ZYXEL
Your Networking Ally

User Guide

방화벽(UTM)보안 기본 설정 가이드

UTM Security Basic Configuration Guide



ZYXEL
Your Networking Ally

Contents

1. 2FA 인증 (E-mail or Google authenticator)

- 관리자 및 VPN 계정에 2단계 인증 적용

2. 비밀번호 정책

- 60일 주기 비밀번호 갱신, 복잡도 요건 강제 설정

3. 보안정책 관리

- 보안 정책 제어 활성화 (ACL, TCP Flood 차단 등 방화벽 정책 활성화)

4. WAN 접근 제한 (장비)

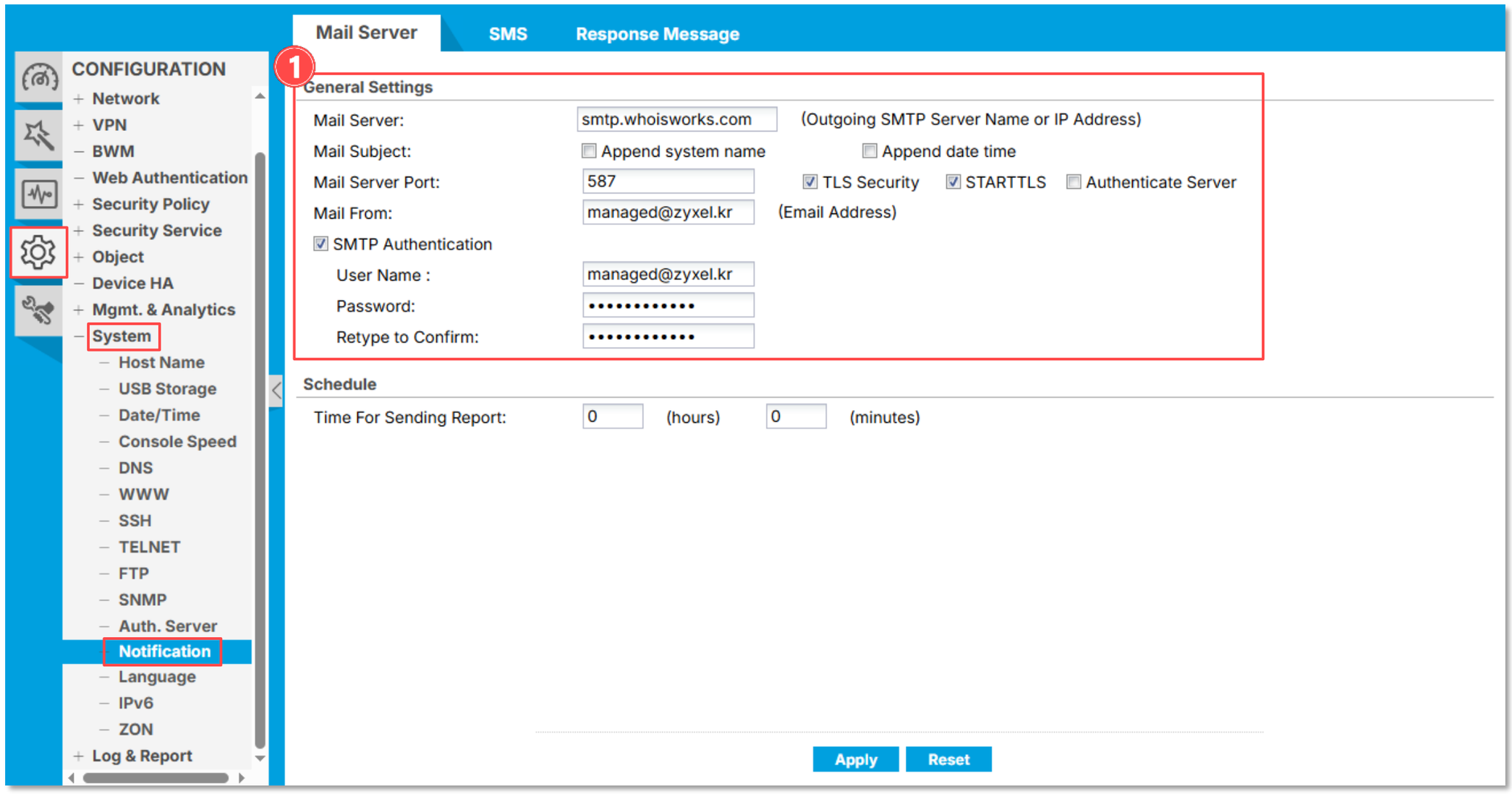
- 불필요한 원격 관리 서비스(HTTP, HTTPS, PING, SSH, SSL VPN 등) 차단
- 허용된 특정 IP / 지역에 한해서만 접근 허용

5. 펌웨어 업데이트

- 최신 펌웨어 업데이트 적용
- 스케줄 펌웨어 업데이트 적용

2FA 인증 : E-mail

메일 서버 설정



Remark

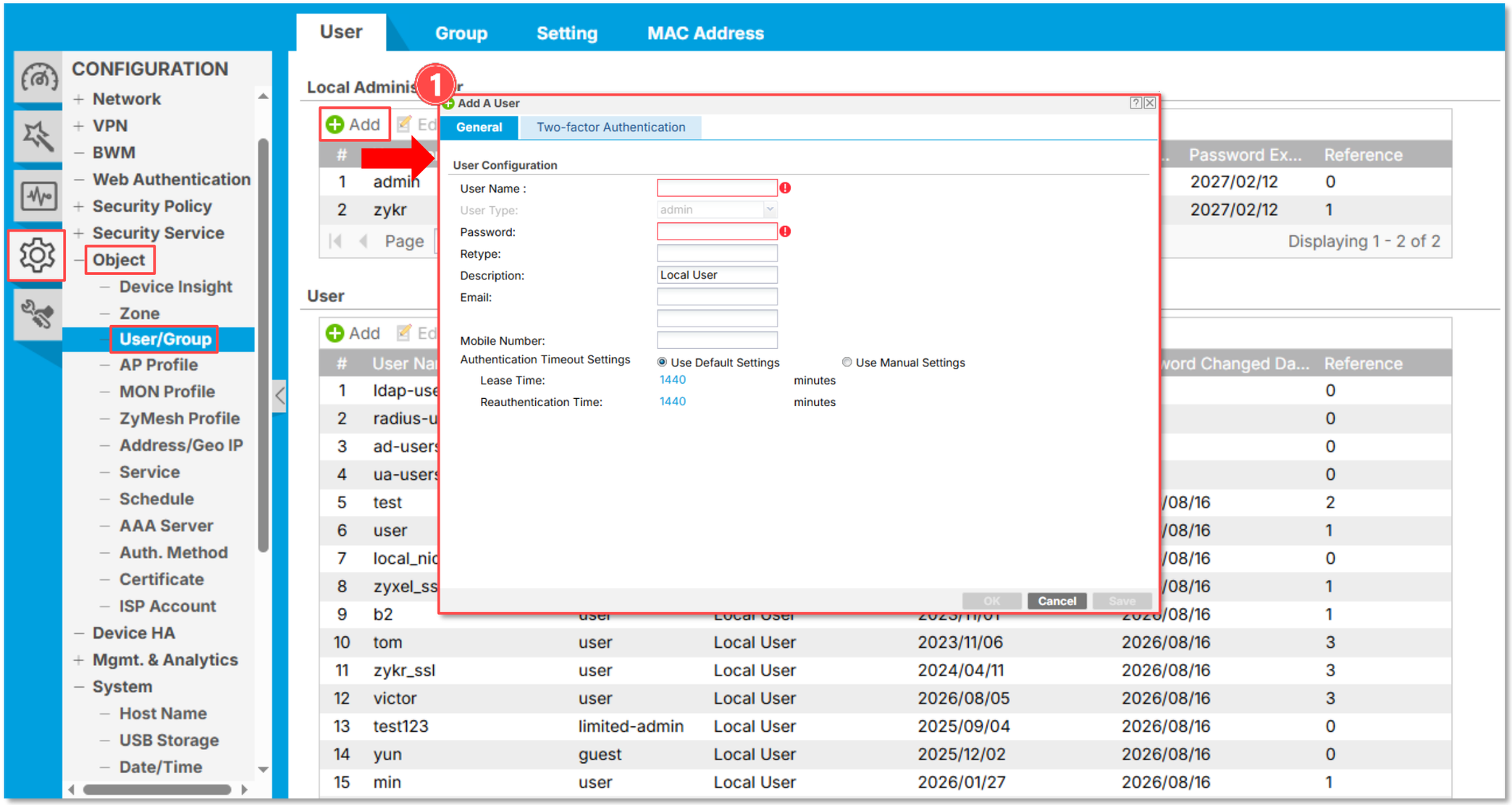
Configure → System → Notification

1 Mail Server 설정 (보내는 사람 설정)

- ✔ Mail Server : SMTP 서버 이름 또는 IP 주소 입력
  (Ex: google의 경우 smtp.google.com)
- ✔ Mail Subject : 장비의 이름 및 날씨/시간을 추가 여부 체크
- ✔ Mail Server Port : 메일 서버에서 사용하는 포트 번호 입력
- ✔ Mail From : 보내는 사람 메일 주소
- ✔ SMTP Authentication : 체크(필수)
  → 메일 계정 정보 입력

