

방화벽 규칙 표

방화벽 2 (사용자망 경계, 192.168.2.0/24 ↔ 라우터)

NoSource	Destination	프로토콜/포트	처리	설명
1 192.168.2.0/24	192.168.1.5 (DNS)	UDP/TCP 53	허용	사용자 → DNS 서버 조회
2 192.168.2.0/24	192.168.1.72 (Web E)	TCP 80	허용	사용자 → 웹 포털 접근
3 192.168.2.0/24	192.168.1.68 (Messenger F)	TCP 5222	허용	사용자 → 메신저 서버 접근
4 192.168.2.0/24	192.168.1.36 (Mail C)	TCP 25	허용	사용자 → 메일 서버 송신 (SMTP)
5 192.168.2.0/24	192.168.1.104 (VoIP D)	UDP 38027	허용	사용자 → VoIP 서버 접근
6 192.168.2.0/24	ANY	ANY	차단	사용자 → 그 외 서버/서비스 차단
7 ANY	ANY	ANY	차단	최종 차단(기본 정책)

방화벽 1 (서버망 경계, 192.168.1.0/24 ↔ 라우터/인터넷)

NoSource	Destination	프로토콜/포트	처리	설명
1 ANY	192.168.1.5 (DNS)	UDP/TCP 53	허용	DNS 서버는 내·외부 누구나 접근 가능
2 192.168.1.72 (Web E)	192.168.1.233 (DB B)	TCP 3306	허용	DB는 웹 포털 서버만 접근 허용
3 ANY	192.168.1.36 (Mail C)	TCP 25	허용	메일 서버는 내·외부 누구나 접근 가능 (SMTP)
4 ANY	192.168.1.104 (VoIP D)	UDP 38027	허용	VoIP 서버는 내·외부 누구나 접근 가능
5 192.168.2.0/24	192.168.1.72 (Web E)	TCP 80	허용	웹 포털은 사용자 영역에서만 접근 허용
6 192.168.2.0/24 (사용자 영역)	192.168.1.68 (Messenger F)	TCP 5222	허용	메신저 서버는 사용자 영역에서만 접근 허용
7 ANY	ANY	ANY	차단	그 외 모든 트래픽 차단(기본 정책)