Metadefender ICAP

[Web Proxy 연동]

웹 프락시 연동을 통한
인터넷 웹 보안 강화

Metadefender ICAP

[Web Proxy 연동]

ICAP 프로토콜이란?

- ICAP(Internet Content Adaptation Protocol)
- ICAP 프로토콜은 원격에서 HTTP 메시지를 전송하여 원격 프로시저를 호출하기 위해 개발 된 프로토콜로 최근 보안 솔루션들이 웹 보안을 위해 ICAP 프로토콜을 지향하고 있음
- 최근 다양한 벤더 사의 웹 프록시 제품들이 ICAP 프로토콜을 기본적으로 지원

Metadefender ICAP

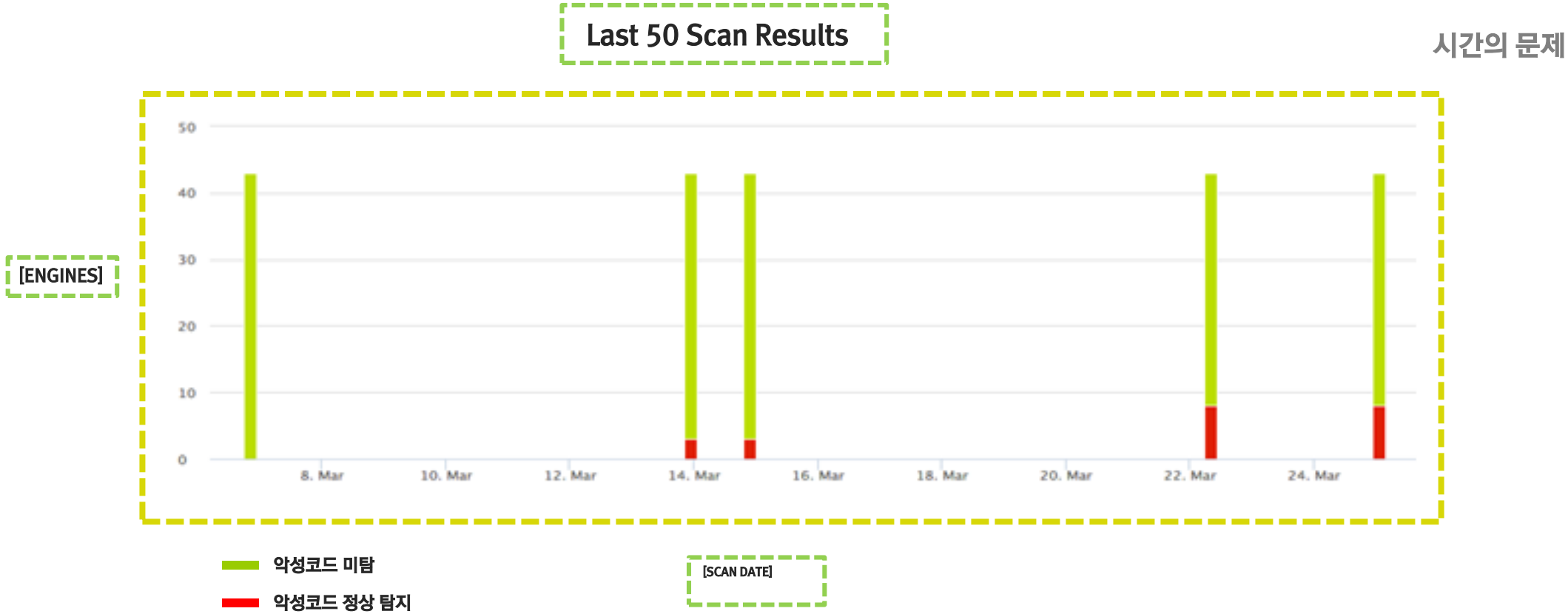
[Web Proxy 연동]

Metadefender ICAP 보안 범위

- **웹 프록시 연동** : 웹 프록시를 이용하는 모든 사용자의 다운로드 행위를 검사하고 위협이 발견 된 다운로드를 차단하여 회사 네트워크 내 악성코드가 유입되는 것을 차단합니다.