2FA 인증 : E-mail

계정 생성



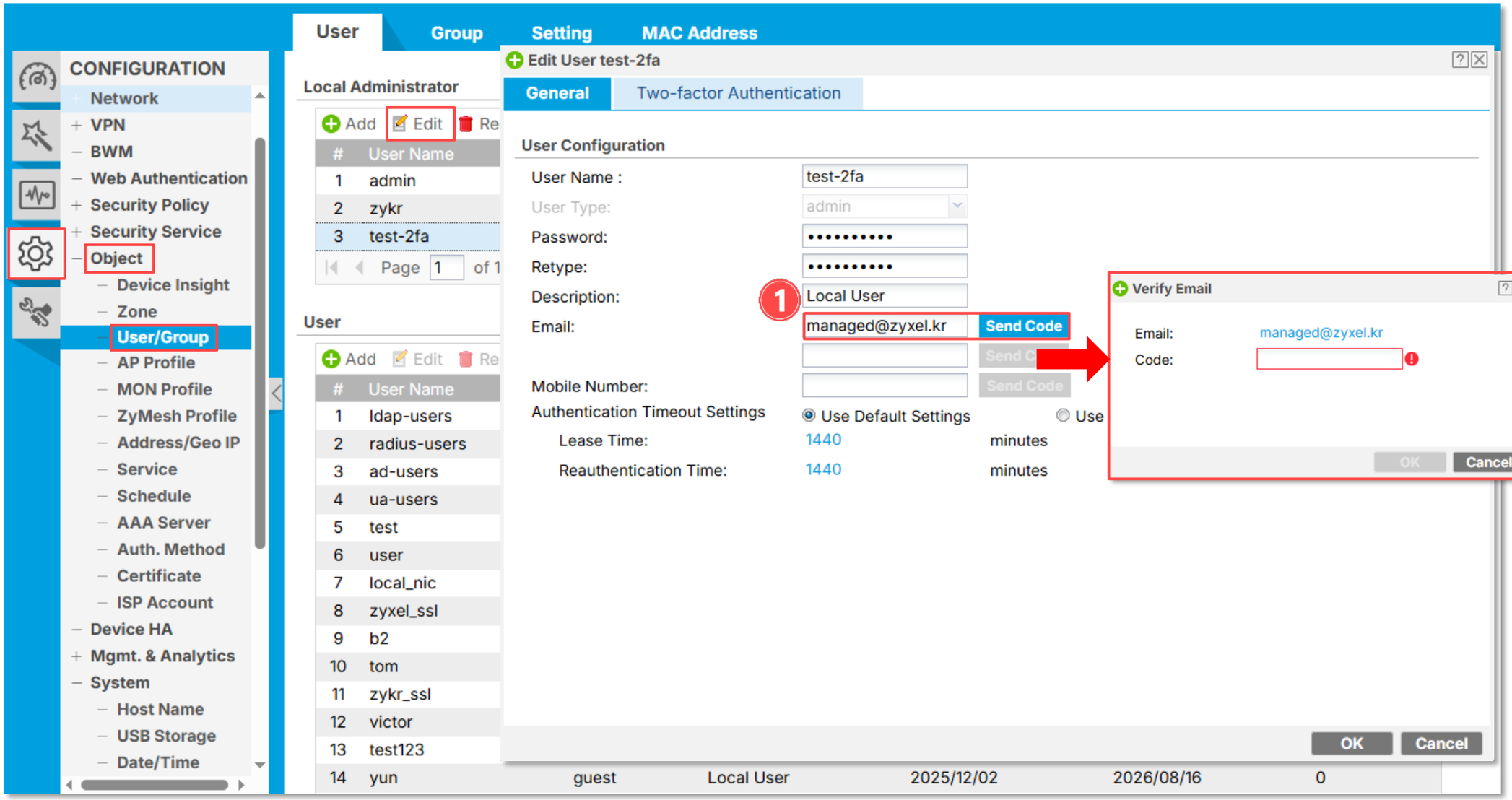
Remark

Configure → Object → User/Group → Local Administrator → +Add

1. Admin 계정 생성
   → User Name / Password / Retype : 계정 정보 입력
   → OK 선택하여 계정 생성
   → 생성된 계정 “Edit”

2FA 인증 : E-mail

메일 인증 설정



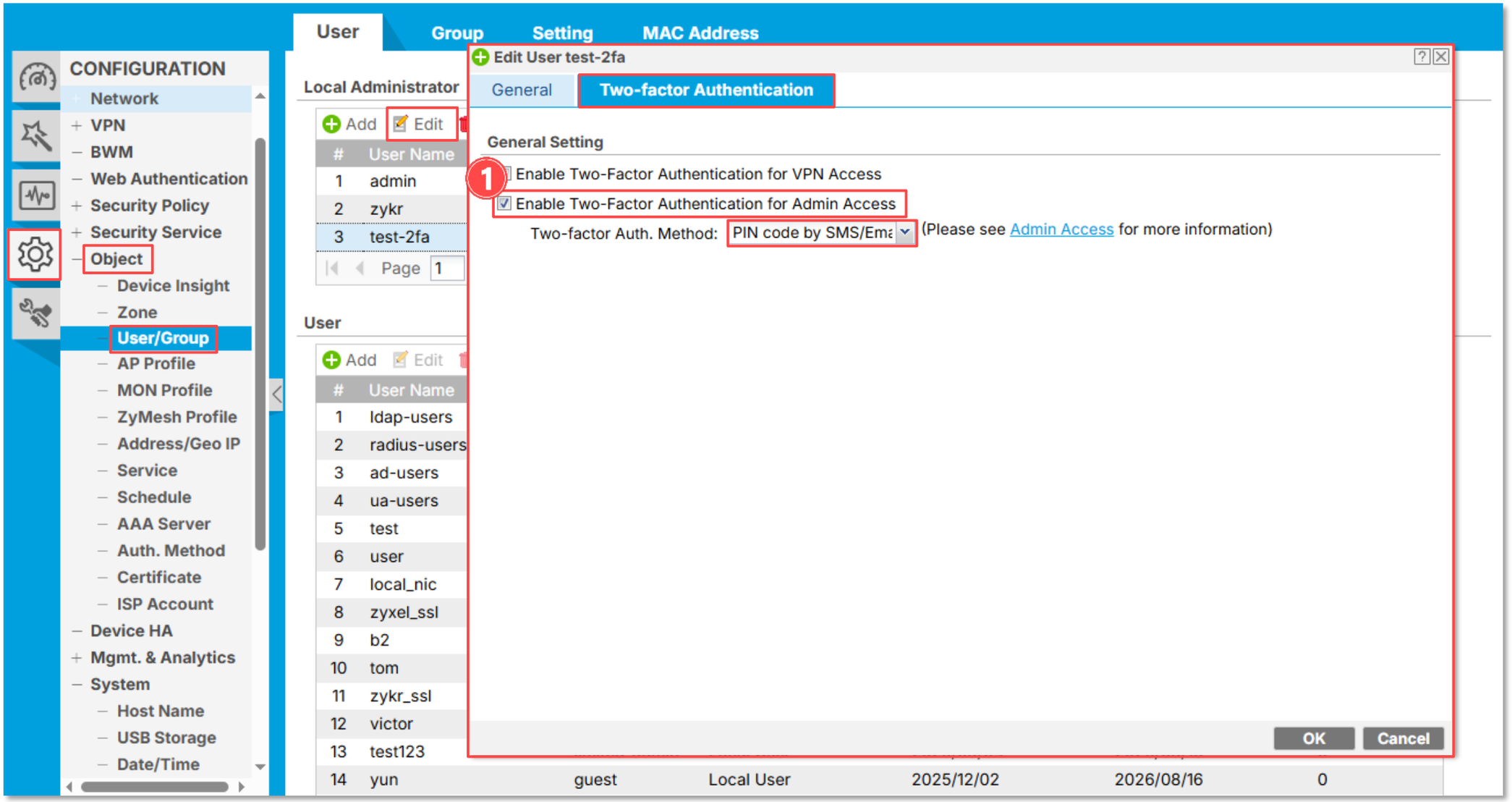
Remark

Configure → Object → User/Group → Local Administrator → Edit

