PGROK

PRIVATE SERVICES. CONNECTED.

내부 서비스에 외부로 통하는 하나의 연결.



현장의 프로그램은 그대로.
PGROK가 내부 웹서비스를 고유한 HTTPS 주소로 연결합니다.

하나의 중계 서버
여러 현장의 연결을 한곳에서

서비스별 공개 주소
다른 포트도 독립된 이름으로

B망 인바운드 개방 없이
클라이언트가 먼저 연결

WHY PGROK

프로그램은 준비됐는데, 접속 환경이 복잡한가요?



내부 서비스의 위치와 외부에서 사용하는 주소를 분리해 연결을 관리합니다.

01

내부에서만 열리는 서비스

현장 PC의 웹프로그램을 외부 사용자에게 전달해야 할 때, 승인된 터널로 연결 경로를 마련합니다.

02

포트가 늘수록 복잡한 운영

8765, 9000, 3000처럼 여러 포트의 서비스를 서로 다른 도메인과 Tunnel ID로 구분합니다.

03

흩어진 접속 설정

Agent와 Tunnel 정의, 연결 상태를 관리 콘솔에서 확인하고 PC별 접속 권한을 구분합니다.

HOW IT WORKS

연결은 안에서 시작하고, 접속은 HTTPS로.

클라이언트가 만든 SSH 역방향 연결을 통해 외부 요청이 내부 서비스에 도달합니다.



01

외부 사용자

서비스 도메인으로 HTTPS 접속

→

02

A망 PGROK 서버

Caddy가 이름별로 요청을 라우팅

→

03

B망 클라이언트

먼저 연결한 SSH 터널로 요청 전달

→

04

내부 프로그램

등록된 호스트와 포트에서 응답 처리

> A망에는 공개 DNS와 필요한 포트포워딩이 필요합니다. HTTP/HTTPS 서비스마다 공유기의 새 포트를 열 필요는 없습니다.

CORE CAPABILITIES

서비스 연결부터 운영 확인까지.



고유한 HTTPS 주소

허용된 서비스 이름과 DNS를 연결하고, 발급 조건을 충족하면 공개 인증서를 자동 발급합니다.

여러 포트 동시 연결

같은 PC에서도 서비스별 터널을 실행합니다. 기존 서비스를 유지하면서 새 서비스를 추가할 수 있습니다.

Agent · Tunnel 관리

어떤 PC가 어떤 서비스에 연결되는지 정의하고, 실제 연결 상태를 관리 콘솔에서 확인합니다.

PC별 접속 분리

별도 Agent 계정과 키, 소켓 디렉터리를 배정해 서로의 연결 자원에 대한 접근을 제한합니다.

지속 운영 구성

Linux systemd와 영속 경로를 사용해 시작·종료·로그 조회를 구성합니다. 재시도 소진 시 운영자가 확인합니다.

관리자 2단계 인증

인증 앱 등록을 완료한 계정은 비밀번호와 OTP 또는 일회용 복구 코드로 콘솔에 로그인합니다.

ONE CLIENT, MULTIPLE SERVICES

포트가 하나 더 생기면, 터널도 하나 더.

기존 hangil은 유지하고 새 서비스 이름·Tunnel ID를 등록합니다. 서비스별 프로세스와 상태·로그 경로를 분리해 운용합니다.



아래는 구조를 설명하는 예시이며 실제 운영 상태를 표시하지 않습니다.

:8765 →	:9000 →	:3000 →
hangil.pgrok.example.com	myapp.pgrok.example.com	dashboard.pgrok.example.com

DNS 설정 → 서버 이름 허용 → Tunnel 등록 → 클라이언트 실행

SECURITY BY LAYER

연결의 보호와 프로그램의 보안을 함께.

PGROK는 연결·권한·관리 인증을 보호합니다. 공개하는 프로그램의 로그인과 취약점 관리는 별도로 필요합니다.



TRANSPORT

신뢰할 수 있는 연결

- SSH 암호화와 공개키 인증
- 서버 호스트 키 검증
- 외부 HTTPS 인증서 검증

ACCESS

제한된 접속 권한

- 전용 SSH의 제한된 명령 실행
- Agent별 Unix 계정과 소켓 분리
- 허용된 이름·정의에 따른 연결

ADMINISTRATION

관리자 계정 보호

- 등록 완료 계정의 OTP 로그인
- 일회용 복구 코드
- 로그인 시도 제한·세션 관리

서비스 운영자가 함께 관리할 부분

공개 프로그램의 접근 제어, 서버·클라이언트 업데이트, 개인키 보관, 로그 점검, 백업·복구. 콘솔 OTP는 공개 웹서비스에 자동 적용되지 않으며 PGROK가 WAF·DDoS 방어를 제공한다고 의미하지 않습니다.

GET STARTED

작은 서비스 하나부터, 검증하면서 확장합니다.



01

현황 확인

원본 주소·포트, 공개 범위와 네트워크를 확인합니다.

02

서버 준비

도메인, 공유기 경로, SSH와 중계 서비스를 구성합니다.

03

클라이언트 연결

Agent 키와 호스트 키를 확인하고 Tunnel을 등록합니다.

04

운영 검증

외부 응답, 인증서, 재연결과 복구 절차를 확인합니다.

Copyright since 2017 FTH-Korea