pill-tong

the easy & open way to include filtering layers

K-Shield Jr. 4 ¦ Maverick

Background

2017년 한국인터넷진흥원에 신고된 사이버 침해사고 390건 중 381건이
상대적으로 보안이 취약한 영세 및 중소기업을 대상으로 한 공격인 것으로 조사되었다.

정보 유출 시
피해가 예상되는
중소기업

81%

50인 미만 중소기업
보안 정책 수립률

13%

중소기업 대상
침해사고 발생 빈도

97%

중소기업
보안 요구

출처 : 한국인터넷진흥원 보고서

Problem

영세 및 중소기업에게도 보안은 매우 중요하며 기업 또한 이를 인지하고 있다.
그러나 효율을 추구하는 중소기업의 특성상 다른 우선순위에 밀리는 경우가 대다수이다.

정보보호에 투자하지 않는 이유

높은 비용 / 전문가 부재 / 기술적 이해 부족

79.7%

데이터를 주고받을 때
메시지를 필터링하는 계층을
모듈화 + 오픈소스화 하여 제공한다면 ?...

쉽게 설치 가 가능하면서도
지속적으로 진화하는 다양한 공격에도
최소한의 대비가 가능하지 않을까

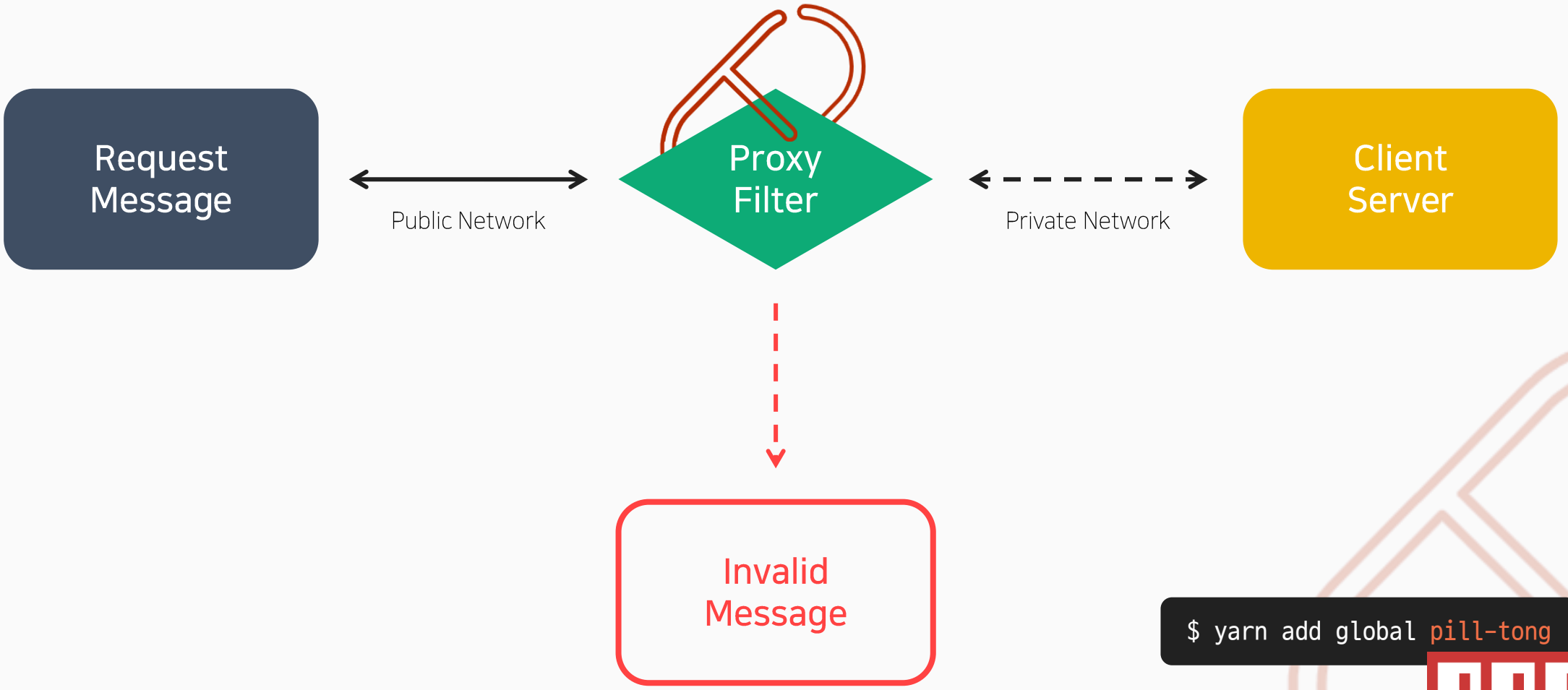
출처 : 지란지교소프트 보안 솔루션 연구소

Solution

Reverse Proxy 를 이용하여 메시지를 필터링 할 수 있는 레이어를 구성.

이를 통해 실제 서버에 도달하기 전 정상 메시지 여부를 판별하도록 하여, 1차적인 기술적 보호 대책을 마련하도록 한다.

또한, 이를 명령 하나로 쉽게 설치할 수 있도록 제공한다.

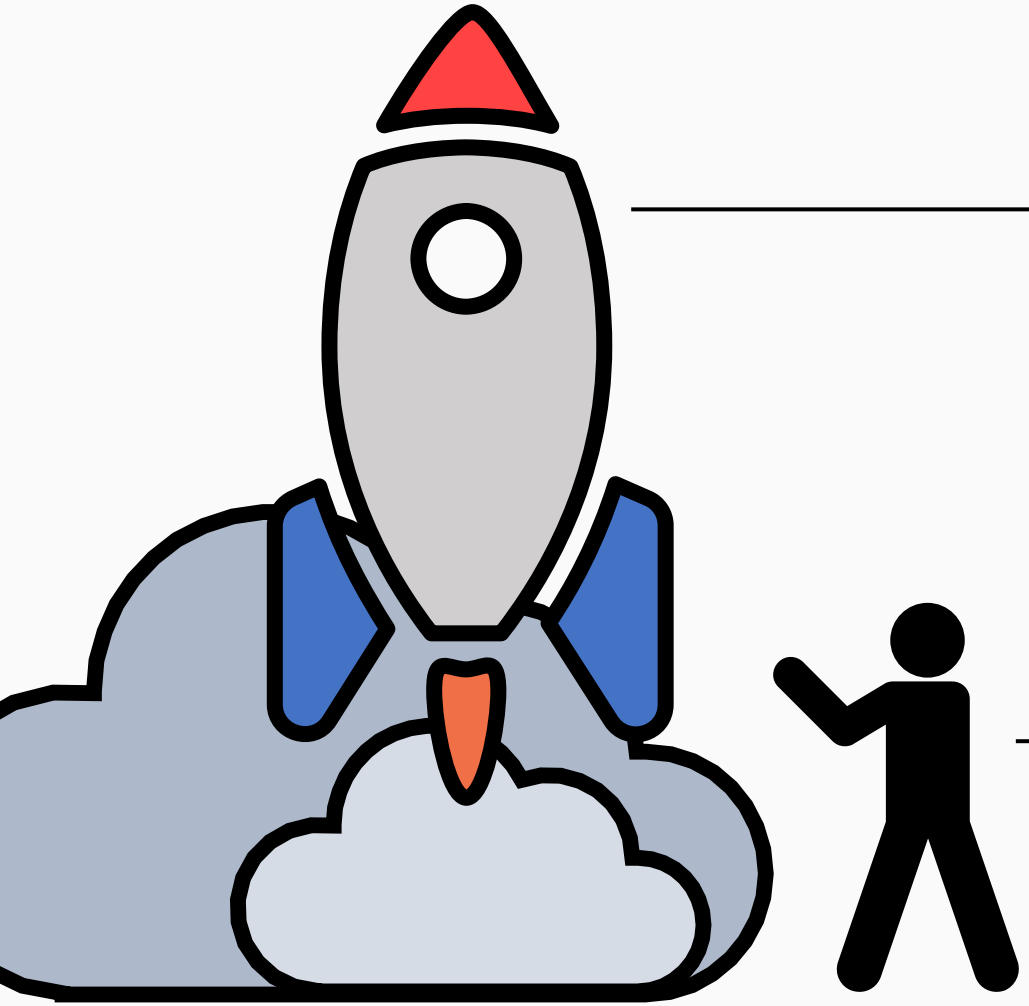



```
$ yarn add global pill-tong
```

Target

상대적으로 보안에 투자하기 어려운 보안 취약 계층을 주 타겟으로 한다.