1. Email : 2FA 인증 코드를 받을 메일 주소 작성
   → Send Code : 해당 메일로 전달받은 코드 번호 입력

2FA 인증 : E-mail

관리자 계정 2차 인증 설정



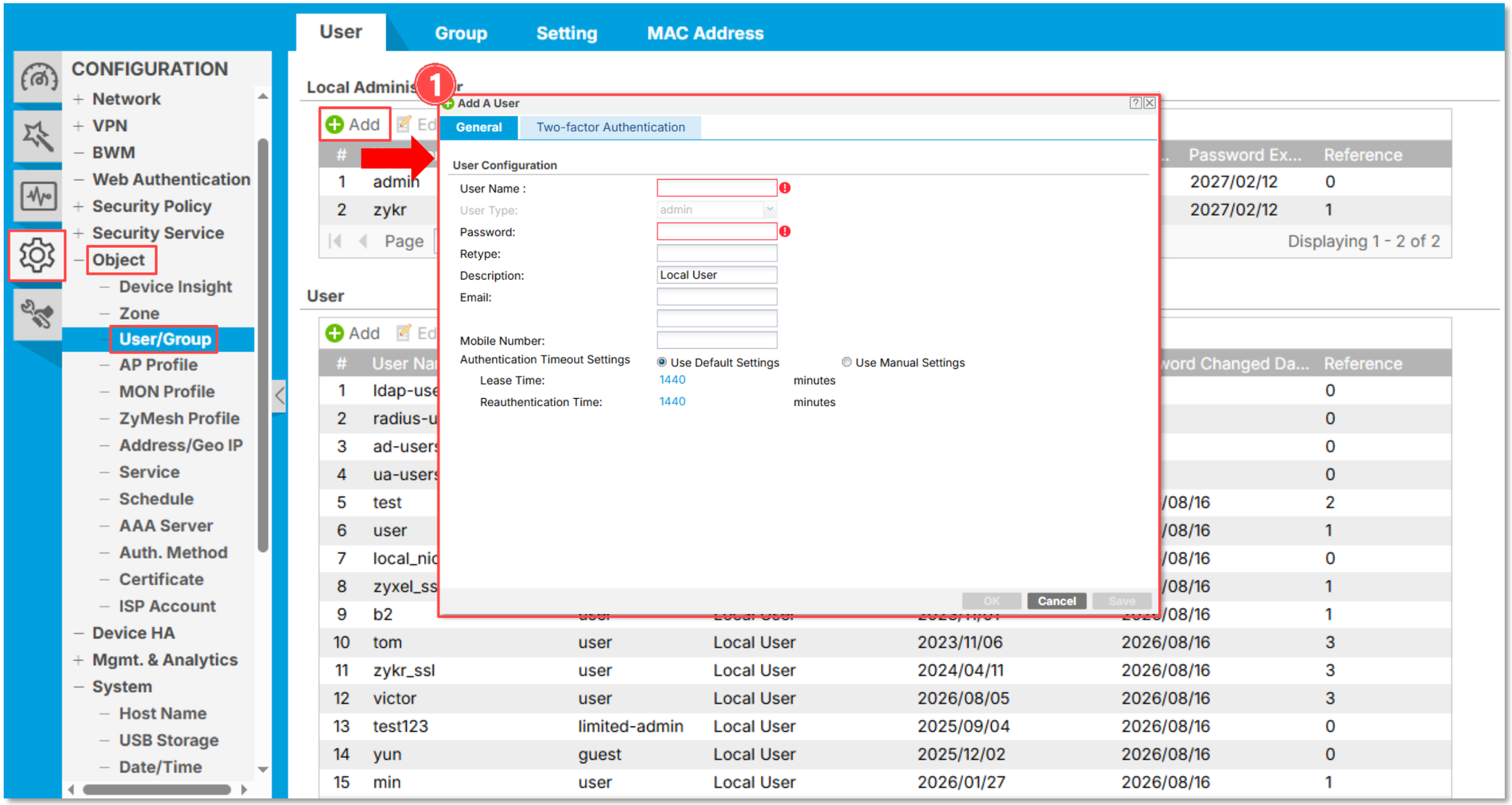
Remark

Configure → Object → User/Group → Local Administrator → Edit → Two-factor Authentication

1. “Enable Two-Factor Authentication for Admin Access” 체크
   → “PIN code by SMS/Email” 선택