- **역방향 프록시 연동** : 악성코드가 기업 내 웹 서버에 업로드 되는 것을 차단합니다.

신종 및 변종 악성코드를 탐지하기까지의 평균 소요 시간



Metadefender ICAP

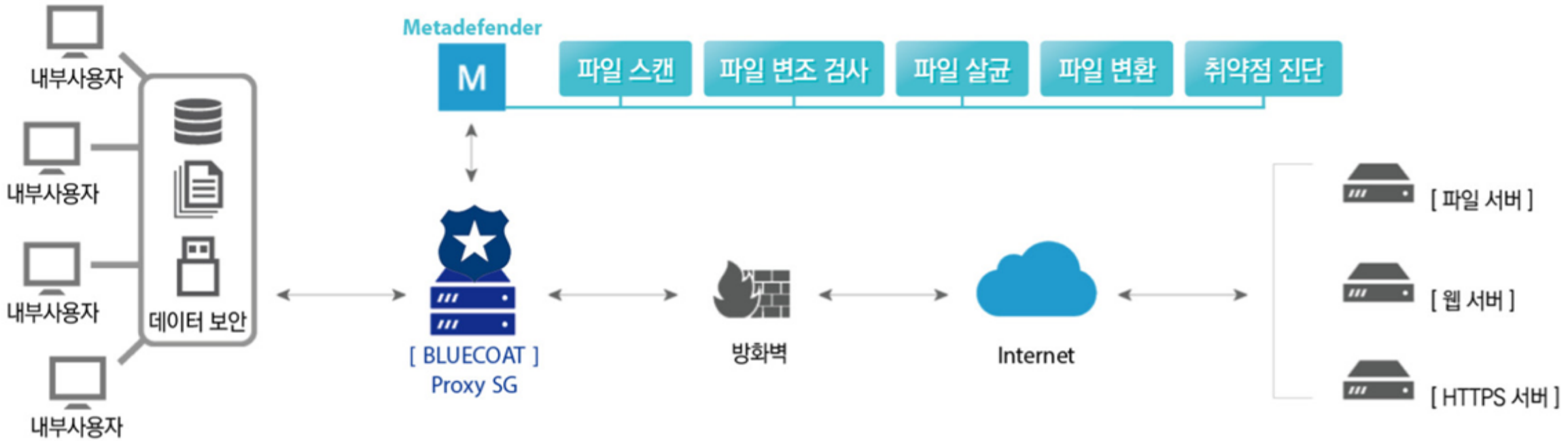
[Web Proxy 연동]

Metadefender 패키지 별 평균 탐지 시간

Metadefender package	악성코드 발생 시 평균 탐지 시간
Metadefender *4*	4 days, 1 hour, 58 minutes
Metadefender *8*	3 days, 9 hours, 42 minutes
Metadefender *12*	1 day, 10 hours, 34 minutes
Metadefender *16*	0 days, 17 hours, 11 minutes
Metadefender *20*	0 days, 8 hours, 52 minutes
Metadefender *30*	0 days, 0 hours, 10 minutes

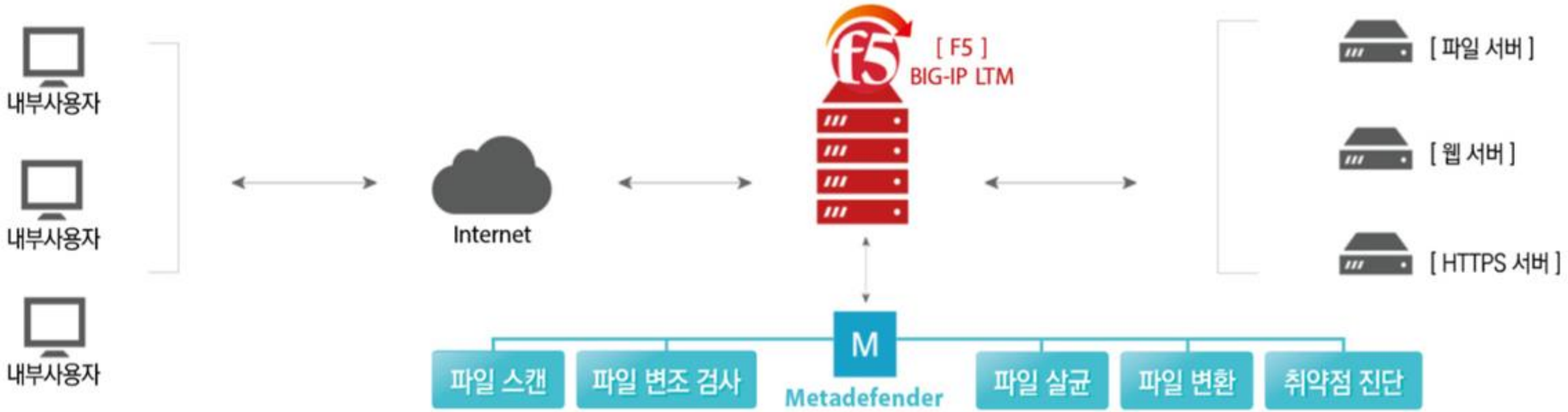
백신 엔진이 많을수록
탐지 시간이 빨라집니다.