1차 타겟은 창업 3년 이하의 소규모 스타트업을, 2차 타겟은 대학 및 일반 연구소를 목표로 하고 있다.



[1차 타겟]

창업 후 3년이 지나지 않은
IT 기술 기반의 소규모 스타트업

약 12,968 개 (1.2%)

[2차 타겟]

대학, 기업부설 및 기관 연구실

약 79,223 개

출처 : 중소벤처기업부 창업기업실태조사, 국가연구안전정보시스템 연구실 실태조사

간단한 설치 및 사용

온라인 리포지토리를 통해 패키지를 배포하여
몇 줄의 명령으로 설치 및 레이어의 구성이 가능하다.

설정 파일을 이용한 필터 모듈화

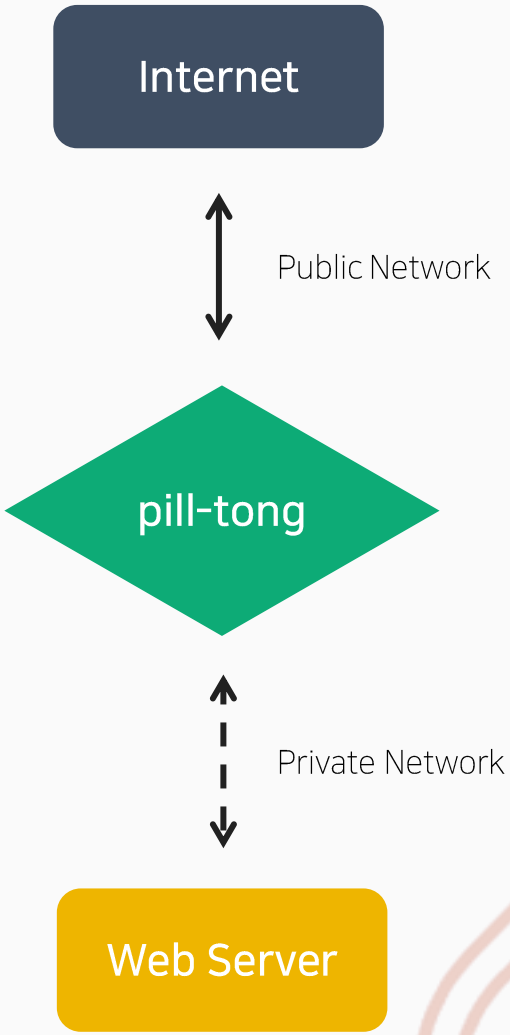
설정 파일을 통해 프록시 서버의 구성이 가능하도록 분리하였다.
이를 통해 사용을 원하는 필터만으로 서버를 구성할 수 있으며,
또한 자신이 직접 필터를 만들 수도 있다.

* 현재 xss, sqli, owasp 필터가 구현됨

```
# client configuration
client:
  host: 'localhost'
  port: 3000

# pill-tong proxy server configuration
proxy:
  port: 80

# filter lists
filters:
  - 'xss-filter'
  - './filter/my-filter'

# ssl configuration
ssl:
  key: './cert/private.pem'
  cert: './cert/public.pem'
```

기존 서버 환경 유지

pill-tong 은 Reverse Proxy 기반으로 동작하기에,
포트를 제외한 기존 서버의 환경 및 코드는 바뀌지 않는다.



HTTPS 지원

pill-tong 은 key, cert 파일을 이용하여
기밀성, 무결성, 인증 세 가지 요소가 보장되는
TLS 프로토콜 또한 지원한다.