2FA 인증 : Google Authenticator

계정 생성



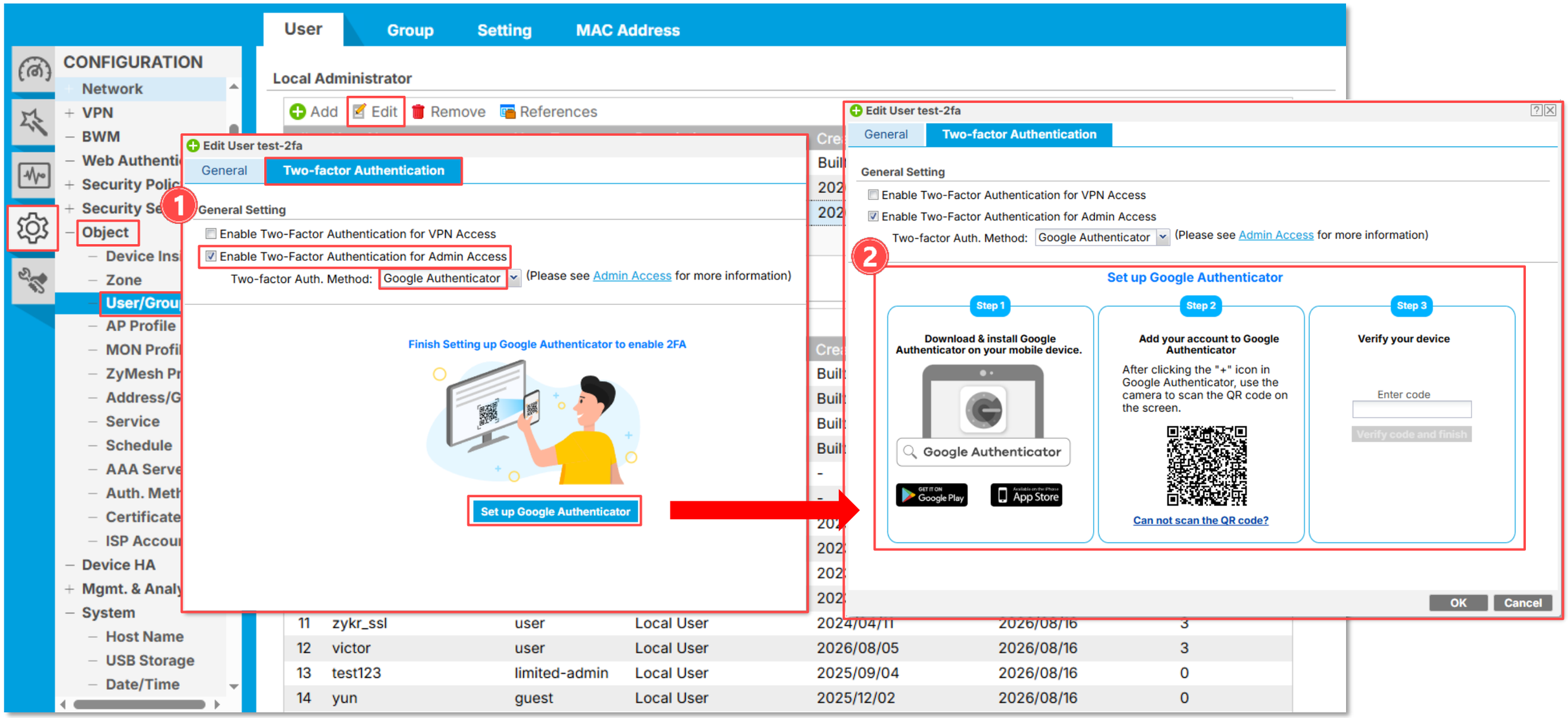
Remark

Configure → Object → User/Group → Local Administrator → +Add

1. Admin 계정 생성
   → User Name / Password / Retype : 계정 정보 입력
   → OK 선택하여 계정 생성
   → 생성된 계정 “Edit”

2FA 인증 : Google Authenticator

관리자 계정 2차 인증 설정



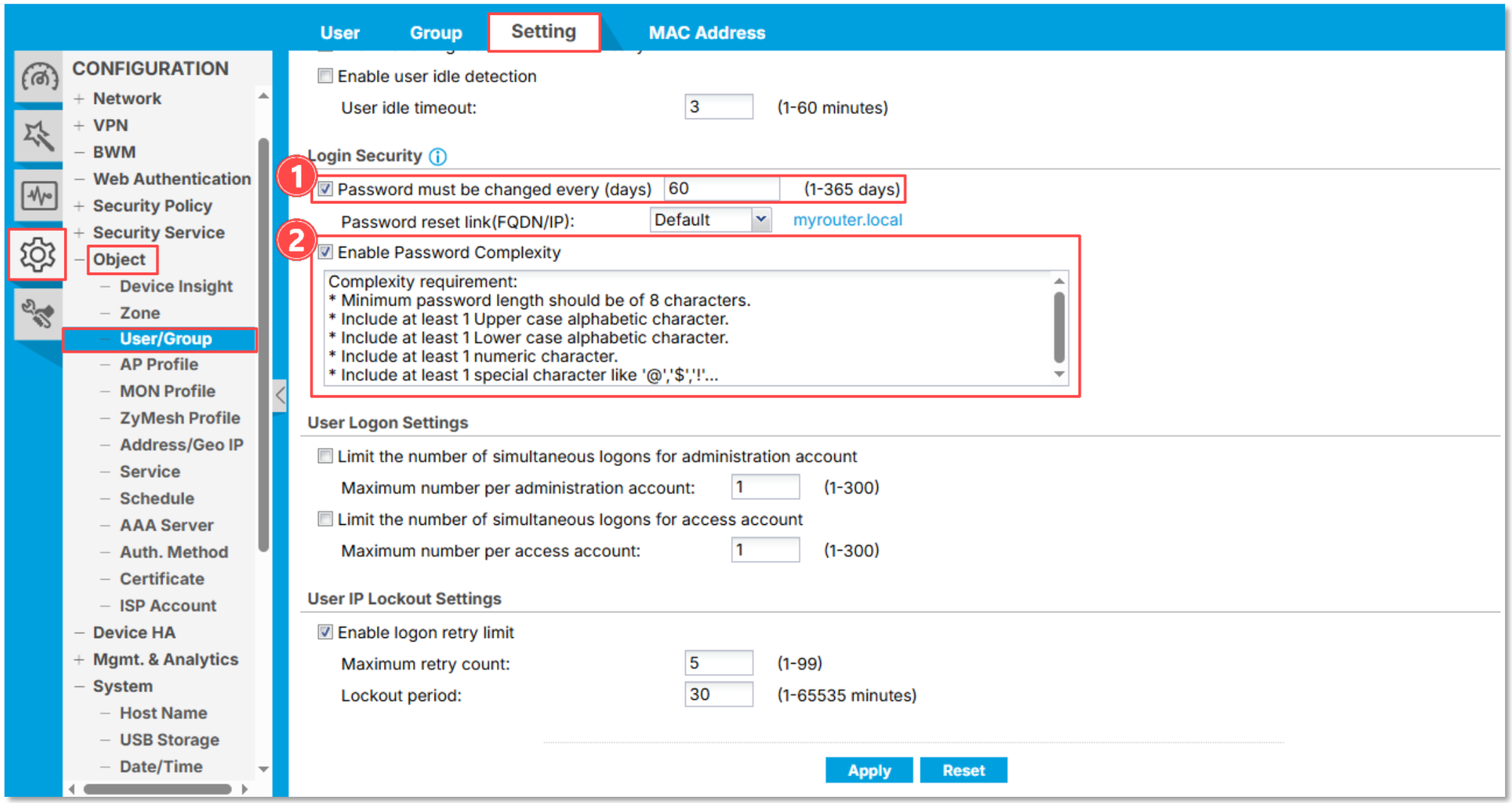
Remark

Configure → Object → User/Group → Local Administrator → Edit → Two-factor Authentication

1. “Enable Two-Factor Authentication for Admin Access” 체크
   → “Google Authenticator” 선택
2. 스마트폰에서 Google Authenticator 어플 설치 → QR 등록 → 생성된 코드 입력

비밀번호 정책

60일 주기 비밀번호 갱신, 복잡도 요건 강제 설정



Remark

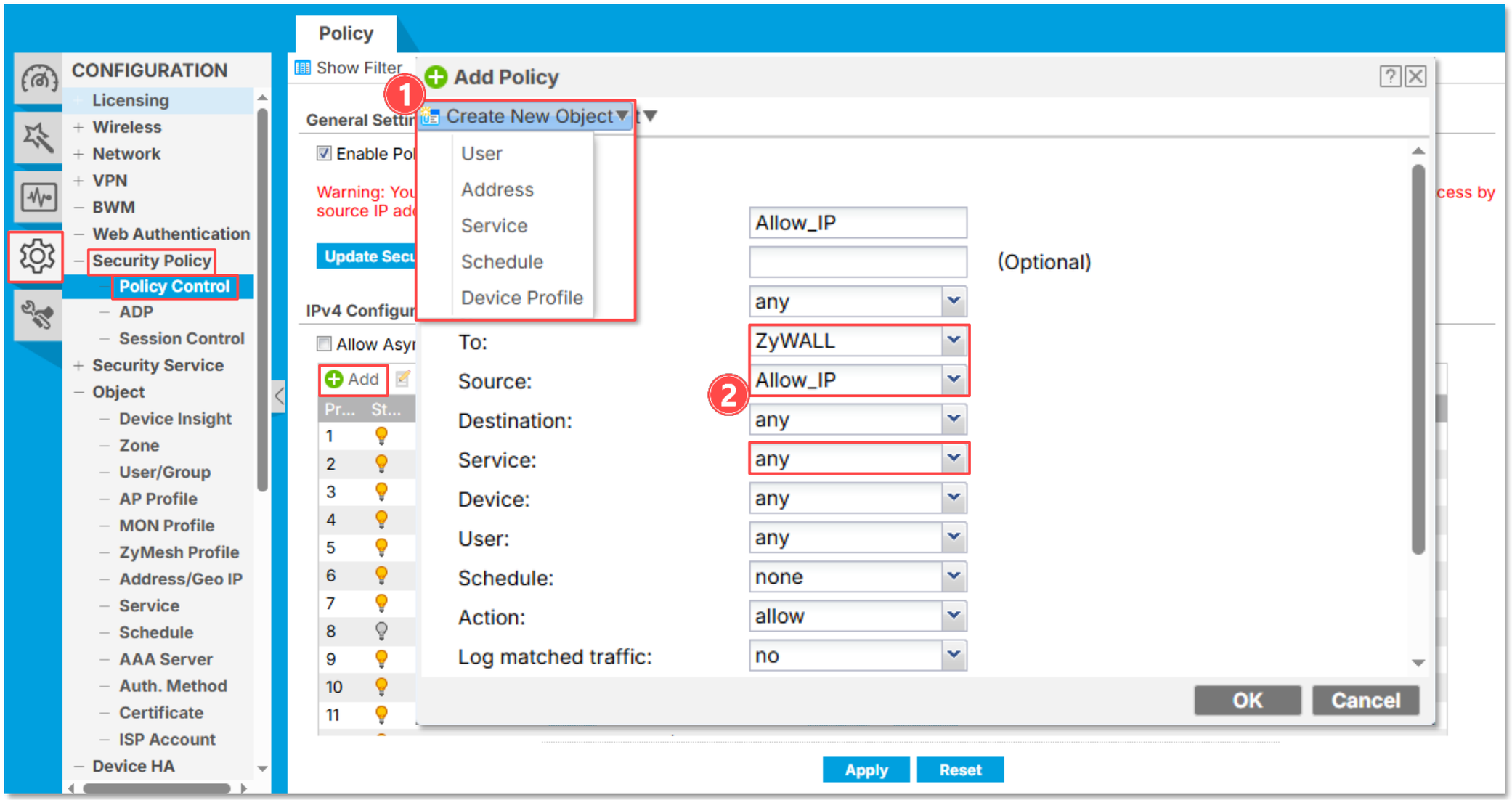
Configure → Object → User/Group → Local Administrator → Edit → Two-factor Authentication

