

MudFIX - 보안 / 방화벽 정책

➤ 방화벽 정책 허용 필요

- Inbound (외부 → Mudfix)

출발지	도착지	Protocol	Port	Action	용도
전체 훈련대상	Mudfix	TCP	443 (HTTPS)	Allow	훈련 링크 접속
관리자 PC		TCP	443 (HTTPS)	Allow	WEB 접속
관리자 PC		TCP	22 (SSH)	Allow	SSH 접속

- Outbound (Mudfix → 외부)

- 필수 사항

출발지	도착지	Protocol	Port	Action	용도
Mudfix	인사DB	TCP	확인필요	Allow	인사연동
	메일 서버	TCP	25 (SMTP)		메일 발신
	update.jiran.com 218.234.23.153	TCP	80 (HTTP) 443 (HTTPS)		라이선스 업데이트
	시간동기화 서버	TCP	37 (TIME)		시간동기화
		UDP	123 (NTP)		
	참조 DNS 서버	TCP/UDP	53 (DNS)		DNS 질의

➤ 보안 정책 허용 필요

출발지	도착지	Port	Action	용도
Mudfix	메일 서버	25 (SMTP)	예외처리	* 스팸 또는 거부되지 않도록 메일 서버 내 허용정책 추가 필요 * MTA 구간에 행위분석 (APT)을 하는 장비 또는 기능이 있을 경우 메일을 검사하지 않도록 예외처리 필요 (메일 서버 포함)
전체 훈련대상	Mudfix	80 (HTTP), 443(HTTPS)	예외처리	* 훈련 링크 접속에 이슈가 발생하지 않도록 웹 방화벽 / IPS 장비 내 허용처리
관리자 PC	Mudfix	80 (HTTP), 443(HTTPS)	예외처리	* 훈련 템플릿 수정 및 웹 접속에 이슈가 발생하지 않도록 웹 방화벽/IPS 이외 보안 장비 내 허용처리

☞ 해당 정책은 내부에서 사용중인 보안장비 List 확인 후 상황에 맞는 예외처리가 필요합니다.