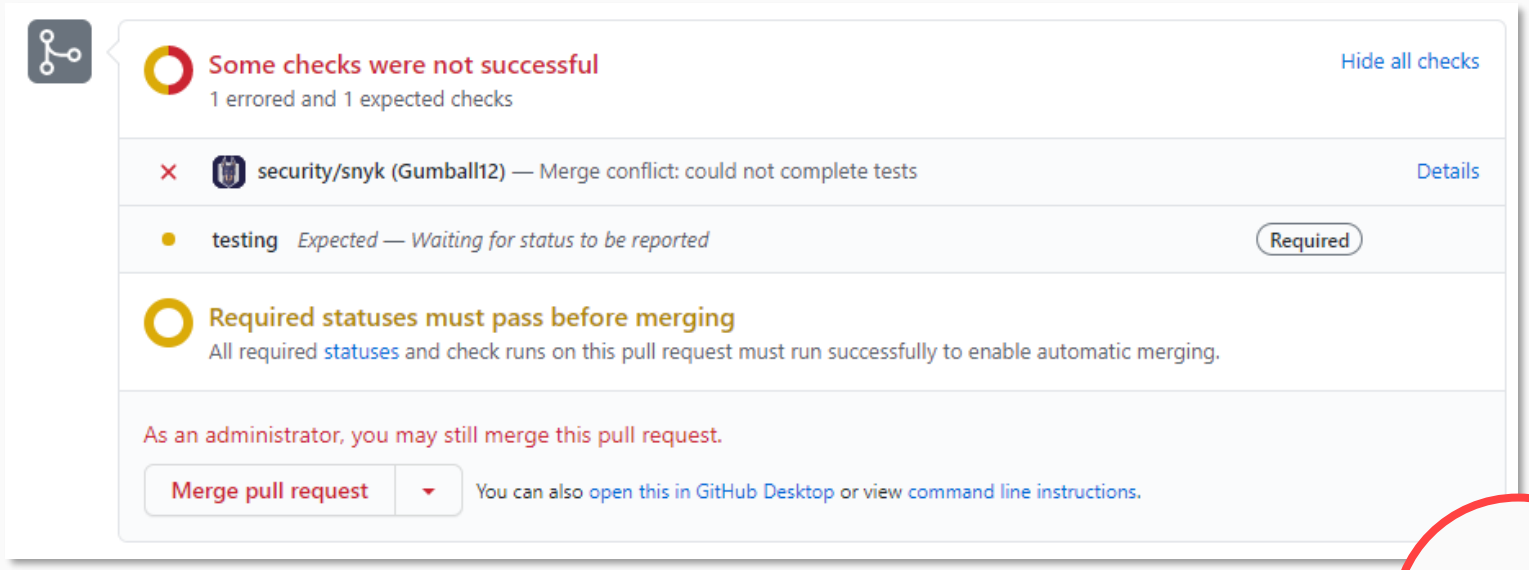

```
# ssl configuration
ssl:
  key: './cert/private.pem'
  cert: './cert/public.pem'
```