1. “Password must be changed every (days)” 체크
   → 비밀번호 갱신 주기 설정

2. “Enable Password Complexity” 체크
   → 복잡도 요건 설정
   → 설정 후 대문자/소문자/특수문자/숫자가 포함된 최소 8자 이상의 비밀번호 설정 강제

보안정책 관리

ACL 설정 (외부 접근 허용 가능한 IP 설정)



Remark

Configure → Security Policy → Policy Control → +Add

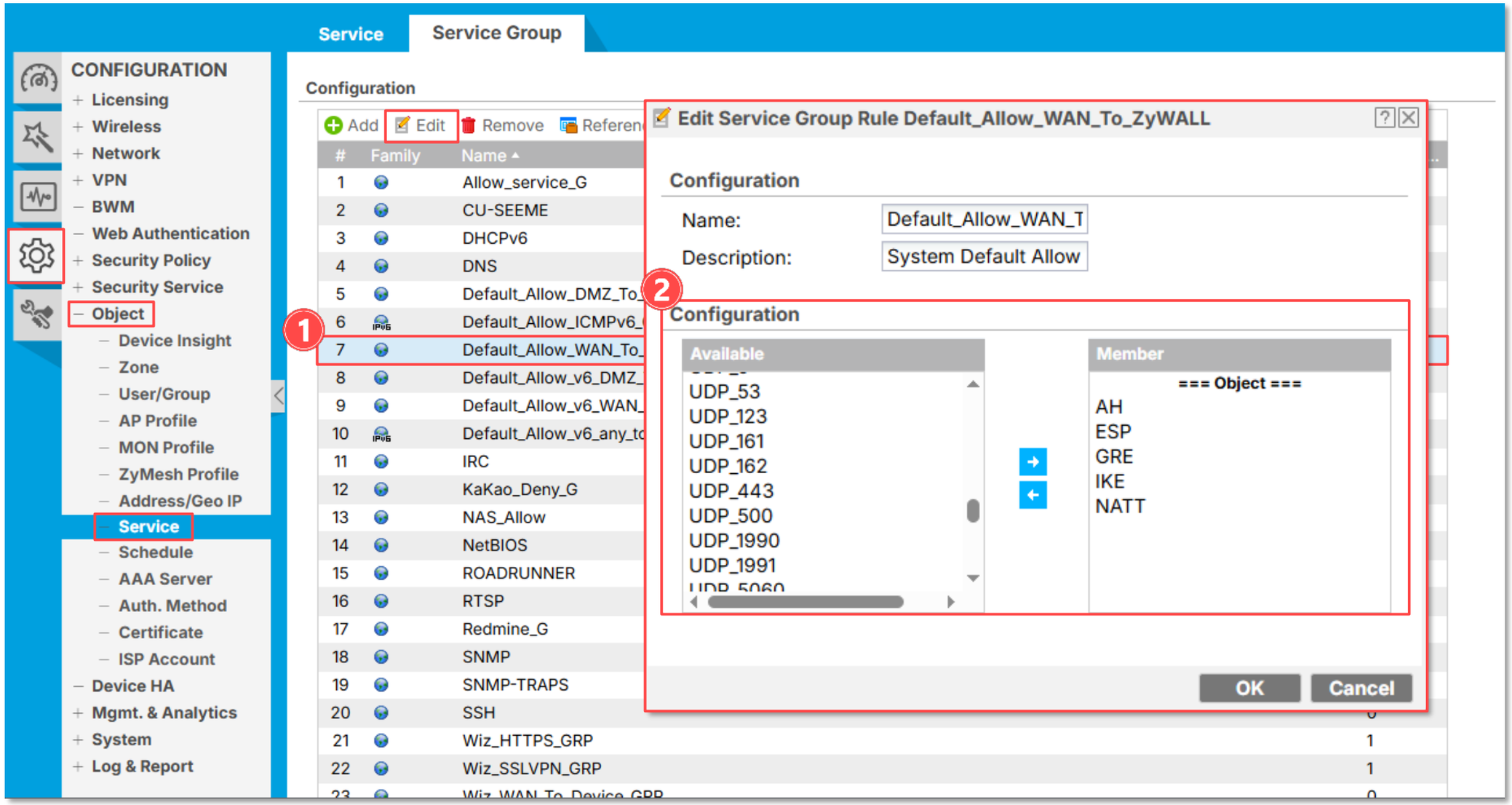
1. “Create New Object” 에서 Address/Service 객체 생성

2. To : ZyWALL
   - ✔ Source : 1 에서 생성한 IP 객체
   - ✔ Service : 1 에서 생성한 서비스 포트 객체

* ZyWALL은 방화벽 설정 GUI/CLI 등의 접근이며 장비 관리자의 IP를 지정하여 외부 침입을 차단할 수 있다.

보안정책 관리

외부 접근 포트 허용



Remark

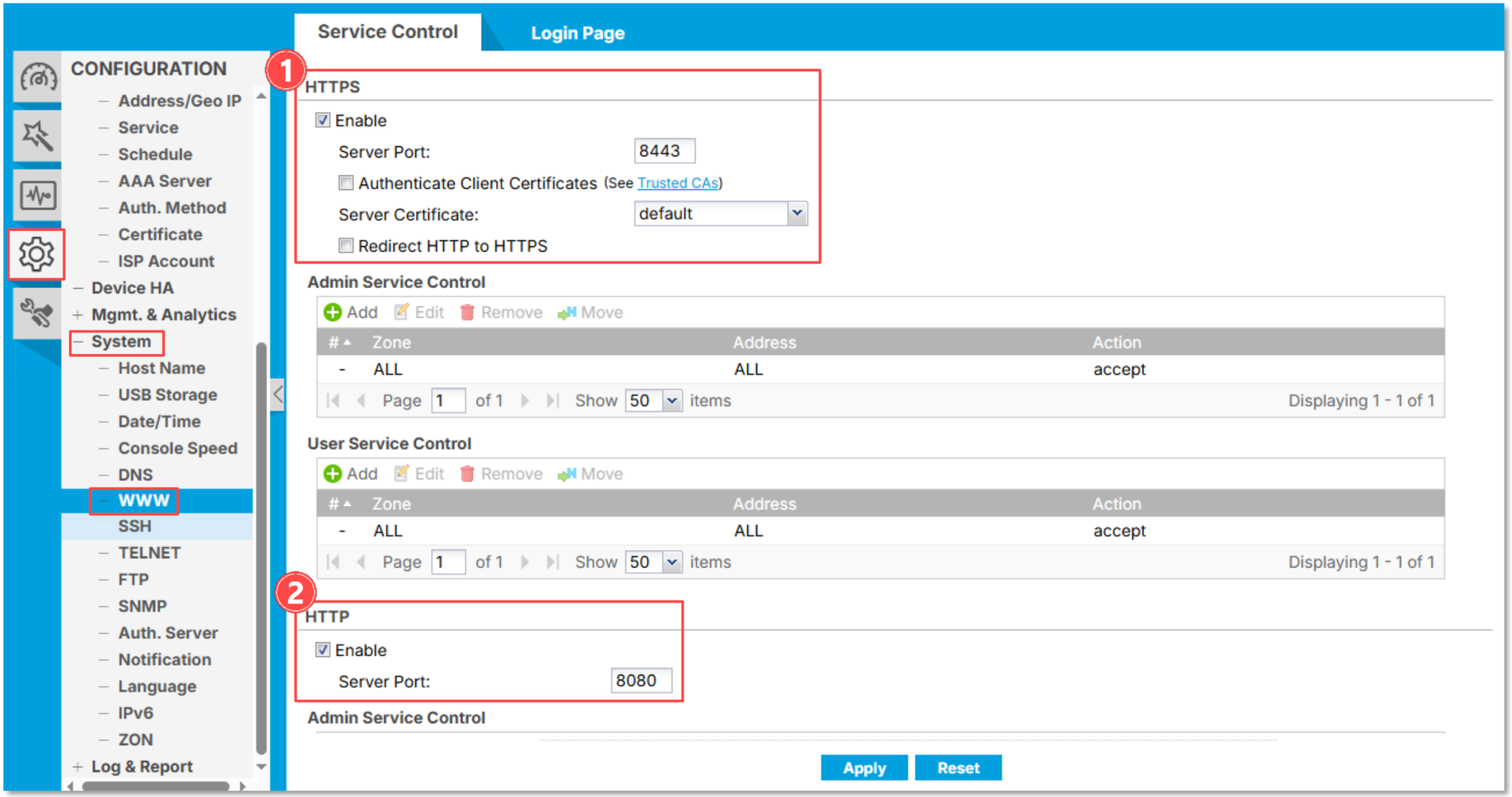
Configure → Object→ Service → Service Group

