Disabling SIP-ALG in your Router or Firewall

Objective

To disable SIP-ALG in your Router or Firewall.

Please note: We highly recommend consulting an IT or network professional when configuring advanced network settings or devices.

Applies To

The below routers are covered in this guide:

- Adtran
- Arris
- ASA
- Cisco (non-ASA)
- D-Link
- Fortinet
- Linksys
- Netgear
- SonicWall
- UBBEE Gateways
- ZyXEL ZyWall USG

Procedure

Device Guidance

ALG settings are typically found in the administration interface of the router, but each router’s configuration setup will differ. Check the manufacturer’s documentation to understand where to find and disable this setting in your device.
The following are general guidelines for popular makes and models. If you don't see your router or manufacturer below, consult the manufacturer's documentation. You can also refer to additional information on generally recommended 8x8 Virtual Office firewall settings.

It is highly recommended you have your network or IT administrator or a qualified professional configure the following in your router or firewall.

**Note:** many routers will re-enable ALG by default if the router is ever reset or powered off then back on.

### Adtran Routers

Add the following:

```
no ip firewall alg sip
```

### Arris Gateways

1. Go to Advanced > Options.
2. Disable (uncheck) SIP.
3. Click Apply.

Arris Gateway IP Address: 192.168.0.1

- **Username:** admin
- **Password:** motorola

### ASA Routers

1. Go to policy-map global_policy > class inspection_default.
2. Enter:

```
no inspect sip
```

### Cisco (non-ASA)

On Cisco devices, SIP-ALG is referred to as **SIP Fixup** and is enabled by default on both routers and Pix devices. Because this is a default setting, no indication of it being "on" or "off" is visible in the configuration.
To disable SIP Fixup, issue the following commands:

**General Routers**

```bash
no ip nat service sip tcp port 5060
no ip nat service sip udp port 5060
```

**Enterprise-Class Routers**

```bash
no ip nat service sip tcp port 5060
no ip nat service sip udp port 5060
```

**Pix Devices**

```bash
no fixup protocol sip 5060
no fixup protocol sip udp 5060
```

**D-Link Routers**

1. From the admin interface page of the router, navigate to Advanced settings.
2. Under Application Level Gateway (ALG) Configuration, uncheck the SIP option.

**Fortinet Routers**

1. From CLI interface, type the following commands:
   ```bash
   config system session-helper
   show system session-helper
   (Look for the session instance that refers to SIP—likely to be #12)
   delete 12
   (Or number corresponding to SIP reference)
   ```
   2. To confirm deletion, run show system session-helper again.
   3. Ensure there is no reference to SIP or port 5060.

**Linksys Routers**

**General Linksys Guidelines**

1. From the ADMIN page of the router, navigate to [Administration] > [Advanced].
2. Look for and disable a SIP ALG option.
Linksys BEFSR41

1. From the **ADMIN** page of the router, navigate to **[APPLICATIONS & GAMING] > [PORT TRIGGERING]**.
2. Enter **[TCP]** as the application.
3. Enter **[5060]** into the **Start Port** and **End Port** for both the **Triggering Range** and **Forwarded Range**.
4. Check **Enable**.
5. **Save Settings**.
6. Reboot IP phone.

Netgear Routers

1. From administration interface, go to **Security > Firewall > Advanced** settings.
2. Uncheck the option for **SIP ALG**.
3. Under **Security > Firewall > Session Limit**, increase the UDP timeout to the 300 seconds.

SonicWall Routers

1. Uncheck the box for **Use SIP Header Transformation**.
2. Disable **consistent NAT**.

When setting the **Global Default UDP timeout value** on a SonicWall firewall, you must still fix the pre-existing rules’ individual UDP timeout values. New rules will inherit the Global Default. Increase the UDP timeout to the suggested 300 seconds both globally on the firewall and the specific out-bound firewall rule (or the default rule, as the case may be).

UBEE Gateways

1. Go to **Advanced > Options**.
2. Disable (uncheck) **SIP**.
3. Disable (uncheck) **RTSP**.
4. Click **Apply**.

ZyXEL ZyWALL USG Routers

1. Go to **Settings > Configuration > Network > ALG**.
2. Disable **SIP ALG**.
Note: If you have mixed models of phones like Polycom/Aastra/Cisco/Panasonic, then you may experience difficulty in using ZyXEL ZyWALL routers. However, if you have only Polycom phones, please review this article to learn how to configure ZyXEL ZyWALL routers for use with Polycom phones.

Additional Information

Disabling SIP-ALG is an essential part of configuring the firewall on your router and optimizing it for 8x8 service, which is why routers sold by 8x8 come preconfigured with ALG disabled. Many ALGs (including Cisco's) have bugs which cause call flow and registration failures. Some ALGs (including Cisco's) intermittently miss some packets (read: do not perform fixup), or in the case of fragmented packets, do not even examine and change headers.

When SIP-ALG is enabled, CP SBCs determine the endpoints are publicly addressed and therefore do not need frequent registration refreshes to keep the firewall port open between SBC and the endpoint. In this case, the firewall can close the port between 8x8 and the device endpoint, causing an inability to receive incoming calls. The most common issues that result from enabled SIP-ALG when using Virtual Office applications include:

- Outbound call status stuck in Dialing...
- An inability to field incoming calls (call continues to ring and cannot be answered)
- Phones not able to register with 8x8

Additional SIP-ALG information and settings can be found at Voip Info: Routers SIP ALG.