



ZyXEL USG Series Configuration for TeleVoIPs

Follow the directions below to ensure proper configuration for the ZyXEL USG firewalls. Please understand, instructions may vary based on the model and firmware version of your device.

I. Go to Configuration (Gears icon in upper left-hand corner)

1. Go to Network > ALG:
2. Uncheck Enable SIP ALG.
3. Uncheck Enable SIP Transformations.
4. Uncheck Enable Configure SIP Inactivity Timeout.
5. Restrict Peer to Peer Signaling Connection: Uncheck.
6. Restrict Peer to Peer Media Connection: Uncheck.
7. Click Apply.

The screenshot shows the ZyXEL USG40 configuration interface. The left sidebar contains a 'CONFIGURATION' menu with options like Licensing, Wireless, Network, and Security Policy. The 'ALG' section is selected. The main content area is divided into three sections: SIP Settings, H.323 Settings, and FTP Settings. In the SIP Settings section, 'Enable SIP ALG', 'Enable SIP Transformations', and 'Enable Configure SIP Inactivity Timeout' are unchecked. 'SIP Media Inactivity Timeout' is set to 120 seconds and 'SIP Signaling Inactivity Timeout' is set to 1800 seconds. 'Restrict Peer to Peer Signaling Connection' and 'Restrict Peer to Peer Media Connection' are also unchecked. The SIP Signaling Port table shows one entry with ID 1 and port 5060. In the H.323 Settings section, 'Enable H.323 ALG' and 'Enable H.323 Transformations' are unchecked. 'H.323 Signaling Port' is set to 1720 (1025-65535) and 'Additional H.323 Signaling Port for Transformations' is empty. In the FTP Settings section, 'Enable FTP ALG' and 'Enable FTP Transformations' are checked. 'FTP Signaling Port' is set to 21 (1-65535) and 'Additional FTP Signaling Port for Transformations' is empty. A notification banner at the top right asks if the user wants to enable the SecuReporter analytics service.

II. Go to Firewall

1. Go to Security Policy > Session Control tab > General Settings:
2. UDP Session Time Out: 300.
3. Click Apply.