1. “Default_Allow_WAN_To_ZyWALL” Edit
2. Available에서 Member로 원하는 서비스 포트 이동

* 해당 서비스 그룹 객체는 외부에서 방화벽으로의 접근을 허용할 포트 설정으로 전체 오픈해야 할 포트만 설정 필요

WAN 접근 제한 (장비)

외부 접근 포트 변경



Remark

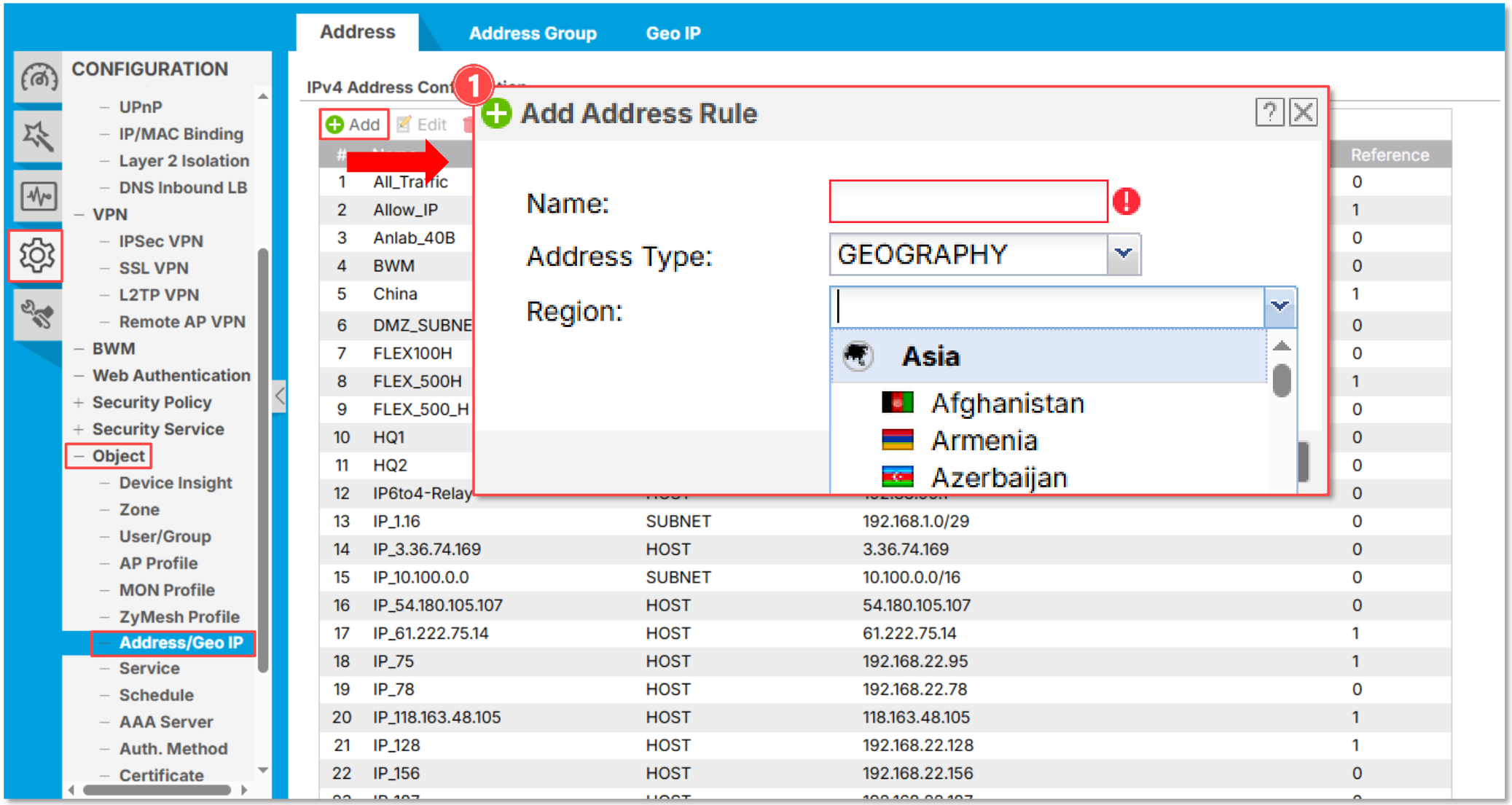
Configure → System → WWW

1. HTTPS : 외부에서 장비 접근을 위한 포트 (기본 443)
   → ex: 기본값 443 -> 8443으로 변경 시 https://공인IP:8443 으로 외부에서 장비 접근 가능

2. HTTP : 외부에서 장비 접근을 위한 포트 (기본 80)
   → Ex: 기본값 80 -> 8080으로 변경 시 http://공인IP:8080 으로 외부에서 장비 접근 가능
   → 보안 관련하여 HTTP는 Disable 권장

WAN 접근 제한 (장비)