웹 보안을 위한 Metadefender 구성 – BLUECOAT SG 연동



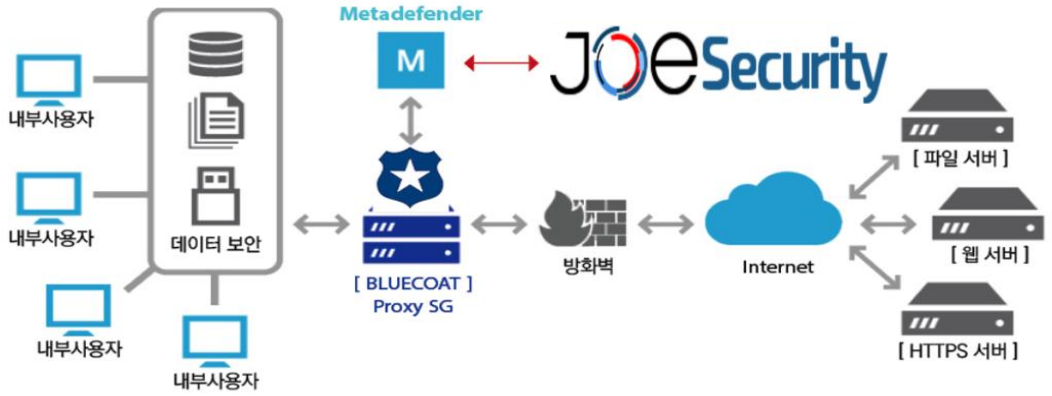
[사용자 웹 보안]

웹 보안을 위한 Metadefender 구성 – F5 BIG-IP 연동

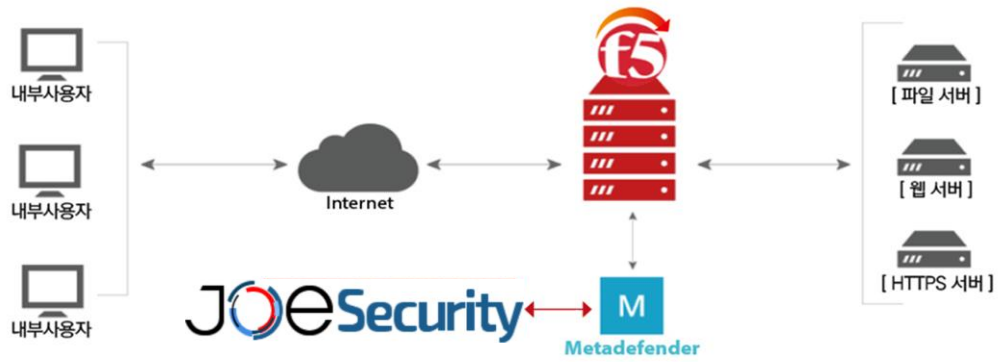


[웹 서버 보안]

