인: ?
```

15. 셀프 테스트

문제 1 · 역할

DNS·라우터·방화벽이 각각 대답하는 질문을 한 문장씩 쓰세요.

문제 2 · 사설 주소

`10.20.30.40` 이 DNS 결과로 나왔습니다. 집 인터넷에서 직접 접속되지 않는 가장 기본적인 이유는 무엇입니까?

문제 3 · VPN

VPN 아이콘이 연결 상태이면 모든 사내 자원 접근 권한이 생깁니까?

문제 4 · 터널

전체 터널과 분할 터널의 차이를 공개 웹 트래픽 기준으로 설명하세요.

문제 5 · 프록시

정방향 프록시와 역방향 프록시는 각각 누구를 대신합니까?

문제 6 · 방화벽 요청

“파트너 사이트 443 열어 주세요”에 최소한 추가해야 할 항목 네 가지를 쓰세요.

문제 7 · 망 분리

내부망에 있으면 모든 자원에 대한 신뢰와 권한이 자동으로 생긴다는 말이 왜 틀렸습니까?

문제 8 · 시간 초과

Connection timed out을 보고 방화벽 차단으로 확정해도 됩니까?

문제 9 · 403

HTTP 403을 받았다면 DNS·TCP·TLS 단계에 관해 무엇을 추정할 수 있고, 무엇은 더 확인해야 합니까?

문제 10 · 문의 문장

다음 기록을 네트워크 문의 한 문장으로 바꾸세요.

```
시각: 2026-07-15 16:10 KST
단말: 관리 PC
출발: 집 인터넷
목적지: api.intra.example:443
VPN 끔: DNS 10.20.30.40, 접속 시간 초과
VPN 켬: HTTP 200
공개 시험 API: 두 조건 모두 HTTP 200
```

16. 정답과 해설

문제 1

- DNS: 이 이름은 어느 IP 주소인가
- 라우터: 이 목적지로 가려면 다음에 어디로 보낼까
- 방화벽: 이 출발·목적지·프로토콜·포트 흐름을 허용할까

문제 2

`10.20.30.40`은 RFC 1918 사설 주소 범위입니다. 공용 인터넷에서 직접 라우팅되지 않으므로 승인된 사내망·VPN·전용 접속 경로가 필요할 수 있습니다.

문제 3

아닙니다. VPN은 경로와 원격 접속 정책의 한 단계입니다. 목적지 대역 라우팅, 방화벽, 단말 정책, 애플리케이션 사용자 권한을 별도로 통과해야 합니다.

문제 4

전체 터널은 공개 웹 트래픽도 기업 VPN 게이트를 거치게 하고, 분할 터널은 지정된 사내 목적지만 VPN으로 보내고 공개 웹은 로컬 인터넷으로 직접 보낼 수 있습니다.

문제 5

정방향 프록시는 클라이언트를 대신해 외부 서버로 요청하고, 역방향 프록시는 원본 서버를 대신해 외부 요청을 받아 뒷단으로 전달합니다.

문제 6

출발 구역·IP, 정확한 목적지 FQDN·IP, 프로토콜 TCP, 방향, 업무 목적, 적용 기간, 담당·승인 정보 중 네 가지 이상을 추가합니다. 목적지 포트 443도 함께 확정합니다.

문제 7

네트워크 위치만으로 사용자·단말·자원에 암묵적 신뢰를 주면 내부 위협과 계정·단말 침해에 취약합니다. 자원마다 인증·권한·단말 상태·데이터 흐름 정책을 확인해야 합니다.

문제 8

확정할 수 없습니다. 시간 초과는 방화벽 드롭, 경로 누락, 응답 경로 문제, 서버 무응답 등 여러 원인이 가능합니다. DNS·라우팅·VPN·프록시·서버 상태와 비교 증거를 확인합니다.

문제 9

HTTP 상태 코드를 받았으므로 이름 해석과 연결·TLS의 상당 부분을 지나 HTTP 응답을 받은 것으로 볼 수 있습니다. 다만 403을 만든 주체가 정방향 프록시·역방향 프록시·원본 애플리케이션 중 어디인지, 인증·권한·정책의 무엇이 거부됐는지 더 확인해야 합니다.

문제 10

예시 답안:

> 2026-07-15 16:10 KST 관리 PC를 집 인터넷에 연결한 상태에서 `api.intra.example:443`은 `10.20.30.40`으로 해석됐지만 VPN을 끄면 시간 초과됐고, 승인된 VPN 연결 뒤에는 HTTP 200으로 성공했습니다. 공개 시험 API는 두 조건 모두 200이므로 사내 목적지의 VPN 라우팅·정책 확인을 요청합니다.

17. 한 장 요약

그림 11. 목적지와 출발 조건을 고정하고 첫 실패와 비교 근거를 찾아 최소 허용 요청으로 끝냅니다.

1 **목적지**

FQDN·IP

프로토콜·포트

2 **출발 조건**

사용자·단말

망·VPN·프록시

4 **첫 실패**

정확한 문구

Timeout≠확정

5 **비교**

환경 변경

성공 조건 대조

경로: 장비 이름부터 출발→목적지

3 **경로**

DNS·라우팅

중간 경계

6 **요청**

최소 허용

기간·목적·담당

흐름과 첫 실패 구간로 설명한다

단계	질문	산출물
1	어디로 가는가	FQDN·IP·프로토콜·포트
2	어디서 누가 가는가	사용자·단말·출발 망·VPN·프록시
3	어떤 경계를 지나는가	DNS·라우팅·VPN·프록시·방화벽·서버·권한
4	처음 어디서 실패했는가	정확한 문구·시각·통과/미도달 구분
5	어떤 조건에서 달라지는가	환경 비교 행렬
6	무엇을 허용·수정해야 하는가	최소 정책 요청·기간·목적·담당

최종 설명: 장비 이름을 추측하지 않고, 출발에서 목적지까지의 흐름과 첫 실패 근거를 보여 줍니다.

18. 다음 학습과 출처

18.1. 다음 매뉴얼

M03-01「화면을 HTML 구조로 읽기」에서는 연결된 웹 화면을 제목·영역·목록·폼·링크 같은 의미 구조로 나누어 읽습니다.

18.2. 함께 사용할 자료

- L02-05 접속 경로 진단 실습
- L02-05 접속 조건 시뮬레이터
- T02-05 네트워크 연계 조건 점검표
- 방화벽·VPN·프록시·망 분리 용어집

18.3. 출처와 확인일

아래 공식 자료는 모두 2026-07-15에 확인했습니다.

- NIST: SP 800-41 Rev. 1 방화벽 지침, SP 800-46 Rev. 2 원격 접속 지침, SP 800-207 제로 트러스트, SP 1800-35 제로 트러스트 구현
- RFC Editor: RFC 1918 사설 IPv4, RFC 3022 NAT, RFC 9110 HTTP 프록시·CONNECT, RFC 2606 예약 시험 도메인
- 개인정보보호위원회: 개인정보의 안전성 확보조치 기준 제2025-9호

- 금융위원회: 금융사 SaaS 활용을 위한 망분리 규제 개선 자료