한국 IP를 제외한 해외 모든 IP 차단 설정



Remark

Configure → Object → +Add

1 ✔ Name : 이름 지정

✔ Address Type : “GEOGRAPHY” 선택

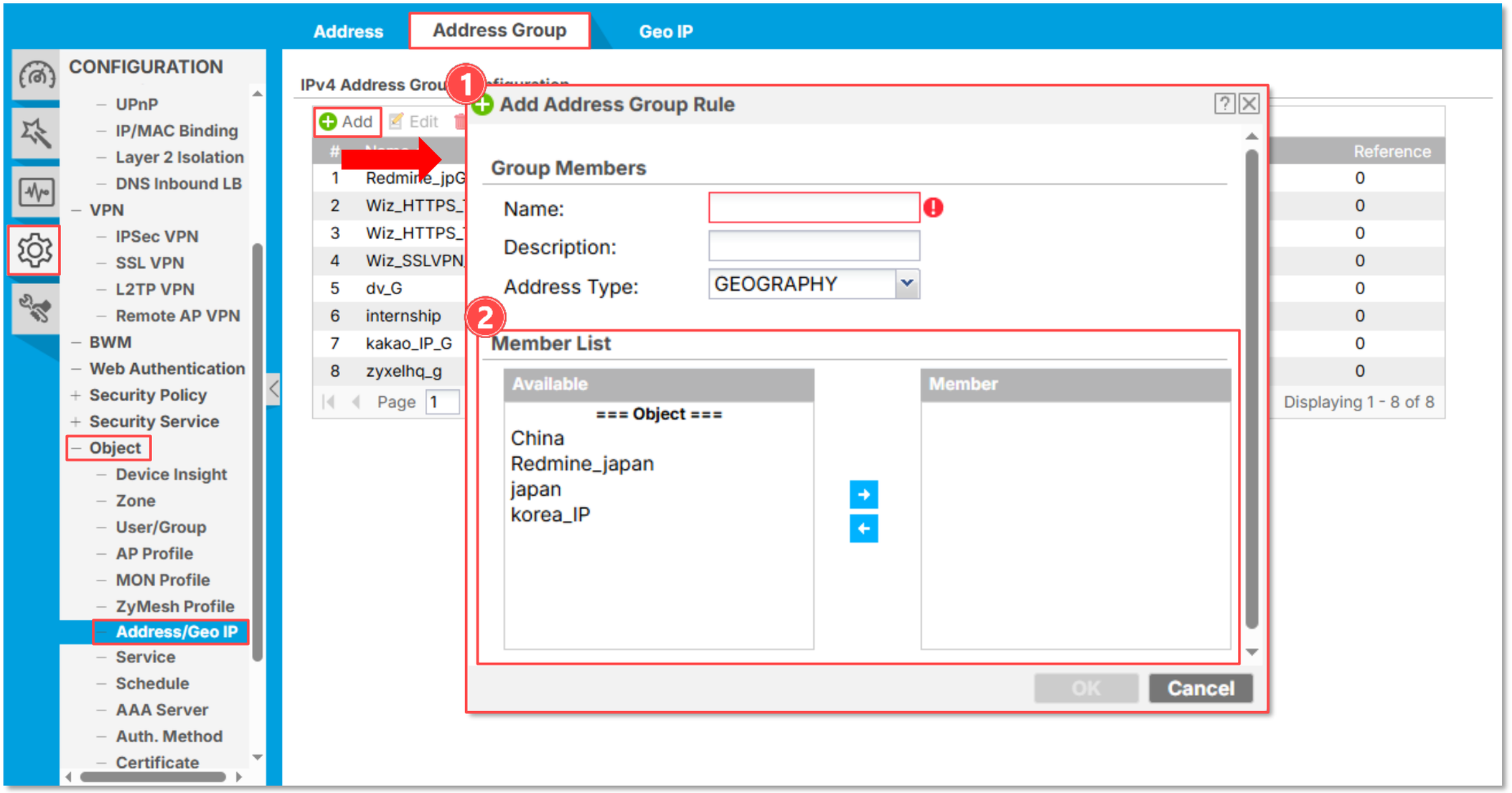
✔ Region : Asia / Europe / Afcica / North America / Oceania / South America / Antarctica … 선택

→ Region은 대륙 별 객체 하나 씩 별도 생성 필요

→ 한국 IP는 모든 허용을 위한 “Republic of Korea” 객체 별도 생성 필요

WAN 접근 제한 (장비)

한국 IP를 제외한 해외 모든 IP 차단 설정



Remark

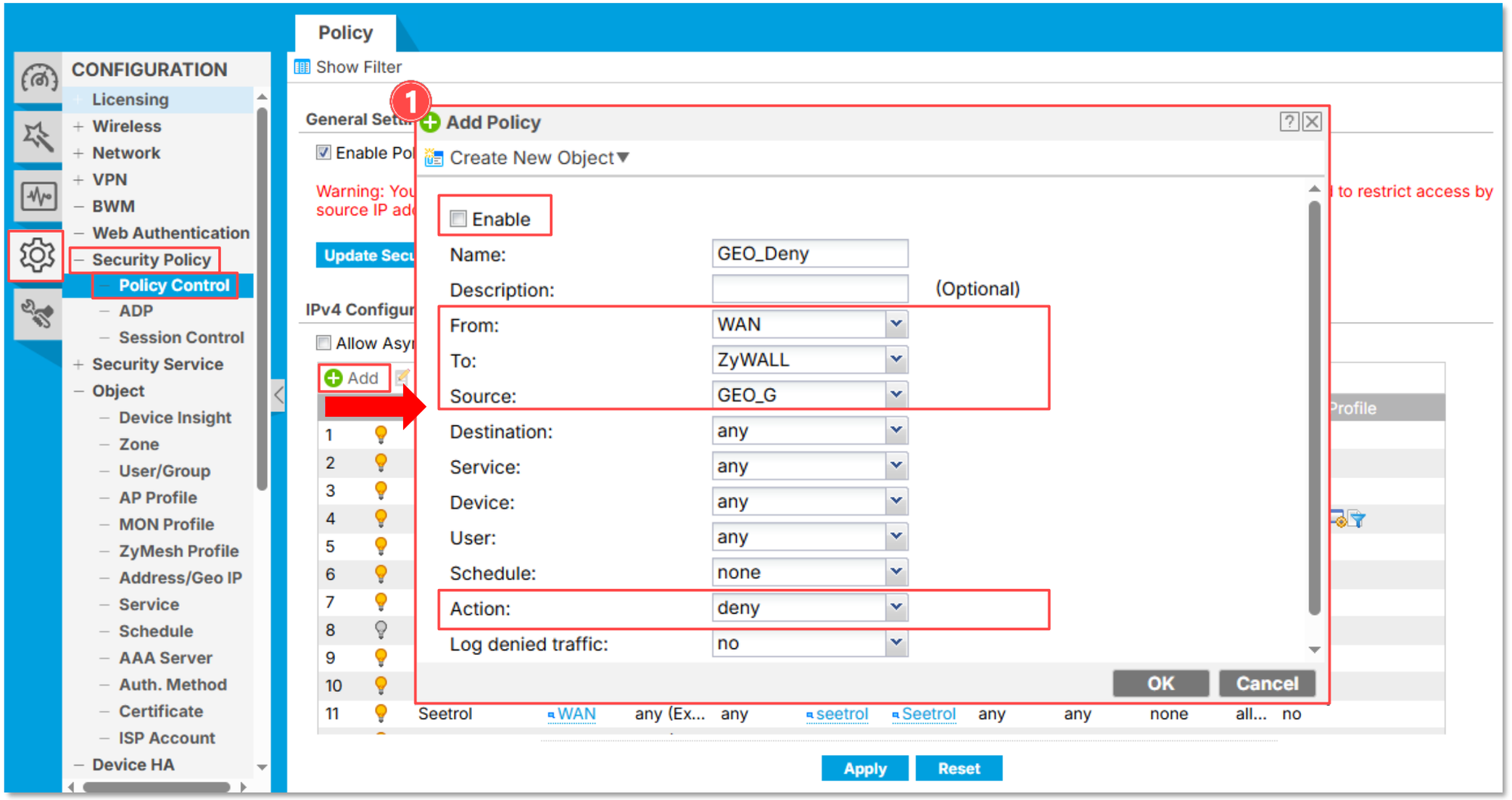
Configure → Object → Address Group → +Add

1. ✔ Name : 이름 지정
   ✔ Address Type : “GEOGRAPHY” 선택
   ✔ Region : Asia / Europe / Afcica / North America / Oceania / South America / Antarctica … 선택

2. Member List
   → Available에 있는 생성한 GEO 객체들 중 모든 대륙을 선택하여 Member로 이동

WAN 접근 제한 (장비)

한국 IP를 제외한 해외 모든 IP 차단 설정



Remark

Configure → Security Policy → Policy Control → +Add

1 ✔ Enable : 체크 해제(필수)

→ 해외 모든 IP 차단 룰이 최상단에 생성된다면 장비 접근 불가능하기 때문에 생성시에는 Disable 상태로 생성

✔ From : WAN (외부에서)