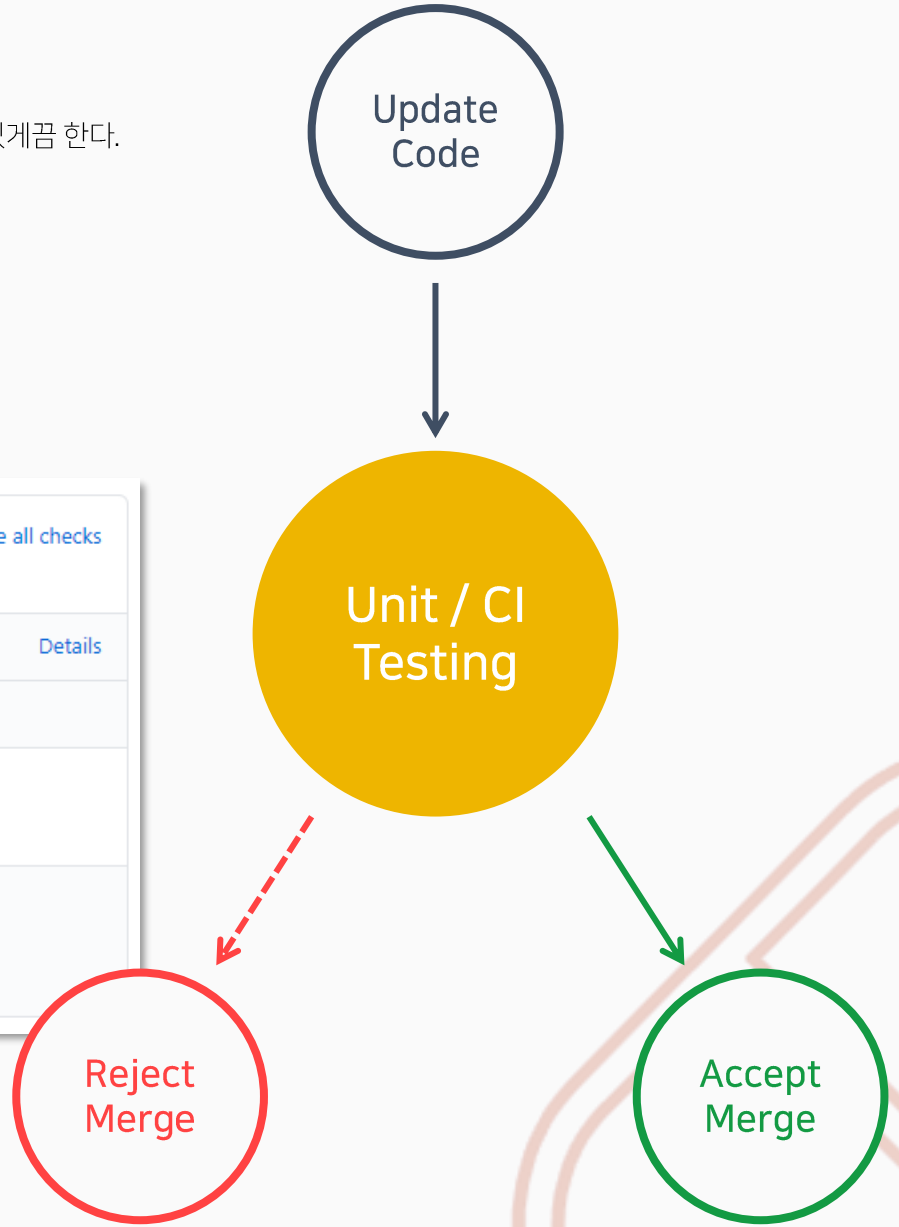
Development Security

pill-tong 은 GitHub Action 기반의 CI & CD 자동화 워크플로우를 구성하였으며,

이를 통해 변경 사항이 발생될 때마다 Unit Testing 및 CI Testing 이 진행되고, 성공 시 자동으로 배포가 진행됩니다.

이는 일정 수준 이상의 품질을 유지할 수 있게 할 뿐만 아니라, 변경 사항으로 인해 발생될 수 있는 보안 이슈 또한 최소화할 수 있게끔 한다.





Development Security

pill-tong은 취약점 탐지 라이브러리인 Snyk 을 이용하여
CI Testing 마다 코드 내 CVE 데이터베이스 기반의 취약점 탐지 및
코드에서 사용하는 다른 모든 라이브러리들에 대한 취약점 발생 여부를 상시 모니터링 하고 있다.

- CVE, CWE 등 취약점 데이터베이스 기반 코드 내 취약점 탐지
- 사용하는 모든 라이브러리에 대한 취약점 발생 여부 모니터링
- 라이브러리 및 코드에 취약점 발생 시 자동 패치 워크플로우 구성

About

pill-tong 은 git 기반의 형상 및 버전 관리를 하고 있으며,

GitHub 및 NPM 리포지토리를 통해 배포를 하고 있다.

(GitHub: https://git.io/JJkZ0, NPM: https://www.npmjs.com/package/pill-tong)