Table of Contents

How to disable SIP ALG

**Scope:**

**Intended Audience:** All End Users

This article will provide several steps for disabling SIP ALG on different firewalls. SIP ALG modifies SIP packets in unexpected ways, corrupting them and making them unreadable. This can give you unexpected behavior, such as phones not registering and incoming calls failing.

**Requirements:**

Access to Firewall

Signs of SIP ALG or Double NAT

# How to disable SIP ALG

| Router Manufacturer | Steps to disable SIP ALG |
|---|---|
| Actiontec | 1. Select Advanced, click Yes to accept the warning, then click ALG's.<br>2. Ensure SIP ALG is disabled by removing the check.<br>3. Click Apply.<br>4. Select Advanced, click Yes to accept the warning, then click Remote Administration.<br>5. Click the checkbox to Allow Incoming WAN ICMP Echo Requests (for traceroute and ping), then click Apply. |
| Adtran | 1. Under Firewall, go to Firewall / ACLs.<br>2. Click on ALG Settings.<br>3. Uncheck the box labeled SIP ALG<br>4. Click Apply.<br>If you are using the terminal, issue the following command:<br>`no ip firewall alg sip` |
| | **Most Arris broadband gateways:** |

| | |
|---|---|
| Arris | 1. Navigate to the gateway's IP (192.168.0.1).<br>2. Username: admin Password: motorola<br>3. Navigate to Advanced, then Options.<br>4. Uncheck the SIP box.<br>5. Click Apply.<br><br>**Arris BGW210**<br><br>1. Navigate to 192.168.1.254.<br><br>Authenticate without a username, and use the password located on the unit's sticker.<br>2. Under the Firewall section, click on Advanced Firewall.<br>3. Change the Set SIP ALG setting to off.<br>4. Turn off the Authentication Header Forwarding.<br>5. Turn off ESP Header Forwarding.<br>6. Click Save. |
| Asus | 1. Under the Advanced Settings section, click WAN.<br>2. Click the NAT Passthrough tab.<br>3. Change the SIP Passthrough setting to "Disable."<br>4. Click Apply. |
| AT&T | **U-Verse Pace 5268AC Gateway**<br>This broadband gateway does not support disabling SIP ALG. We recommend configuring your gateway to function only as a modem, not a router (Bridge Mode). You will need to use another router that supports disabling SIP ALG. |
| Cisco | **Cisco General and Enterprise-Class routers:**<br>`no ip nat service sip tcp port 5060`<br>`no ip nat service sip udp port 5060`<br>**Cisco PIX routers:**<br>`no fixup protocol sip 5060`<br>`no fixup protocol sip udp 5060`<br>**Cisco ASA routers:**<br>Locate 'Class inspection_default' under 'Policy-map global_policy'. Execute this command:<br>`no inspect sip` |
| | 1. Click on Advanced Settings.<br>2. Locate the Application Level Gateway (ALG) Configuration.<br>3. Uncheck the SIP option.<br>4. Click Save.<br><br>**DIR-655:** |

| | |
|---|---|
| D-Link | DIR-655:<br>1. Click Advanced, located along the top.<br>2. Click Firewall Settings on the left side of the screen.<br>3. Uncheck Enable SPI<br>4. Set both UDP and TCP Endpoint Filtering to Endpoint Independent.<br>5. Uncheck SIP from Application Level Gateway Configuration.<br>6. Click Save. |
| Fortinet | 1. Use the following commands from the CLI interface:<br>`config system session-helper`<br>`show system session-helper`<br>1. Find the SIP session instance, typically indicated by #12<br>2. Delete #12 or the appropriate number<br>3. Confirm its deletion by executing this command:<br>`show system session-helper` |
| Linksys | **Linksys Smart Wi-Fi (E-series):**<br>1. On the left side of the screen, click on Connectivity.<br>2. Click the Administration tab.<br>3. Under Application Layer Gateway, verify SIP is unchecked.<br>4. Click Apply or Save.<br>**Older Linksys models:**<br>1. Go to the 'Advanced' section on the Admin page<br>2. Disable the SIP ALG feature.<br>**Linksys BEFSR41 routers:**<br>1. Click on Applications and Gaming on the Admin page.<br>2. Click on Port Triggering.<br>3. Type in 'TCP' as the application.<br>4. Type in '5060' into the Start Port and End Port for the 'Triggering Range' and 'Forwarded Range' fields.<br>5. Check 'Enable'.<br>6. Click on Save and Reboot. |
| Mikrotik | For Mikrotik routers, SIP ALG is known as SIP Helper.<br>1. Use the company's winbox software.<br>2. Navigate to IP, then Firewall.<br>3. Click on the Service Ports tab and disable it through the GUI.<br>You may also run this command from the terminal:<br>`/ip firewall service-port disable sip` |