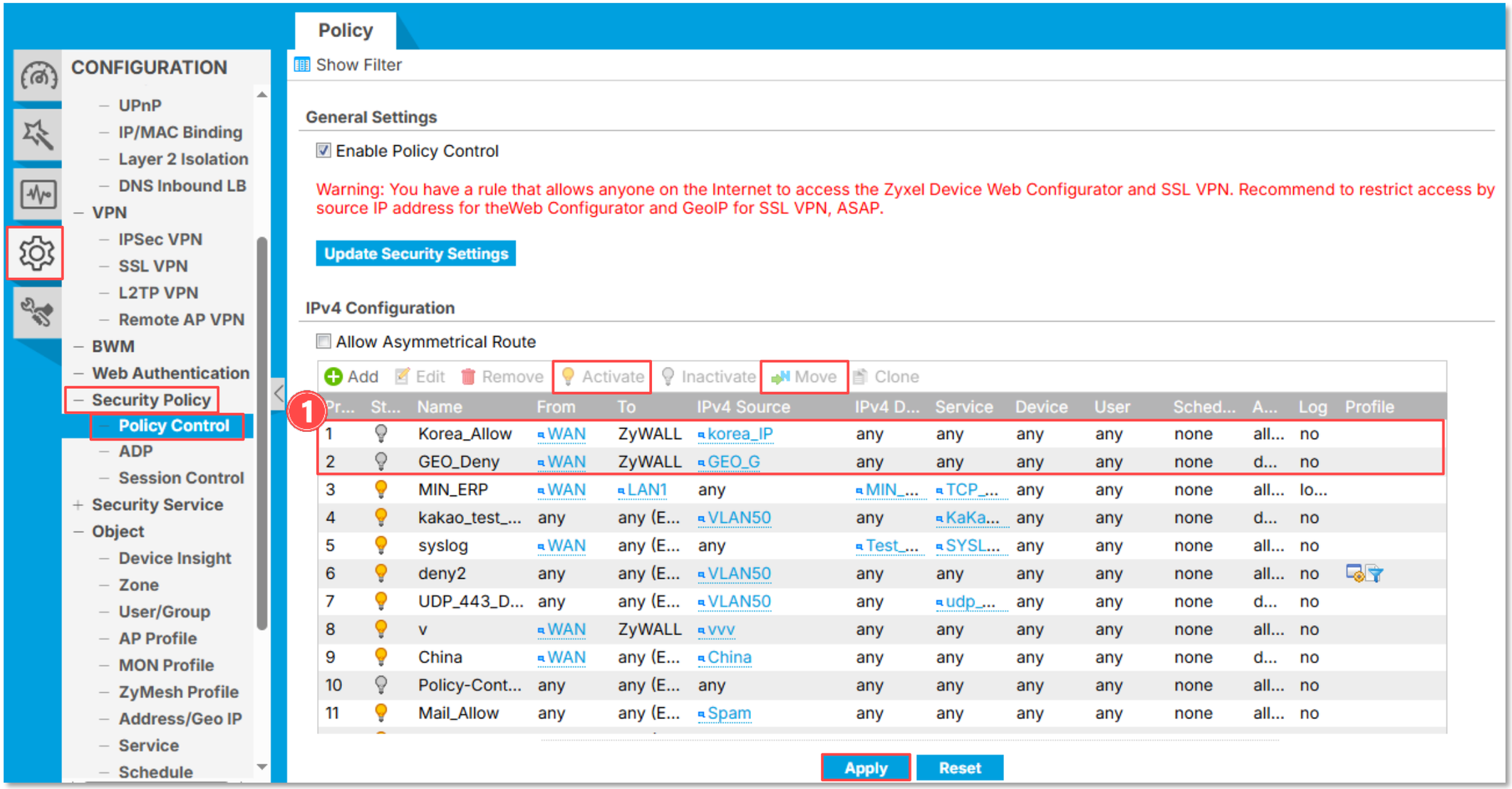
✔ To : ZyWALL (방화벽으로 접근하는)

✔ Source : 생성한 GEO Group 선택 (해외 모든 IP를)

✔ Action : deny (차단한다)

WAN 접근 제한 (장비)

한국 IP를 제외한 해외 모든 IP 차단 설정



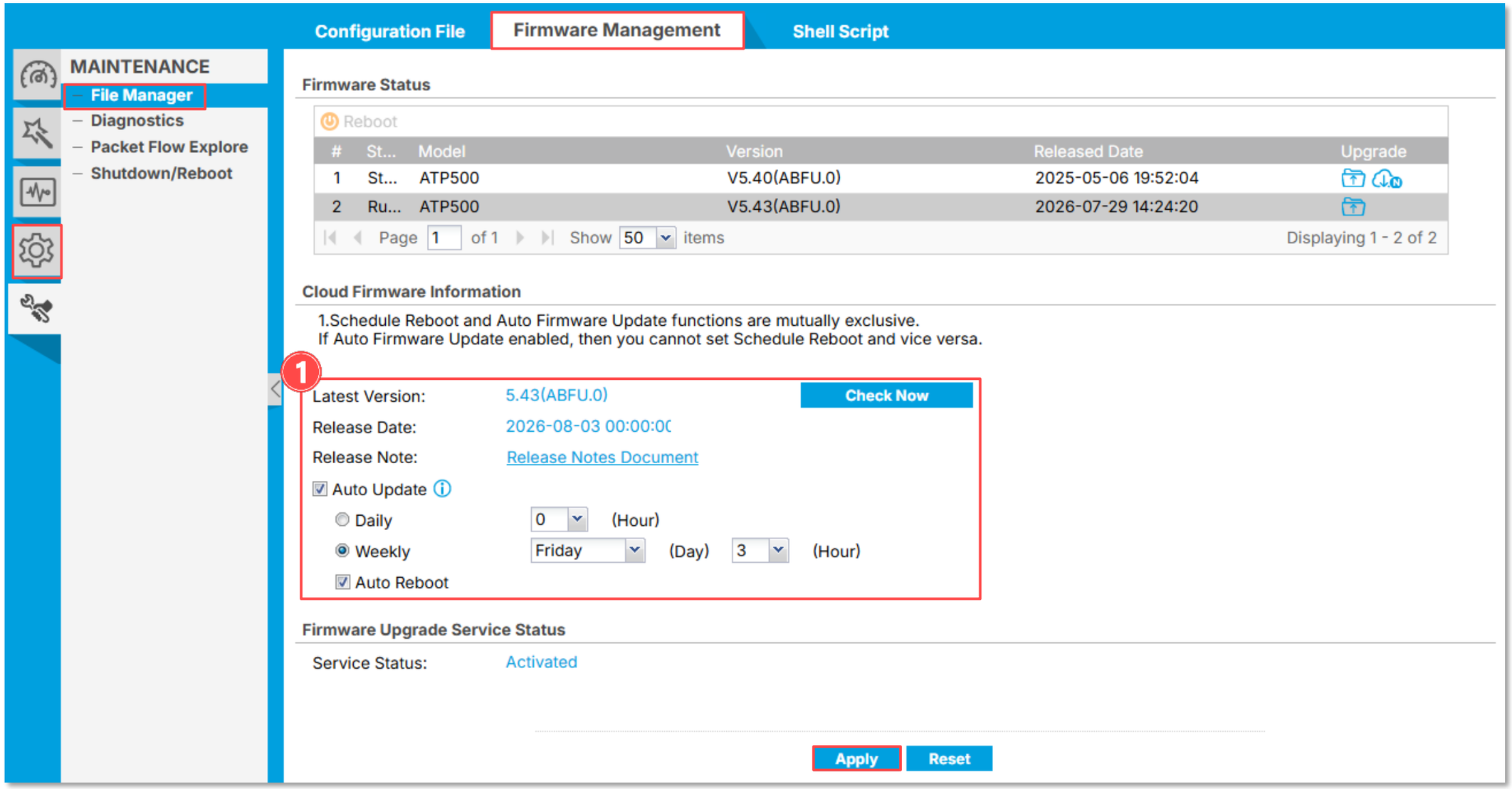
Remark

Configure → Security Policy → Policy Control → +Add

1. “GEO_Deny”와 “Korea_Allow” 두개의 룰 중 “Korea_Allow” 룰이 더 위에 있는것을 확인하고 “Activate” → “Apply” 선택
   → GEO_Deny 룰이 더 위에 있다면 우선순위가 높기 때문에 “Move” 설정으로 우선순위를 변경
   (Priority 번호 순으로 정렬 필수)

펌웨어 업데이트

스케쥴 펌웨어 업데이트



Remark

Configure → Security Policy → Policy Control → +Add

1 “Check Now” 버튼을 통해 최신 펌웨어 버전 확인

→ “Auto Update” 체크

→ Daily or Weekly 중 업데이트 진행 시간 선택

→ “Auto Reboot” 체크하여 자동 재부팅 진행 (업데이트는 재부팅이 진행되어야 정상 적용)

ZYXEL

Your Networking Ally