웹 보안을 위한 Metadefender 구성 – 웹 프록시 + 행위 분석 시스템 연동

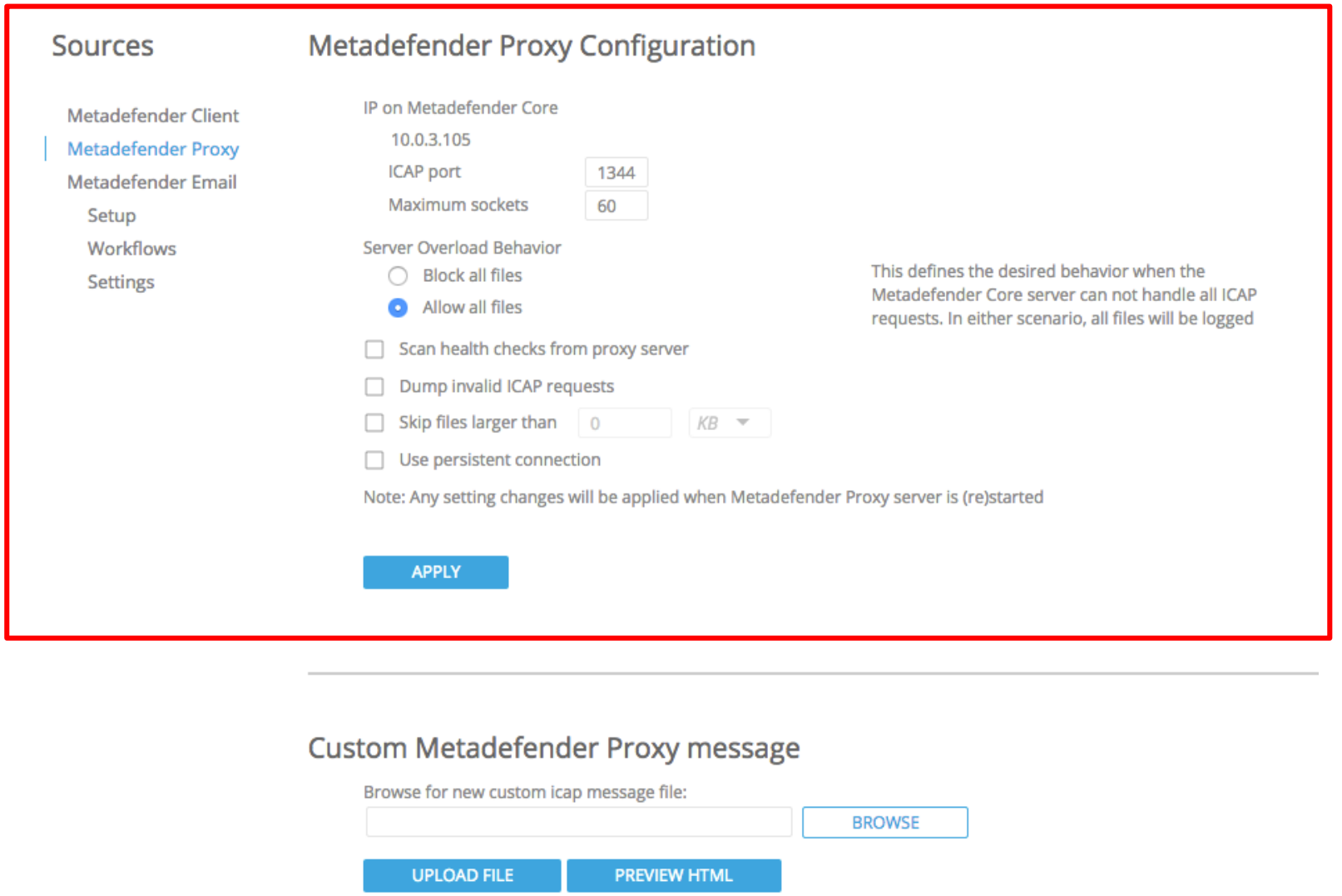


BlueCoat Proxy SG + Joe Sandbox 연동

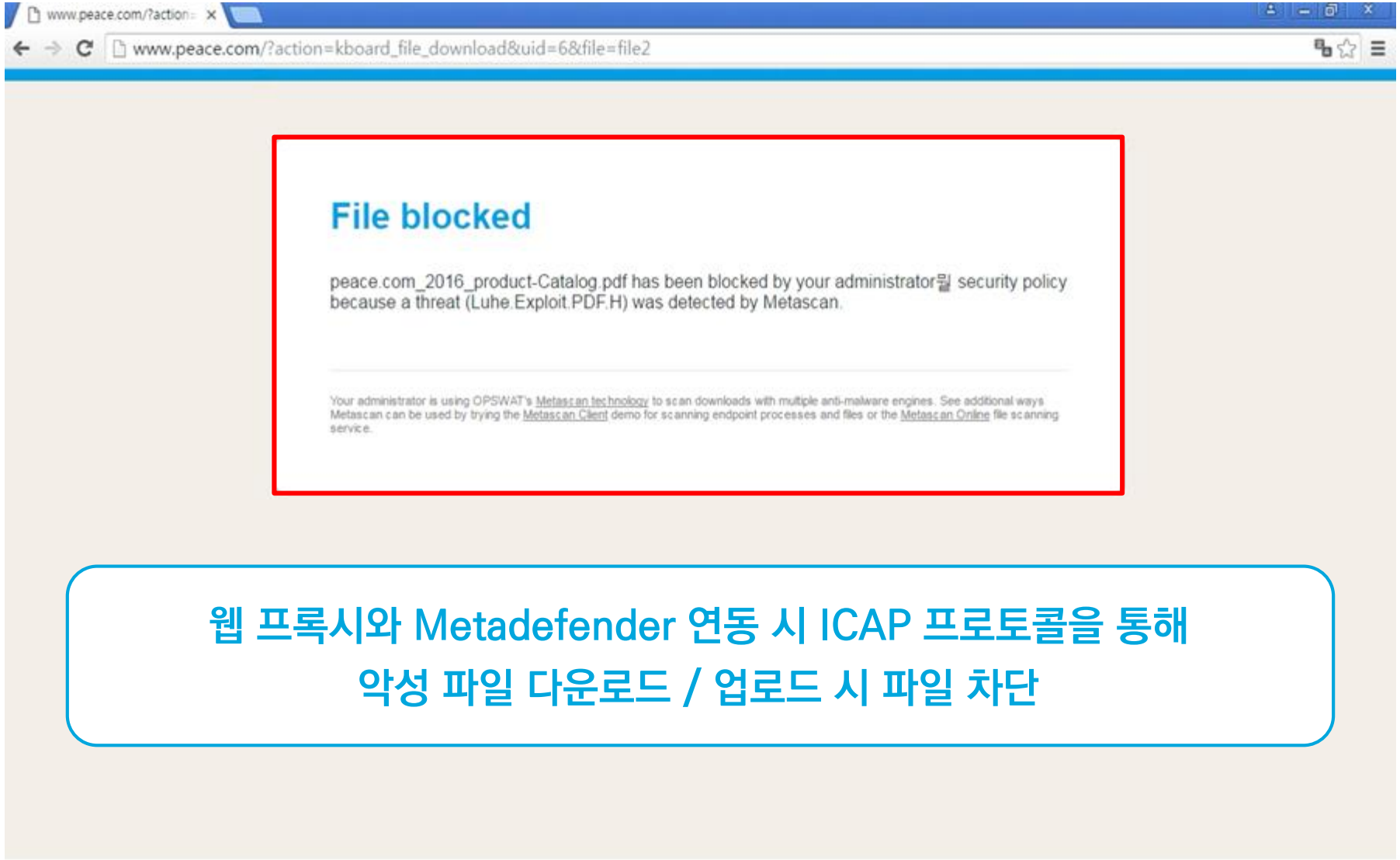


F5 BIG-IP + Joe Sandbox 연동

Metadefender ICAP Server 설정



Metadefender ICAP Server 설정



웹 프록시와 Metadefender 연동 시 ICAP 프로토콜을 통해
악성 파일 다운로드 / 업로드 시 파일 차단

웹 보안을 위한 연동 제품

ICAP 프로토콜을 지원하는 웹 프록시 제품들은 전부 연동이 가능합니다

Squid Proxy

BlueCoat ProxySG

F5 BIG IP

ARA network JAGUAR5000

McAfee Web Gateway