| | |
|---|---|
| Netgear | **For Netgear routers with the Genie interface:**<br>1. **Select the Advanced tab at the top.**<br>2. Expand the Setup menu on the left side of the screen.<br>3. Click WAN Setup.<br>4. Check the box labeled Disable SIP ALG.<br>**Other Netgear routers:**<br>1. Under the Security/Firewall, click on Advanced Settings.<br>2. Disable SIP ALG.<br>3. Locate Session Limit under Security/Firewall.<br>4. Increase the UDP timeout to 300 sec. |
| SonicWall | 1. Under System Setup on the left side of the screen, click on VoIP.<br>2. Check 'Enable Consistent NAT'<br>3. Uncheck 'Enable SIP Transformations'.<br>4. Click Accept.<br>5. To increase UDP timeouts, navigate to the Firewall Settings, then Flood Protection.<br>6. Click on the UDP tab and modify the default UDP connection timeout to 300 seconds.<br>7. Click the Accept button to save the changes. |
| TP-Link | **Newer TP-Link routers (Archer series):**<br>1. Click on the Advanced Tab.<br>2. Expand the NAT Forwarding menu on the left side of the screen.<br>3. Uncheck SIP ALG, RTSP ALG, and H323 ALG checkboxes.<br>4. Click Save.<br>**Older TP-Link routers:**<br>1. Use the Telnet client from the Command Prompt.<br>2. Apply the following command:<br>`ip nat service sip sw off` |
| UBEE | 1. Go to Advanced, then Options.<br>2. Uncheck the SIP and the RTSP checkboxes.<br>3. Click Apply. |
| | **UniFi Security Gateway**<br>1. Sign in to your UniFi security gateway.<br>2. Click on Routing & Firewall along the left side.<br>3. Click the Firewall tab at the top and click Settings from the sub-menu.<br>4. Toggle H.323 and SIP to off.<br>5. Click the Apply Changes button.<br>**EdgeRouters (ER-x)** |

| | |
|---|---|
| Ubiquiti | **EdgeRouters (ER-X)**<br><br>1. Access the router's administrative interface, typically at 192.168.1.1.<br>2. Use the Config Tree or a command-line interface to disable SIP ALG.<br><br>**Config Tree:**<br><br>1. Select config tree in the top right-hand corner.<br>2. Expand system, conntrack, modules, and sip.<br>3. Click the plus sign next to disable.<br>4. Click the Preview option.<br>5. Click Apply.<br><br>**Command Line Interface:**<br><br>1. From the administrative interface, choose CLI located at the top right corner of the screen.<br>2. From here, we can also increase UDP timeouts as well.<br>3. Enter these commands into the terminal:<br><br>`configure`<br><br>`set system conntrack modules sip disable`<br><br>`set system conntrack timeout udp stream 300`<br><br>`set system conntrack timeout udp other 300`<br><br>`commit`<br><br>`save`<br><br>`exit` |
| Verizon FiOS | **G1100**<br>This broadband gateway does not support disabling SIP ALG. We recommend configuring your gateway to function only as a modem, not a router. You will need to use another router that supports disabling SIP ALG. |
| ZyXEL | **ZyXEL ZyWALL/USG60:**<br><br>1. Click on Configuration and expand the Network settings.<br>2. Click ALG along the left side.<br>3. Uncheck all the checkboxes on the right side:<br>4. Uncheck Enable SIP ALG.<br>5. Uncheck Enable SIP Transformations.<br>6. Click Apply.<br><br>**ZyXEL C1000Z/C1100Z (CenturyLink):**<br><br>1. Click on Advanced Setup.<br>2. Click on SIP ALG along the left side.<br>3. Toggle the SIP ALG setting to Disable. |

| | |
|---|---|
| ZyXEL | 3. Toggle the SIP ALG setting to Disable.<br>4. Click Apply.<br><br>**ZyXEL P600:**<br><br>1. Telnet to the router (192.168.1.1) and enter the password.<br>2. The default password is 1234. Type “24” and press enter.<br>3. Then “8” and press enter.<br>4. Provide this command:<br><br>`ip nat service sip active 0`<br><br>1. When done, press Enter |

disable sip alg